



HUAWEI NetEngine80E/40E Router

V600R003C00

Configuration Guide - IP Routing

Issue 02

Date 2011-09-10

Copyright © Huawei Technologies Co., Ltd. 2011. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://www.huawei.com>

Email: support@huawei.com

About This Document

Purpose

This document is a guide to configuring IP routing for the NE80E/40E. It describes routing features and the basic principles of routing protocols, detailed configuration procedures for different scenarios, and provides examples.

 **NOTE**

- This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.
- In NE80E/40E series (except for the NE40E-X1/X2), line processing boards are called Line Processing Units (LPUs) and switching fabric boards are called Switching Fabric Units (SFUs). The NE40E-X1/X2 has no LPU and SFU, and packet switching and forwarding are centrally performed by the Network Processing Unit (NPU).

Related Versions

The following table lists the product versions related to this document.

Product Name	Version
HUAWEI NetEngine80E/40E Router	V600R003C00






Intended Audience

This document is intended for:

- Commissioning Engineer
- Data Configuration Engineer
- Network Monitoring Engineer
- System Maintenance Engineer

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Alerts you to a high risk hazard that could, if not avoided, result in serious injury or death.
 WARNING	Alerts you to a medium or low risk hazard that could, if not avoided, result in moderate or minor injury.
 CAUTION	Alerts you to a potentially hazardous situation that could, if not avoided, result in equipment damage, data loss, performance deterioration, or unanticipated results.
 TIP	Provides a tip that may help you solve a problem or save time.
 NOTE	Provides additional information to emphasize or supplement important points in the main text.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in boldface .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[]	Items (keywords or arguments) in brackets [] are optional.
{ x y ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x y ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x y ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x y ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Changes in Issue 02 (2011-09-10)

Second commercial release.

Changes in Issue 01 (2011-06-30)

Initial commercial release.

Contents

About This Document.....	ii
1 IP Routing Overview.....	1
1.1 Routing Management.....	2
1.1.1 Displaying of the Routing Table.....	2
1.1.2 Displaying of the Routing Management Module.....	2
1.1.3 FRR Principle.....	3
1.2 Configuring IPv4 Multi-Topology.....	4
1.2.1 Establishing the Configuration Task.....	4
1.2.2 Creating an IPv4 Topology Instance.....	5
1.2.3 Binding an Interface to an IPv4 Topology Instance.....	6
1.2.4 Checking the Configuration.....	6
1.3 Configuring IPv6 Multi-Topology.....	7
1.3.1 Establishing the Configuration Task.....	7
1.3.2 Creating an IPv6 Topology Instance.....	8
1.3.3 Binding an Interface to an IPv6 Topology Instance.....	9
1.3.4 Checking the Configuration.....	10
1.4 Configuring IP FRR on the Public Network.....	10
1.4.1 Establishing the Configuration Task.....	10
1.4.2 Configuring a Route-Policy.....	11
1.4.3 Enabling IP FRR on the Public Network.....	12
1.4.4 Checking the Configuration.....	12
1.5 Configuring VRRP for Direct Routes.....	13
1.5.1 Establishing the Configuration Task.....	13
1.5.2 Configuring a VRRP Backup Group.....	14
1.5.3 Associating an Interface with a VRRP Backup Group.....	15
1.5.4 Checking the Configuration.....	16
1.6 Configuration Example.....	17
1.6.1 Example for Configuring IP FRR on the Public Network.....	17
1.6.2 Example for Configuring VRRP for Direct Routes.....	20
2 IP Static Route Configuration.....	28
2.1 Introduction of IP Static Route.....	29
2.1.1 Static Route.....	29

2.1.2 Static Routing Features Supported by the NE80E/40E.....	29
2.2 Configuring an IPv4 Static Route.....	30
2.2.1 Establishing the Configuration Task.....	30
2.2.2 Configuring an IPv4 Static Route.....	32
2.2.3 (Optional) Setting the Default Preference for IPv4 Static Routes.....	32
2.2.4 (Optional) Configuring Static Route Selection Based on Relay Depth.....	33
2.2.5 (Optional) Configuring Permanent Advertisement of IPv4 Static Routes.....	33
2.2.6 Configuring Static IPv4 Routes in a Topology Instance.....	34
2.2.7 Checking the Configuration.....	35
2.3 Configuring an IPv6 Static Route.....	35
2.3.1 Establishing the Configuration Task.....	35
2.3.2 Configuring an IPv6 Static Route.....	36
2.3.3 (Optional) Setting the Default Preference for IPv6 Static Routes.....	36
2.3.4 Configuring Static IPv6 Routes in a Topology Instance.....	37
2.3.5 Checking the Configuration.....	38
2.4 Configuring BFD for IPv4 Static Routes on the Public Network.....	38
2.4.1 Establishing the Configuration Task.....	38
2.4.2 Configuring an IPv4 Static Route.....	39
2.4.3 Configuring a BFD Session.....	39
2.4.4 Binding a Static Route to a BFD Session.....	39
2.4.5 Checking the Configuration.....	40
2.5 Configuring BFD for IPv6 Static Routes on the Public Network.....	41
2.5.1 Establishing the Configuration Task.....	41
2.5.2 Configuring an IPv6 Static Route.....	41
2.5.3 Configuring a BFD Session.....	42
2.5.4 Binding a Static Route to a BFD Session.....	42
2.5.5 Checking the Configuration.....	43
2.6 Configuring NQA for IPv4 Static Routes.....	43
2.6.1 Establishing the Configuration Task.....	43
2.6.2 Configuring an ICMP Type NQA Test Instance.....	44
2.6.3 Binding an IPv4 Static Route to an NQA Test Instance.....	46
2.6.4 Checking the Configuration.....	47
2.7 Configuration Examples.....	48
2.7.1 Example for Configuring IPv4 Static Routes.....	48
2.7.2 Example for Configuring IPv6 Static Routes.....	51
2.7.3 Example for Configuring BFD for IPv4 Static Routes.....	54
2.7.4 Example for Configuring BFD for IPv6 Static Routes.....	57
2.7.5 Example for Configuring NQA for IPv4 Static Routes.....	60
2.7.6 Example for Configuring Permanent Advertisement of IPv4 Static Routes.....	67
3 RIP Configuration.....	73
3.1 Introduction to RIP.....	75
3.1.1 Overview of RIP.....	75

3.1.2 RIP Features Supported by the NE80E/40E.....	76
3.2 Configuring Basic RIP Functions.....	76
3.2.1 Establishing the Configuration Task.....	76
3.2.2 Enabling RIP.....	77
3.2.3 Enabling RIP on the Specified Network Segment.....	77
3.2.4 Configuring RIP Version Number.....	78
3.2.5 Checking the Configuration.....	79
3.3 Configuring RIP Route Attributes.....	81
3.3.1 Establishing the Configuration Task.....	81
3.3.2 Configuring Additional Metrics of an Interface.....	82
3.3.3 Configuring RIP Preference.....	83
3.3.4 Setting the Maximum Number of Equal-Cost Routes.....	83
3.3.5 Checking the Configuration.....	84
3.4 Controlling the Advertising of RIP Routing Information.....	85
3.4.1 Establishing the Configuration Task.....	85
3.4.2 Configuring RIP to Advertise Default Routes.....	85
3.4.3 Disabling an Interface from Sending Update Packets.....	86
3.4.4 Configuring RIP to Import External Routes.....	87
3.4.5 Checking the Configuration.....	88
3.5 Controlling the Receiving of RIP Routing Information.....	89
3.5.1 Establishing the Configuration Task.....	89
3.5.2 Disabling an Interface from Receiving RIP Update Packets.....	89
3.5.3 Disabling RIP from Receiving Host Routes.....	90
3.5.4 Configuring RIP to Filter the Received Routes.....	91
3.5.5 Checking the Configuration.....	91
3.6 Configuring RIP-2 Features.....	92
3.6.1 Establishing the Configuration Task.....	92
3.6.2 Configuring RIP-2 Route Summarization.....	93
3.6.3 Configuring Packet Authentication of RIP-2.....	94
3.6.4 Checking the Configuration.....	95
3.7 Optimizing a RIP Network.....	95
3.7.1 Establishing the Configuration Task.....	95
3.7.2 Configuring RIP Timers.....	96
3.7.3 Setting the Interval for Sending Packets and the Maximum Number of the Sent Packets.....	97
3.7.4 Configuring Split Horizon and Poison Reverse.....	98
3.7.5 Enabling replay-protect Function.....	99
3.7.6 Configuring RIP to Check the Validity of Update Packets.....	100
3.7.7 Configuring RIP Neighbors.....	101
3.7.8 Checking the Configuration.....	101
3.8 Configuring RIP GR.....	102
3.8.1 Establishing the Configuration Task.....	102
3.8.2 Enabling RIP GR.....	103

3.8.3 Checking the Configuration.....	103
3.9 Configuring the Network Management Function in RIP.....	104
3.9.1 Establishing the Configuration Task.....	104
3.9.2 Binding RIP to MIBs.....	104
3.9.3 Checking the Configuration.....	105
3.10 Maintaining RIP.....	105
3.10.1 Resetting RIP.....	105
3.10.2 Clearing RIP.....	106
3.11 Configuration Examples.....	106
3.11.1 Example for Configuring RIP Version.....	106
3.11.2 Example for Configuring RIP to Import External Routes.....	110
4 RIPng Configuration.....	114
4.1 Introduction to RIPng.....	115
4.1.1 RIPng Overview.....	115
4.1.2 RIPng Features Supported by the NE80E/40E.....	116
4.2 Configuring Basic RIPng Functions.....	116
4.2.1 Establishing the Configuration Task.....	116
4.2.2 Enabling RIPng and Entering the RIPng View.....	117
4.2.3 Enabling RIPng in the Interface View.....	117
4.2.4 Checking the Configuration.....	118
4.3 Configuring RIPng Route Attributes.....	120
4.3.1 Establishing the Configuration Task.....	120
4.3.2 Configuring the RIPng Preference.....	120
4.3.3 Configuring Additional Metrics of an Interface.....	121
4.3.4 Configuring the Maximum Number of Equal-Cost Routes.....	122
4.3.5 Checking the Configuration.....	122
4.4 Controlling the Advertising of RIPng Routing Information.....	123
4.4.1 Establishing the Configuration Task.....	123
4.4.2 Configuring RIPng Route Summarization.....	124
4.4.3 Configuring RIPng to Advertise the Default Routes.....	124
4.4.4 Configuring the Default Cost for External Routes Imported by RIPng.....	125
4.4.5 Configuring RIPng to Import External Routes.....	125
4.4.6 Checking the Configuration.....	126
4.5 Controlling the Receiving of RIPng Routing Information.....	126
4.5.1 Establishing the Configuration Task.....	127
4.5.2 Configuring RIPng to Filter the Received Routes.....	127
4.5.3 Checking the Configuration.....	128
4.6 Optimizing a RIPng Network.....	128
4.6.1 Establishing the Configuration Task.....	128
4.6.2 Configuring RIPng Timers.....	129
4.6.3 Setting the Interval for Sending Update Packets and the Maximum Number of Packets Sent Each Time.....	129

4.6.4	Configuring Split Horizon and Poison Reverse.....	130
4.6.5	Enabling the Zero Field Check for RIPng Packets.....	131
4.6.6	Checking the Configuration.....	131
4.7	Configuring IPsec Authentication for RIPng.....	132
4.7.1	Establishing the Configuration Task.....	132
4.7.2	Configuring IPsec Authentication in a RIPng Process.....	133
4.7.3	Configuring IPsec Authentication on a RIPng Interface.....	133
4.7.4	Checking the Configuration.....	134
4.8	Configuration Examples.....	135
4.8.1	Example for Configuring RIPng to Filter the Received Routes.....	135
5	OSPF Configuration.....	139
5.1	Introduction to OSPF.....	141
5.1.1	OSPF Overview.....	141
5.1.2	OSPF Features Supported by the NE80E/40E.....	144
5.2	Configuring Basic OSPF Functions.....	148
5.2.1	Establishing the Configuration Task.....	149
5.2.2	Enabling OSPF and Entering the OSPF View.....	149
5.2.3	Configuring the Network Segments Included by Each Area.....	150
5.2.4	Checking the Configuration.....	151
5.3	Establishing or Maintaining OSPF Neighbor Relationship.....	152
5.3.1	Establishing the Configuration Task.....	152
5.3.2	Configuring the Interval for Sending Hello Packets.....	153
5.3.3	Configuring Smart-discover.....	153
5.3.4	Configuring Dead Time of Neighbor Relationship.....	154
5.3.5	Configuring OSPF Retransmission Limit.....	155
5.3.6	Configuring the Interval for Updating and Receiving LSAs.....	155
5.3.7	Restricting the Flooding of Update LSAs.....	157
5.3.8	Checking the Configuration.....	157
5.4	Configuring OSPF Stub Areas.....	158
5.4.1	Establishing the Configuration Task.....	158
5.4.2	Defining the Current Area to be a Stub Area.....	159
5.4.3	Configuring Metrics of Default Routes Sent to Stub Areas.....	159
5.4.4	Checking the Configuration.....	160
5.5	Configuring OSPF NSSA Areas.....	160
5.5.1	Establishing the Configuration Task.....	161
5.5.2	Defining the Current Area to Be an NSSA Area.....	161
5.5.3	Configuring Metrics of Default Routes Sent to NSSA Areas.....	162
5.5.4	Checking the Configuration.....	163
5.6	Configuring OSPF Virtual Links.....	163
5.6.1	Establishing the Configuration Task.....	163
5.6.2	Configuring OSPF Virtual Links.....	164
5.6.3	Checking the Configuration.....	165

