



IPv6 for Enterprise Networks

The practical guide to deploying IPv6 in campus, WAN/branch, data center, and virtualized environments

Shannon McFarland, CCIE® No. 5245
Muninder Sambi, CCIE No. 13915
Nikhil Sharma, CCIE No. 21273
Sanjay Hooda, CCIE No. 11737

IPv6 for Enterprise Networks

Shannon McFarland
Muninder Sambhi
Nikhil Sharma
Sanjay Hooda

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

IPv6 for Enterprise Networks

Shannon McFarland, Muninder Sambhi, Nikhil Sharma, and Sanjay Hooda

Copyright © 2011 Cisco Systems, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

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

Printed in the United States of America

Third Printing June 2012

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

ISBN-13: 978-1-58714-227-7

ISBN-10: 1-58714-227-9

Warning and Disclaimer

This book is designed to provide information about the IPv6 deployment options for an Enterprise network. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact: International Sales international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Business Operation Manager, Cisco Press: Anand Sundaram

Associate Publisher: Dave Dusthimer

Manager, Global Certification: Erik Ullanderson

Executive Editor: Brett Bartow

Technical Editors: Jim Bailey, Ciprian P. Popoviciu

Managing Editor: Sandra Schroeder

Copy Editor: John Edwards

Development Editor: Dayna Isley

Proofreader: Apostrophe Editing Services

Project Editor: Seth Kerney

Editorial Assistant: Vanessa Evans

Book Designer: Louisa Adair

Composition: Mark Shirar

Indexer: Tim Wright



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

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

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

About the Authors

Shannon McFarland, CCIE No. 5245, is a corporate consulting engineer for Cisco, working as a technical consultant for enterprise IPv6 deployment and data center design with a focus on application deployment and virtual desktop infrastructure. Over the last 16 years, he has worked on large-scale enterprise campus and WAN/branch network design, data center design and optimization for Microsoft operating systems and server applications, as well as design and optimization of virtual desktop infrastructure deployments. For the past 10 years, Shannon has been a frequent speaker at IPv6 events worldwide (notably Cisco Live [formerly Networkers]), IPv6 summits, and other industry events. He has authored many papers and Cisco Validated Designs (CVD) on IPv6, IP Multicast, Microsoft Exchange, VMware View, and other applications, as well as contributed to many Cisco Press books. Prior to his time at Cisco, Shannon worked as a consultant for a value-added reseller and also as a network engineer in the healthcare industry. Shannon lives with his wife and children in Castle Rock, CO.

Muninder Sambi, CCIE No. 13915, is a manager of product marketing for the Cisco Catalyst 4500/4900 series platform. As a product line manager, he is responsible for defining product strategies on the multi-billion-dollar Catalyst 4500 and 4900 series platforms, which include next-generation product architectures both for user access in Campus and Server access in the Data Center. Prior to this role, Muninder played a key role in defining the long-term Software and Services strategy for Cisco's modular switching platforms (Catalyst 6500 and 4500/4900 series) including a focus on IPv6 innovations. Some of these innovations enabled dual-stack IPv6 deployments in large enterprise and service provider networks. Muninder is also a core member of Cisco's IPv6 development council. Muninder has represented Cisco as part of multiple network design architecture reviews with large enterprise customers. Over the last 12+ years, Muninder has worked on multiple Enterprise Campus, WAN, and Data Center designs. Prior to working at Cisco, Muninder worked as a network consultant for one of India's leading network integrators and was responsible for designing and implementing LAN, WAN, and hosted Data Center networks. Muninder lives with his wife and children in Fremont, California.

Nikhil Sharma, CCIE No. 21273, is a technical marketing engineer at Cisco, where he is responsible for defining new features, both hardware and software, for the Catalyst 4500 product line. Over the last 10 years, Nikhil has worked with various enterprise customers to design and troubleshoot both large and midsize campus and data center networks.

Sanjay Hooda, CCIE No. 11737, is a technical leader at Cisco, where he works with embedded systems and helps define new product architectures. His current focus areas include high availability and messaging in large-scale distributed switching systems. Over the last 14 years, Sanjay's experience spans various areas, including SCADA (Supervisor Control and Data Acquisition), large-scale software projects, and enterprise campus and LAN, WAN, and data center network design.

About the Technical Reviewers

Jim Bailey, CCIE No. 5275 (Routing and Switching; Service Provider) and CCDE No. 20090008, is an AS technical leader at Cisco Systems with over 18 years of experience in networking. As part of the Global Government Solutions Group Advanced Services team, he focuses on the architecture, design, and implementation of large U.S. government civilian agency and military networks. He has focused on IPv6 integration into those networks for the last five years.

Ciprian P. Popoviciu, Ph.D., is director of Cloud and Network3.0 practices in the Enterprise Services Group at Technodyne. Previously he held several leadership roles within Cisco, where over the past eight years he worked in close collaboration with standards bodies and large customers worldwide on the IPv6 protocol and product development, IPv6 strategy and planning, and IPv6-enabled, next-generation architecture and deployment. Ciprian coauthored two extensively referenced Cisco Press IPv6 books, four RFCs, and multiple papers on IPv6 technology, strategy, and adoption. He is a senior member of the IEEE, a member of several research advisory boards, and an active speaker at IPv6 industry events.

Dedications

I want to give thanks to my Savior Jesus Christ—I was once lost but now I am found. This book is dedicated to Linda, Zack, and Carter. I am so blessed to have you all in my life, and I am so proud of the honorable young men my sons have become. Thanks for putting up with me for these many months. I also want to thank my mom for her unconditional love and prayers and my dad for the desire to never quit learning. To my mother- and father-in-law, thanks for bringing Linda into this world and into my life; she is the very best. Bob (dad), thanks for being my friend and mentor and always showing me what hard work really is.

—*Shannon McFarland*

First of all, I would like to dedicate this book to my grandfather (Gyani Gurcharan Singh) for being an inspiration as an author, poet, and classical musician. I would like to thank my family: Dad (Surinder Singh Sambhi), Mom (Sukhdev Kaur), my brother (Dr. Ravinder Singh Sambhi), my sister-in-law (Amrit Kaur), and wife (Avnit Kaur) for their unconditional support during the writing of this book. I would also like to dedicate this book to my daughter (Japjot), twins (Kabir Singh and Charan Kanwal Singh) and my nephews (Kanwal and Bhanwra).

—*Muninder Singh Sambhi*

First of all I would like to thank my parents: Dad (Satbir Singh) and Mom (Indrawati) and wife (Suman) for their support during the writing of the book. This book is dedicated to my children Pulkit and Apoorva.

—*Sanjay Hooda*

I would like to thank my wife Parul for her endless support during the process. This book is dedicated to my daughter Anshi for showing me how small things in life bring true happiness.

—*Nikhil Sharma*

Acknowledgments

I would like to thank a number of people who have contributed to my knowledge and experience of IPv6 and supported my time spent on it (especially in the early days), and those who have provided me support over these many years: My friends and biggest supporters, Freddie Tsao, Steve Pollock, Chris O'Brien, and Mark Montanez. I have been blessed with many great managers who have been so very patient with me over the years and offered great support, especially on IPv6. A few of the many: Todd Truitt, Vince Spina, Kumar Reddy, Mauricio “Mo” Arregoces, Dave Twinam, and Mark Webb. Additionally, I would like to thank the following individuals at Cisco (past and present) who have contributed to this effort directly or indirectly: Patrick Grossetete, Chip Popoviciu, Eric Vyncke, Gunter Van de Velde, Tarey Treasure, Darlene Maillet, Angel Shimelish, Chris Jarvis, Gabe Dixon, Tim Szigeti, Mike Herbert, Neil Anderson, Dave West, Darrin Miller, Stephen Orr, Ralph Droms, Salman Asadullah, Yenu Gobena, Tony Hain, Benoit Lourdelet, Eric Levy-Abegnoli, Jim Bailey, Fred Baker, and countless others. Finally, I would like to thank John Spence and Yurie Rich for years of great feedback and real-world IPv6 deployment validation.

—*Shannon McFarland*

First of all, I would like to thank my co-authors Sanjay Hooda, Nikhil Sharma, and Shannon McFarland for all their cooperation during the writing of the book. Special thanks to Shannon for keeping us motivated and guiding us through some of the difficult topics.

Thanks to my mentor and dear friend who introduced me to networking, Sanjay Thyamagundalu, for supporting me through the writing of this book.

I would also like to thank my Director Sachin Gupta for his support and motivation towards completion of the book. I would also thank the technical reviewers, Jim Bailey and Chip Popoviciu, for sharing their technical expertise on IPv6 and for always being available for a follow-up to review the comments.

Finally, I would like to thank the Cisco Press team, especially Brett Bartow and Dayna Isley, for guiding us through the process and being patient as we went through the initial drafts and the review process.

—*Muninder Singh Sambi*

First of all, I would like to thank my co-authors Muninder, Shannon, and Nikhil, who have been very supportive during the course of writing. Additionally I would like to thank my great friend Sanjay Thyamagundalu and my manager Vinay Parameswarannair for their support during the writing of this book. Sanjay Thyamagundalu has provided not only inspiration, but also thought-provoking insights into various areas.

Thanks as well to Brett Bartow, Dayna Isley, and all the folks at Cisco Press for their patience as I struggled to meet the timelines.

—*Sanjay Hooda*

First and foremost, I would like to thank my mentor and greatest friend Muninder Sambi for introducing me to networking. Without access to Sanjay Hooda's lab, this book could not have happened. Shannon kept the team motivated by showing us the finish line when at times we saw it far away.

Thanks to my friends who have always answered when I called: Amol Ramakant, Deepinder Babbar, Jagdeep Sagoo, Nitin Chopra, and the 24/7 speed dial on my phone, 1-800-Call-Manu.

—*Nikbil Sharma*

We would like to give special recognition to technical reviewers Chip Popoviciu and Jim Bailey for providing their expert technical knowledge in reviewing the book.

Finally, we want to thank our fantastic editors, Brett Bartow and Dayna Isley, and the Cisco Press team for all their support, patience, and quality work.

Contents at a Glance

	Introduction	xix
Chapter 1	Market Drivers for IPv6 Adoption	1
Chapter 2	Hierarchical Network Design	17
Chapter 3	Common IPv6 Coexistence Mechanisms	45
Chapter 4	Network Services	67
Chapter 5	Planning an IPv6 Deployment	91
Chapter 6	Deploying IPv6 in Campus Networks	107
Chapter 7	Deploying Virtualized IPv6 Networks	185
Chapter 8	Deploying IPv6 in WAN/Branch Networks	225
Chapter 9	Deploying IPv6 in the Data Center	261
Chapter 10	Deploying IPv6 for Remote Access VPN	291
Chapter 11	Managing IPv6 Networks	303
Chapter 12	Walk Before Running: Building an IPv6 Lab and Starting a Pilot	343
	Index	361

Contents

Introduction xix

Chapter 1 Market Drivers for IPv6 Adoption 1

IPv4 Address Exhaustion and the Workaround Options 2

IPv6 Market Drivers 3

IPv4 Address Considerations 4

Government IT Strategy 5

Infrastructure Evolution 5

Operating System Support 6

Summary of Benefits of IPv6 6

Commonly Asked Questions About IPv6 6

Does My Enterprise Need IPv6 for Business Growth? 6

Will IPv6 Completely Replace IPv4? 9

Is IPv6 More Complicated and Difficult to Manage and Deploy Compared to IPv4? 9

Does IPv6 continue to allow my enterprise network to be multihomed to several service providers? 10

Is quality of service better with IPv6? 10

Is IPv6 automatically more secure than IPv4? 10

Does the lack of NAT support in IPv6 reduce security? 10

IPv6 in the IETF 11

Enterprise IPv6 Deployment Status 12

Summary 15

Additional References 15

Chapter 2 Hierarchical Network Design 17

Network Design Principles 18

Modularity 19

Hierarchy 21

Resiliency 24

Enterprise Core Network Design 24

Enterprise Campus Network Design 25

Distribution Layer 25

Layer 2 Access Design 25

Routed Access Design 27

Virtual Switching System Distribution Block 28

	<i>Comparing Distribution Block Designs</i>	28
	Access Layer	29
	Enterprise Network Services Design	29
	Enterprise Data Center Network Design	31
	Aggregation Layer	31
	Access Layer	32
	Data Center Storage Network Design	33
	<i>Collapsed Core Topology</i>	35
	<i>Core Edge Topology</i>	35
	Enterprise Edge Network Design	37
	Headquarters Enterprise Edge Network Components	38
	Headquarters Enterprise Edge Network Design	39
	Branch Network Architecture	39
	Branch Edge Router Functionality	41
	Typical Branch Network Design	42
	Summary	43
	Additional References	43
Chapter 3	Common IPv6 Coexistence Mechanisms	45
	Native IPv6	47
	Transition Mechanisms	48
	Dual-Stack	48
	IPv6-over-IPv4 Tunnels	49
	<i>Manually Configured Tunnel</i>	51
	<i>IPv6-over-IPv4 GRE Tunnel</i>	53
	<i>Tunnel Broker</i>	54
	<i>6to4 Tunnel</i>	55
	<i>Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)</i>	57
	IPv6 over MPLS	58
	<i>IPv6 over Circuit Transport over MPLS</i>	58
	<i>IPv6 Using IPv4 Tunnels on Customer Edge (CE) Routers</i>	60
	<i>IPv6 MPLS with IPv4-Based Core (6PE/6VPE)</i>	60
	Protocol Translation/Proxy Mechanisms	62
	NAT-PT	63
	NAT64	64
	Summary	64
	Additional References	65

Chapter 4 Network Services 67

Multicast 67

IPv6 Multicast Addressing 69

Multicast Listener Discovery (MLD) for IPv6 71

Multicast Routing: Protocol Independent Multicast (PIM) 72

PIM Sparse Mode (PIM-SM) 73*PIM Source Specific Multicast (PIM-SSM)* 74*Bidirectional PIM (PIM-Bidir)* 76

Quality of Service (QoS) 76

Differences Between IPv6 and IPv4 QoS 76

IPv6 Extension Headers 78

IPv4 and IPv6 Coexistence 79

IPv6 Routing 80

OSPFv3 80

EIGRPv6 83

IS-IS 85

Single Topology 86*Multitopology* 86*Configuring IS-ISv6* 86

BGP 87

Multiprotocol BGP for IPv6 88

Summary 89

Additional References 89

Chapter 5 Planning an IPv6 Deployment 91

Determining Where to Begin 91

Benefit Analysis 92

Cost Analysis 93

Risks 94

Business Case 94

Transition Team 95

Training 96

Planning a Pilot 96

Assessment 96

Design 97

IPv6 Addressing Plan 97

Transition Mechanisms 98

	Network Services	98
	Security	98
	New Features in IPv6	99
	Scalability and Reliability	99
	Service Level Agreements	99
	Lessons Learned and Implementation	99
	Client/Server IPv6 Migration Scenarios	100
	<i>IPv6 Core Deployment: “Start at the Core”</i>	101
	<i>Localized IPv6 Server-Side Deployment</i>	102
	<i>Client-Side Deployment</i>	102
	<i>Client/Server Deployment: Dual-Stack Configuration</i>	103
	Planning Address Allocation	104
	Summary	104
	Additional References	105
Chapter 6	Deploying IPv6 in Campus Networks	107
	Campus Deployment Models Overview	107
	Dual-Stack Model	108
	<i>Benefits and Drawbacks of the DSM</i>	108
	<i>DSM Topology</i>	109
	<i>DSM-Tested Components</i>	109
	Hybrid Model	109
	<i>Benefits and Drawbacks of the HM</i>	114
	<i>HM Topology</i>	115
	<i>HM-Tested Components</i>	115
	Service Block Model	115
	<i>Benefits and Drawbacks of the SBM</i>	116
	<i>SBM Topology</i>	117
	<i>SBM-Tested Components</i>	119
	General Campus IPv6 Deployment Considerations	119
	Addressing	119
	Physical Connectivity	120
	VLANs	121
	Routing	121
	High Availability	122
	QoS	123
	Security	125