5.7 Configuring OSPF Attributes in Different Types of Networks.....	166
5.7.1 Establishing the Configuration Task.....	166
5.7.2 Configuring Network Types of OSPF Interfaces.....	167
5.7.3 Configuring DR Priorities of OSPF Interfaces.....	167
5.7.4 Disabling the Function of Checking the Network Mask on a P2MP Network.....	168
5.7.5 Configuring Neighbors for NBMA Networks.....	169
5.7.6 Configuring the Interval for Sending Poll Packets in NBMA Networks.....	169
5.7.7 Checking the Configuration.....	170
5.8 Configuring OSPF Route Attributes.....	171
5.8.1 Establishing the Configuration Task.....	171
5.8.2 Configuring the Link Cost of OSPF.....	171
5.8.3 Configuring OSPF Precedence.....	172
5.8.4 Setting the Convergence Priority of OSPF Routes.....	173
5.8.5 Configuring the Maximum Number of Equal-Cost Routes.....	174
5.8.6 Checking the Configuration.....	175
5.9 Controlling OSPF Routing Information.....	176
5.9.1 Establishing the Configuration Task.....	176
5.9.2 Configuring OSPF Route Aggregation.....	176
5.9.3 Configuring OSPF to Filter the Received Routes.....	177
5.9.4 Configuring OSPF to Filter ABR Type3 LSA.....	178
5.9.5 Configuring OSPF to Import External Routes.....	179
5.9.6 Checking the Configuration.....	180
5.10 Optimizing an OSPF Network.....	181
5.10.1 Establishing the Configuration Task.....	182
5.10.2 Configuring the Delay for Transmitting LSAs on the Interface.....	182
5.10.3 Configuring the Interval for Retransmitting LSAs.....	183
5.10.4 Configuring the Local Router to Filter the LSAs to Be Sent.....	184
5.10.5 Suppressing the Interface from Receiving and Sending OSPF Packets.....	185
5.10.6 Configuring the Interval for SPF Calculation.....	185
5.10.7 Configuring Stub Routers.....	186
5.10.8 Enabling the Mesh-Group Function.....	187
5.10.9 Configuring the MTU in DD Packets.....	188
5.10.10 Configuring the Maximum Number of External LSAs in the LSDB.....	188
5.10.11 Configuring RFC 1583 Compatible External Routing.....	189
5.10.12 Checking the Configuration.....	189
5.11 Configuring Local MT.....	191
5.11.1 Establishing the Configuration Task.....	191
5.11.2 Enabling Local MT.....	191
5.11.3 (Optional) Controlling the Scale of the MIGP Routing Table.....	192
5.11.4 Checking the Configuration.....	193
5.12 Configuring OSPF IP FRR.....	193
5.12.1 Establishing the Configuration Task.....	193

5.12.2 Enabling OSPF IP FRR.....	194
5.12.3 (Optional) Configuring OSPF IP FRR Filtering Policies.....	195
5.12.4 (Optional) Binding IP FRR and BFD in an OSPF Process.....	195
5.12.5 (Optional) Binding IP FRR and BFD on a Specified OSPF Interface.....	196
5.12.6 Checking the Configuration.....	196
5.13 Configuring OSPF GR.....	197
5.13.1 Establishing the Configuration Task.....	197
5.13.2 Enabling the Opaque-LSA of OSPF.....	198
5.13.3 Enabling the Default Feature of OSPF GR.....	198
5.13.4 (Optional) Configuring the GR Session Parameters on the Restarter.....	199
5.13.5 (Optional) Configuring GR Session Parameters on the Helper.....	200
5.13.6 (Optional) Configuring the Router not to Enter the Helper Mode.....	201
5.13.7 Checking the Configuration.....	201
5.14 Configuring BFD for OSPF.....	202
5.14.1 Establishing the Configuration Task.....	202
5.14.2 Configuring Global BFD.....	202
5.14.3 Configuring BFD for OSPF.....	203
5.14.4 (Optional) Preventing an Interface from Dynamically Setting Up a BFD Session.....	204
5.14.5 (Optional) Configuring BFD on the Specified Interface.....	204
5.14.6 Checking the Configuration.....	205
5.15 Configuring the Network Management Function of OSPF.....	205
5.15.1 Establishing the Configuration Task.....	206
5.15.2 Configuring OSPF MIB Binding.....	206
5.15.3 Configuring OSPF Trap.....	206
5.15.4 Configuring OSPF Log.....	207
5.15.5 Checking the Configuration.....	207
5.16 Improving Security of an OSPF Network.....	208
5.16.1 Establishing the Configuration Task.....	208
5.16.2 Configuring the OSPF GTSM Functions.....	209
5.16.3 Adjusting GTSM.....	209
5.16.4 Configuring the Area Authentication Mode.....	210
5.16.5 Configuring the Interface Authentication Mode.....	211
5.16.6 Checking the Configuration.....	212
5.17 Maintaining OSPF.....	213
5.17.1 Resetting OSPF.....	213
5.17.2 Clearing OSPF.....	213
5.18 Configuring Examples.....	214
5.18.1 Example for Configuring Basic OSPF Functions.....	214
5.18.2 Example for Configuring OSPF Stub Areas.....	219
5.18.3 Example for Configuring OSPF NSSAs.....	224
5.18.4 Example for Configuring DR Election of OSPF.....	229
5.18.5 Example for Configuring OSPF Virtual Links.....	234

5.18.6 Example for Configuring OSPF Load Balancing.....	237
5.18.7 Example for Configuring Local MT.....	242
5.18.8 Example for Configuring OSPF IP FRR.....	250
5.18.9 Example for Configuring OSPF GR.....	253
5.18.10 Example for Configuring BFD for OSPF.....	257
5.18.11 Example for Configuring OSPF-BGP.....	262
5.18.12 Example for Configuring OSPF GTSM.....	271
6 OSPFv3 Configuration.....	275
6.1 Introduction to OSPFv3.....	277
6.1.1 OSPFv3.....	277
6.1.2 OSPFv3 Features Supported by NE80E/40E.....	277
6.2 Configuring Basic OSPFv3 Functions.....	278
6.2.1 Establishing the Configuration Task.....	278
6.2.2 Enabling OSPFv3.....	278
6.2.3 Enabling OSPFv3 on an Interface.....	279
6.2.4 Entering the OSPFv3 Area View.....	280
6.2.5 Checking the Configuration.....	280
6.3 Establishing or Maintaining OSPFv3 Neighbor Relationship.....	281
6.3.1 Establishing the Configuration Task.....	281
6.3.2 Configuring the Interval for Sending Hello Packets.....	282
6.3.3 Configuring Dead Time of Neighbor Relationship.....	283
6.3.4 Configuring the Interval for Retransmitting LSAs to Neighboring Routers.....	283
6.3.5 Configuring the Delay for Transmitting LSAs on the Interface.....	284
6.3.6 Checking the Configuration.....	285
6.4 Configuring OSPFv3 Areas.....	285
6.4.1 Establishing the Configuration Task.....	285
6.4.2 Configuring OSPFv3 Stub Areas.....	286
6.4.3 Configuring OSPFv3 Virtual Links.....	286
6.4.4 Checking the Configuration.....	287
6.5 Configuring OSPFv3 NSSA Areas.....	288
6.5.1 Establishing the Configuration Task.....	288
6.5.2 Defining the Current Area to Be an NSSA Area.....	288
6.5.3 Checking the Configuration.....	289
6.6 Configuring OSPFv3 Route Attributes.....	290
6.6.1 Establishing the Configuration Task.....	290
6.6.2 Setting the Cost of the OSPFv3 Interface.....	290
6.6.3 Setting the Maximum Number of Equal-Cost Routes.....	291
6.6.4 Checking the Configuration.....	291
6.7 Controlling OSPFv3 Routing Information.....	292
6.7.1 Establishing the Configuration Task.....	292
6.7.2 Configuring OSPFv3 Route Aggregation.....	293
6.7.3 Configuring OSPFv3 to Filter the Received Routes.....	294

6.7.4 Configuring OSPFv3 to Import External Routes.....	295
6.7.5 Checking the Configuration.....	296
6.8 Optimizing an OSPFv3 Network.....	296
6.8.1 Establishing the Configuration Task.....	297
6.8.2 Configuring the SPF Timer.....	297
6.8.3 Setting the Interval for Receiving LSAs.....	298
6.8.4 Configuring an Intelligent Timer for Generating LSAs.....	299
6.8.5 Suppressing an Interface from Sending and Receiving OSPFv3 Packets.....	300
6.8.6 Configuring DR Priority of an Interface.....	300
6.8.7 Configuring Stub Routers.....	301
6.8.8 Ignoring MTU Check on DD Packets.....	302
6.8.9 Checking the Configuration.....	302
6.9 Configuration OSPFv3 GR.....	303
6.9.1 Establishing the Configuration Task.....	303
6.9.2 Enabling OSPFv3 GR.....	303
6.9.3 Enabling the Helper of OSPFv3 GR.....	304
6.9.4 Check the Configuration.....	305
6.10 Configuring BFD for OSPFv3.....	305
6.10.1 Establishing the Configuration Task.....	305
6.10.2 Enabling BFD for OSPFv3.....	306
6.10.3 Configuring OSPFv3 BFD Parameters at Process Level.....	307
6.10.4 Enabling OSPFv3 BFD at Interface Level.....	307
6.10.5 Configuring OSPFv3 BFD Parameters at Interface Level.....	308
6.10.6 Checking the Configuration.....	308
6.11 Configuring OSPFv3 IPsec.....	308
6.11.1 Establishing the Configuration Task.....	309
6.11.2 Enabling IPsec in an OSPFv3 Process.....	309
6.11.3 Enabling IPsec in an OSPFv3 Area.....	310
6.11.4 Enabling IPsec on an Interface.....	311
6.11.5 Enabling IPsec on the Virtual Link.....	311
6.11.6 Enabling IPsec on the Sham Link.....	312
6.11.7 Checking the Configuration.....	312
6.12 Configuring the Network Management Function of OSPFv3.....	315
6.12.1 Establishing the Configuration Task.....	315
6.12.2 Configuring OSPFv3 MIB Binding.....	315
6.12.3 Configuring OSPFv3 Trap.....	316
6.12.4 Check the Configuration.....	316
6.13 Maintaining OSPFv3.....	316
6.13.1 Resetting OSPFv3.....	316
6.14 Configuration Examples.....	317
6.14.1 Example for Configuring OSPFv3 Areas.....	317
6.14.2 Example for Configuring OSPFv3 DR Election.....	322

6.14.3 Example for Configuring OSPFv3 Virtual Links.....	326
6.14.4 Example for Configuring OSPFv3 GR.....	330
6.14.5 Example for Configuring BFD for OSPFv3.....	333
7 IS-IS Configuration.....	339
7.1 Introduction to IS-IS.....	341
7.1.1 Basic Concepts of IS-IS.....	341
7.1.2 IS-IS Features Supported by the NE80E/40E.....	342
7.2 Configuring Basic IS-IS Functions.....	348
7.2.1 Establishing the Configuration Task.....	348
7.2.2 Starting an IS-IS Process.....	349
7.2.3 Configuring an NET.....	349
7.2.4 Configuring the Level of a router.....	350
7.2.5 Enabling IS-IS on a Specified Interface.....	350
7.2.6 Checking the Configuration.....	351
7.3 Establishing or Maintaining IS-IS Neighbor Relationships or Adjacencies.....	352
7.3.1 Establishing the Configuration Task.....	352
7.3.2 Configuring IS-IS Timers for Packets.....	353
7.3.3 Configuring LSP Parameters.....	355
7.3.4 Checking the Configuration.....	358
7.4 Configuring IS-IS Attributes in Different Types of Networks.....	359
7.4.1 Establishing the Configuration Task.....	359
7.4.2 Configuring the Network Type of IS-IS Interface.....	360
7.4.3 Configuring the DIS Priority of an Interface.....	360
7.4.4 Configuring the Negotiation Model on a P2P Link.....	361
7.4.5 Configuring OSICP Check on PPP Interfaces.....	362
7.4.6 Configuring IS-IS Not to Check the IP Address in a Received Hello Packet.....	363
7.4.7 Checking the Configuration.....	364
7.5 Configuring IS-IS Route Attributes.....	364
7.5.1 Establishing the Configuration Task.....	364
7.5.2 Configuring the Cost of an IS-IS Interface.....	365
7.5.3 Configuring the Preference of IS-IS.....	368
7.5.4 Configuring IS-IS Load Balancing.....	370
7.5.5 Checking the Configuration.....	371
7.6 Controlling the Advertisement of IS-IS Routes.....	372
7.6.1 Establishing the Configuration Task.....	372
7.6.2 Configuring IS-IS Route Aggregation.....	373
7.6.3 Configuring IS-IS to Generate Default Routes.....	373
7.6.4 Controlling the Route Leaking from a Level-2 Area to a Level-1 Area.....	374
7.6.5 Controlling the Route Leaking from a Level-1 Area to a Level-2 Area.....	374
7.6.6 Checking the Configuration.....	375
7.7 Controlling the Receiving of IS-IS Routes.....	376
7.7.1 Establishing the Configuration Task.....	376

7.7.2	Configuring IS-IS to Filter the Received Routes.....	376
7.7.3	Configuring IS-IS to Import External Routes.....	377
7.7.4	Checking the Configuration.....	378
7.8	Adjusting and Optimizing an IS-IS Network.....	379
7.8.1	Establishing the Configuration Task.....	379
7.8.2	Configuring the Level of an IS-IS Interface.....	379
7.8.3	Setting the Status of IS-IS Interface to Suppressed.....	380
7.8.4	Configuring SPF Parameters.....	381
7.8.5	Configuring LSP Fast Flooding.....	382
7.8.6	Configuring IS-IS Dynamic Hostname Mapping.....	382
7.8.7	Configuring the LSDB Overload Bit.....	384
7.8.8	Configuring the Output of the Adjacency Status.....	385
7.8.9	Checking the Configuration.....	385
7.9	Configuring Local MT.....	386
7.9.1	Establishing the Configuration Task.....	386
7.9.2	Enabling Local MT.....	387
7.9.3	Controlling the Scale of the MIGP Routing Table.....	388
7.9.4	Checking the Configuration.....	388
7.10	Configuring IS-IS IPv6.....	389
7.10.1	Establishing the Configuration Task.....	389
7.10.2	Enabling IPv6 on an IS-IS Process.....	390
7.10.3	Enabling IPv6 on an IS-IS Interface.....	390
7.10.4	Configuring the IPv6 Route Cost on an Interface.....	391
7.10.5	Configuring the Attributes of IS-IS IPv6 Routes.....	391
7.10.6	Checking the Configuration.....	395
7.11	Configuring IS-IS Auto FRR.....	396
7.11.1	Establishing the Configuration Task.....	396
7.11.2	Enabling IS-IS Auto FRR.....	397
7.11.3	Checking the Configuration.....	398
7.12	Configuring IPv6 IS-IS Auto FRR.....	399
7.12.1	Establishing the Configuration Task.....	399
7.12.2	Enabling IPv6 IS-IS Auto FRR.....	401
7.12.3	(Optional) Disabling an Interface from Participating in LFA Calculation.....	402
7.12.4	Checking the Configuration.....	402
7.13	Configuring IS-IS GR.....	404
7.13.1	Establishing the Configuration Task.....	404
7.13.2	Enabling IS-IS GR.....	405
7.13.3	Configuring Parameters of an IS-IS GR Session.....	406
7.13.4	Checking the Configuration.....	406
7.14	Configuring Static BFD for IS-IS.....	407
7.14.1	Establishing the Configuration Task.....	407
7.14.2	Configuring BFD One-hop Detection.....	408

7.14.3	Enabling IS-IS Fast Detection.....	409
7.14.4	Checking the Configuration.....	410
7.15	Configuring Dynamic BFD for IS-IS.....	411
7.15.1	Establishing the Configuration Task.....	411
7.15.2	Configuring Global BFD.....	412
7.15.3	Configuring Dynamic BFD for an IS-IS Process.....	412
7.15.4	(Optional) Preventing an Interface from Dynamically Setting Up a BFD Session.....	413
7.15.5	Configuring BFD for a Specified Interface.....	413
7.15.6	Checking the Configuration.....	414
7.16	Configuring Dynamic IPv6 BFD for IS-IS.....	415
7.16.1	Establishing the Configuration Task.....	415
7.16.2	Enable Global BFD.....	418
7.16.3	Configuring IPv6 BFD for IS-IS.....	418
7.16.4	Checking the Configuration.....	419
7.17	Improving Security of an IS-IS Network.....	420
7.17.1	Establishing the Configuration Task.....	420
7.17.2	Configuring the Area or Domain Authentication.....	421
7.17.3	Configuring the Interface Authentication.....	422
7.17.4	Checking the Configuration.....	423
7.18	Configuring IS-IS Multi-Topology (IPv4).....	424
7.18.1	Establishing the Configuration Task.....	424
7.18.2	Enabling IS-IS Multi-Topology (IPv4).....	425
7.18.3	(Optional) Setting IS-IS Parameters in IPv4 Topology Instances.....	426
7.18.4	Enabling IS-IS Multi-Topology on a Specified Interface.....	427
7.18.5	(Optional) Setting IS-IS Interface Parameters in IPv4 Topology Instances.....	427
7.18.6	Checking the Configuration.....	428
7.19	Configuring IS-IS Multi-Topology (IPv6).....	430
7.19.1	Establishing the Configuration Task.....	430
7.19.2	Enabling IS-IS Multi-Topology (IPv6).....	431
7.19.3	(Optional) Setting IS-IS Parameters in IPv6 Topology Instances.....	431
7.19.4	Enabling IS-IS Multi-Topology on a Specified Interface.....	433
7.19.5	(Optional) Setting IS-IS Interface Parameters in IPv6 Topology Instances.....	433
7.19.6	Checking the Configuration.....	434
7.20	Maintaining IS-IS.....	435
7.20.1	Resetting IS-IS Data Structure.....	435
7.20.2	Resetting a Specific IS-IS Neighbor.....	436
7.21	Configuration Examples.....	436
7.21.1	Example for Configuring Basic IS-IS Functions.....	437
7.21.2	Example for Configuring IS-IS in an NBMA Network.....	441
7.21.3	Example for Configuring Route Aggregation.....	445
7.21.4	Example for Configuring the DIS Election of IS-IS.....	448
7.21.5	Example for Configuring IS-IS Load Balancing.....	453

7.21.6 Example for Configuring IS-IS to Interact with BGP.....	457
7.21.7 Example for Configuring IS-IS MT.....	461
7.21.8 Example for Configuring Local MT.....	467
7.21.9 Example for Configuring Basic IS-IS IPv6 Functions.....	474
7.21.10 Example for Configuring IS-IS Auto FRR (IP protecting IP).....	479
7.21.11 Example for Configuring IS-IS Auto FRR (TE protecting IP).....	485
7.21.12 Example for Configuring IS-IS GR.....	501
7.21.13 Example for Configuring Static BFD for IS-IS.....	504
7.21.14 Example for Configuring Dynamic BFD for IS-IS.....	508
7.21.15 Example for Configuring Dynamic IPv6 BFD for IS-IS.....	513
8 BGP Configuration.....	520
8.1 Introduction of BGP.....	522
8.1.1 BGP Overview.....	522
8.1.2 BGP Features Supported by the NE80E/40E.....	522
8.2 Configuring Basic BGP Functions.....	528
8.2.1 Establishing the Configuration Task.....	528
8.2.2 Starting a BGP Process.....	529
8.2.3 Configuring a BGP Peer.....	530
8.2.4 (Optional) Configuring the Local Interface for a BGP Connection.....	531
8.2.5 Checking the Configuration.....	532
8.3 Configuring BGP Route Attributes.....	532
8.3.1 Establishing the Configuration Task.....	532
8.3.2 Configuring the BGP Preference.....	533
8.3.3 Configuring the BGP Preferred Value for Routing Information.....	534
8.3.4 Configuring the Default Local_Pref Attribute.....	535
8.3.5 Configuring the MED Attribute.....	535
8.3.6 Configuring the Next_Hop Attribute.....	538
8.3.7 Configuring BGP to Advertise the Community Attribute.....	540
8.3.8 Configuring the AS-Path Attribute.....	541
8.3.9 Checking the Configuration.....	545
8.4 Configuring BGP Filters.....	545
8.4.1 Establishing the Configuration Task.....	545
8.4.2 Configuring Related Access Lists.....	547
8.4.3 Configuring Related Routing Policies.....	549
8.4.4 Configuring the Policy for Advertising BGP Routing Information.....	551
8.4.5 Configuring the Policy for Receiving BGP Routing Information.....	553
8.4.6 Configuring BGP Soft Resetting.....	555
8.4.7 Checking the Configuration.....	557
8.5 Controlling the Advertisement of BGP Routing Information.....	557
8.5.1 Establishing the Configuration Task.....	557
8.5.2 Configuring BGP to Advertise Local Routes.....	558
8.5.3 Configuring BGP Route Aggregation.....	558

8.5.4 Configuring a Router to Advertise Default Routes to Its Peer.....	560
8.5.5 Checking the Configuration.....	560
8.6 Controlling the Import of Routing Information.....	561
8.6.1 Establishing the Configuration Task.....	561
8.6.2 Configuring BGP to Import Default Routes.....	561
8.6.3 Configuring BGP to Import Routes.....	562
8.6.4 Checking the Configuration.....	562
8.7 Configuring BGP Route Dampening.....	563
8.7.1 Establishing the Configuration Task.....	563
8.7.2 Configuring BGP Route Dampening.....	563
8.7.3 Checking the Configuration.....	564
8.8 Configuring Parameters of a BGP Peer Connection.....	564
8.8.1 Establishing the Configuration Task.....	565
8.8.2 Configuring BGP Timers.....	566
8.8.3 Configuring the Interval for Sending Update Packets.....	567
8.8.4 Setting the BGP ConnectRetry Interval.....	568
8.8.5 Enabling Fast Reset of EBGp Connections.....	569
8.8.6 Checking the Configuration.....	569
8.9 Configuring BFD for BGP.....	570
8.9.1 Establishing the Configuration Task.....	570
8.9.2 Configuring BFD for BGP in the Public Network Instance.....	571
8.9.3 Configuring BFD for BGP in a Private Network.....	572
8.9.4 Checking the Configuration.....	574
8.10 Configuring BGP Auto FRR.....	574
8.10.1 Establishing the Configuration Task.....	574
8.10.2 Enabling BGP Auto FRR.....	575
8.10.3 Checking the Configuration.....	575
8.11 Configuring BGP Tracking.....	576
8.11.1 Establishing the Configuration Task.....	576
8.11.2 Enabling BGP Tracking.....	576
8.11.3 Checking the Configuration.....	577
8.12 Configuring Prefix-based BGP ORF.....	578
8.12.1 Establishing the Configuration Task.....	578
8.12.2 Enabling Prefix-based BGP ORF.....	578
8.12.3 Checking the Configuration.....	579
8.13 Configuring Path MTU Auto Discovery.....	579
8.13.1 Establishing the Configuration Task.....	579
8.13.2 Enabling Path MTU Auto Discovery.....	580
8.13.3 (Optional) Setting the IPv4 Path MTU Aging Time.....	580
8.13.4 Checking the Configuration.....	581
8.14 Configuring the BGP Next Hop Delayed Response.....	581
8.14.1 Establishing the Configuration Task.....	581

8.14.2	Configuring the BGP Next Hop Delayed Response.....	582
8.14.3	Checking the Configuration.....	583
8.15	Configuring BGP Load Balancing.....	583
8.15.1	Establishing the Configuration Task.....	583
8.15.2	Setting the Number of Routes for BGP Load Balancing.....	584
8.15.3	Checking the Configuration.....	585
8.16	Configuring a BGP Peer Group.....	585
8.16.1	Establishing the Configuration Task.....	585
8.16.2	Creating an IBGP Peer Group.....	586
8.16.3	Creating a Pure EBGP Peer Group.....	587
8.16.4	Creating a Mixed EBGP Peer Group.....	587
8.16.5	Checking the Configuration.....	588
8.17	Configuring a BGP Route Reflector.....	588
8.17.1	Establishing the Configuration Task.....	589
8.17.2	Configuring a Route Reflector and Specifying Clients.....	589
8.17.3	(Optional) Disabling the Route Reflection Between Clients.....	590
8.17.4	(Optional) Configuring the Cluster ID for a Route Reflector.....	590
8.17.5	(Optional) Preventing BGP Routes from Being Added into the IP Routing Table.....	591
8.17.6	Checking the Configuration.....	592
8.18	Configuring a BGP Confederation.....	592
8.18.1	Establishing the Configuration Task.....	592
8.18.2	Configuring a BGP Confederation.....	593
8.18.3	Checking the Configuration.....	594
8.19	Configuring BGP Accounting.....	594
8.19.1	Establishing the Configuration Task.....	594
8.19.2	Configuring the Routing Policy for Setting the Traffic Index.....	595
8.19.3	Applying the Routing Policy Configured with the Traffic Index.....	596
8.19.4	Applying the BGP Accounting to an Interface.....	596
8.19.5	Checking the Configuration.....	597
8.20	Configuring BGP GR.....	597
8.20.1	Establishing the Configuration Task.....	597
8.20.2	Enabling BGP GR.....	598
8.20.3	Configuring Parameters of a BGP GR Session.....	598
8.20.4	Checking the Configuration.....	599
8.21	Configuring BGP Security.....	600
8.21.1	Establishing the Configuration Task.....	600
8.21.2	Configuring MD5 Authentication.....	601
8.21.3	Configuring Keychain Authentication.....	601
8.21.4	Configuring Basic BGP GTSM Functions.....	602
8.21.5	Checking the Configuration.....	603
8.22	Maintaining BGP.....	604
8.22.1	Resetting BGP Connections.....	604