<i>Making Reconnaissance More Difficult Through Complex Address Assignment</i>	126
<i>Controlling Management Access to the Campus Switches</i>	126
<i>IPv6 Traffic Policing</i>	128
<i>Using Control Plane Policing (CoPP)</i>	129
<i>Controlling Ingress Traffic from the Access Layer</i>	130
<i>First-Hop Security</i>	130
<i>Blocking the Use of Microsoft Teredo</i>	131
Multicast	131
Network Management	132
Address Management	132
Scalability and Performance	135
<i>Scalability and Performance Considerations for the DSM</i>	135
<i>Scalability and Performance Considerations for the HM</i>	136
<i>Scalability and Performance Considerations for the SBM</i>	137
Implementing the Dual-Stack Model	137
Network Topology	138
Physical/VLAN Configuration	140
Routing Configuration	143
First-Hop Redundancy Configuration	145
QoS Configuration	147
Multicast Configuration	149
Routed Access Configuration	151
Cisco Virtual Switching System with IPv6	155
<i>VSS Configuration</i>	157
<i>VSS Physical Interface IPv6 Configuration</i>	160
Implementing the Hybrid Model	161
Network Topology	161
Physical Configuration	162
Tunnel Configuration	163
QoS Configuration	171
Infrastructure Security Configuration	173
Implementing the Service Block Model	174
Network Topology	174
Physical Configuration	176
Tunnel Configuration	178
QoS Configuration	180

Summary 181
Additional References 182

Chapter 7 Deploying Virtualized IPv6 Networks 185

Virtualization Overview 186
 Virtualization Benefits 186
 Virtualization Categories 186
Network Virtualization 188
 Switch Virtualization 188
 Network Segmentation 188
 Virtual Routing and Forwarding (VRF-Lite) 189
 Transporting IPv6 Across the MPLS Backbone 193
 Virtual Private LAN Services 211
 Network Services Virtualization 212
 Virtualized Firewall 213
 Cisco Adaptive Security Appliance (ASA)
 Virtualization Architecture 213
 Understanding Virtual Contexts on the Cisco ASA 214
 Configuring Multiple Contexts on the Cisco ASA 215
 Configuring IPv6 Access Lists 219
Desktop Virtualization 220
 IPv6 and Desktop Virtualization 221
 Desktop Virtualization Example: Oracle Sun Ray 222
Server Virtualization 223
Summary 223
Additional References 224

Chapter 8 Deploying IPv6 in WAN/Branch Networks 225

WAN/Branch Deployment Overview 226
 Single-Tier Profile 226
 Dual-Tier Profile 227
 Redundancy 228
 Scalability 228
 WAN Transport 228
 Multitier Profile 228
General WAN/Branch IPv6 Deployment Considerations 229
 Addressing 230
 Physical Connectivity 230

VLANs	231
Routing	232
High Availability	232
QoS	233
Security	233
Multicast	236
Management	236
Scalability and Performance	238
WAN/Branch Implementation Example	238
Tested Components	239
Network Topology	240
WAN Connectivity	240
Branch LAN Connectivity	241
Firewall Connectivity	241
Head-End Configuration	242
Branch WAN Access Router Configuration	245
Branch Firewall Configuration	247
EtherSwitch Module Configuration	250
Branch LAN Router Configuration	252
WAN/Branch Deployment over Native IPv6	254
Summary	258
Additional References	258

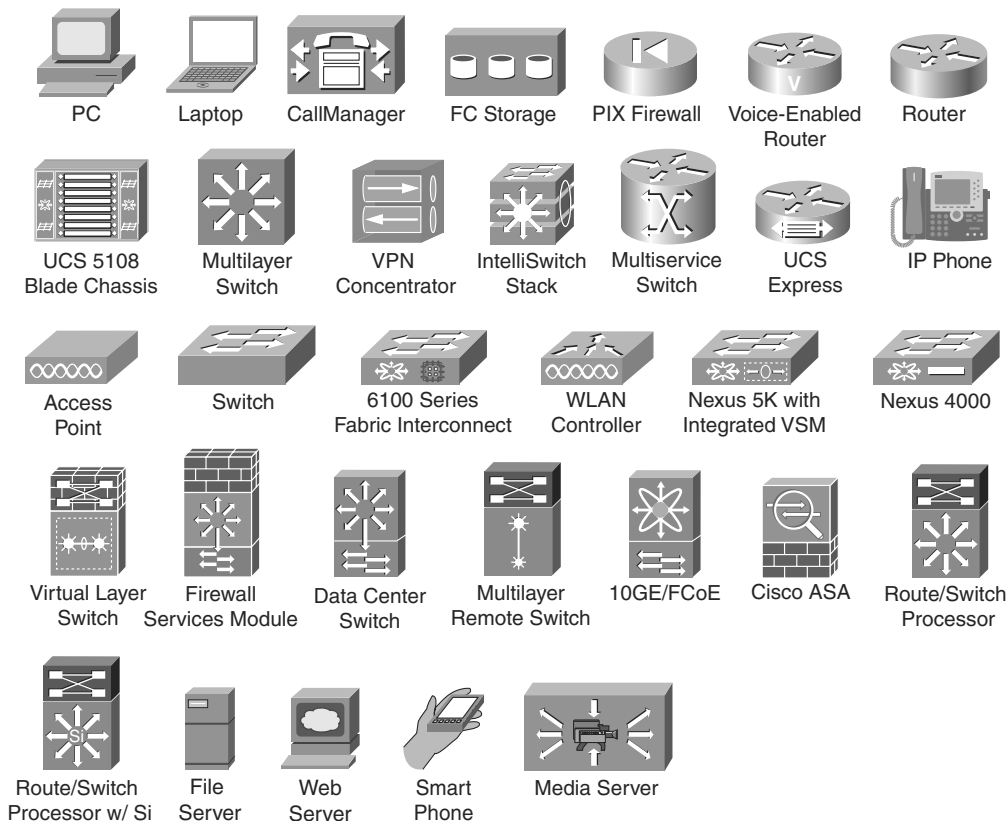
Chapter 9 Deploying IPv6 in the Data Center 261

Designing and Implementing a Dual-Stack Data Center	262
Data Center Access Layer	264
<i>Configuring Access Layer Devices for IPv6</i>	265
<i>NIC-Teaming Considerations</i>	267
Data Center Aggregation Layer	269
<i>Bypassing IPv4-Only Services at the Aggregation Layer</i>	269
<i>Deploying an IPv6-Only Server Farm</i>	271
<i>Supporting IPv4-Only Servers in a Dual-Stack Network</i>	271
<i>Deploying IPv6-Enabled Services at the Aggregation Layer</i>	272
Data Center Core Layer	279
Implementing IPv6 in a Virtualized Data Center	279

Implementing IPv6 for the SAN	281
FCIP	281
iSCSI	284
Cisco MDS Management	285
Designing IPv6 Data Center Interconnect	286
Design Considerations: Dark Fibre, MPLS, and IP	287
DCI Services and Solutions	288
Summary	289
Additional References	289
Chapter 10 Deploying IPv6 for Remote Access VPN	291
Remote Access for IPv6 Using Cisco AnyConnect	292
Remote Access for IPv6 Using Cisco VPN Client	297
Summary	301
Additional References	301
Chapter 11 Managing IPv6 Networks	303
Network Management Framework: FCAPS	304
Fault Management	305
Configuration Management	305
Accounting Management	306
Performance Management	306
Security Management	306
IPv6 Network Management Applications	307
IPv6 Network Instrumentation	308
Network Device Management Using SNMP MIBs	308
<i>Relevance of IPv6 MIBs</i>	311
IPv6 Application Visibility and Monitoring	312
<i>Flexible NetFlow</i>	312
<i>NetFlow Versions</i>	313
<i>NetFlow version 9 (Flexible NetFlow [FnF])</i>	314
IPFIX	320
IP SLA for IPv6	322
Automation Using Flexible Programming with Embedded Event Manager	328

IPv6 Network Management	330
Monitoring and Reporting	331
<i>SNMP over IPv6</i>	331
<i>Syslog over IPv6</i>	332
<i>ICMPv6</i>	332
Network Services	333
<i>TFTP</i>	333
<i>NTP</i>	333
Access Control and Operations	334
<i>Telnet</i>	334
<i>SSH</i>	335
<i>HTTP</i>	336
IPv6 Traffic-Monitoring Tools	337
SPAN, RSPAN, and ERSPAN	337
<i>Configuring SPAN Types</i>	338
<i>Mini Protocol Analyzer</i>	339
VLAN Access Control List (VACL) Capture	340
Summary	341
Additional References	342
Chapter 12 Walk Before Running: Building an IPv6 Lab and Starting a Pilot	343
Sample Lab Topology	344
Sample Lab Addressing	347
Configuring the Networking Devices	348
Operating System, Application, and Management Deployment	348
Moving to a Pilot	359
Summary	360
Additional References	360
Index	361

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a show command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Internet Protocol version 6 (IPv6) is the next version of the protocol that is used for communication among devices of all types on the Internet. IPv6 has been in existence for many years, but recently the deployment of IPv6 has accelerated greatly in the enterprise. IPv6 has been under continuous development and is maturing as real-world deployments expose gaps in either the protocol or the deployment methodology of the protocol.

Enterprises around the world are being exposed to IPv6 by either deploying operating systems and applications that automatically use IPv6 (at times without their knowledge), or they are proactively deploying IPv6 to fill requirements for the following: additional addressing, expansion into emerging markets, dealing with merger-and-acquisition challenges, and leveraging the new capabilities of the protocol for cutting-edge endpoints and applications. Whatever the reason, it is critical for the enterprise to fully understand the deployment options available with IPv6 and to take an aggressive but well-thought-out planning and design approach to their deployment.

IP is pervasive; it is everywhere. So, to properly plan and deploy IPv6 in an enterprise network, the IT staff must break the deployment down into places in their network such as the campus, data center, WAN, and so on and then focus on all the places where IPv4 is used today. Then, based on the business and technical drivers, the staff must implement IPv6 alongside of IPv4. There will be times when IPv6 is deployed in new areas where IPv4 is no longer needed and also times when IPv6 might not be needed everywhere that IPv4 is. This book breaks down the enterprise into various places in the network and gives design and deployment guidance on how to implement IPv6 in these areas.

Goals and Methods

Enterprises often get bogged down in the political issues and business justification of a new project and often end up with a technical design and implementation that is sourced from a “figure it out as we go along” mind-set. The goal of this book is to give the reader a practical and proven way to break down the massive task of IPv6 deployment into consumable sections based on places in the network and to provide the reader with validated configuration examples that can be used to build a lab, pilot, and production network.

This book has a pretty consistent flow to the information that is to provide an introduction to each area of deployment, diagrams to show the example topologies (where applicable), and then various configuration examples to help reinforce the deployment concepts. This book will help you understand the options for IPv6 deployment in the enterprise and see how to implement those deployment options.

Who Should Read This Book

This book is intended to be read by people working in an enterprise IT environment and partners or consultants who support enterprise IT. You should already know the fundamental concepts of IPv6 to include addressing, neighbor and router communication, and

routing. While some of the chapters are introductions to certain topics and principles, none of them are in-depth enough to be the sole resource for an IPv6 newcomer as they relate to the basic mechanics of the protocol. This book assumes that the reader has a thorough understanding of networking technologies and network design and deployment. The book will work from long-standing design best practices from Cisco related to Layer 2 and Layer 3 design and is not a primer for network design or an introduction to IPv6.

How This Book Is Organized

Although this book could be read from cover to cover, it is designed to be flexible and to allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with.

An introduction to enterprise IPv6 deployment is given in Chapters 1–4 and covers the following introductory topics:

- **Chapter 1, “Market Drivers for IPv6 Adoption”:** This chapter discusses the common business and technical drivers for IPv6 deployment in the enterprise. Growing deployment trends and common use cases are given.
- **Chapter 2, “Hierarchical Network Design”:** This chapter gives an overview of the well-known and mature hierarchical design model for networks and allows the reader to have a basic foundation for network design principles that will be built on throughout the book.
- **Chapter 3, “Common IPv6 Coexistence Mechanisms”:** This chapter discusses a few of the most common coexistence mechanisms (also called transition mechanisms) used in the enterprise. Dual-stack, ISATAP, 6to4, and others are introduced in this chapter.
- **Chapter 4, “Network Services”:** This chapter examines the common network services used in most IPv6 deployments and includes IPv6 multicast, quality of service (QoS), and routing protocols. Other chapters in the book will show more examples of how these services are deployed.

Chapters 5–12 focus on the actual deployment of IPv6 in an enterprise network and are much more technical in nature:

- **Chapter 5, “Planning an IPv6 Deployment”:** This chapter provides information on the high-level predeployment and deployment considerations and phases. The chapter offers a systematic view of planning for the deployment of IPv6.
- **Chapter 6, “Deploying IPv6 in Campus Networks”:** This chapter covers the deployment options most often used in a campus network environment. Various coexistence mechanisms are discussed in detail as well as the configurations for making a highly available IPv6 deployment a success in the campus. Advanced technologies such as the Cisco Virtual Switching System are also discussed.

- **Chapter 7, “Deploying Virtualized IPv6 Networks”:** This chapter discusses various network, device, desktop, and server virtualization solutions and provides configuration examples for some of these solutions to include 6PE and 6VPE.
- **Chapter 8, “Deploying IPv6 in WAN/Branch Networks”:** This chapter provides the reader with various design scenarios for the WAN and branch areas of the network and gives detailed configuration examples for different WAN/branch devices and services to include Dynamic Multipoint VPNs and the Cisco ASA.
- **Chapter 9, “Deploying IPv6 in the Data Center”:** This chapter covers the common technologies, services, and products in the data center and works from a common design to give the reader various configurations that can be used in his or her own environment. Various data center–focused products, such as the Cisco Nexus 7000, 1000v, and MDS 9000, are discussed along with Cisco NAM, ASA, and other products and technologies.
- **Chapter 10, “Deploying IPv6 for Remote Access”:** This chapter discusses the options for enabling IPv6 in a remote-access VPN environment. Examples are shown to allow IPv6 over a legacy VPN (non-IPv6-supported products) and also to use the Cisco ASA and AnyConnect SSL VPN solutions in an IPv6 environment.
- **Chapter 11, “Managing IPv6 Networks”:** This chapter covers the common management components used in enterprise IPv6 deployments. These components include management applications and tools, instrumentation, and management information transported over IPv6.
- **Chapter 12, “Walk Before Running: Building an IPv6 Lab and Starting a Pilot”:** This chapter discusses the need and purpose of a dedicated lab and the importance of a pilot for IPv6. A practical and systematic view of how to build a lab, perform application testing, and move to a pilot environment is discussed.

This page intentionally left blank

Deploying IPv6 in WAN/Branch Networks

This chapter covers the following subjects:

WAN/branch deployment overview: This section describes the single-tier, dual-tier, and multitier branch deployment models.

General WAN/branch IPv6 deployment considerations: Details on generic IPv6 considerations that apply to any of the WAN/branch deployment models are presented.

WAN/branch implementation example: Detailed configuration information is provided for a WAN/branch design that combines elements of the single-tier, dual-tier, and multi-tier profiles.

WAN/branch deployment over native IPv6: Configuration details are shown for branch-to-WAN head-end deployments, where the Internet Protocol used between sites is IPv6 instead of IPv6-over-IPv4 shown in other examples.