8.22.2 Clearing BGP Information.....	604
8.23 Configuration Examples.....	605
8.23.1 Example for Configuring Basic BGP Functions.....	605
8.23.2 Example for Configuring AS-Path Filter.....	610
8.23.3 Example for Configuring BGP to Interact with IGP.....	615
8.23.4 Example for Configuring BGP Load Balancing and the MED Attribute.....	619
8.23.5 Example for Configuring the BGP Community Attribute.....	624
8.23.6 Example for Configuring a BGP Route Reflector.....	627
8.23.7 Example for Configuring a BGP Confederation.....	632
8.23.8 Example for Configuring a BGP Routing Policy.....	637
8.23.9 Example for Configuring the BGP Accounting.....	654
8.23.10 Example for Configuring BFD for BGP.....	659
8.23.11 Example for Configuring BGP Auto FRR.....	664
8.23.12 Example for Configuring Prefix-based BGP ORF.....	668
8.23.13 Example for Configuring BGP GTSM.....	672
9 BGP4+ Configuration.....	682
9.1 Introduction of BGP4+.....	684
9.1.1 BGP4+ Overview.....	684
9.1.2 BGP4+ Features Supported by the NE80E/40E.....	684
9.2 Configuring Basic BGP4+ Functions.....	685
9.2.1 Establishing the Configuration Task.....	685
9.2.2 Starting a BGP Process.....	685
9.2.3 Configuring an IPv6 Peer.....	686
9.2.4 (Optional) Configuring the Local Interfaces Used for BGP4+ Connections.....	688
9.2.5 Checking the Configuration.....	689
9.3 Configuring BGP4+ Route Attributes.....	689
9.3.1 Establishing the Configuration Task.....	689
9.3.2 Configuring the BGP4+ Preference.....	690
9.3.3 Configuring BGP4+ Preferred Value for Routing Information.....	691
9.3.4 Configuring the Default Local_Pref Attribute of the Local Router.....	691
9.3.5 Configuring the MED Attribute.....	692
9.3.6 Configuring the Next_Hop Attribute.....	693
9.3.7 Configuring the AS-Path Attribute.....	694
9.3.8 Configuring the BGP4+ Community Attribute.....	696
9.3.9 Checking the Configuration.....	697
9.4 Controlling the Advertising and Receiving of BGP4+ Routing Information.....	698
9.4.1 Establishing the Configuration Task.....	698
9.4.2 Configuring BGP4+ to Advertise Local IPv6 Routes.....	699
9.4.3 Configuring BGP4+ Route Aggregation.....	699
9.4.4 Configuring BGP4+ to Import and Filter External Routes.....	700
9.4.5 Configuring Routers to Advertise Default Routes to Peers.....	701
9.4.6 Configuring the Policy for Advertising BGP4+ Routing Information.....	702

9.4.7 Configuring the Policy for Receiving BGP4+ Routing Information.....	703
9.4.8 Configuring BGP4+ Soft Resetting.....	704
9.4.9 Checking the Configuration.....	705
9.5 Configuring Parameters of a Connection Between BGP4+ Peers.....	706
9.5.1 Establishing the Configuration Task.....	706
9.5.2 Configuring BGP4+ Timers.....	707
9.5.3 Configuring the Interval for Sending Update Packets.....	708
9.5.4 Setting the BGP4+ ConnectRetry Interval.....	708
9.5.5 Checking the Configuration.....	709
9.6 Configuring BFD for BGP4+.....	710
9.6.1 Establishing the Configuration Task.....	711
9.6.2 Configuring BFD for BGP4+ in the Public Network Instance.....	711
9.6.3 Configuring BFD for BGP4+ in a Private Network.....	712
9.6.4 Checking the Configuration.....	714
9.7 Configuring BGP4+ Tracking.....	714
9.7.1 Establishing the Configuration Task.....	714
9.7.2 Enabling BGP4+ Tracking.....	715
9.7.3 Checking the Configuration.....	716
9.8 Configuring BGP4+ Route Dampening.....	716
9.8.1 Establishing the Configuration Task.....	716
9.8.2 Configuring BGP4+ Route Dampening.....	717
9.8.3 Checking the Configuration.....	717
9.9 Configuring BGP4+ Load Balancing.....	718
9.9.1 Establishing the Configuration Task.....	718
9.9.2 Setting the Number of Routes for BGP4+ Load Balancing.....	718
9.9.3 Checking the Configuration.....	719
9.10 Configuring a BGP4+ Peer Group.....	719
9.10.1 Establishing the Configuration Task.....	719
9.10.2 Creating an IBGP Peer Group.....	720
9.10.3 Creating a Pure EBGP Peer Group.....	721
9.10.4 Creating a Mixed EBGP Peer Group.....	722
9.10.5 Checking the Configuration.....	723
9.11 Configuring a BGP4+ Route Reflector.....	723
9.11.1 Establishing the Configuration Task.....	723
9.11.2 Configuring a Route Reflector and Specifying Clients.....	723
9.11.3 (Optional) Disabling a Route Reflection Between Clients.....	724
9.11.4 (Optional) Configuring the Cluster ID for a Route Reflector.....	725
9.11.5 Checking the Configuration.....	725
9.12 Configuring a BGP4+ Confederation.....	726
9.12.1 Establishing the Configuration Task.....	726
9.12.2 Configuring a BGP Confederation.....	726
9.12.3 Checking the Configuration.....	727

9.13 Configuring BGP4+ 6PE.....	728
9.13.1 Establishing the Configuration Task.....	728
9.13.2 Configuring a 6PE Peer.....	728
9.13.3 (Optional) Enabling 6PE Routes Sharing the Explicit Null Label.....	729
9.13.4 Checking the Configuration.....	730
9.14 Configuring BGP4+ 6PE FRR.....	730
9.14.1 Establishing the Configuration Task.....	730
9.14.2 Configuring BGP 6PE Peers.....	731
9.14.3 Enabling 6PE FRR.....	731
9.14.4 Checking the Configuration.....	732
9.15 Configuring BGP4+ Security.....	732
9.15.1 Establishing the Configuration Task.....	732
9.15.2 Configuring MD5 Authentication.....	733
9.15.3 Configuring Keychain Authentication.....	734
9.15.4 Configuring Basic BGP4+ GTSM Functions.....	735
9.15.5 Checking the Configuration.....	736
9.16 Maintaining BGP4+.....	736
9.16.1 Resetting BGP4+ Connections.....	736
9.16.2 Clearing BGP4+ Statistics.....	737
9.17 Configuration Examples.....	738
9.17.1 Example for Configuring Basic BGP4+ Functions.....	738
9.17.2 Example for Configuring a BGP4+ Route Reflection.....	742
9.17.3 Example for Configuring BFD for BGP4+.....	747
9.17.4 Example for Configuring BGP4+ 6PE.....	753
9.17.5 Example for Configuring BGP4+ 6PE FRR.....	759
10 Routing Policy Configuration.....	768
10.1 Introduction of Routing Policy.....	769
10.1.1 Overview of the Routing Policy.....	769
10.1.2 Routing Policy Features Supported by the NE80E/40E.....	770
10.2 Configuring the IP-Prefix List.....	771
10.2.1 Establishing the Configuration Task.....	771
10.2.2 Configuring an IPv4 Prefix List.....	772
10.2.3 Configuring an IPv6 Prefix List.....	773
10.2.4 Checking the Configuration.....	773
10.3 Configuring the Route-Policy.....	774
10.3.1 Establishing the Configuration Task.....	774
10.3.2 Creating a Route-Policy.....	775
10.3.3 (Optional) Configuring the If-Match Clause.....	776
10.3.4 (Optional) Configuring the Apply Clause.....	777
10.3.5 Checking the Configuration.....	778
10.4 Applying Filters to Received Routes.....	779
10.4.1 Establishing the Configuration Task.....	779

10.4.2 Filtering Routes Received by RIP.....	780
10.4.3 Filtering Routes Received by OSPF.....	780
10.4.4 Filtering Routes Received by IS-IS.....	781
10.4.5 Filtering Routes Received by BGP.....	781
10.4.6 Checking the Configuration.....	782
10.5 Applying Filters to Advertised Routes.....	783
10.5.1 Establishing the Configuration Task.....	783
10.5.2 Filtering Routes Advertised by RIP.....	784
10.5.3 Filtering Routes Advertised by OSPF.....	784
10.5.4 Filtering Routes Advertised by IS-IS.....	785
10.5.5 Filtering Routes Advertised by BGP.....	785
10.5.6 Checking the Configuration.....	787
10.6 Applying Filters to Imported Routes.....	787
10.6.1 Establishing the Configuration Task.....	787
10.6.2 Applying Route-Policy to Routes Imported by RIP.....	788
10.6.3 Applying Route-Policy to Routes Imported by OSPF.....	789
10.6.4 Applying Route-Policy to Routes Imported by IS-IS.....	789
10.6.5 Applying Route-Policy to Routes Imported by BGP.....	790
10.6.6 Checking the Configuration.....	790
10.7 Controlling the Valid Time of the Routing policy.....	791
10.7.1 Establishing the Configuration Task.....	791
10.7.2 Configuring the Delay for Applying the Routing Policy.....	792
10.7.3 Checking the Configuration.....	792
10.8 Maintaining the Routing Policy.....	793
10.9 Configuration Examples.....	793
10.9.1 Example for Filtering Received and Advertised Routes.....	793
10.9.2 Example for Applying the Routing Policy When Importing Routes.....	798
A Glossary.....	803
B Acronyms and Abbreviations.....	807

1 IP Routing Overview

About This Chapter

IP routing is the basic element of data communication networks.

[1.1 Routing Management](#)

To forward data, routers need to establish and refresh routing tables and forward packets according to routing tables.

[1.2 Configuring IPv4 Multi-Topology](#)

By configuring multi-topology on an IPv4 network, you can properly allocate network resources.

[1.3 Configuring IPv6 Multi-Topology](#)

By configuring multi-topology on an IPv6 network, you can properly allocate network resources.

[1.4 Configuring IP FRR on the Public Network](#)

IP FRR on the public network is applicable to the services that are very sensitive to packet loss and delay on the public network.

[1.5 Configuring VRRP for Direct Routes](#)

If VRRP for direct routes is configured on a master device of an IPv4 network, the master device effectively diagnoses a link fault, improving the security of the IPv4 network.

[1.6 Configuration Example](#)

IP routing configuration examples explain networking requirements, networking diagrams, configuration notes, configuration roadmap, and configuration procedures.

1.1 Routing Management

To forward data, routers need to establish and refresh routing tables and forward packets according to routing tables.

1.1.1 Displaying of the Routing Table

Checking routing tables helps to know network topology and locate faults.

Prerequisite

Checking information about routing tables helps fault location. The following lists common commands for displaying information about the routing table.

The display commands can be run in all views.

Procedure

- Run the **display ip routing-table** command to check brief information about current active routes.
- Run the **display ip routing-table verbose** command to check detailed information about the IP routing table.
- Run the **display ip routing-table ip-address** [*mask* | *mask-length*] [**longer-match**] [**verbose**] command to check the routes to a specified destination address.
- Run the **display ip routing-table ip-address1** { *mask1* | *mask-length1* } *ip-address2* { *mask2* | *mask-length2* } [**verbose**] command to check the routes whose destination addresses are within a specified address range.
- Run the **display ip routing-table acl** { *acl-number* | *acl-name* } [**verbose**] command to check the routes filtered by a specified basic ACL.
- Run the **display ip routing-table ip-prefix** *ip-prefix-name* [**verbose**] command to check the routes filtered by a specified IP prefix list.
- Run the **display ip routing-table protocol** *protocol* [**inactive** | **verbose**] command to check the routes discovered by a specified protocol.
- Run the **display ip routing-table statistics** command to check statistics about the IP routing table.
- Run the **display ip routing-table vpn-instance** *vpn-instance-name* command to check brief information about the VPN routing table.
- Run the **display ip routing-table vpn-instance** *vpn-instance-name* **verbose** command to check detailed information about the VPN routing table.

---End

1.1.2 Displaying of the Routing Management Module

By using the display commands of the routing management module, you can locate routing problems.

Context

You can use display commands of the routing management (RM) module to locate routing problems.

display commands can be run in all views.

Procedure

- Run the **display rm interface** [*interface-type interface-number*] command to check RM information of a specified interface.
- Run the **display rm ipv6 interface** [*interface-type interface-number*] command to check IPv6 RM information of a specified interface.
- Run the **display rm interface vpn-instance** *vpn-instance-name* command to check RM information of the private network interface.