This chapter focuses on providing you with various options for connecting branch offices to the regional or headquarters site using IPv6. As has been discussed in other chapters, there are times when IPv6 needs to be encapsulated into IPv4 to traverse the WAN transport. This happens most often because of the lack of native IPv6 support by the WAN provider and not by lacking features or capabilities of the networking gear. There are a wide variety of deployment options in WAN/branch scenarios that can provide you with a way to provide IPv6 connectivity to branch users and access applications and services located at the main site and beyond.

Native IPv6 deployment is also discussed in this chapter. When port-to-port IPv6 access is available by the WAN service provider, the dependency for encapsulating IPv6 into IPv4 IPsec or SSL is no longer present. IPv6 over IPsec can be deployed today between Cisco IOS branch routers and the WAN head-end routers.

WAN/Branch Deployment Overview

The following sections provide a high-level overview of the three most commonly deployed Cisco branch profiles and the associated WAN head-end. These sections provide a basic understanding of how IPv6 can be integrated into the following branch profiles:

- Single-tier profile
- Dual-tier profile
- Multitier profile

Single-Tier Profile

The single-tier branch profile is a fully integrated design and based on the Cisco Dynamic Multipoint Virtual Private Network (DMVPN) solution. The requirements for LAN and WAN connectivity and security are met by a single Integrated Services Router (ISR). More information about the Cisco ISR platform can be found in the references section of this chapter. Figure 8-1 shows a high-level view of the single-tier branch profile.

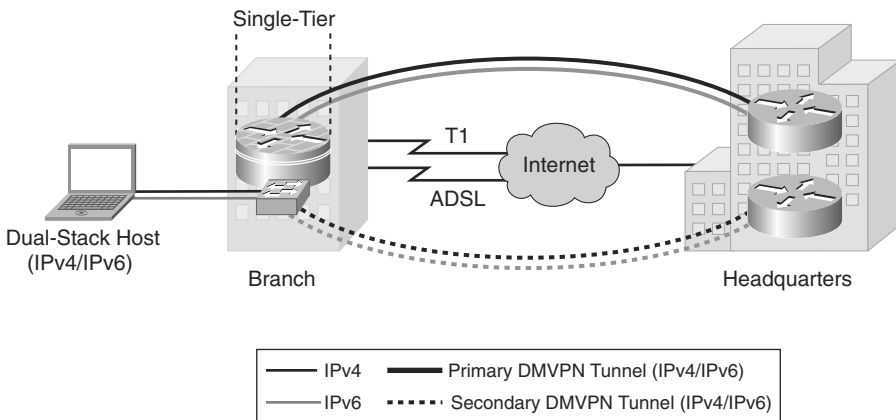


Figure 8-1 *Single-Tier Profile Overview*

The single-tier uses a single ISR and is used to provide WAN connectivity through a T1/E1 line to an Internet service provider (ISP). This T1/E1 is used as the primary link to the headquarters (HQ) site. For WAN redundancy, a backup connection is made through asymmetric digital subscriber line (ADSL). There are many alternatives that can be used in this design, such as a different WAN media type and VPN type.

IPv4 and IPv6 connectivity to the HQ site is provided by IPv4 IPsec using DMVPN technologies (DMVPN supports both IPv4 and IPv6-over-IPv4 IPsec). DMVPN works by encapsulating both IPv4 and IPv6 traffic into a generic routing encapsulation (GRE) tunnel, encrypted by IPv4 IPsec and forwarded between sites. The DMVPN tunnels traverse the T1 link as the primary path and establish backup tunnels over the ADSL link.

All traffic leaving the branch traverses the VPN connections to the HQ, including the Internet-bound traffic. Generally, Cisco does not recommend the use of split tunneling at the branch site. If the customer requires split tunneling (that is, Internet traffic leaves the branch directly while corporate-bound traffic traverses the VPN connection), Cisco recommends a careful analysis and testing of the routing and the security implications of such a deployment.

LAN connectivity is provided by an integrated switch module (EtherSwitch Service Module). Dual-stack (running both an IPv4 TCP/IP stack and IPv6 TCP/IP stack) is used on the VLAN interfaces at the branch.

In addition to all the security policies in place at the HQ, local security for both IPv4 and IPv6 is provided by a common set of infrastructure security features and configurations. Additionally, an integrated firewall such as the Cisco IOS Firewall or the Cisco IOS Zone-based Firewall is used. Quality of service (QoS) for IPv4 and IPv6 is integrated into a single policy.

The obvious disadvantage of the single-tier profile is the lack of router and switch redundancy. There is redundancy for the link to the Internet and the VPN connections to HQ. However, because there is a single integrated switch and single router, if either component fails, the site is completely disconnected from HQ. The dual-tier or multitier profile is the solution for customers requiring additional redundancy for the network components (switches, routers, firewalls, and HQ connections).

Dual-Tier Profile

The dual-tier profile separates the routing and switching roles in the branch and provides device and link redundancy for the branch routers.

Figure 8-2 shows a high-level view of the dual-tier profile.

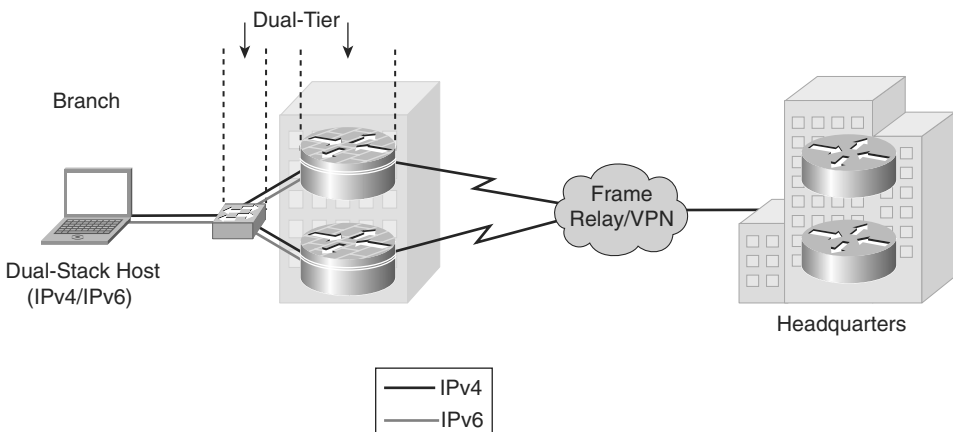


Figure 8-2 *Dual-Tier Profile Overview*

There are three primary differences between the single-tier and dual-tier profile:

- Redundancy
- Scalability
- WAN transport

Redundancy

The dual-tier separates the LAN (switch) and WAN (router) components to offer fault tolerance. A single switch or multiple switches can be used to provide LAN access in the branch. There are two WAN routers redundantly connected to the Frame Relay cloud (or other WAN/VPN type), in addition to being redundantly connected to the LAN switch.

Scalability

The dual-tier scales better because the single-tier is pretty much an “everything but the kitchen sink” approach. In other words, every network role required in the branch is performed by the ISR. This is great for cost and manageability but can limit availability and scalability. The larger the branch and the more services enabled on the ISR, the higher the risk gets for overextending the performance capabilities of the ISR. This can be alleviated by using a more powerful ISR model, but this does not help with the fault-tolerance requirement. If additional LAN switches are needed at the branch, the Catalyst switches can be used together using the Cisco StackWise technology.

WAN Transport

The WAN connections in the dual-tier model can use Frame Relay, point-to-point IPsec VPN, DMVPN, Multiprotocol Label Switching (MPLS), or whatever WAN type is available. IPv6 is fully supported over Frame Relay in Cisco IOS, and therefore there is no need to run tunnels of any kind between the branch and HQ. This is a great advantage for deployment and management because dual-stack is used all the way from the hosts in the branch LAN across the WAN and into the HQ network. This greatly eases the operational aspects of deploying IPv6 in the branch because no special tunnel considerations (such as availability, security, QoS, and multicast) need to be made.

Security for the dual-tier profile is the same as for the single-tier with the exception that both routers in the dual-tier provide security services.

Multitier Profile

The goal of the multitier profile is complete separation of roles and to offer device and link redundancy at each tier or layer in the branch network. Basically, the multitier is a combination of the single-tier and dual-tier with an additional focus on availability, scalability, and more robust firewall services. The multitier, for the most part, looks like a small campus deployment, and both very often use the same or similar products, design

concepts, and configurations. The differences between a small campus and the multitier are more around the presence of the firewall and WAN routers in the multitier example.

Figure 8-3 shows a high-level view of the multitier profile.

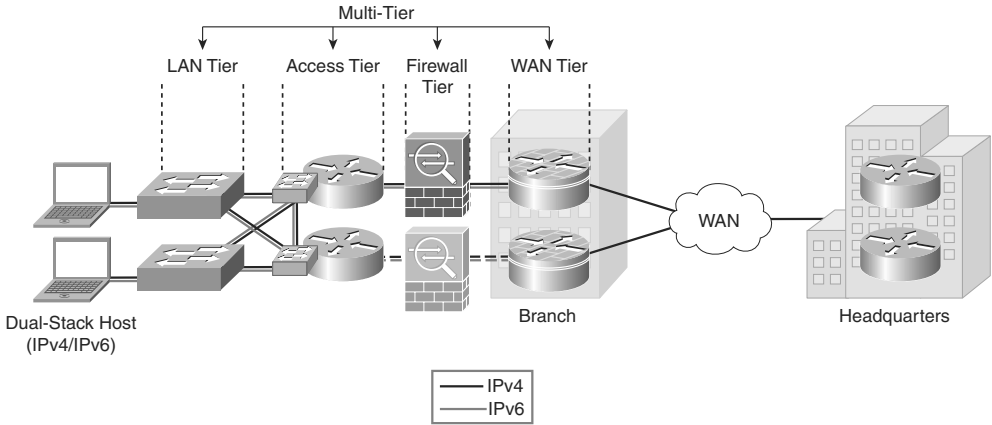


Figure 8-3 *Multitier Profile Overview*

Figure 8-3 shows how the tiers or roles are distributed. Several changes are evident with the multitier versus the dual-tier:

- **Firewall tier:** Firewall services are now separated from the WAN routers. The Cisco ASA 5500 series is shown here and is providing stateful firewall services for both IPv4 and IPv6. The second ASA (the bottom ASA in Figure 8-3) is in stateful failover mode. In a stateful failover configuration, the ASA is operating in an active/standby (shown in Figure 8-3) or active/active mode.
- **Access tier:** The access tier is used for internal service and VLAN termination for the LAN tier. The access tier is like a campus distribution layer in many ways.
- **LAN tier:** The LAN tier is the same as with the dual-tier LAN switch. There are just more of them to account for the larger-scale requirements that are most likely found in a larger branch.

General WAN/Branch IPv6 Deployment Considerations

Some general considerations apply to the deployment profiles described in this chapter. The following sections describe the general considerations to take into account when deploying IPv6 in a branch network, regardless of the deployment profile being used. If a specific consideration should be understood, the specific profile is called out, along with the consideration for that profile.

The branch IPv6 profiles described in this chapter leverage the existing Cisco branch network design best practices as the foundation for all aspects of the deployment. The IPv6 components of the profiles are deployed in the same way as IPv4 whenever possible.

It is critical to understand the Cisco branch design best practice recommendations before deploying IPv6 in the branch profiles described in this chapter. The Cisco branch design best practice documents can be found under the “Branch Office” and “WAN” sections at http://www.cisco.com/en/US/netsol/ns816/networking_solutions_program_home.html.

Addressing

In most cases, the use of a /64 prefix on point-to-point (P2P) links is just fine. IPv6 was designed to have a large address space, and even with the poor address management in place, the customer should not experience address constraints.

Some network administrators think that a /64 prefix for P2P links is a waste of address space. There has been quite a bit of discussion within the IPv6 community about the practice of using longer prefixes for P2P links. For those network administrators who want to more tightly control the address space, it is safe to use a /126 prefix on P2P links in much the same way as /30 is used with IPv4. A /127 prefix can be used if you are aware of the potential address overlap with special use addresses. IPv6 address considerations can be found in RFC 5375 at <http://www.ietf.org/rfc/rfc5375.txt>.

The P2P configurations shown in this chapter use a /64 prefix. The assignment of end-host IPv6 addresses is done either by using Stateless Address Autoconfiguration (SLAAC) (see RFC 4862, “IPv6 Stateless Address Autoconfiguration”), which advertises an IPv6 prefix (through an RA) on the router subinterface for the VLAN where PCs are located, or through stateful DHCPv6. The options for Domain Name System (DNS) server and domain name are assigned using stateless DHCPv6 or stateful DHCPv6. The configurations for the SLAAC, stateless, and stateful DHCPv6 will be shown later in the chapter.

More information can be found on IPv6 addressing services at the following URL: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/15_0/ipv6_15_0_book.html.

Physical Connectivity

Considerations for physical connectivity with IPv6 are the same as with IPv4, plus five additional elements:

- **Sufficient bandwidth:** One important factor for deployment of any new technology, protocol, or application is to ensure that there is a sufficient amount of bandwidth for both existing and new traffic. This issue is especially true with the branch because, in many cases, the connections to the WAN are low-speed links and the reliance on QoS to solve bandwidth problems goes only so far. Bandwidth requirements for IPv6 are outside the scope of this chapter because there are many variables to account for and should therefore be considered on a case-by-case basis.

- **Maximum transmission unit (MTU) and fragmentation:** The minimum MTU size for IPv6 is 1280 bytes. If the link layer does not support the MTU requirement, link-layer fragmentation and reassembly must be provided and be transparent to IPv6. A good starting point for understanding MTU and Path MTU Discovery (PMTUD) for IPv6 is with RFC 2460 (<http://www.ietf.org/rfc/rfc2460.txt>) and RFC 1981 (<http://www.ietf.org/rfc/rfc1981.txt>).
- **IPsec VPN:** When IPsec is used with GRE or manual tunnels, it is important to account for how to adjust the MTU value on the routers to ensure that the router is not forced to perform fragmentation of the IPv4 traffic because of the IPsec header and the additional tunnel overhead. By manually configuring the MTU values prior to IPv6 encapsulation, the MTU requirements can be met for IPv6 without fragmentation concerns. More information on this can be found in any of the IPsec design guides at http://www.cisco.com/en/US/tech/tk583/tk372/tech_design_guides_list.html.
- **IPv6 over wireless LANs (WLAN):** IPv6 should operate correctly over WLAN access points in much the same way as IPv6 operates over Layer 2 switches. However, there are considerations to IPv6 with WLAN environments such as managing WLAN devices (APs and controllers) through IPv6 and controlling IPv6 traffic through AP or controller-based QoS, VLANs, and access control lists (ACL). IPv6 must be supported on the AP and controller devices to take advantage of these more intelligent services on the WLAN devices. At the time of writing this chapter, Cisco does not yet have robust IPv6 support on its WLAN product family.
- **IPv6 phone ports:** It is important to point out that Cisco supports the use of IPv6-enabled hosts that are directly attached to Cisco IP Phone ports. These IP phone ports are switch ports and operate in much the same way as plugging the host directly into a Catalyst Layer 2 switch.

In addition to the previous considerations, Cisco recommends that a thorough analysis of the existing traffic profiles, memory use, and CPU use on both the hosts and network equipment, and the service level agreement (SLA) language, be completed prior to implementing any of the IPv6 models described in this chapter.

VLANs

VLAN considerations for IPv6 are mostly the same as for IPv4. When dual-stack configurations are used, both IPv4 and IPv6 traverse the same VLAN. For the current VLAN design recommendations, refer to the Cisco branch-LAN design best practice documents at <http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/Overview.html>.

The use of IPv6 on data VLANs that are trunked along with voice VLANs (behind IP phones) is fully supported. Care must be taken to ensure that the correct firmware and proper Cisco Unified Communications Manager configurations are made to ensure that the data and voice VLANs do not allow IPv6 router advertisements (multicast-based) to be bled between VLANs.

For more information on IPv6 and Cisco IP Phones and how to best support VLANs for those endpoints, refer to the section “Unified Communications Endpoints” at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/ipv6/ipv6srnd.html. For information on how to deploy IPv6 on the Cisco Unified Communications Manager, refer to http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/ipv6/ipv6srnd.html.

Routing

Choosing an interior gateway protocol (IGP) to run in the branch network is based on a variety of factors: Platform capabilities, IT staff expertise, and the size of network are just a few. In this chapter, the IGP for both IPv4 and IPv6 is Enhanced IGRP (EIGRP). Open Path Shortest First version 2 (OSPFv2) for IPv4 and OSPFv3 for IPv6 can also be used.

As previously mentioned, every effort to implement the current Cisco branch design best practices has been made. Both the IPv4 and IPv6 IGP have been tuned according to the current best practices for the branch. It should be one of the top priorities of any network design to ensure that the IGPs are tuned to provide a stable, scalable, and fast-converging routing protocol.

EIGRP has been configured to provide authentication for both IPv4 and IPv6 adjacencies and updates.

High Availability

Many aspects of High Availability (HA) are not applicable to or are outside the scope of this chapter. Many of the HA requirements and recommendations are met by leveraging the existing Cisco branch design best practices. The primary HA components described in this chapter are

- **Redundant WAN connections:** The deployment of redundant WAN links can vary greatly from customer to customer. Some customers deploy a T1 with a backup connection over a different connection, such as a broadband DSL connection. Redundant Frame Relay connections and/or MPLS connections are also quite common.
- **Redundant routing and forwarding paths:** This is accomplished by leveraging EIGRP for IPv4 and IPv6. In some cases, Equal Cost Multi-Path (ECMP) is used, and in other cases (IPsec GRE and manual tunnels), one path is preferred over another, but the secondary path is available for redundancy.
- **High availability of the first-hop gateways:** This level of HA applies to any branch and/or WAN head-end connection where there are two or more routers. HSRPv2 for IPv4 and IPv6 can provide first-hop gateway redundancy in this chapter. Cisco also supports gateway load balancing protocol (GLBP) for IPv4 and IPv6.

QoS

Cisco recommends that QoS policies be implemented in an application- or service-dependent methodology instead of a protocol- (IPv4 or IPv6) dependent methodology. Basically, if the existing QoS policy has specific classification, policing, and queuing for an application, that policy should treat the IPv4 and IPv6 traffic for that application equally.

The key consideration as far as Modular QoS CLI (MQC) is concerned is the removal of the `ip` keyword in the QoS `match` and `set` statements when IPv6 QoS is required.

Table 8-1 shows the modification in the QoS syntax to support IPv6 and IPv4.

There are QoS features that work for both IPv6 and IPv4 but require no modification to the command-line interface (CLI), for example, Weighted Random Early Detection (WRED), policing, and Weighted Round Robin (WRR).

Cisco provides an extensive collection of QoS recommendations for the WAN/branch. See the references section at the end of this chapter for a complete list.

Table 8-1 QoS Syntax Modifications

IPv4-Only QoS Syntax	IPv4/IPv6 QoS Syntax
<code>match ip dscp</code>	<code>match dscp</code>
<code>match ip precedence</code>	<code>match precedence</code>
<code>set ip dscp</code>	<code>set dscp</code>
<code>set ip precedence</code>	<code>set precedence</code>

Security

Many of the common threats and attacks on existing IPv4 campus networks also apply to IPv6. Unauthorized access, spoofing, routing attacks, viruses, worms, denial of service (DoS), and man-in-the-middle attacks are just a few that plague both IPv4 and IPv6.

There are many new threats with IPv6 that do not exist with IPv4 or they operate differently from IPv4. There are inherent differences in how IPv6 handles neighbor and router advertisement and discovery, headers, and even fragmentation. Based on all of these variables and possibilities, IPv6 security is an involved topic in general, and detailed security recommendations and configurations are outside the scope of this chapter. There are numerous efforts both within Cisco and the industry to identify, understand, and resolve IPv6 security threats. There is an excellent Cisco Press book dedicated to the topic of IPv6 security: *IPv6 Security*, by Scott Hogg and Eric Vyncke. (See the “Additional References” section at the end of this chapter for more information.)

This chapter points out some possible areas to address within the branch and gives basic examples of how to provide basic protection of IPv6 dual-stack and tunneled traffic.

Note The examples given in this chapter are in no way meant to be recommendations or guidelines, but rather are intended to challenge you to carefully analyze your own security policies as they apply to IPv6 in the branch/WAN.

General security considerations for network device protection that apply to branch profiles are as follows:

- **Controlling management access to the branch routers and switches:** All the branch/WAN routers and switches for each profile have configurations in place to provide management access protection to the devices. All routers have loopback interfaces configured for management and routing purposes.

To more tightly restrict access to a particular switch/router through IPv6, an ACL is used to permit access to the management interface (line vty) by way of the loopback interface. The permitted source network is from the enterprise IPv6 prefix. To make ACL generation more scalable for a wide range of network devices, the ACL definition can permit the entire enterprise prefix as the primary method for controlling management access to the device instead of filtering to a specific interface on the device. The IPv6 prefix used in this enterprise site (for example only) is 2001:db8:cafe::/48. See Example 8-1.

Example 8-1 Router VTY Configuration

```
interface Loopback0
  ipv6 address 2001:DB8:CAFE:1F3::9/128
!
  ipv6 access-list MGMT-IN
  remark Permit MGMT only to Loopback0
  permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:1F3::9
  deny ipv6 any any log-input
!
  line vty 0 4
  session-timeout 3
  access-class MGMT-IN-v4 in
  password 7 08334D400E1C17
  ipv6 access-class MGMT-IN in          #Apply IPv6 ACL to restrict
                                       #access

  logging synchronous
  login local
  exec prompt timestamp
  transport input ssh
```

- **Controlling access through HTTP:** At the time of this writing, Cisco IOS does not support the use of IPv6 HTTP ACLs to control access to the device. This is important because switches and routers that currently use **ip http access-class** ACLs for

IPv4 do not have the same level of protection for IPv6. This means that subnets or users who were previously denied access through HTTP/HTTPS for IPv4 now have access to the switch or router through IPv6.

- **Control Plane Policing (CoPP):** CoPP protects the router by preventing DoS or unnecessary traffic from negatively impacting CPU resources. Priority is given to important control plane/management traffic. The configuration of CoPP is based on a wide variety of factors, and no single deployment recommendation can be made because the specifics of the policy are determined on a case-by-case basis. You can find more information about CoPP at http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlmt.html.
- **Controlling ingress traffic from the branch LAN:** Filter which prefixes are allowed to source traffic. This is most commonly done on ingress on the LAN or subinterface on the branch router. Controlling IPv6 traffic based on source prefix can help protect the network against basic spoofing.

Example 8-2 shows a basic ACL example: applied ingress on a branch router's LAN interface.

Example 8-2 Basic Branch LAN Ingress ACL

```

ipv6 access-list DATA_LAN-v6
remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:1004::/64
permit icmp 2001:DB8:CAFE:1004::/64 any
remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:1004::/64
permit ipv6 2001:DB8:CAFE:1004::/64 any
remark PERMIT ICMPv6 PACKETS SOURCED BY HOSTS USING LINK-LOCAL
permit icmp FE80::/10 any
remark PERMIT DHCPv6 ALL-DHCP-AGENTS REQUESTS FROM HOSTS
permit udp any eq 546 any eq 547
remark DENY ALL OTHER IPv6 PACKETS AND LOG
deny ipv6 any any log-input
!
interface GigabitEthernet0/0.104
description VLAN-PC
ipv6 traffic-filter DATA_LAN-v6 in

```

Cisco IOS IPv6 ACLs contain implicit permit entries for IPv6 neighbor discovery. If **deny ipv6 any any** is configured, the implicit neighbor discovery entries are overridden. It is important that if a manually configured catch-all **deny** statement is used for logging purposes, the following two permit entries must be added back in: **permit icmp any any nd-na** and **permit icmp any any nd-ns**.

- **IPv6 stateful firewall services:** Firewalls provide a stateful security inspection for IPv6 traffic entering or leaving a branch network. At the time of this writing, the Cisco ASA 5500 Series, Cisco IOS Firewall, and Cisco IOS Zone-based Firewall support IPv6 inspection at various levels. It is critical that you consult with Cisco

documentation, a Cisco account team, and/or a Cisco partner to understand which Cisco Firewall solution is appropriate for the customer environment.

- **Disabling unused services:** Many services, such as HTTP server, are supported for IPv4 and IPv6. Enabling or disabling these services generally applies to both protocols. It is a long-standing recommendation to disable any services that are not in use.

Multicast

IPv6 multicast is an important service for any enterprise network design. One of the most important factors to IPv6 multicast deployment is to ensure that host/group control is handled properly in the branch LAN. Multicast Listener Discovery (MLD) in IPv6 is the equivalent to Internet Group Management Protocol (IGMP) in IPv4. Both are used for host multicast group membership control. MLD snooping is the ability to control the distribution of multicast traffic only to the ports that have listeners. Without it, multicast traffic meant for only a single receiver (or group of receivers) would be flooded to all ports on the branch LAN switch belonging to the same VLAN. In the branch LAN, it is important that the switches support MLD snooping for MLD version 1 and/or version 2.

Today, Cisco IOS supports the following Protocol Independent Multicast (PIM) implementations: PIM-SM, PIM-BSR, PIM-SSM, Bidirectional PIM, Embedded-RP, and Multiprotocol BGP for the IPv6 Multicast Address Family.

There are several documents on Cisco.com and within the industry that describe IPv6 multicast in detail. Other than generic references to the commands that are used to enable IPv6 multicast and requirements for Embedded-RP definition, no other configuration notes are made in this chapter. For more information, refer to the following URLs:

- **Cisco IPv6 multicast:**
http://www.cisco.com/en/US/technologies/tk648/tk828/tk363/technologies_white_paper0900aecd8014d6dd.html
- **Cisco IOS IPv6 multicast configuration:**
http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a0080203f7a.shtml

Management

Management for IPv6 is under development and has a long way to go. Many of the traditional management tools used in IPv4 also support IPv6. In this chapter, the only considerations for management of the branch network are related to basic control of management services (Telnet, SSH, and SNMP). All the IPv6-enabled devices in the two branch profiles described are manageable over IPv6 through the previously mentioned services except SNMP.

The deployment of Simple Network Management Protocol (SNMP) for IPv6 is the same as with IPv4. In the branch profiles described in this chapter, SNMPv3 (AuthNoPriv) can provide polling capabilities for the Cisco Network Management Systems (NMS) servers

located in the HQ data center. Here is an example of the SNMPv3 configuration used in the branch routers in this chapter:

```
snmp-server contact John Doe - ipv6rocks@example.com
snmp-server group IPv6-ADMIN v3 auth write v1default
snmp-server user jdoe IPv6-ADMIN v3 auth md5 cisco1234
```

If information needs to be sent to a Cisco NMS server, an SNMP host can be defined. The host can be defined to send SNMP information over IPv4 and/or IPv6:

```
snmp-server host 2001:DB8:CAFE:100::60 version 3 auth jdoe
```

Another area of management that must be thoroughly researched is that of address management. The process of assigning large hexadecimal addresses to many network devices should, at some point, be automated or at least made more user-friendly than it is today.

Today, one way to help with the deployment of address prefixes on a Cisco router is through the use of the general prefix feature. This feature enables the customer to define a prefix or prefixes in the global configuration of the router with a user-friendly name. That user-friendly name can be used on a per-interface basis to replace the usual IPv6 prefix definition on the interface. The general prefix feature is most applicable in deployments where there is or can be frequent changes in the address prefix, such as during a pilot or in early production when the final IPv6 address policy is not fully nailed down. The following is an example of how to use the general prefix feature:

Step 1. Define the general prefix:

```
br1-1(config)# ipv6 general-prefix BRANCH-1 2001:DB8:CAFE::/48
```

Step 2. Configure the general prefix named BRANCH-1 on a per-interface basis:

```
br1-1(config-if)# ipv6 address BRANCH-1 ::1005:0:0:0:1/64
```

Step 3. Verify that the general prefix was correctly assigned to the interface:

```
br1-1# show ipv6 interface g1/0.100
GigabitEthernet1/0.100 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::217:94FF:FE90:2829
  No Virtual link-local address(es):
  Description: DATA VLAN for Computers
  Global unicast address(es):
    2001:DB8:CAFE:1005::1, subnet is 2001:DB8:CAFE:1005::/64
```

You can find more information on the general prefix feature at the Cisco IOS IPv6 documentation page at http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con_ps10591_TSD_Products_Configuration_Guide_Chapter.html#wp1132473.

Cisco supports the management of IPv6-enabled network devices through a variety of network management products to include DNS, DHCPv6, device management and monitoring, and network management, troubleshooting, and reporting. You can find more

information on the various Cisco Network Management solutions at <http://www.cisco.com/en/US/products/sw/netmgtsw/index.html>.

Chapter 11, “Managing IPv6 Networks,” goes into greater detail on IPv6 management.

Scalability and Performance

This chapter is not meant to analyze scalability and performance information for the various platforms tested. The coverage of scale and performance is more focused on general considerations when planning and deploying IPv6 in the branch versus a platform-specific view.

Scalability and performance considerations for the branch network devices are as follows:

- **Traffic utilization:** In IPv6 implementations, it is common to see a change in traffic utilization ratios on the branch network links. As IPv6 is deployed, IPv4 traffic utilization is often reduced as users leverage IPv6 as the transport for applications that were historically IPv4-only. There is often a slight increase in overall network utilization, which usually derives from control traffic for routing and, if deployed, tunnel overhead.
- **Routing/forwarding:** It is important to understand the routing and forwarding capabilities of the branch routers. If the existing branch router is already running at high CPU and memory utilization rates for the handling of IPv4 routing tables and updates, it is a bad idea to add IPv6 to the existing router. If the routing platform is hardware based, the impact is less of a concern.
- **ACL processing:** It is imperative that the deployment of ACLs be carefully planned. IPv6 ACLs in the branch routers are used for QoS (classification and marking of ingress packets from the access layer), for security (controlling DoS, snooping, and unauthorized access for ingress traffic in the access layer), and for a combination of QoS + security to protect the control plane of the router from attack. The router can also provide Cisco IOS stateful firewalling services, intrusion detection systems/intrusion prevention systems (IDS/IPS), and voice services for IPv4 and new services for IPv6. Advanced services that are added to the branch router should support both IPv4 and IPv6. Performance will be impacted with all these added services plus the newly enabled IPv6 configuration.

Cisco has an IPv4/IPv6 performance comparison document that goes into some detail on these topics at http://www.cisco.com/web/strategy/docs/gov/IPv6perf_wp1f.pdf.

WAN/Branch Implementation Example

Much of the configuration and design among the three different WAN/branch deployment profiles is similar. The largest variables are usually the number of devices within a branch for high-availability purposes and the scale of the overall environment.

The implementation example given in this chapter combines properties from each of the three WAN/branch profiles so that you can get a basic understanding of the various tiers, network roles, and specific products and features when configured for IPv6 support.

Throughout the remainder of this chapter, the example topology is called the “hybrid branch example,” or HBE. Again, this is just an example configuration that is meant to combine elements from each of the three WAN/branch profiles and is not meant to be a recommended best practice design.

Figure 8-4 shows the high-level overview of the HBE environment.