---End

1.1.3 FRR Principle

FRR is a technique to allow the physical layer or data link layer to report a fault to the upper layer routing system and allow packets to be forwarded over a backup link if a fault occurs.

Context

On traditional IP networks, after a forwarding device such as the router detects a fault on the lower layer link, it takes the system several seconds to complete route convergence (that is, to re-select an available route).

A second-level convergence may seriously affect the services that are extremely sensitive to packet loss and delay, leading to service interruption. In the case of the VoIP service, the maximum convergence time tolerable is about 50 ms when network interruption occurs.

Therefore, to prevent services from being seriously affected by faults on the link, the forwarding system must be able to fast detect and rectify faults, and to restore the affected services as soon as possible.

Fast Reroute (FRR) is applicable to the services that are very sensitive to packet loss and delay. After FRR is configured, when a fault is detected at the lower layer (physical layer or link layer), the fault is reported to the upper layer routing system. Meanwhile, packets are forwarded over a backup link. In this manner, the impact of link faults on services is minimized.

According to the application scope, FRR is classified into IP FRR and VPN FRR. IP FRR can be further classified into IP FRR on the public network and VPN IP FRR.

- IP FRR on the public network: protects routers on the public network.
- VPN IP FRR: protects CE routers.
- VPN FRR: protects PE routers.

For detailed introduction of FRR, see the *HUAWEI NetEngine80E/40E Router Feature Description- IP Route*.

For detailed configuration of VPN IP FRR and VPN FRR, see the *HUAWEI NetEngine80E/40E Router Configuration Guide - VPN*.

FRR can provide backup for direct routes, static routes, and dynamic routes (including RIP routes, OSPF routes, IS-IS routes, and BGP routes) of NE80E/40Es.

1.2 Configuring IPv4 Multi-Topology

By configuring multi-topology on an IPv4 network, you can properly allocate network resources.

1.2.1 Establishing the Configuration Task

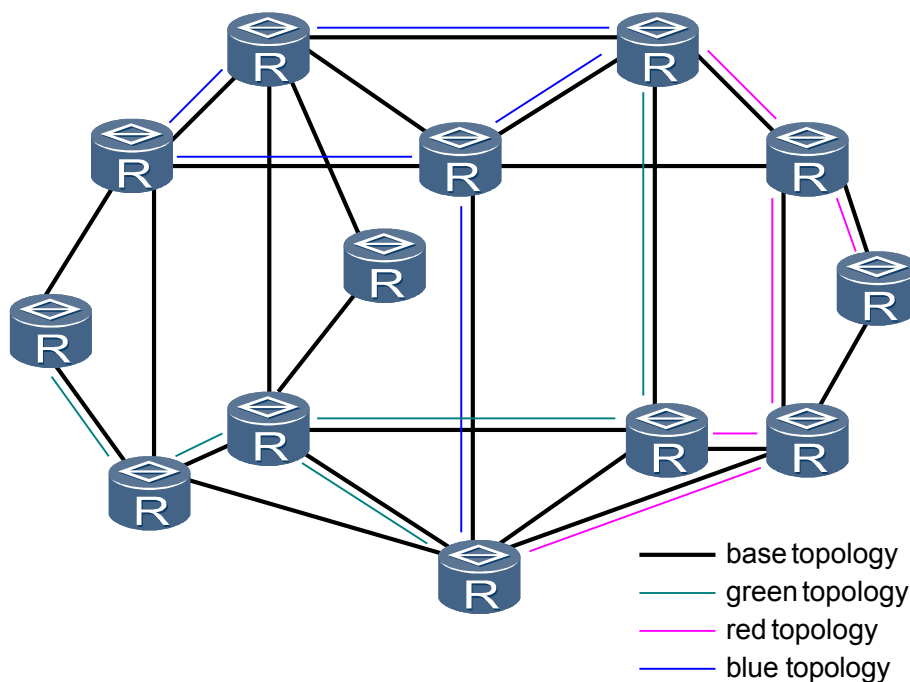
Before configuring IPv4 multi-topology, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

On a traditional IP network, only one unicast topology exists, and only one unicast forwarding table exists on the forwarding plane. Services to the same destination IPv4 address share the same per-hop forwarding behavior. This means that various end-to-end services (for example, voice and data services) share the same physical link. Some links may be heavily congested while other links are relatively idle. A solution to this problem is to divide a physical network into different logical topologies for different services. Such a solution is called multi-topology.

As shown in [Figure 1-1](#), multi-topology is configured on the network; the base topology includes all devices on the network; other topology instances (such as the green topology, red topology, and blue topology) just include some devices because they bear their respective services. By deploying services (for example, voice and data services) in different topology instances as required, you can isolate network resources on a network.

Figure 1-1 Networking diagram of multi-topology



Multi-topology is usually applied to multicast services.

Pre-configuration Tasks

None.

Data Preparation

To configure IPv4 multi-topology, you need the following data.

No.	Data
1	Name of the IPv4 topology instance

1.2.2 Creating an IPv4 Topology Instance

By configuring IPv4 topology instances, you can make proper use of network resources.

Context

Before configuring multi-topology on an IPv4 network, you need to create an IPv4 topology instance.

Each topology instance is a subset of base topology instance. Each topology instance bears a type of services and maintains its own routing table and forwarding table.

Do as follows on the device where an IPv4 topology instance needs to be created:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip topology topology-name
```

An IPv4 topology instance is created, and the topology view is displayed.

By default, there are only base topology instances in the system.

Generally, "base" is the name of a base topology instance, and "multicast" is the name of a multicast topology instance. A maximum of 32 IPv4 topology instances (including 1 base topology instance, 1 multicast topology instance, and 30 unicast topology instances) can be created.

Step 3 (Optional) Run:

```
routing-table limit number { alert-percent | simply-alert }
```

You can set the maximum number of routes supported by a specified topology instance to prevent a device from importing too many routes.

By default, the maximum number of routes supported by a topology instance is not set.

When a large number of routes exist on a device but only some important routes need to be imported for a topology instance, you are recommended to run the **routing-table limit** command to set the maximum number of routes supported by the topology instance.

---End

1.2.3 Binding an Interface to an IPv4 Topology Instance

To add direct routes of an interface to an IPv4 topology instance, you need to bind the interface to the IPv4 topology instance.

Context

Before configuring multi-topology on an IPv4 network, you need to create an IPv4 topology instance. To add direct routes or IS-IS routes of an interface to the topology instance, you need to bind the interface to the topology instance.

Do as follows on the interface where an IPv4 topology instance needs to be bound:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-name
```

The interface view is displayed.

Step 3 Run:

```
ip topology topology-name enable
```

Multi-topology is configured in the specified interface view, and the specified interface is bound to the specified topology instance.

By default, the interface is bound to the base topology instance only.

An interface can be bound to multiple topology instances, and multiple interfaces can be bound to the same topology instance.

---End

1.2.4 Checking the Configuration

After IPv4 multi-topology is configured, you can check information about the created topology instance.

Prerequisite

All configurations of IPv4 multi-topology are complete.

Procedure

- Run the **display ip topology** [*topology-name*] [**verbose**] command to check IPv4 multi-topology information.

- Run the **display ip routing-table topology** *topology-name* [**verbose**] command to check the routing table of IPv4 multi-topology.

---End

Example

Run the **display ip topology** *topology-name* **verbose** command after configuring IPv4 multi-topology. If the following is displayed, it means that the configuration succeeds.

```
<HUAWEI> display ip topology red verbose
Topology Name       : red
Topology ID        : 0x0100
Maximum Routes Limit : 1000
Threshold Routes Limit : 50%
Interface:
  GigabitEthernet1/0/0
  GigabitEthernet1/0/1
```

1.3 Configuring IPv6 Multi-Topology

By configuring multi-topology on an IPv6 network, you can properly allocate network resources.

1.3.1 Establishing the Configuration Task

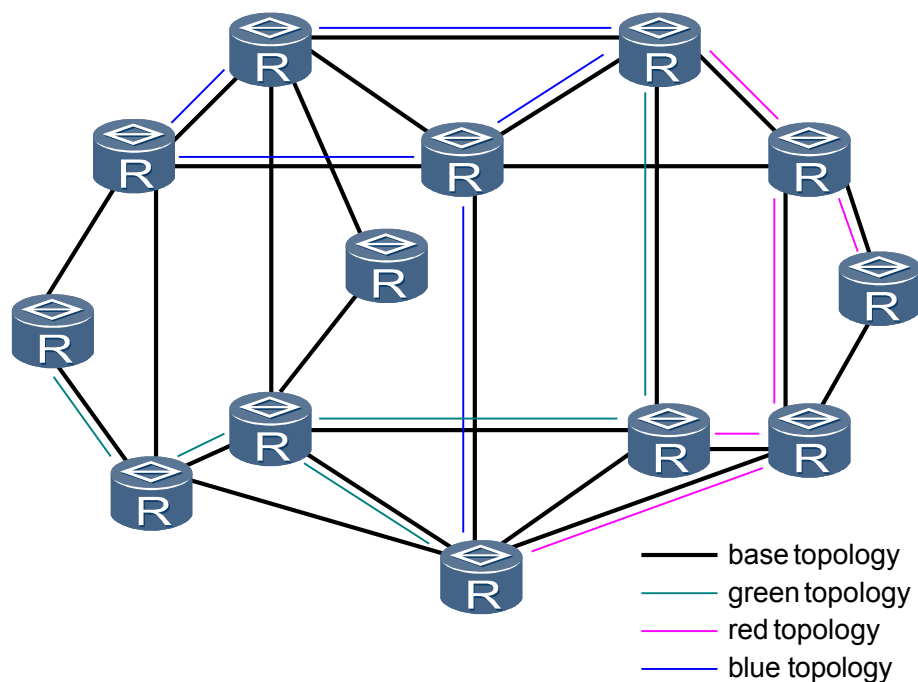
Before configuring IPv6 multi-topology, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

On a traditional IP network, only one unicast topology exists, and only one unicast forwarding table exists on the forwarding plane. Services to the same destination IPv6 address share the same per-hop forwarding behavior. This means that various end-to-end services (for example, voice and data services) share the same physical link. Some links may be heavily congested while other links are relatively idle. A solution to this problem is to divide a physical network into different logical topologies for different services. Such a solution is called multi-topology.

As shown in [Figure 1-2](#), multi-topology is configured on the network; the base topology includes all devices on the network; other topology instances (such as the green topology, red topology, and blue topology) just include some devices because they bear their respective services. By deploying services (for example, voice and data services) in different topology instances as required, you can isolate network resources on a network.

Figure 1-2 Networking diagram of multi-topology



Multi-topology is usually applied to multicast services.

Pre-configuration Tasks

None.

Data Preparation

To configure IPv6 multi-topology, you need the following data.

No.	Data
1	Name of the IPv6 topology instance

1.3.2 Creating an IPv6 Topology Instance

By configuring IPv6 topology instances, you can make proper use of network resources.

Context

Before configuring multi-topology on an IPv6 network, you need to create an IPv6 topology instance.

Each topology instance is a subset of the base topology instance. Each topology instance bears a type of services and maintains its own routing table and forwarding table.

Do as follows on the device where an IPv6 topology instance needs to be created:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ipv6 topology topology-name
```

An IPv6 topology instance is created, and the IPv6 topology view is displayed.

By default, there are only base topology instances in the system.

Generally, "base" is the name of a base topology instance, and "multicast" is the name of a multicast topology instance. A maximum of 32 IPv6 topology instances (including 1 base topology instance, 1 multicast topology instance, and 30 unicast topology instances) can be created.

Step 3 (Optional) Run:

```
routing-table limit number { alert-percent | simply-alert }
```

The maximum number of routes supported by a specified IPv6 topology instance is set.

By default, the maximum number of routes supported by a topology instance is not set.

When a large number of routes exist on a device but only some important routes need to be imported for a topology instance, you are recommended to run the **routing-table limit** command to set the maximum number of routes supported by the topology instance.

---End

1.3.3 Binding an Interface to an IPv6 Topology Instance

To add direct routes of an interface to an IPv6 topology instance, you need to bind the interface to the IPv6 topology instance.

Context

Before configuring multi-topology on an IPv6 network, you need to create an IPv6 topology instance. To add direct routes or IS-IS routes of an interface to the topology instance, you need to bind the interface to the topology instance.

Do as follows on the interface where an IPv6 topology instance needs to be bound:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-name
```

The interface view is displayed.

Step 3 Run:

```
ipv6 topology topology-name enable
```

Multi-topology is configured in the specified interface view, and the specified interface is bound to the specified topology instance.

By default, the interface is bound to the base topology instance only.

An interface can be bound to multiple topology instances, and multiple interfaces can be bound to the same topology instance.

----End

1.3.4 Checking the Configuration

After IPv6 multi-topology is configured, you can check information about the created topology instance.

Prerequisite

All configurations of IPv6 multi-topology are complete.

Procedure

- Run the **display ipv6 topology** [*topology-name*] [**verbose**] command to check IPv6 multi-topology information.
- Run the **display ipv6 routing-table topology** *topology-name* [**verbose**] command to check the routing table of IPv6 multi-topology.