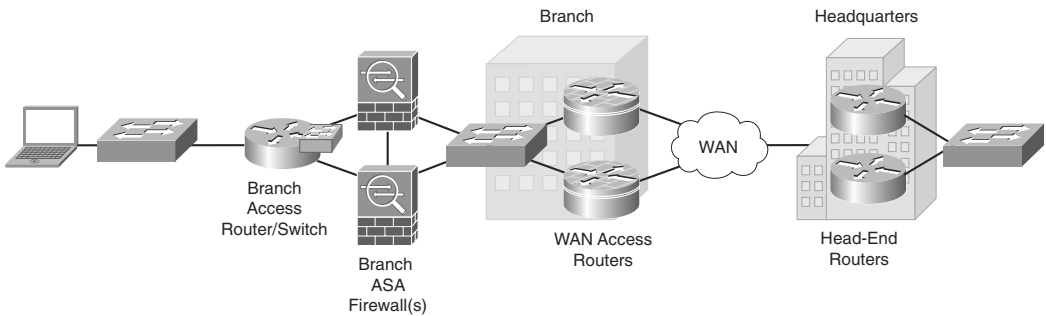


Figure 8-4 *Hybrid Branch Example Overview*

The HBE has the flexibility to run almost any WAN type to include Frame Relay, MPLS, point-to-point IPsec VPN, DMVPN, and so on. In this example, the branch has redundant WAN access routers that connect to the HQ through redundant head-end routers. Behind the WAN access routers in the branch there is a Cisco ASA 5500 series firewall. Optionally a redundant ASA can be added for additional availability. There is a Cisco ISR series router with either a built-in Cisco EtherSwitch Module or a separate Catalyst switch that can connect local host resources such as PCs, printers, and other network-attached resources.

Additional devices might be required to meet the business requirements for each branch, such as additional routers, switches, and other network devices that can augment the high-availability, security, or robust network services goals of the branch.

Note The configurations shown are not full-device configurations but rather snippets of the full configuration and reveal only the most relevant portions of the IPv6 side of the deployment.

Tested Components

Table 8-2 lists the components that were used and tested in the hybrid branch example.

Table 8-2 HBE-Tested Components

Role	Hardware	Software
Router	Integrated Services Router: 2800 and 3800 Series	Advanced Enterprise Services 15.0.1M1
Switch	Cisco Catalyst 3750E/3560E	12.2(46)SE
Firewall	Cisco ASA 5510	8.2(2)
Host devices	Various laptops—PC	Microsoft Windows Vista, Windows 7

Network Topology

Figure 8-5 serves as a reference for all the configurations for the HBE. The figure shows the IPv6 addressing layout for the branch and HQ connections.

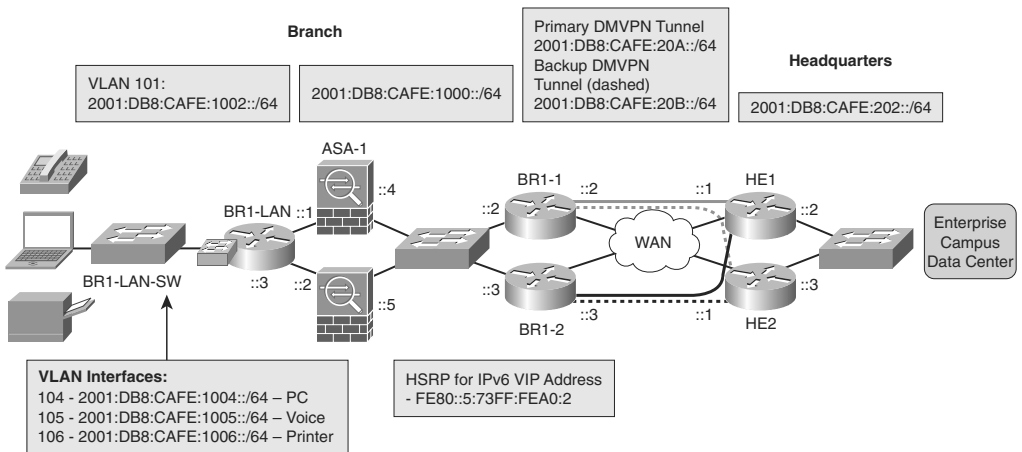


Figure 8-5 HBE IPv6 Addressing Details

The following sections discuss the physical and logical connectivity of the WAN access, branch LAN, and firewalls.

WAN Connectivity

The HBE uses the Dual DMVPN Cloud Topology with spoke-to-spoke support, as outlined in the Cisco DMVPN Design Guide at http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/DMVPDG.html.

The Dual DMVPN Cloud Topology has each branch site configured with a primary (solid lines between branch and HW) and secondary (dashed lines) DMVPN tunnel configuration. Each tunnel configuration is on a separate IPv4 and IPv6 network. The IGP is tuned

to prefer one tunnel over another, and if the primary tunnel fails, the IGP reconverges and traffic flows between the branch routers and the secondary head-end router using the secondary tunnel configuration.

The HBE could easily use a traditional Frame Relay, MPLS, or point-to-point IPsec VPN as well. DMVPN was selected for this example to give the reader a usable configuration for Cisco DMVPN support with IPv6.

Being that this is just an example and that there are many variables that could influence how this network is connected and configured, a simplistic approach was taken for addressing and physical connectivity. The important thing to take away from the HBE shown here is that most things are the same as with IPv4. The goal is to illustrate the minor syntax adjustments.

Branch LAN Connectivity

The LAN connectivity between the WAN access routers and the Cisco ASA is through a Catalyst switch. Each router is configured as a Hot Standby Router Protocol (HSRP) group member for both IPv4 and IPv6. The Cisco ASA has a default route to the HSRP standby address.

The LAN access router and ASA connect to each other using the EtherSwitch Module in the router. Alternatively a dedicated Catalyst switch could be used.

The LAN access portion of the branch uses a Catalyst switch to provide network access for hosts, IP phones, and printers. There are three VLANs in use in the HBE that are used for host access:

- **VLAN 104:** Used as the PC data VLAN. IPv4 addressing is provided by a local DHCP pool on the router. IPv6 addressing is provided by the branch router using SLAAC, and DNS/domain name are provided by a local DHCP pool for IPv6. Optionally, full DHCP for IPv4 and IPv6 can be used at the HQ site.
- **VLAN 105:** Used as the voice VLAN. IPv4 addressing is provided by a local DHCP pool on the router to include any voice-specific options (TFTP server). IPv6 addressing is provided by stateful DHCPv6. Optionally, stateless DHCP IPv6 can be used.
- **VLAN 106:** Used as the printer VLAN. IPv4 addressing is provided by a local DHCP pool on the router. The print server cards located in the branch automatically receive an IPv6 address from the router interface through stateless autoconfiguration. Optionally, full DHCP for IPv4 and IPv6 can be used at the HQ site.

Firewall Connectivity

Depending on the branch design and the security policy, a dedicated firewall might or might not be deployed. Some sites deploy a firewall at the branch if local Internet access for that branch is permitted (split-tunneling scenario) or if the firewall itself is used as the branch VPN device. Also, firewall support on the WAN access routers can be enabled to offer perimeter protection instead of using a dedicated ASA.

In the HBE, the Cisco ASA Firewall is used and configured in a basic way. There is an “outside” interface and an “inside” interface. The Cisco ASA can be deployed as a single standalone firewall with no redundancy, or the ASA can be configured in a stateful failover deployment, where a second ASA is deployed and used as standby unit (as shown earlier in Figure 8-4).

The Cisco ASA can be deployed in a *routed mode* or a *transparent mode* (sometimes known as *bridge mode*). Routed mode is what is used in this chapter and is the most popular of the deployment choices. Routed mode, simply put, is where the ASA has distinct Layer 3 interfaces, each on a different IPv4 and IPv6 network, and acts as a routed hop in the network (static and dynamic routing is supported in this mode). Transparent mode has the ASA in a Layer 2 configuration where packets are bridged across and inspected; the ASA is basically a bump-in-the-wire. These are oversimplified explanations of the routed and transparent modes, and the reader should fully understand the differences of each and their pros/cons. More information on routed and transparent mode can be found at <http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/fwmode.html>.

Head-End Configuration

The HBE WAN configuration begins at that headquarters site, where there are two Cisco routers acting as head-end termination points for the Dual DMVPN Cloud Topology.

Note Depending on the size/scale requirements, the platform and model of the router may vary. Work with a Cisco account team and/or Cisco partner to determine the most appropriate product to fill this role.

The two head-end routers (HE1 and HE2) have connections to the ISP through Fast Ethernet connections but could just as easily be T1/E1, DS3, and any other connection option. Fast Ethernet was the option selected to generate the configurations for this chapter.

DMVPN is the VPN technology that carries both IPv4 and IPv6. The DMVPN configuration used in this chapter uses Phase 3 of Cisco IOS support for DMVPN. The following three phases are defined for DMVPN:

- **Phase 1:** Hub-and-spoke capability only
- **Phase 2:** Initial spoke-to-spoke capability
- **Phase 3:** Support for IPv6 and enhancements for spoke-to-spoke to support larger-scale nonbroadcast multiaccess (NBMA) networks

More information on the theory, operation, and configuration of DMVPN for IPv6, Phase 3 enhancements, and next hop resolution protocol (NHRP) operation can be found at the following URLs:

- **Implementing DMVPN for IPv6:**
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dmvpn_ps10591_TSD_Products_Configuration_Guide_Chapter.html
- **Shortcut switching enhancements for NHRP:**
http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_nhrp_dmvpn.html#wp1072593
- **Configuring NHRP:**
http://cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_cfg_nhrp.html#wp1078234

You need to configure different features and values for the DMVPN configuration such as keys, hold times, and so on.

HE1 and HE2 have one tunnel configuration each. HE1 is the primary head-end, and because this a dual DMVPN cloud configuration, the tunnel used on HE1 is in a different IPv4 and IPv6 network than the tunnel used by HE2. One thing to note is that when IPv6 multicast is enabled on a router, Protocol Independent Multicast (PIM) uses tunnel numbers 0 and 1 to communicate with rendezvous points (RP) and tunnel sources. It is recommended to use tunnel numbers beginning at 2.

The configuration for HE1 is shown in Example 8-3. The configuration for HE2 is identical with the exception of different IPv4 and IPv6 addressing and route preference. The configuration for HE2 is not shown.

Example 8-3 HE1 Configuration

```

ipv6 unicast-routing
ipv6 cef
!
crypto isakmp policy 1          #Set ISAKMP Policy using pre-shared
                               #keys
    encr aes 256
    authentication pre-share
    group 2
!
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set HUB esp-aes 256 esp-sha-hmac
!

```

continues

Example 8-3 *HE1 Configuration continued*

```

crypto ipsec profile HUB
  set transform-set HUB
!
interface Tunnel2                                #If deployed, PIMv6 uses
                                                #tunnel 0 and 1 by default
                                                #so it is recommended to start
                                                #at 2

  description DMVPN Tunnel 1
  ip address 10.126.1.1 255.255.255.0
  no ip redirects
  no ip unreachable
  no ip proxy-arp
  ipv6 address 2001:DB8:CAFE:20A::1/64
  ipv6 mtu 1416                                  #Set MTU to account for
                                                #Tunnel/IPSec overhead

  ipv6 eigrp 10                                  #Enable IPv6 EIGRP
  ipv6 hold-time eigrp 10 35
  no ipv6 next-hop-self eigrp 10
  no ipv6 split-horizon eigrp 10
  ipv6 nhrp authentication CISCO                 #Set authentication string
                                                #for NHRP
  ipv6 nhrp map multicast dynamic               #Automatically add routers to
                                                #NHRP mappings
  ipv6 nhrp network-id 10                       #Enables NHRP on interface
  ipv6 nhrp holdtime 600
  ipv6 nhrp redirect                             #Phase 3 NHRP redirect for
                                                #spoke-to-spoke

  tunnel source Serial1/0
  tunnel mode gre multipoint                     #Multipoint GRE to support
                                                #multiple end-points

  tunnel key 10
  tunnel protection ipsec profile HUB           #Apply IPsec profile
!
interface GigabitEthernet2/0                   #LAN interface to HQ network
  description to HQ
  ip address 10.123.1.2 255.255.255.0
  ipv6 address 2001:DB8:CAFE:202::2/64
  ipv6 eigrp 10
  standby version 2
  standby 2 ipv6 autoconfig
  standby 2 priority 120
  standby 2 preempt delay minimum 30
  standby 2 authentication CISCO
  standby 2 track 2 decrement 90

```

```

!
interface FastEthernet0/0
  description to ISP
  ip address 172.16.1.1 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 172.16.1.2
!
ipv6 router eigrp 10                                #Enable EIGRP for IPv6
no shutdown

```

Branch WAN Access Router Configuration

The branch routers have serial (T1/E1) connections to the ISP. Again, these connections can be broadband (DSL/cable/wireless), Ethernet, DS3, and so on. The branch WAN access routers have IPv4-only connectivity to the ISP and should have ACLs permitting access to/from the ISP for only the necessary ports/protocols required to establish DMVPN connectivity to the head-end routers. (This assumes that no split tunneling is allowed.) The IPv6 portion of the configuration is similar to that of the head-end, where the IPv6 configuration applies to the local branch Ethernet interface and the DMVPN tunnel interfaces.

Both branch WAN access routers (BR1-1 and BR1-2) are configured nearly identically. The differences are in the unique IPv4 and IPv6 addressing, routing preferences, and HSRP preferences. The configuration for BR1-1 is shown in Example 8-4 (only one of the two DMVPN tunnel configurations is shown).

Example 8-4 *BR1-1 Configuration*

```

ipv6 unicast-routing
ipv6 cef
!
crypto isakmp policy 1
  encr aes 256
  authentication pre-share
  group 2
!
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set SPOKE esp-aes 256 esp-sha-hmac
!
crypto ipsec profile SPOKE
  set transform-set SPOKE
!
interface Tunnel2

```

continues

Example 8-4 *BR1-1 Configuration continued*

```

description to HUB
 ip address 10.126.1.2 255.255.255.0
 no ip redirects
 no ip unreachable
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:20A::2/64
 ipv6 mtu 1416
 ipv6 eigrp 10
 ipv6 hold-time eigrp 10 35
 no ipv6 next-hop-self eigrp 10
 no ipv6 split-horizon eigrp 10
 ipv6 nhrp authentication CISCO
 ipv6 nhrp map 2001:DB8:CAFE:20A::1/64 172.16.1.1
 ipv6 nhrp map multicast 172.16.1.1
 ipv6 nhrp network-id 10
 ipv6 nhrp holdtime 600
 ipv6 nhrp nhs 2001:DB8:CAFE:20A::1
 ipv6 nhrp shortcut
 tunnel source Serial1/0
 tunnel mode gre multipoint
 tunnel key 10
 tunnel protection ipsec profile SPOKE
interface Serial1/0
 description to ISP
 ip address 172.16.1.9 255.255.255.252
!
interface GigabitEthernet2/0
 description to BRANCH LAN
 ip address 10.124.1.2 255.255.255.0
 negotiation auto
 ipv6 address 2001:DB8:CAFE:1000::2/64
 ipv6 eigrp 10
 standby version 2
 standby 1 ip 10.124.1.1
 standby 1 priority 120
 standby 1 preempt delay minimum 30
 standby 1 authentication CISCO
 standby 1 track 1 decrement 90
 standby 2 ipv6 autoconfig
 standby 2 priority 120
 standby 2 preempt delay minimum 30
 standby 2 authentication CISCO
 standby 2 track 2 decrement 90
!

```

```

router eigrp 10
  network 10.0.0.0
  !
ip route 0.0.0.0 0.0.0.0 172.16.1.10
!
ipv6 router eigrp 10
  no shutdown

```

Branch Firewall Configuration

As was previously mentioned, the Cisco ASA firewall deployment in the HBE is simple and meant only as a reference for you. Many customers avoid the cost and management of a branch firewall because they believe the branch is a trusted site connected to the HQ through a trusted private WAN or VPN link. Because of this, the customer often configures some ACLs on the WAN access router to protect against basic attacks. The common thinking is that because the branch is configured to not enable direct Internet access by branch users, no comprehensive firewall policies are required, and the cost and complexity of deploying a dedicated firewall (and redundant pair of them) are avoided.