----End

Example

Run the **display ipv6 topology** *topology-name* **verbose** command after configuring IPv6 multi-topology. If the following is displayed, it means that the configuration succeeds.

```
<HUAWEI> display ipv6 topology red verbose
Topology Name       : red
Topology ID        : 0x0100
Maximum Routes Limit : 1000
Threshold Routes Limit : 50%
Interface:
  GigabitEthernet1/0/0
  GigabitEthernet1/0/1
```

1.4 Configuring IP FRR on the Public Network

IP FRR on the public network is applicable to the services that are very sensitive to packet loss and delay on the public network.

1.4.1 Establishing the Configuration Task

Before configuring IP FRR on the public network, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

IP FRR on the public network is applicable to the services that are very sensitive to packet loss and delay on the public network.

Pre-configuration Tasks

Before configuring IP FRR on the public network, complete the following tasks:

- Configuring a static route or an IGP to ensure that nodes are reachable
- Setting different costs to generate two routes

Data Preparation

To configure IP FRR on the public network, you need the following data.

No.	Data
1	Name of the route-policy and the number of the node
2	Outbound interface of the backup route
3	Next hop of the backup route

1.4.2 Configuring a Route-Policy

When configuring IP FRR on the public network, you can use a route-policy to correctly establish the backup relationship between routes.

Context

Do as follows on the router to which IP FRR on the public network is applied:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
route-policy route-policy-name { permit | deny } node node
```

The node of the route-policy is created and the route-policy view is displayed.

Step 3 (Optional) Run:

```
if-match
```

The matching condition is set to filter the routes to be backed up.

You can use the **if-match** command according to the description in [\(Optional\) Configuring the If-Match Clause](#).

If the matching condition is not set, IP FRR backs up outbound interfaces and next hops for all routes in the routing table. In this manner, certain routes that do not need to be backed up are also configured with backup information. Therefore, you need to correctly set the relationship between routes to be backed up and backup routes. Using the matching condition to specify the routes to be backed up is recommended.

Step 4 Run:

```
apply backup-interface interface-type interface-number
```

The backup outbound interface is specified.

Step 5 Run:

```
apply backup-nexthop ip-address
```

The backup next hop is specified.

 **TIP**

- If a backup next hop is specified, a backup outbound interface also needs to be specified.
- If a backup outbound interface is specified on a P2P link, no backup next hop needs to be specified.
- If a backup outbound interface is specified on a non-P2P link, a backup next hop also needs to be specified.

---End

1.4.3 Enabling IP FRR on the Public Network

After IP FRR is configured on the public network, when the primary link fails, service traffic can be switched to the backup link immediately. This ensures the normal transmission of service traffic.

Context

Do as follows on the router to which IP FRR on the public network is applied:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip frr route-policy route-policy-name
```

IP FRR is enabled.

Before applying IP FRR, use this command to enable IP FRR. In this manner, the route-policy used to specify backup outbound interfaces and backup next hops can take effect.

---End

1.4.4 Checking the Configuration

After IP FRR on the public network is configured, you can check backup information about routes.

Prerequisite

The configurations of IP FRR on the public network are complete.

Procedure

- Run the **display route-policy** [*route-policy-name*] command to check the route-policy.
- Run the **display ip routing-table verbose** command to check backup outbound interfaces and backup next hops in the routing table.
- Run the **display ip routing-table ip-address** [*mask* | *mask-length*] [**longer-match**] **verbose** command to check the backup outbound interface and the backup next hop in the routing table.
- Run the **display ip routing-table ip-address1** { *mask1* | *mask-length1* } *ip-address2* { *mask2* | *mask-length2* } **verbose** command to check the backup outbound interface and the backup next hop in the routing table.

----End

1.5 Configuring VRRP for Direct Routes

If VRRP for direct routes is configured on a master device of an IPv4 network, the master device effectively diagnoses a link fault, improving the security of the IPv4 network.

1.5.1 Establishing the Configuration Task

Before configuring VRRP for direct routes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain data. This will help you complete the configuration task quickly and accurately.

Applicable Environment

As the Internet develops, the demand for higher reliability is increasing. To help LAN users access the Internet at any time, the VRRP provides reliability for LAN hosts.

On an IP RAN enabled with VRRP, if a UPE recovers from a fault, its interface connected to the RSG goes Up and generates a direct route, allowing a traffic switchback. As the UPE does not learn the RSG's MAC address, the UPE fails to switch back some packets. To help prevent the problem, the direct route has to be generated only after the VRRP status changes to Master. If VRRP for direct routes is configured, the UPE adjusts the direct route's cost based on the VRRP status. This allows the UPE to perform a successful traffic switchback if recovering from a fault.

For detailed configurations of an IP RAN, see the section "IP RAN Configuration" in the *HUAWEI NetEngine80E/40E Router Configuration Guide - VPN*.

Pre-configuration Tasks

Before configuring VRRP for direct routes, complete the following task:

- Configuring parameters for a data link layer protocol and IP addresses for interfaces to ensure that the data link layer protocol on the interfaces is Up

Data Preparation

To configure VRRP for direct routes, you need the following data.

No.	Data
1	VRRP backup group ID
2	Virtual IP address of a VRRP backup group
3	Priority levels of routers in a VRRP backup group
4	Name of an interface associated with a VRRP backup group

1.5.2 Configuring a VRRP Backup Group

A VRRP backup group allows LAN hosts to communicate with external networks in a reliable manner.

Context

VRRP groups multiple routers to a virtual router. The virtual router uses a mechanism to switch traffic to another router if a fault occurs on the current router, providing continuous and reliable communication services.

VRRP works in master/backup mode to provide IP address backup. A virtual router (a VRRP backup group) in master/backup mode consists of a master router and one or multiple backup routers. The master and backup routers form a backup group. In master/backup mode, only one VRRP backup group is set up. Routers in the VRRP backup group are prioritized. The router with the highest priority functions as the master router and other routers function as backup routers.

- The master router transmits all services if it works properly.
- If the master router fails, a backup router takes over services.

For detailed configurations of a VRRP backup group, see the section "VRRP Configuration" in the *HUAWEI NetEngine80E/40E Router Configuration Guide - Reliability*.

Do as follows on devices in a VRRP backup group:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
vrrp vrid virtual-router-id virtual-ip virtual-address
```

A VRRP backup group is configured and its virtual IP address is assigned.

 **NOTE**

- The virtual IP addresses of VRRP backup groups must be different.
- All devices in a VRRP backup group must be assigned the same virtual router ID.
- Virtual router IDs set on different interfaces of one device can be the same.

If the first virtual IP address is assigned to a VRRP backup group, the system automatically creates the VRRP backup group. If another virtual IP address is assigned to the VRRP backup group, the system only adds the virtual IP address to the virtual IP address list for the VRRP backup group.

On a network where a VRRP backup group is the gateway for multiple hosts, a default gateway address saved on any host does not change even if the VRRP backup group's location changes. To help hosts adapt to changes in the VRRP backup group's location, the VRRP backup group is assigned multiple virtual IP addresses for different hosts. A maximum of 16 virtual IP addresses is assigned to a VRRP backup group.

Step 4 Run:

```
vrrp vrid virtual-router-id priority priority-value
```

The priority value of a device in a backup group is set.

By default, the priority value is 100.

- Priority 0: is reserved for special use.
- Priority 255: is reserved for the IP address owner. The priority of the IP address owner is fixed.

The configurable priority value ranges from 1 to 254.

Step 5 Run:

```
vrrp vrid virtual-router-id timer advertise advertise-interval
```

The interval at which a VRRP Advertisement packet is sent is set.

By default, a VRRP Advertisement packet is sent every second. If multiple VRRP backup groups are configured on a device, the interval can be increased to prevent frequent VRRP status switchovers.

----End

1.5.3 Associating an Interface with a VRRP Backup Group

After an interface is associated with a VRRP backup group, the cost of the direct route in a network segment, to which the interface belongs, changes based on the VRRP status.

Context

The VRRP status changes during a master/backup switchover. Associating an interface with a VRRP backup group allows the cost of the direct route in the network segment to which the interface belongs to change based on the VRRP status.

Do as follows on the interface to be associated with a VRRP backup group:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
direct-route track vrrp vrid virtual-router-id degrade-cost cost
```

The interface is associated with a VRRP backup group.

By default, the interface is associated with no VRRP backup group.

VRRP for direct routes works as follows:

- If the VRRP status becomes Backup, the direct route's cost increases by **degrade-cost cost**, lowering the direct route's priority. The direct route will no longer be an optimal route.
- If the VRRP status becomes Master, the direct route's cost is set to 0, allowing the direct route's priority to be the highest. The direct route will be an optimal route.

----End

1.5.4 Checking the Configuration

After VRRP for direct routes has been configured successfully, view information about the VRRP backup group status.

Prerequisite

The configurations of a VRRP backup group are complete.

Procedure

- Run the **display vrrp** [**interface interface-type interface-number** [**virtual-router-id**]] [**brief**] command to check the VRRP backup group status.
- Run the **display ip routing-table** [**verbose**] command to check the information about the IPv4 routing table.

----End

Example

If a VRRP backup group is configured successfully, run the **display vrrp** command, and you can view the VRRP backup group status. For example, the VRRP backup group status is Master.

```
<HUAWEI> display vrrp
GigabitEthernet2/0/0 | Virtual Router 1
  State : Master
  Virtual IP : 10.1.3.111
  Master IP : 10.1.3.1
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 120
  Preempt : YES   Delay Time : 0
  TimerRun : 10
  TimerConfig : 10
  Auth Type : NONE
```



```
Virtual Mac : 0000-5e00-0102
Check TTL : YES
Config type : normal-vrrp
Create time : 2010-08-16 12:02:57
Last change time : 2010-08-17 10:27:11
```

1.6 Configuration Example

IP routing configuration examples explain networking requirements, networking diagrams, configuration notes, configuration roadmap, and configuration procedures.

NOTE

Examples in this document use interface numbers and link types of the NE40E-X8. In real world situations, the interface numbers and link types may be different from those used in this document.

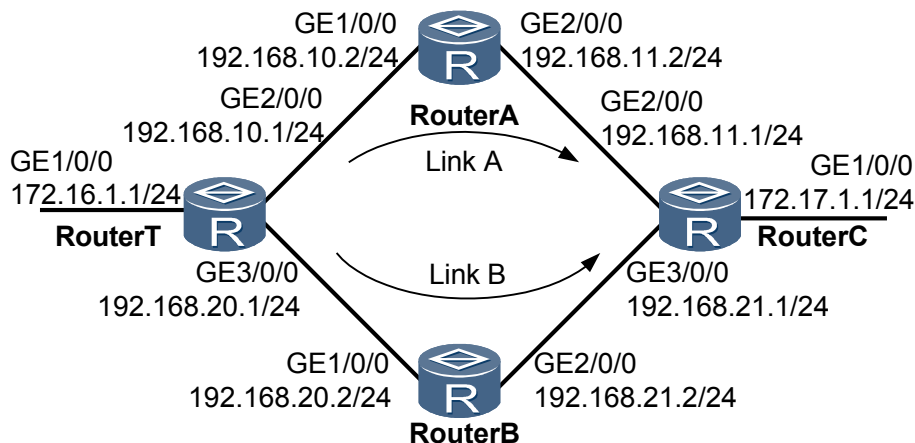
1.6.1 Example for Configuring IP FRR on the Public Network

After IP FRR on the public network is configured, traffic can be rapidly switched to the backup link if the primary link becomes faulty.

Networking Requirements

As shown in [Figure 1-3](#), it is required that link B functions as the backup of link A. In this manner, if a fault occurs on link A, traffic can be rapidly switched to link B.

Figure 1-3 Networking diagram for configuring IP FRR on the public network



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic OSPF functions on each router to allow them to learn routes from each other..
2. Set a greater cost for GE 3/0/0 of Router T and Router C so that OSPF prefers link A.
3. Configure a route-policy on Router T, configure the backup outbound interface and backup next hop, and enable IP FRR on the public network to ensure that link B functions as the backup of link A

Data Preparation

To complete the configuration, you need the following data:

- Cost (100) of an OSPF interface
- Name of the route-policy and number of the node
- Backup outbound interface (GE 3/0/0) and backup next hop (192.168.20.2)

Configuration procedure

1. Configure an IP address for each interface.

The configuration details are not described here.