This chapter is not meant to argue the values of having a dedicated branch firewall but rather offers a basic design and configuration example if you do plan to include a dedicated Cisco ASA Firewall as a part of your branch design.

The following configuration is for a Cisco ASA Firewall running version 8.2(2), and there are two firewalls for redundancy sake. The firewalls are configured for a routed mode deployment.

Because the application types and ACL options are so diverse from customer to customer, no comprehensive security policies are provided in this chapter. Rather, a basic ACL example is shown for reference.

Note As was previously mentioned, only relevant portions of the IPv6 side of the configurations are shown. The Cisco ASA configurations shown in this section are not complete as they relate to including all the necessary configurations to fully deploy a product-quality firewall in the branch. You should not assume that the configurations are best practices for the Cisco ASA or for security in general.

The configuration example begins with defining an alias that associates an IPv6 prefix with a user-defined name; prefix 2001:DB8:CAFE:1003::/64 is known as “BR1-LAN.” Another alias is created for associating a full IPv6 address with a user-defined name (in this case, a server located at the branch that is IPv6-enabled).

The “outside” and “inside” interfaces are defined with the security level, IPv4 addresses, and IPv6 addresses. The **standby** keyword defines the peer address of the redundant ASA Firewall.

An example object group is configured (this is not required) for RDP using TCP port 3389. This object group is used by the ACL, permitting any source from 2001:DB8:CAFE::/48 to the previously defined branch server (Br1-v6-Server) over RDP. The configured ACLs are applied inbound on the “outside” interface.

At the time of this writing, the Cisco ASA supports dynamic routing only for IPv4 IGP. For IPv6, static routing must be used. The example shown has a route configured for the inside branch LAN networks as well as the network between the Cisco ASA and the EtherSwitch Module located in the BR1-LAN router. This route uses one of the aliases defined previously. A static default route is configured for the outside interface, and the next hop is defined as the HSRP virtual link-local address of both the branch WAN access routers.

Interface GigabitEthernet0/3 will be used as the failover interface, and this ASA (ASA-1) is configured to be the primary unit. On the failover interface, the administrator must choose between defining an IPv4 or IPv6 address; both are not supported. In this case, an IPv6 address was used for the failover interface IP address.

Finally, Secure Shell (SSH) is permitted on the “inside” interface from the prefix shown.

Note Configurations for the Cisco ASA are shown through the command-line interface (CLI). Alternatively, the configurations can be deployed through the Cisco Adaptive Security Device Manager (ASDM) GUI.

Example 8-6 ASA-1 Configuration

```
name 2001:db8:cafe:1003:: BR1-LAN description VLAN on EtherSwitch
name 2001:db8:cafe:1004:9db8:3df1:814c:d3bc Br1-v6-Server
!
interface GigabitEthernet0/0
  description TO WAN
  nameif outside
  security-level 0
  ip address 10.124.1.4 255.255.255.0 standby 10.124.1.5
  ipv6 address 2001:db8:cafe:1000::4/64 standby 2001:db8:cafe:1000::5
!
interface GigabitEthernet0/1
  description TO BRANCH LAN
  nameif inside
  security-level 100
  ip address 10.124.3.1 255.255.255.0 standby 10.124.3.2
  ipv6 address 2001:db8:cafe:1002::1/64 standby 2001:db8:cafe:1002::2
!
interface GigabitEthernet0/3
  description LAN Failover Interface
```

```

!
object-group service RDP tcp
  description Microsoft RDP
  port-object eq 3389
!
ipv6 route inside BR1-LAN/64 2001:db8:cafe:1002::3
ipv6 route inside 2001:db8:cafe:1004::/64 2001:db8:cafe:1002::3
ipv6 route inside 2001:db8:cafe:1005::/64 2001:db8:cafe:1002::3
ipv6 route inside 2001:db8:cafe:1006::/64 2001:db8:cafe:1002::3

#Default route to HSRP address on WAN access routers
ipv6 route outside ::/0 fe80::5:73ff:fea0:2
ipv6 access-list v6-ALLOW permit icmp6 any any
ipv6 access-list v6-ALLOW permit tcp 2001:db8:cafe::/48 host Br1-v6-Server object-
group RDP
failover
failover lan unit primary
failover lan interface FO-LINK GigabitEthernet0/3
failover interface ip FO-LINK 2001:db8:cafe:1001::1/64 standby
2001:db8:cafe:1001::2
access-group v6-ALLOW in interface outside
ssh 2001:db8:cafe::/48 inside

```

Example 8-7 output shows the summary of the failover interface (G0/3) configuration.

Example 8-7 ASA-1 show failover interface Command Output

```

asa-1# show failover interface
      interface FO-LINK GigabitEthernet0/3
                System IP Address: 2001:db8:cafe:1001::1/64
                My IP Address      : 2001:db8:cafe:1001::1
                Other IP Address   : 2001:db8:cafe:1001::2

```

A general view of the failover state and configuration is shown in Example 8-8. The output shows that this ASA is the primary unit and is active. Interface information for both the “outside” and “inside” interfaces is shown. The information shows the IPv4 and IPv6 address information that is used on both interfaces for failover tracking.

Example 8-8 ASA-1 show failover Command Output

```

asa-1# show failover
Failover On
Failover unit Primary
Failover LAN Interface: FO-LINK GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds

```

continues

Example 8-8 ASA-1 show failover Command Output *continued*

```

Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 160 maximum
Version: Ours 8.2(2), Mate 8.2(2)
Last Failover at: 05:15:12 UTC Apr 12 2010
  This host: Primary - Active
    Active time: 48 (sec)
    slot 0: ASA5520 hw/sw rev (2.0/8.2(2)) status (Up Sys)
      Interface outside (10.124.1.4/fe80::21e:7aff:fe81:8e2c): Normal
      Interface inside (10.124.3.1/fe80::21e:7aff:fe81:8e2d): Normal
    slot 1: ASA-SSM-4GE hw/sw rev (1.0/1.0(0)10) status (Up)
  Other host: Secondary - Standby Ready
    Active time: 261 (sec)
    slot 0: ASA5520 hw/sw rev (2.0/8.2(2)) status (Up Sys)
      Interface outside (10.124.1.5/fe80::21d:a2ff:fe59:5fe4): Normal
      Interface inside (10.124.3.2/fe80::21d:a2ff:fe59:5fe5): Normal
    slot 1: ASA-SSM-4GE hw/sw rev (1.0/1.0(0)10)
status (Up)

```

The output in Example 8-9 shows the connection state of the firewall. There is a TCP connection between a host on the outside and a host on the inside over TCP port 23 (Telnet).

Example 8-9 Connection State of the Firewall

```

asa-1# show conn
6 in use, 13 most used
TCP outside 2001:db8:cafe:1000::2:23 inside
2001:db8:cafe:1004:c53c:2d6a:ccef:f2c5:1044, idle 0:02:49, bytes 115, flags UIO

```

EtherSwitch Module Configuration

The EtherSwitch Module is an optional component and can be replaced with a traditional Catalyst switch. It is shown in this chapter to give you a view of the configuration that is almost identical to that of a Catalyst 3560/3750 switch. The EtherSwitch Module used in this example is an NME-16ES-1G.

In the HBE, the EtherSwitch Module connects the branch LAN access router and the two ASA firewalls. Before enabling IPv6 features and functionality on the EtherSwitch Module, the Switch Database Management (SDM) template needs to be configured to support both IPv4 and IPv6. The three SDM templates that support IPv4 and IPv6 are

- Dual IPv4 and IPv6 default template
- Dual IPv4 and IPv6 routing template
- Dual IPv4 and IPv6 VLAN template

The dual IPv4 and IPv6 SDM template configuration is defined from the global configuration mode as follows:

```
BR1-EtherSwitch(config)#sdm prefer dual-ipv4-and-ipv6 {default | routing | vlan}
```

The device needs to be rebooted for the changes to take effect. After the EtherSwitch Module has rebooted, the **show sdm prefer** command (shown in Example 8-10) can verify that the correct SDM template is in use.

Example 8-10 *EtherSwitch Module show sdm prefer Command Output*

```
BR1-EtherSwitch# show sdm prefer
The current template is "desktop IPv4 and IPv6 default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:           2K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:             3K
number of directly-connected IPv4 hosts:   2K
number of indirect IPv4 routes:            1K
number of IPv6 multicast groups:          1.125k
number of directly-connected IPv6 addresses: 2K
number of indirect IPv6 unicast routes:    1K
number of IPv4 policy based routing aces:  0
number of IPv4/MAC qos aces:              0.5K
number of IPv4/MAC security aces:         1K
number of IPv6 policy based routing aces:  0
number of IPv6 qos aces:                  0.625k
number of IPv6 security aces:             0.5K
```

More information on the SDM template configuration can be found at http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_25_see/configuration/guide/swsdm.html#wp1077854.

The IPv6 portion of the EtherSwitch Module configuration is straightforward. In the HBE, there are only three interfaces that are in use on the module. There is the EtherSwitch-to-router internal interface (GigabitEthernet 1/0/2) and two Ethernet interfaces connecting the two Cisco ASA firewalls.

At the time of this writing, the Cisco ASA does not yet support dynamic routing for IPv6, so a default static route is configured on the module that points to the failover IPv6 address of the Cisco ASA. Optionally, EIGRP for IPv6 is enabled so that the default route can be advertised to the internal “BR1-LAN” router and so that all internal routes on that device can be advertised to the EtherSwitch Module. Static routes on “BR1-LAN” and the

EtherSwitch Module work as well. The configuration for the EtherSwitch Module is shown in Example 8-11.

Example 8-11 *EtherSwitch Module Configuration*

```

ipv6 unicast-routing
!
interface FastEthernet1/0/1
  description TO ASA-1
  switchport access vlan 101
!
interface FastEthernet1/0/2
  description TO ASA-2
  switchport access vlan 101
!
interface GigabitEthernet1/0/2      #Interface connecting to
                                     #branch LAN access
                                     #router (EtherSwitch internal
                                     #interface)

  description to BR1-LAN
  no switchport
  ip address 10.124.4.2 255.255.255.0
  ipv6 address 2001:DB8:CAFE:1003::2/64
  ipv6 eigrp 10                      #Optional - dynamic routing
                                     #for IPv6 inside the branch
!
interface Vlan101
  ip address 10.124.3.3 255.255.255.0
  ipv6 address 2001:DB8:CAFE:1002::3/64  #VLAN for network
                                             #connecting ASA

  ipv6 eigrp 10
!
ipv6 route ::/0 2001:DB8:CAFE:1002::1    #Default route pointing
                                             #to ASA
ipv6 router eigrp 10                     #Enable EIGRP for IPv6
  redistribute static                    #Redistribute default route
                                             #to LAN router
passive-interface Vlan101                #Do not attempt adjacency on
                                             #VLAN101

```

Branch LAN Router Configuration

The BR1-LAN branch LAN access router (configuration shown in Example 8-12) acts as a Layer 3 distribution device for the branch. BR1-LAN terminates the VLAN trunks from the Layer 2 access switch (BR1-LAN-SW) that the individual hosts connect to. In addition to basic L3 termination and routing, the BR1-LAN router provides basic addressing serv-

ices to IPv6-attached hosts through stateless DHCPv6 (RFC 3736) and provides stateful DHCPv6 relay functionality (RFC 3315). With stateless DHCPv6, the router provides IPv6 addressing services through SLAAC (RFC 4862), but other information, such as DNS name and DNS server, is provided through a stateless DHCPv6 pool (G0/0.104 example). With stateful DHCPv6 relay, the router forwards on the DHCP requests to a defined DHCPv6 server (G0/0.105 example).

Example 8-12 BR1-LAN Configuration Example

```

ipv6 unicast-routing
ipv6 cef
!
ipv6 dhcp pool DATA_W7                                #DHCPv6 pool name
  dns-server 2001:DB8:CAFE:102::8                      #Primary IPv6 DNS server
  domain-name cisco.com                                #DNS domain name passed
                                                       #to client
!
interface GigabitEthernet0/0
  description to BR1-LAN-SW
  no ip address
  duplex auto
  speed auto
!
interface GigabitEthernet0/0.104
  description VLAN-PC
  encapsulation dot1Q 104
  ip address 10.124.104.1 255.255.255.0
  ipv6 address 2001:DB8:CAFE:1004::1/64                #Client uses SLAAC
                                                       #with this prefix
  ipv6 nd other-config-flag                            #Set flag in RA to instruct
                                                       #host how to obtain "other"
                                                       #information such as domain
  ipv6 dhcp server DATA_W7                            #Use DHCP pool above for
                                                       #options
  ipv6 eigrp 10
!
interface GigabitEthernet0/0.105
  description VLAN-PHONE
  encapsulation dot1Q 105
  ip address 10.124.105.1 255.255.255.0
  ipv6 address 2001:DB8:CAFE:1005::1/64
  ipv6 nd prefix 2001:DB8:CAFE:1005::/64 0 0 no-autoconfig #Do
                                                       #not use prefix for
                                                       #autoconfiguration
  ipv6 nd managed-config-flag                          #Set flag in RA to instruct

```

continues

Example 8-12 *BR1-LAN Configuration Example continued*

```

                                #host to use DHCPv6
ipv6 dhcp relay destination 2001:DB8:CAFE:102::9    #Relay for
                                                    #DHCPv6 server

ipv6 eigrp 10
interface GigabitEthernet0/0.106
description VLAN-PRINTER
encapsulation dot1Q 106
ip address 10.124.106.1 255.255.255.0
ipv6 address 2001:DB8:CAFE:1006::1/64
ipv6 eigrp 10
!
interface GigabitEthernet1/0
description TO ETHERSWITCH MODULE
ip address 10.124.4.1 255.255.255.0
ipv6 address 2001:DB8:CAFE:1003::1/64
ipv6 eigrp 10
!
ipv6 router eigrp 10
no shutdown

```

The BR1-LAN-SW Catalyst switch is configured with an interface connected to the BR1-LAN router and is configured for IEEE 802.1Q trunking. VLANs 104–106 are carried over the trunk link. No relevant IPv6 configurations are made on the BR1-LAN-SW except that a management interface is defined that is reachable over both IPv4 and IPv6. The configuration for the BR1-LAN-SW device is not shown.

WAN/Branch Deployment over Native IPv6

At the time of this writing, it is rare for an enterprise to have full end-to-end reachability over native IPv6 from a branch site to a WAN head-end. As more and more service providers deploy IPv6 services to their customers, the enterprise can use IPv6 as the means of transporting encrypted IPv6 traffic between sites and leave behind the IPv6-in-IPv4 encrypted tunnel deployments that have been discussed in this chapter thus far.

Cisco supports the deployment of IPsec over IPv6 in Cisco IOS. The following section provides a basic configuration example of how to deploy IPsec over IPv6 on Cisco IOS between two routers.

Figure 8-6 shows a network topology of two routers connected to the Internet through IPv6. In this case, the routers are not running dual-stack (IPv4 and IPv6) but they could be; instead they are IPv6-only routers with IPv6-only devices attached.

The configuration is straightforward and closely resembles that of a point-to-point IPsec configuration over IPv4. The differences are mostly with the addressing for the interfaces.

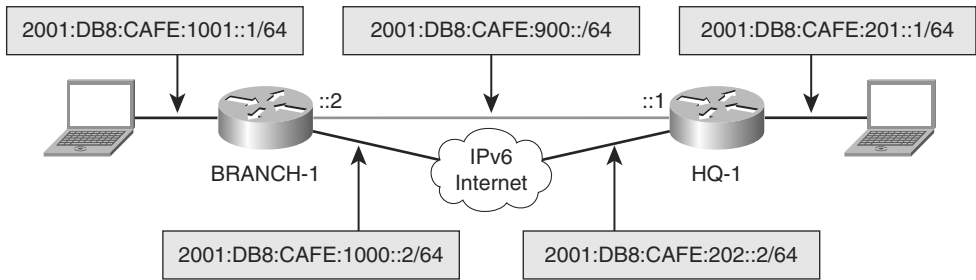


Figure 8-6 IPsec VPN over IPv6 Internet

Example 8-13 shows the basic configuration on the HQ-1 router. The Internet security association and key management protocol (ISAKMP) and IPsec policy information is the same as what was used in the HBE discussed earlier. The difference comes in the tunnel configuration. The tunnel source and destination are now IPv6 addresses instead of IPv4, as shown previously. Also, the tunnel mode is now using IPsec over IPv6 transport. Finally, the serial interface has an IPv6 address that is used for the connection to the IPv6-enabled ISP. Unicast Reverse Path Forwarding (uRPF) is enabled to help with spoofing. In a production deployment, there would be a set of ACLs used to enable only certain protocols and source/destinations (between branch and HQ) ingress on the serial interface.

Example 8-13 HQ-1 Configuration

```

ipv6 unicast-routing
ipv6 cef
!
crypto isakmp policy 1
  encr aes 256
  authentication pre-share
  group 2
crypto isakmp key CISCO address ipv6 ::/0
!
crypto ipsec transform-set HUB esp-aes 256 esp-sha-hmac
!
crypto ipsec profile HUB
  set transform-set HUB
!
interface Tunnel12
  no ip address
  ipv6 address 2001:DB8:CAFE:900::1/64
  ipv6 eigrp 10
  tunnel source 2001:DB8:CAFE:202::2      #Source is now using IPv6
  tunnel mode ipsec ipv6                  #IPSec over IPv6 tunnel mode

```

continues

Example 8-13 *HQ-1 Configuration continued*

```

tunnel destination 2001:DB8:CAFE:1000::2 #Dest. now using IPv6
tunnel protection ipsec profile HUB
!
interface GigabitEthernet1/0
description LAN
no ip address
ipv6 address 2001:DB8:CAFE:201::1/64
ipv6 eigrp 10
!
interface Serial2/0
description to ISP
no ip address
ipv6 address 2001:DB8:CAFE:202::2/64 #v6 connection to ISP
ipv6 verify unicast reverse-path #uRPF for IPv6
!
ipv6 route ::/0 2001:DB8:CAFE:202::1 #Default to ISP
ipv6 router eigrp 10
eigrp router-id 1.1.1.2

```

Example 8-14 shows the configuration for BRANCH-1. It is similar to the configuration for HQ-1, with the exception of addressing and the IPsec profile name.

Example 8-14 *BRANCH-1 Configuration*

```

ipv6 unicast-routing
ipv6 cef
!
crypto isakmp policy 1
encr aes 256
authentication pre-share
group 2
crypto isakmp key CISCO address ipv6 ::/0
!
crypto ipsec transform-set SPOKE esp-aes 256 esp-sha-hmac
!
crypto ipsec profile SPOKE
set transform-set SPOKE
!
interface Tunnel2
no ip address
ipv6 address 2001:DB8:CAFE:900::2/64
ipv6 eigrp 10
tunnel source 2001:DB8:CAFE:1000::2
tunnel mode ipsec ipv6

```

```

tunnel destination 2001:DB8:CAFE:202::2
tunnel protection ipsec profile SPOKE
!
interface GigabitEthernet1/0
description LAN
no ip address
ipv6 address 2001:DB8:CAFE:1001::1/64
ipv6 eigrp 10
!
interface Serial2/0
description to ISP
no ip address
ipv6 address 2001:DB8:CAFE:1000::2/64
ipv6 verify unicast reverse-path
!
ipv6 route ::/0 2001:DB8:CAFE:1000::1
ipv6 router eigrp 10
eigrp router-id 1.1.1.3

```

Example 8-15 shows the status of the ISAKMP peers and security association (SA) state.

Example 8-15 ISAKMP Peer and SA Output on HQ-1

```

HQ-1# show crypto isakmp peers
Peer: 2001:DB8:CAFE:1000::2 Port: 500 Local: 2001:DB8:CAFE:202::2
Phase1 id: 2001:DB8:CAFE:1000::2

HQ-1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status

IPv6 Crypto ISAKMP SA

dst: 2001:DB8:CAFE:1000::2
src: 2001:DB8:CAFE:202::2
state: QM_IDLE          conn-id: 1002 status: ACTIVE

dst: 2001:DB8:CAFE:202::2
src: 2001:DB8:CAFE:1000::2
state: QM_IDLE          conn-id: 1003 status: ACTIVE

```


Summary

This chapter describes how to deploy IPv6 in the branch network. The branch profiles described were the single-tier, dual-tier, and multitier. The configuration example was based on a hybrid branch example that included elements of each of the three tiers. In addition to IPv6-over-IPv4 VPN solutions, a native IPv6 IPsec example was given for those customers who have service provider support for end-to-end IPv6 transport. The profiles described are certainly not the only ways to deploy IPv6 in this environment, but they provide options that can be leveraged based on the branch environment.

Additional References

Many notes and disclaimers in this document discuss the need to fully understand the technology and protocol aspects of IPv6. There are many design considerations associated with the implementation of IPv6 that include security, QoS, availability, management, IT training, and application support.

The following references are a few of the many that provide more details on IPv6, Cisco design recommendations, products and solutions, and industry activity:

Popoviciu, Ciprian P, Eric Levy-Abegnoli, and Patrick Grossetete. *Deploying IPv6 Networks*. Cisco Press. (ISBN10: 1-58705-210-5; ISBN13: 978-1-58705-210-1).

Hogg, Scott and Eric Vyncke. *IPv6 Security*. Cisco Press. (ISBN10: 1-58705-594-5; ISBN13: 978-1-58705-594-2).

Szigeti, Tim and Christina Hattingh. *End-to-END QoS Network Design*. Cisco Press. (ISBN10: 1-58705-176-1; ISBN13: 978-1-58705-176-0).

Cisco. Cisco IOS IPv6 Configuration Guide:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/15_0/ipv6_15_0_book.html.

Cisco. Design Zone for Branch:

http://www.cisco.com/en/US/netsol/ns816/networking_solutions_program_home.html.

Cisco. Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/ipv6/ipv6srnd.html.

Cisco. IPsec Design Guides:

http://www.cisco.com/en/US/tech/tk583/tk372/tech_design_guides_list.html.

Cisco. Cisco IOS Control Plane Policing:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlmt.html.

Cisco. Enterprise QoS Solution Reference Network Design Guide:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html.

Cisco. Cisco IOS IPv6 Multicast Technologies:

http://www.cisco.com/en/US/technologies/tk648/tk828/tk363/technologies_white_paper_0900aecd8014d6dd.html.

Cisco. Cisco IOS IPv6 Multicast Configuration:

http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a0080203f7a.shtml.

Cisco. Cisco Implementing IPv6 Multicast:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast_ps10591_TSD_Products_Configuration_Guide_Chapter.html.

Cisco. Defining and Using IPv6 General Prefixes:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con_ps10591_TSD_Products_Configuration_Guide_Chapter.html#wp1132473.

Cisco. Network Management and Automation:

<http://www.cisco.com/en/US/products/sw/netmgtsw/index.html>.

Cisco. Dynamic Multipoint VPN (DMVPN) Design Guide:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/DMVPDG.html.

Cisco. Cisco IOS Release 15.0 - Implementing Dynamic Multipoint VPN for IPv6:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dmvpn_ps10591_TSD_Products_Configuration_Guide_Chapter.html.

Cisco. Shortcut Switching Enhancements for NHRP in DMVPN Networks:

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_nhrp_dmvpn.html#wp1072593.

Cisco. Configuring NHRP:

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_cfg_nhrp.html#wp1078234.

Cisco. Catalyst 3560 Switch Configuration Guide: Configuring SDM Templates:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_25_see/configuration/guide/swsdm.html#wp1077854.

Cisco. Branch Routers (including ISR):

http://www.cisco.com/en/US/products/ps10906/Products_Sub_Category_Home.html.

Savola, P. RFC 3627, "Use of /127 Prefix Length Between Routers Considered Harmful."

<http://www.ietf.org/rfc/rfc3627.txt>.

Hinden, R. and S. Deering. RFC 3513, "Internet Protocol Version 6 (IPv6) Addressing Architecture."

<http://www.ietf.org/rfc/rfc3513.txt>.

Savola, P. and B. Haberman. RFC 3956, "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address."

<http://www.ietf.org/rfc/rfc3956.txt>.

Deering, S. and R. Hinden. RFC 2460, "Internet Protocol, Version 6 (IPv6) Specification."

<http://www.ietf.org/rfc/rfc2460.txt>.

Thomson, S., T. Narten, and T. Jinmei. RFC 4862, “IPv6 Stateless Address Autoconfiguration.” <http://www.ietf.org/rfc/rfc4862.txt>.

Droms, R. RFC 3736, “Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6.” <http://www.ietf.org/rfc/rfc3736.txt>.

McCann, J., S. Deering, and J. Mogul. RFC 1981, “Path MTU Discovery for IP version 6.” <http://www.ietf.org/rfc/rfc1981.txt>.

Arkko, J. (Ed.), J. Kempf, and P. Nikander. RFC 3971, “SEcure Neighbor Discovery (SEND).” <http://www.ietf.org/rfc/rfc3971.txt>.

Templin, F., T. Gleeson, M. Talwar, and D. Thaler. RFC 4214, “Intra-Site Automatic Tunnel Addressing Protocol (ISATAP).” <http://www.ietf.org/rfc/rfc4214.txt>.

Van de Velde, G., T. Chown, O. Bonness, and C. Hahn. RFC 5375, “IPv6 Unicast Address Assignment Considerations.” <http://www.ietf.org/rfc/rfc5375.txt>.

Index

Numerics

- 6PE (IPv6 Provider Edge), 60
 - configuring, 193-202
- 6to4 tunnels, 55-57
- 6VPE (IPv6 VPN Provider Edge), 61
 - configuring, 202-211

A

access layer

- campus network design, 29-30
- data center module, 32-33
- dual-stack data center IPv6 deployment, 264-269
- ingress traffic, controlling, 130
- access lists, configuring, 219-220
- accounting management, 306
- address exhaustion (IPv4), workarounds, 2-3
- addressing, 119-120
 - allocation, 104

- campus network deployment, 132-134
- IPv6 deployment planning, 97-98
- sample lab, 347-348
- WAN/branch IPv6 deployment, 230
- admin context (Cisco ASA), 215
- adoption of IPv6
 - Google, “trusted adopter” program, 14
 - market drivers, 1-2
 - vertical market deployment, 12-14
- aggregation layer
 - data center module, 31-32
 - dual-stack data center IPv6 deployment, 269-279
- allocating IPv6 addresses, 104
- applications, network management, 307-308
- assessment, pilot/trial, 96-97
- automatic address allocation (IPv6), 7

B

- benefit analysis, IPv6 deployment, 92-93
- benefits of IPv6, 6-8
- BGP (Border Gateway Protocol), 87-89
 - MP-BGP, 88-89
 - path attributes, 87
- blocking Teredo, 131
- branch network
 - branch edge routers, 41
 - edge module, 39-40
- building a sample lab, 343-344
- business case, IPv6 deployment, 94-95

C

- campus deployment models
 - DSM, 108-110
 - topology*, 109
 - hybrid model, 109-115
 - connectivity flow*, 111-112
 - topology*, 115
 - SBM, 115-119
- campus module
 - access layer, 29-30
 - distribution layer, 25-29
 - Layer 2 access design*, 25-26
 - routed access design*, 27-28
 - VSS distribution block*, 28
 - enterprise networks, 19
- campus network deployment
 - addressing, 119-120, 132-134
 - DSM, 137-161
 - first-hop redundancy*,
configuring, 145-146
 - multicast, configuring*, 149-151
 - network topology*, 138-139
 - physical/VLAN configuration*,
140-143
 - QoS, configuring*, 147-148
 - routed access, configuring*,
151-155
 - routing configuration*, 143-145
 - high availability, 122
 - hybrid model, 161-174
 - network topology*, 161-162
 - physical configuration*, 162-163
 - QoS configuration*, 171-173
 - tunnel configuration*, 163-171
 - multicast, 131-132
 - network management, 132
 - physical connectivity, 120-121
 - QoS, 123-125
 - routing, 121-122
 - SBM, 174-181
 - network topology*, 174-176
 - physical configuration*, 176-178
 - QoS configuration*, 180-181
 - scalability and performance, 135-137
 - security, 125-131
 - first-hop security*, 130
 - switch access, restricting*,
126-127
 - traffic policing*, 128-129
 - VLANs, 121
- Cisco AnyConnect, remote access VPN IPv6 deployment, 292-297
- Cisco ASA
 - AnyConnect, configuring, 292-297
 - virtual contexts, 214-219
 - virtualization architecture, 213-214
- Cisco VPN client, remote access VPN IPv6 deployment, 297-300

- client-side deployment, 102
- coexistence of IPv4 and IPv6, 9, 45-47
 - dual stack, 48-49
 - IPv6 over MPLS, 58-62
 - IPv6-over-IPv4 tunnels, 49-58
 - 6to4 tunnels*, 55-57
 - GRE tunnels*, 53-54
 - ISATAP*, 57-58
 - manually configured tunnels*, 51-53
 - tunnel broker*, 54-55
 - native IPv6, 47-48
 - QoS, 79-80
 - translation mechanisms
 - NAT64*, 64
 - NAT-PT*, 63-64
- collapsed core topology, 35
- comparing IPv6 and IPv4, 6-8
 - QoS, 76-78
 - security, 10
- configuration management, 305
- configuring
 - 6PE, 193-202
 - 6VPE, 202-211
 - access lists, 219-220
 - Cisco ASA
 - AnyConnect*, 292-297
 - multiple contexts*, 215-219
 - first-hop redundancy, 145-146
 - IS-IS, 86-87
 - multicast on DSM, 149-151
 - QoS on DSM, 147-148
 - routing on DSM, 143-145
 - sample lab network devices, 348
 - SPAN, 338-339

- tunnels on HM, 163-171
- VRF, 189-193
- VSS on DSM, 157-161
- WAN/branch IPv6 deployment
 - HBE*, 240-254
- connecting data centers, DCI (Data Center Interconnect), 286-289
- connectivity flow, hybrid campus deployment model, 111-112
- contexts (Cisco ASA), 214-219
- CoPP (Control Plane Policing), 129
- core deployment migration scenario, 101
- core edge topology, 35-36
- core layer, dual-stack data center IPv6 deployment, 279
- core module
 - enterprise networks, 24-25
- core module, enterprise networks, 19
- corporate headquarters, edge module, 38-40
- cost analysis, IPv6 deployment, 93-94

D

- data center IPv6 deployment, 261-262
 - DCI, designing, 286-289
 - dual-stack data center, 262-279
 - access layer*, 264-269
 - aggregation layer*, 269-279
 - core layer*, 279
 - SAN IPv6 deployment
 - FCIP*, 281-284
 - iSCSI*, 284-287
 - virtualized data centers, 279-281
- data center module, 31-33
 - access layer, 32-33
 - aggregation layer, 31-32