2. Configure OSPF on Router T, Router A, Router B, and Router C.
3. Set a cost on an OSPF interface.

Set a cost on Gigabit Ethernet 3/0/0 of Router T so that OSPF prefers link A.

```
[RouterT] interface gigabitethernet 3/0/0
[RouterT-GigabitEthernet3/0/0] ospf cost 100
[RouterT-GigabitEthernet3/0/0] quit
```

Set a greater cost on Gigabit Ethernet 3/0/0 of Router C so that OSPF prefers link A.

```
[RouterC] interface gigabitethernet 3/0/0
[RouterC-GigabitEthernet3/0/0] ospf cost 100
[RouterC-GigabitEthernet3/0/0] quit
```

4. Configure a route-policy.

Configure a route-policy on Router T, configure the backup outbound interface and backup next hop, and configure an **if-match** clause to limit the application scope.

```
[RouterT] ip ip-prefix frr1 permit 172.17.1.1 24
[RouterT] route-policy ip_frr_rp permit node 10
[RouterT-route-policy] if-match ip-prefix frr1
[RouterT-route-policy] apply backup-nexthop 192.168.20.2
[RouterT-route-policy] apply backup-interface gigabitethernet3/0/0
[RouterT-route-policy] quit
```

5. Enable IP FRR on the public network.

```
[RouterT] ip frr route-policy ip_frr_rp
```

Check information about the backup outbound interface and backup next hop on Router T.

```
<RouterT> display ip routing-table 172.17.1.0 verbose
Route Flags: R - relay, D - download to fib
```

```
-----
Routing Table : Public
Summary Count : 1
```

```
Destination: 172.17.1.0/24
  Protocol: OSPF                Process ID: 1
  Preference: 10                 Cost: 3
  NextHop: 192.168.10.2          Neighbour: 0.0.0.0
  State: Active Adv              Age: 00h06m49s
  Tag: 0                          Priority: low
  Label: NULL                     QoSInfo: 0x0
  IndirectID: 0x0
  RelayNextHop: 0.0.0.0          Interface: GigabitEthernet2/0/0
  TunnelID: 0x0                   Flags: D
  BkNextHop: 192.168.20.2        BkInterface: GigabitEthernet3/0/0
  BkLabel: NULL                   SecTunnelID: 0x0
  BkPETunnelID: 0x0              BkPESecTunnelID: 0x0
  BkIndirectID: 0x0
```

6. If IP FRR is not required, run the **undo ip frr** command to disable IP FRR.

```
[RouterT] undo ip frr

# After IP FRR is disabled, check information about the backup outbound interface and
# backup next hop.

<RouterT> display ip routing-table 172.17.1.0 verbose
Route Flags: R - relay, D - download to fib
-----
Routing Table : Public
Summary Count : 1

Destination: 172.17.1.0/24
  Protocol: OSPF                Process ID: 1
  Preference: 10                Cost: 3
  NextHop: 192.168.10.2         Neighbour: 0.0.0.0
  State: Active Adv             Age: 00h00m01s
  Tag: 0                         Priority: low
  Label: NULL                    QoSInfo: 0x0
  IndirectID: 0x0
  RelayNextHop: 0.0.0.0         Interface: GigabitEthernet2/0/0
  TunnelID: 0x0                 Flags: D
```

Configuration Files

- Configuration file of Router T

```
#
sysname RouterT
#
ip frr route-policy ip_frr_rp
#
interface GigabitEthernet2/0/0
ip address 192.168.10.1 255.255.255.0
#
interface GigabitEthernet3/0/0
ip address 192.168.20.1 255.255.255.0
ospf cost 100
#
interface GigabitEthernet1/0/0
ip address 172.16.1.1 255.255.255.0
#
interface NULL0
#
ospf 1
area 0.0.0.0
network 192.168.10.0 0.0.0.255
network 192.168.20.0 0.0.0.255
area 0.0.0.1
network 172.16.1.0 0.0.0.255
#
ip ip-prefix fr1 permit 172.17.1.1 24
#
route-policy ip_frr_rp permit node 10
if-match ip-prefix fr1
apply backup-nexthop 192.168.20.2
apply backup-interface GigabitEthernet3/0/0
#
return
```

- Configuration file of Router A

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
ip address 192.168.10.2 255.255.255.0
#
interface GigabitEthernet2/0/0
ip address 192.168.11.2 255.255.255.0
#
ospf 1
```

```
area 0.0.0.0
 network 192.168.10.0 0.0.0.255
 network 192.168.11.0 0.0.0.255
#
return
```

- Configuration file of Router B

```
#
sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 192.168.20.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.21.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.20.0 0.0.0.255
  network 192.168.21.0 0.0.0.255
#
return
```

- Configuration file of Router C

```
#
sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 172.17.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.11.1 255.255.255.0
#
interface GigabitEthernet3/0/0
 ip address 192.168.21.1 255.255.255.0
 ospf cost 100
#
ospf 1
 area 0.0.0.0
  network 192.168.11.0 0.0.0.255
  network 192.168.21.0 0.0.0.255
 area 0.0.0.2
  network 172.17.1.0 0.0.0.255
#
return
```

1.6.2 Example for Configuring VRRP for Direct Routes

If VRRP for direct routes is configured, the master UPE's interface adjusts the direct route's cost based on the VRRP status. This allows the master UPE to perform a traffic switchback if recovering from a fault.

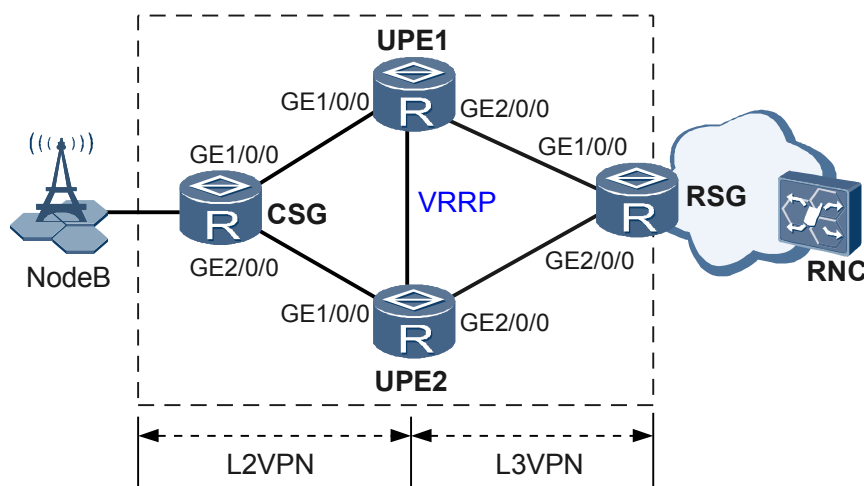
Networking Requirements

On the IP RAN shown in [Figure 1-4](#), if UPE1 recovers from a fault, its interface connected to the RSG goes Up and then a direct route is generated, allowing a traffic switchback. As UPE1 has not learned the RSG's MAC address, UPE1 fails to switch back some packets. To help prevent the problem, the direct route has to be generated after the VRRP status changes to Master.

Devices run OSPF to communicate with each other. UPE1 and UPE2 form a VRRP backup group, which functions as a default gateway for the RSG. UPE1 functions as the master and UPE2 functions as the backup. UPE2 takes over services from UPE1 if UPE1 fails. UPE1's interface connected to the RSG is associated with the VRRP backup group, enabling the cost of the direct route to the network segment where the interface resides to change based on the VRRP status. VRRP for direct routes works as follows:

- If the VRRP status becomes Backup, the direct route's cost increases, lowering the direct route's priority level. The direct route will no longer be an optimal route.
- If the VRRP status becomes Master, the direct route's cost is set to 0, allowing the direct route's priority to be the highest. The direct route will be an optimal route.

Figure 1-4 Networking diagram for configuring VRRP for direct routes



Device	Interface	IP Address	Device	Interface	IP Address
CSG	GE 1/0/0	10.1.1.1/24	UPE2	GE 1/0/0	10.1.2.2/24
	GE 2/0/0	10.1.2.1/24		GE 2/0/0	10.1.3.2/24
	Loopback0	1.1.1.1/32		Loopback0	3.3.3.3/32
UPE1	GE 1/0/0	10.1.1.2/24	RSG	Loopback0	4.4.4.4/32
	GE 2/0/0	10.1.3.1/24			
	Loopback0	2.2.2.2/32			

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure OSPF on the CSG, UPE1, UPE2, and the RSG.
2. Create backup group 1 on GE 2/0/0 of UPE1, and assign a priority higher than the default one to UPE1 so that UPE1 will function as the master.
3. Create backup group 1 on GE 2/0/0 of UPE2, and set the default priority for UPE2 so that UPE2 will function as the backup.
4. Associate GE 2/0/0 on UPE1 with backup group 1, enabling the cost of the direct route to the network segment where GE 2/0/0 resides to change based on the VRRP status.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID

- ID and virtual IP address of a VRRP backup group
- Priority level of each device in a VRRP backup group
- Link cost of an interface associated with a VRRP backup group

Procedure

Step 1 Assign IP addresses to interfaces.

Create VLAN 10 on the RSG and add GE 1/0/0 and GE 2/0/0 to VLAN 10.

```
<RSG> system-view
[RSG] interface gigabitethernet 1/0/0
[RSG-GigabitEthernet1/0/0] portswitch
[RSG-GigabitEthernet1/0/0] quit
[RSG] interface gigabitethernet 2/0/0
[RSG-GigabitEthernet2/0/0] portswitch
[RSG-GigabitEthernet2/0/0] quit
[RSG] vlan 10
[RSG-vlan10] port gigabitethernet 1/0/0
[RSG-vlan10] port gigabitethernet 2/0/0
```

Assign IP addresses to physical interfaces. For detailed configurations, see configuration files in this example.

Step 2 Configure OSPF to enable devices to communicate with each other. The details are not provided here.

Step 3 Configure a VRRP backup group.

Create backup group 1 on UPE1 and set the priority level of UPE1 to 120 so that UPE1 functions as the master.

```
<UPE1> system-view
[UPE1] interface gigabitethernet 2/0/0
[UPE1-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.3.111
[UPE1-GigabitEthernet2/0/0] vrrp vrid 1 priority 120
[UPE1-GigabitEthernet2/0/0] vrrp vrid 1 timer advertise 10
[UPE1-GigabitEthernet2/0/0] quit
```

Create backup group 1 on UPE2 and set the priority level of UPE2 to 100 (the default value) so that UPE2 functions as the backup.

```
<UPE2> system-view
[UPE2] interface gigabitethernet 2/0/0
[UPE2-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.3.111
[UPE2-GigabitEthernet2/0/0] quit
```

Step 4 Verify the configuration.

After the preceding configuration, run the **display vrrp** command on UPE1 and UPE2. You can view that the VRRP status of UPE1 is Master and the VRRP status of UPE2 is Backup. The command output on UPE1 and UPE2 is as follows:

```
[UPE1] display vrrp
GigabitEthernet2/0/0 | Virtual Router 1
  State : Master
  Virtual IP : 10.1.3.111
  Master IP : 10.1.3.1
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 120
  Preempt : YES   Delay Time : 0
  TimerRun : 10 s
  TimerConfig : 10 s
```

```

Auth Type : NONE
Virtual Mac : 0000-5e00-0102
Check TTL : YES
Config type : normal-vrrp
Create time : 2010-08-16 12:02:57
Last change time : 2010-08-17 10:27:11
[UPE2] display vrrp
GigabitEthernet2/0/0 | Virtual Router 1
  State : Backup
  Virtual IP : 10.1.3.111
  Master IP : 10.1.3.1
  PriorityRun : 100
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES Delay Time : 0
  TimerRun : 10 s
  TimerConfig : 1 s
  Auth Type : NONE
  Virtual Mac : 0000-5e00-0102
  Check TTL : YES
  Config type : normal-vrrp
  Create time : 2010-08-16 12:26:05
  Last change time : 2010-08-17 10:24:09
    
```

Run the **display ip routing-table** command on UPE1 and UPE2. You can view that a direct route to the virtual IP address of the VRRP backup group exists in the UPE1's routing table and an OSPF route to the virtual IP address of the VRRP backup group exists in the UPE2's routing table. The command output on UPE1 and UPE2 is as follows:

```

[UPE1] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 10          Routes : 11

Destination/Mask    Proto    Pre  Cost    Flags NextHop         Interface
-----
  10.1.1.0/24      Direct   0    0        D   10.1.1.2
GigabitEthernet1/0/0
  10.1.1.2/32      Direct   0    0        D   127.0.0.1         InLoopBack0
  10.1.2.0/24      OSPF     10   2        D   10.1.1.1
GigabitEthernet1/0/0
  OSPF             10   2        D   10.1.3.2
GigabitEthernet2/0/0
  10.1.3.0/24      Direct   0    0        D   10.1.3.1
GigabitEthernet2/0/0
  10.1.3.1/32      Direct   0    0        D   127.0.0.1         InLoopBack0
  10.1.3.111/32    Direct   0    0        D   127.0.0.1         InLoopBack0
  127.0.0.0/8      Direct   0    0        D   127.0.0.1         InLoopBack0
  127.0.0.1/32     Direct   0    0        D   127.0.0.1         InLoopBack0
[UPE2] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 10          Routes : 11

Destination/Mask    Proto    Pre  Cost    Flags NextHop         Interface
-----
  10.1.1.0/24      OSPF     10   2        D   10.1.2.1
GigabitEthernet2/0/0
  OSPF             10   2        D   10.1.3.1
GigabitEthernet1/0/0
  10.1.2.0/24      Direct   0    0        D   10.1.2.2
GigabitEthernet2/0/0
  10.1.2.2/32      Direct   0    0        D   127.0.0.1         InLoopBack0
  10.1.3.0/24      Direct   0    0        D   10.1.3.2
GigabitEthernet1/0/0
  10.1.3.2/32      Direct   0    0        D   127.0.0.1         InLoopBack0
  10.1.3.111/32    OSPF     10   2        D   10.1.3.1
    
```

```
GigabitEthernet1/0/0
 127.0.0.0/8   Direct 0    0          D   127.0.0.1   InLoopBack0
 127.0.0.1/32 Direct 0    0          D   127.0.0.1   InLoopBack0
```

Step 5 Associate an interface with the VRRP backup group.

Associate UPE1's GE 2/0/0 with backup group 1.