- enterprise networks, 19
- SANs, 33
- DCI (Data Center Interconnect), designing, 286-289**
- depletion of IPv4 addresses, 4**
- deploying IPv6, 9**
 - addressing, 119-120
 - benefit analysis, 92-93
 - business case, 94-95
 - campus deployment models, 107-119
 - cost analysis, 93-94
 - dual-tier WAN/branch deployment, 227-228
 - high availability, 122
 - multitier WAN/branch deployment, 228-229
 - physical connectivity, 120-121
 - pilot/trial, 96-103
 - QoS, 123-125
 - routing, 121-122
 - security, 125-131
 - single-tier WAN/branch deployment, 226-227
 - training, 96
 - transition team, 95-96
 - vertical market deployment, 12-14
 - VLANs, 121
- desktop virtualization, 220-223**
- distribution layer, campus network design, 25-29**
 - Layer 2 access, 25-26
 - routed access design, 27-28
 - VSS distribution block, 28
- DSM (Dual-Stack Model), 108-110**
 - campus network deployment, 137-161
 - network topology, 138-139*
 - physical/VLAN configuration, 140-143*

- first-hop redundancy, configuring, 145-146
- multicast, configuring, 149-151
- QoS, configuring, 147-148
- routed access, configuring, 151-155
- routing configuration, 143-145
- topology, 109
- VSS, configuring, 157-161
- dual stack, 48-49**
- dual-stack configuration migration scenario, 103**
- dual-stack data center IPv6 deployment, 262-279**
 - access layer, 264-269
 - aggregation layer, 269-279
 - core layer, 279
- dual-tier branch networks, 41**
- dual-tier WAN/branch IPv6 deployment, 227-228**

E

- edge module, 37-42**
 - branch network, 39-40
 - branch edge routers, 41*
 - corporate headquarters, 38-40
 - enterprise networks, 20
- edge routers, 40**
- EEM (Embedded Event Manager), 328-330**
- EIGRPv6, 83-85**
- encapsulation, IPv6-over-IPv4 tunnels, 50**
- enterprise networks**
 - core network design, 24-25
 - modules, 19-21
- EoR (End of Row) deployment model, 32**

ERSPAN (Encapsulated Remote SPAN), 337

examples of WAN/branch IPv6 deployment, implementation example, 238-254

extension headers, IPv6, 78

F

FAQs about IPv6, 6-11

fault management, 305

FCAPS (Fault, Configuration, Accounting, Performance, and Security Management), 304-307

FCIP (Fibre Channel over IP), 36, 281-284

FCoE (Fibre Channel over Ethernet), 36

first-hop redundancy, configuring, 145-146

first-hop security, campus network deployment, 130

Flexible NetFlow, 312-320

flow labels, 8

G

globalization as market driver for IPv6 adoption, 4

Google, “trusted adopter” program, 14

government IT strategy as market driver for IPv6 adoption, 5

GRE tunnels, IPv6-over-IPv4 tunneling, 53-54

H

hierarchical network design, 17-18

campus module, 25-30

core module, 24-25

data center module, 31-33

access layer, 32-33

aggregation layer, 31-32

edge module, 37-42

network services module, 29-30

hierarchy as network design principle, 21-24

high availability

campus network deployment, 122

WAN/branch IPv6 deployment, 232

HM (hybrid model), 161-174

network topology, 161-162

physical configuration, 162-163

QoS configuration, 171-173

tunnel configuration, 163-171

host-to-host tunneling, 50

host-to-router tunneling, 50

HTTP, 336

hybrid campus deployment model, 109-115

connectivity flow, 111-112

I

IANA (Internet Assigned Numbers Authority), 1

reserved IPv6 addresses,

ICANN (Internet Corporation for Assigned Numbers and Names), 1

ICMPv6, 332-333

ietf (Internet Engineering Task Force), 2

- standards, 11

- inefficient address use as market driver for IPv6 adoption, 4

- infrastructure evolution as market driver for IPv6 adoption, 5

- ingress traffic from access layer, controlling, 130

- inner switches, 40

- IP SLA for IPv6, 322-330

- IPFIX (Internet Protocol Flow Information eXport), 320-322

- IPv4 address exhaustion, workarounds, 2-3

IPv6

- automatic address allocation, 7

- coexistence of IPv4 and IPv6, 45-47

- dual stack, 48-49*

- IPv6 over MPLS, 58-62*

- IPv6-over-IPv4 tunnels, 49-58*

- native IPv6, 47-48*

- deploying, 9

- pilot/trial, 96-103*

- within vertical markets, 12-14*

- extension headers, 78

- FAQs, 6-11

- market drivers

- government IT strategy, 5*

- infrastructure evolution, 5*

- IPv4 address considerations, 4-5*

- operating system support, 6*

- multihoming, 10

- QoS, 10

- comparing with IPv4, 76-78*

- routing, OSPFv3, 80-83

IPv6 Forum, 11**IPv6 over MPLS, 58-62****IPv6 Ready Logo Committee, 11****IPv6-over-IPv4 tunnels**

- 6to4 tunnels, 55-57

- GRE tunnels, 53-54

- ISATAP, 57-58

- manually configured tunnels, 51-53

- tunnel broker, 54-55

- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 57-58

- IS-IS, 85-87

- configuring, 86-87

J-K-L

- Layer 2 access design, 25-26

- local SPAN, 337

- localized IPv6 server-side deployment, 102

- LSAs (link-state advertisements), 80, 82

M

- M&A (mergers and acquisitions) as market driver for IPv6 adoption, 4

- manually configured tunnels, 51-53

- market drivers for adoption of IPv6, 1-2

- government IT strategy, 5

- infrastructure evolution, 5

- IPv4 address considerations, 4-5

- operating system support, 6

- messages, MLD, 71

- MIBs (Management Information Bases), 308-312

- migrating to a pilot, 359

- migration scenarios, 100-103

- client-side deployment, 102

- core deployment, 101

- dual-stack configuration, 103

- localized IPv6 server-side deployment, 102

Mini Protocol Analyzer, 339-340
 MIP (Mobile IP), 8
 MLD (Multicast Listener Discovery) for IPv6, 71-72
 mobile devices, as market driver for IPv6 adoption, 4
 mobility, MIP, 8
 modularity as network design principle, 19-21
 monitoring and reporting
 ICMPv6, 332-333
 SNMP, 331-332
 syslog, 332
 MP-BGP (Multiprotocol BGP for IPv6), 88-89
 multicast, 67-76
 campus network deployment, 131-132
 IPv6 multicast addressing, 69-71
 MLD for IPv6, 71
 PIM, 72-76
 PIM-Bidir, 76
 PIM-SM, 73-74
 PIM-SSM, 74-75
 WAN/branch IPv6 deployment, 236
 multihoming IPv6, 10
 multiple contexts, configuring on Cisco ASA, 215-219
 multitier branch networks, 41
 multitier WAN/branch IPv6 deployment, 228-229
 multitopology mode (IS-IS), 86

N

NAT (Network Address Translation), 2
 NAT64, 64
 native IPv6, 47-48
 WAN/branch over native IP6 deployment, 254-257
 NAT-PT (Network Address Translation - Protocol Translation), 62-64
 NetFlow, 312-320
 network design
 data center storage network design, 33
 enterprise networks
 campus module, 25-29
 core layer, 24-25
 hierarchical network design
 campus module, 25-30
 core module, 24-25
 data center module, 31-33
 edge module, 37-42
 network services module, 29-30
 principles, 18-24
 hierarchy, 21-24
 modularity, 19-21
 resiliency, 24
 network management, 303-305
 applications, 307-308
 campus network deployment, 132
 FCAPS, 304-307
 HTTP, 336
 ICMPv6, 332-333
 NTP, 333-334
 SNMP, 331-332
 SSH, 335-336
 syslog, 332
 Telnet, 334-335
 TFTP, 333
 tools
 Flexible NetFlow, 312-320
 IP SLA for IPv6, 322-330
 IPFIX, 320-322
 SNMP, 308-312
 WAN/branch IPv6 deployment, 236-238

network services

multicast, 67-76

IPv6 multicast addressing, 69-71

MLD for IPv6, 71-72

PIM, 72-76

QoS, 76-80

coexistence of IPv4 and IPv6,
79-80

comparing IPv6 and IPv4, 76-78

IPv6 extension headers, 78

routing

BGP, 87-89

EIGRPv6, 83-85

IS-IS, 85-87

OSPFv3, 80-83

network services module, 29-30

enterprise networks, 17

network virtualization, 188-220

Cisco ASA virtualization architecture,
213-214

IPv6 access lists, configuring,
219-220

segmentation, 188-212

6PE, 193-202

6VPE, 202-211

VPLS, 211-212

switch virtualization, 188

virtualized firewall, 213

NMS (network management system), 307**NTP (Network Time Protocol), 333-334****O****operating system deployment, sample lab, 348-358**

operating system support as market driver for IPv6 adoption, 6

Oracle Sun Ray, desktop virtualization example, 222-223

OSPFv3, 80-83

LSAs, 80, 82

P

path attributes (BGP), 87

performance

campus network deployment,
135-137

WAN/branch IPv6 deployment, 238

performance management, 306

phases of IPv6 deployment, 13-14

physical configuration

hybrid model, 162-163

on SBM, 176-178

physical connectivity

campus network deployment,
120-121

WAN/branch IPv6 deployment,
230-231

physical/VLAN configuration

DSM, 140-143

pilot/early deployment phase, 14

pilot/trial, 96-103

assessment, 96-97

design, 97-98

migrating to, 359

migration scenarios, 100-103

client-side deployment, 102

core deployment, 101

dual-stack configuration, 103

localized IPv6 server-side deployment, 102

- network services, 98
- scalability and reliability, 99
- security, 98
- transition mechanisms, 98
- PIM (Protocol Independent Multicast), 72-76**
 - PIM-Bidir, 76
 - PIM-SM, 73-74
- PIM-Bidir, 76**
- PIM-SM (PIM-Sparse Mode), 73-74**
- PIM-SSM (PIM-Source Specific Multicast), 74-75**
- planning IPv6 deployment**
 - address allocation, 104
 - benefit analysis, 92-93
 - business case, 94-95
 - cost analysis, 93-94
 - pilot/trial
 - assessment, 96-97*
 - design, 97-98*
 - migration scenarios, 100-103*
 - network services, 98*
 - scalability and reliability, 99*
 - security, 98*
 - transition mechanisms, 98*
 - training, 96
 - transition team, 95-96
- preliminary research phase, IPv6 deployment, 13**
- principles of network design**
 - hierarchy, 21-24
 - modularity, 19-21
 - resiliency, 24
- production phase of IPv6 deployment, 14**
- protocol translation**
 - NAT64, 64
 - NAT-PT, 63-64

Q

QoS, 76-80

- campus network deployment, 123-125
- configuring
 - on DSM, 147-148*
 - on HM, 171-173*
 - on SBM, 180-181*
- for IPv6, 10
- WAN/branch IPv6 deployment, 233

R

- redundancy, configuring first-hop redundancy, 145-146**

- remote access VPN IPv6 deployment, 291-292**

- Cisco AnyConnect, 292-297
- Cisco VPN client, 297-300

- reserved IPv6 addresses, 70-71**

- resiliency as network design principle, 24**

- resource flow, flow labels, 8**

- restricting switch access, 126-127**

- RIRs (Regional Internet Registries), 2, 104**

- routed access design, 27-28**

- configuring on DSM, 151-155

- router-to-router tunneling, 50**

routing

- campus network deployment, 121-122
- DSM, configuring, 143-145
- WAN/branch IPv6 deployment, 232

routing protocols

- BGP, 87-89
- EIGRPv6, 83-85

IS-IS, 85-87

configuring, 86-87

OSPFv3, 80-83

LSAs, 82

RSPAN (Remote SPAN), 337

S

sample lab, 343-344

addressing, 347-348

network devices, configuring, 348

operating system deployment,
348-358

topology, 344-346

VMware ESXi, configuring, 348-351

SANs (storage-area networks), 33

collapsed core topooogy, 35

core edge topology, 35-36

IPv6 deployment

FCIP, 281-284

iSCSI, 284-287

**SBM (service block model),
115-119, 174-181**

components, 119

network topology, 174-176

performance, 137

physical configuration, 176-178

QoS configuration, 180-181

topology, 117-118

tunnel configuration, 178-180

scalability

and performance, WAN/branch IPv6
deployment, 238

and reliability

*campus network deployment,
135-137*

pilot/trial, 99

security

access layer, 33

campus network deployment,
125-131

addressing, 126

IPv6 traffic policing, 128-129

comparing IPv6 and IPv4, 8, 10

pilot/trial, 98

virtualized firewall, 213

WAN/branch IPv6 deployment,
233-236

security management, 306-307

segmentation, 188-212

6PE, configuring, 193-202

6VPE, configuring, 202-211

VPLS, 211-212

VRF, configuring, 189-193

server virtualization, 223

single topology mode (IS-IS), 86

single-tier branch networks, 41

**single-tier WAN/branch IPv6
deployment, 226-227**

SLAs (service-level agreements), 99

IP SLA for IPv6, 322-330

**SNMP (Simple Network Management
Protocol), 331-332**

configuring, 127

MIBs, 308-312

**SPAN (Switch Port ANalyzer),
337-340**

configuring, 338-339

Mini Protocol Analyzer, 339-340

sparse mode (PIM), 73-74

SSH (Secure Shell), 335-336

standards, IETF, 11

**switch access, restricting in campus
networks, 126-127**

switches, virtualization, 188

syslog, 332
 system context (Cisco ASA), 214-215

T

Telnet, 334-335
 Teredo, blocking use of, 131
 TFTP, 333
 topology
 campus deployment models, 115
 DSM, 109
 campus network deployment,
 138-139
 hybrid model, 161-162
 sample lab, 344-346
 SBM, 117-118, 174-176
 WAN/branch IPv6 deployment
 implementation example,
 240-254
 ToR (Top of Rack) deployment, 32
 traffic policing, 128-129
 traffic-monitoring tools, 337-341
 SPAN, 337-340
 Mini Protocol Analyzer, 339-340
 VACL capture, 340-341
 training, IPv6 deployment, 96
 transition team, IPv6 deployment,
 95-96
 ”trusted adopter” program (Google), 14
 tunnel broker, 54-55
 tunneling
 IPv6-over-IPv4 tunnels, 49-58
 6to4 tunnels, 55-57
 GRE tunnels, 53-54
 ISATAP, 57-58
 manually configured tunnels,
 51-53
 tunnel broker, 54-55

U-V

Unified Fabric, 37
 user contexts (Cisco ASA), 215
 VACL (VLAN Access Control List)
 capture, 340-341
 vertical market deployment of IPv6,
 12-14
 virtualization, 186
 data centers, IPv6 deployment,
 279-281
 desktop virtualization, 220-223
 as market driver for IPv6 adoption, 4
 network virtualization, 188-220
 server virtualization, 223
 virtualized firewall, 213
 VLANs
 campus network deployment, 121
 network virtualization, segmentation,
 188-212
 WAN/branch IPv6 deployment,
 231-232
 VMware ESXi, configuring for sample
 lab, 348-351
 VPLS (Virtual Private LAN Services),
 211-212
 VPNs
 remote access VPN IPv6 deployment,
 291-292
 VPNs, remote access VPN IPv6
 deployment
 Cisco AnyConnect, 292-297
 Cisco VPN client, 297-300
 VRF (Virtual Routing and
 Forwarding), configuring, 189-193
 VSS (Virtual Switching System),
 155-161
 VSS distribution block, 28

W-X-Y-Z

WAN/branch IPv6 deployment

- addressing, 230
- dual-tier, 227-228
- HBE, configuring, 240-254
- high availability, 232
- implementation example, 238-254
- management, 236-238
- multicast, 236
- physical connectivity, 230-231
- QoS, 233
- routing, 232
- security, 233-236
- single-tier, 226-227
- VLANs, 231-232

WAN/branch over native IP6 deployment, 254-257

Windows 7 client, sample lab configuration, 353-358

workarounds for IPv4 address exhaustion, 2-3