```
<UPE1> system-view
[UPE1] interface gigabitethernet 2/0/0
[UPE1-GigabitEthernet2/0/0] direct-route track vrrp vrid 1 degrade-cost 10203040
[UPE1-GigabitEthernet2/0/0] quit
```

Step 6 Verify that UPE2 becomes the master if UPE1 fails and UPE1 preempts the master after it recovers.

Run the **shutdown** command on UPE1's GE 2/0/0 to simulate a fault.

```
[UPE1] interface gigabitethernet 2/0/0
[UPE1-GigabitEthernet2/0/0] shutdown
[UPE1-GigabitEthernet2/0/0] quit
```

Run the **display vrrp** command on UPE2. You can view that the VRRP status is Master. This indicates that after UPE1 fails, UPE2 is able to become the master.

```
[UPE2] display vrrp
GigabitEthernet2/0/0 | Virtual Router 1
  State : Master
  Virtual IP : 10.1.3.111
  Master IP : 10.1.3.2
  PriorityRun : 100
  PriorityConfig : 100
  MasterPriority : 100
  Preempt : YES   Delay Time : 0
  TimerRun : 1 s
  TimerConfig : 1 s
  Auth Type : NONE
  Virtual Mac : 0000-5e00-0102
  Check TTL : YES
  Config type : normal-vrrp
  Create time : 2010-08-16 12:26:05
  Last change time : 2010-08-17 12:02:07
```

Run the **undo shutdown** and **display vrrp** commands on UPE1's GE 2/0/0. You can view that the VRRP status of UPE1 is Backup.

```
[UPE1] display vrrp
GigabitEthernet2/0/0 | Virtual Router 1
  State : Backup
  Virtual IP : 10.1.3.111
  Master IP : 10.1.3.2
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 0
  Preempt : YES   Delay Time : 0
  TimerRun : 10 s
  TimerConfig : 10 s
  Auth Type : NONE
  Virtual Mac : 0000-5e00-0102
  Check TTL : YES
  Config type : normal-vrrp
  Create time : 2010-08-16 12:02:57
  Last change time : 2010-08-17 12:05:02
```

Run the **display ip routing-table** command on UPE1 to view routing information. The cost of the direct route to 10.1.3.0/24 is 10203040. 10.1.3.0/24 is the network segment where GE 2/0/0 resides.

```
[UPE1] display ip routing-table
```



```

Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
    Destinations : 9          Routes : 9

Destination/Mask    Proto  Pre  Cost    Flags NextHop          Interface
-----
      10.1.1.0/24   Direct  0    0        D   10.1.1.2
GigabitEthernet1/0/0
      10.1.1.2/32   Direct  0    0        D   127.0.0.1          InLoopBack0
      10.1.2.0/24   OSPF   10    2        D   10.1.1.1
GigabitEthernet1/0/0
      10.1.3.0/24 Direct  0   10203040  D   10.1.3.1
GigabitEthernet2/0/0
      10.1.3.1/32   Direct  0    0        D   127.0.0.1          InLoopBack0
      127.0.0.0/8   Direct  0    0        D   127.0.0.1          InLoopBack0
      127.0.0.1/32   Direct  0    0        D   127.0.0.1          InLoopBack0
  
```

Step 7 Verify the configuration.

Wait 10 seconds for UPE1 to become the master, and run the **display ip routing-table** command on UPE1 to view routing information. The cost of the direct route to 10.1.3.0/24 becomes 0. 10.1.3.0/24 is the network segment where GE 2/0/0 resides.

```

[UPE1] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
    Destinations : 10         Routes : 11

Destination/Mask    Proto  Pre  Cost    Flags NextHop          Interface
-----
      10.1.1.0/24   Direct  0    0        D   10.1.1.2
GigabitEthernet1/0/0
      10.1.1.2/32   Direct  0    0        D   127.0.0.1          InLoopBack0
      10.1.2.0/24   OSPF   10    2        D   10.1.1.1
GigabitEthernet1/0/0
      OSPF   10    2        D   10.1.3.2
GigabitEthernet2/0/0
      10.1.3.0/24 Direct  0    0        D   10.1.3.1
GigabitEthernet2/0/0
      10.1.3.1/32   Direct  0    0        D   127.0.0.1          InLoopBack0
      10.1.3.111/32 Direct  0    0        D   127.0.0.1          InLoopBack0
      127.0.0.0/8   Direct  0    0        D   127.0.0.1          InLoopBack0
      127.0.0.1/32   Direct  0    0        D   127.0.0.1          InLoopBack0
  
```

----End

Configuration Files

- Configuration file of the CSG

```

#
sysname CSG
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
  
```

```
network 10.1.2.0 0.0.0.255
#
return
```

- Configuration file of UPE1

```
#
sysname UPE1
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.1.3.1 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.3.111
vrrp vrid 1 priority 120
vrrp vrid 1 timer advertise 10
direct-route track vrrp vrid 2 degrade-cost 10203040
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.1.3.0 0.0.0.255
#
return
```

- Configuration file of UPE2

```
#
sysname UPE2
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.1.3.2 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.3.111
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.2.2 255.255.255.0
#
interface LoopBack0
ip address 3.3.3.3 255.255.255.255
#
ospf 1
area 0.0.0.0
network 10.1.2.0 0.0.0.255
network 10.1.3.0 0.0.0.255
#
return
```

- Configuration file of the RSG

```
#
sysname RSG
#
vlan batch 10
#
interface GigabitEthernet1/0/0
portswitch
undo shutdown
port default vlan 10
#
interface GigabitEthernet2/0/0
portswitch
undo shutdown
port default vlan 10
#
interface LoopBack0
```

```
ip address 4.4.4.4 255.255.255.255  
#  
return
```

2 IP Static Route Configuration

About This Chapter

Static routes are applicable to simple networks. Properly configuring and using static routes improve the network performance and help ensure bandwidth for important services.

[2.1 Introduction of IP Static Route](#)

On a simple network, you only need to configure static routes for the network to run properly.

[2.2 Configuring an IPv4 Static Route](#)

On an IPv4 network, you can accurately control route selection by configuring IPv4 static routes.

[2.3 Configuring an IPv6 Static Route](#)

On an IPv6 network, you can accurately control route selection by configuring IPv6 static routes.

[2.4 Configuring BFD for IPv4 Static Routes on the Public Network](#)

On an IPv4 network, configuring BFD for IPv4 static routes on the public network can speed up route convergence and improve network reliability.

[2.5 Configuring BFD for IPv6 Static Routes on the Public Network](#)

On an IPv6 network, you can configure BFD for IPv6 static route on the public network to speed up route convergence and improve network reliability.

[2.6 Configuring NQA for IPv4 Static Routes](#)

On an IPv4 network, if Bidirectional Forwarding Detection (BFD) for static IPv4 routes of the public network cannot be configured because one of communicating devices does not support BFD, Network Quality Analysis (NQA) for static IPv4 routes can be configured to detect faults in links. An NQA test instance is used to detect the link status to allow a fast link switchover after a fault occurs in a link. This prevents long-time service interruption.

[2.7 Configuration Examples](#)

Static route configuration examples explain networking requirements, networking diagrams, configuration notes, configuration roadmap, and configuration procedures.

2.1 Introduction of IP Static Route

On a simple network, you only need to configure static routes for the network to run properly.

2.1.1 Static Route

Static routes are a special type of routes that need to be manually configured.

On a simple network, you only need to configure static routes so that the network can run properly. Properly using static routes improves the network performance and provides the guaranteed bandwidth for important applications.

The disadvantage of static routes is that if a fault occurs on the network or the network topology changes, static routes cannot automatically change and must be changed manually by the administrator.

2.1.2 Static Routing Features Supported by the NE80E/40E

The system supports various static routes, including IPv4 static routes, IPv6 static routes, default routes, BFD for static routes, and permanent advertisement of static routes.

IPv4 Static Route

IPv4 static routes need to be manually configured by the administrator. IPv4 static routes are applicable to simple IPv4 networks.

If the destination address of an IPv4 static route is 0.0.0.0 with the mask length being 0, this IPv4 static route is an IPv4 default route.

If the destination address of an IPv4 packet fails to match any entry in the routing table, the router uses the IPv4 default route to forward the IPv4 packet.

The NE80E/40E supports ordinary static routes and the static routes associated with Virtual Private Network (VPN) instances. The static routes associated with VPN instances are used to manage VPN routes. For details of VPN instances, see the *HUAWEI NetEngine80E/40E Router Feature Description - VPN*.

IPv6 Static Route

Similar to IPv4 static routes, IPv6 static routes need to be manually configured by the administrator. IPv6 static routes are applicable to simple IPv6 networks.

If the destination address of an IPv6 static route is ::/0 with the mask length being 0, this IPv6 static route is an IPv6 default route.

If the destination address of an IPv6 packet fails to match any entry in the routing table, the router uses the IPv6 default route to forward the IPv6 packet.

NOTE

The main differences between IPv6 static routes and IPv4 static routes are their destination addresses and next-hop addresses. The next-hop address of an IPv6 static route is an IPv6 address, whereas the next-hop address of an IPv4 static route is an IPv4 address.

Default Route

Default routes are a special type of routes. Generally, administrators can manually configure default routes. Default routes can also be generated by dynamic routing protocols such as Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS).

Default routes are used only when packets to be forwarded fail to match any entry in the routing table. In the routing table, the destination address and subnet mask of a default route are both 0.0.0.0. You can run the **display ip routing-table** command to check whether the default route is configured.

If the destination address of a packet does not match any entry in the routing table, the router uses the default route to forward this packet. If no default route exists and the destination address of the packet does not match any entry in the routing table, the packet is discarded. An Internet Control Message Protocol (ICMP) packet is then sent back to the originating host, informing that the destination host or network is unreachable.

BFD for Static Route

Unlike dynamic routing, static routing does not have a detection mechanism. If a fault occurs on the network, administrator involvement is required. Bidirectional Forwarding Detection (BFD) for static route is used to bind BFD sessions to static routes on the public network. The BFD sessions are used to detect the link status of a static route, and the system determines whether to add static routes to its IP routing table based on the detection results.

After BFD for static route is configured, each static route can be bound to a BFD session.

- When the BFD session on the link of a static route detects that the link changes from Up to Down, BFD reports the fault to the routing management (RM), and then the RM sets the route to inactive. Subsequently, the route becomes unavailable and is deleted from the routing table.
- When a BFD session is established on the link of a static route (the link changes from Down to Up), BFD reports the success to the RM, and then the RM sets the route to active. Subsequently, the route becomes available and is added to the IP routing table.

Permanent Advertisement of Static Routes

Permanent advertisement of static routes provides a low-cost and simple link detection mechanism and improves compatibility between Huawei devices and non-Huawei devices. If service traffic needs to be forwarded along a specified path, you can detect links by pinging the destination addresses of static routes. In this manner, you can monitor services at a very low cost.

2.2 Configuring an IPv4 Static Route

On an IPv4 network, you can accurately control route selection by configuring IPv4 static routes.

2.2.1 Establishing the Configuration Task

Before configuring an IPv4 static route, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

When configuring an IPv4 static route, note the following:

- Destination address and mask

In the **ip route-static** command, the IPv4 destination address is in dotted decimal notation, and the mask can be either expressed in dotted decimal notation or replaced by the mask length (namely, the number of consecutive 1s in the mask).

- Outbound interface and next-hop address

When configuring a static route, you can specify either *interface-type interface-number* or *nexthop-address* according to the actual situation.

In practice, every routing entry requires a next-hop address. When sending a packet, the router first searches for the matched route in the routing table according to the destination address. The link layer cannot find the associated link layer address to forward the packet unless the next-hop address of the packet is specified.

In some cases, for example, the link layer is encapsulated with PPP, you can also specify outbound interfaces when configuring the router even if the remote address is not known. In this manner, it is unnecessary to modify the router configuration when the remote address changes.

When specifying the outbound interface, note the following:

- For a Point-to-Point (P2P) interface, the next-hop address is specified after the outbound interface is specified. That is, the address of the remote interface (interface on the peer device) connected to this interface is the next-hop address. For example, if a POS interface is Point-to-Point Protocol (PPP) encapsulated, the peer IP address is obtained by using PPP negotiation. In this case, only the outbound interface needs to be specified.
- Non-Broadcast Multiple-Access (NBMA) interfaces (such as ATM interfaces) are applicable to Point-to-Multipoint (P2MP) networks. Therefore, you need to configure IP routes and the mappings between IP addresses and link layer addresses. In this case, a next-hop IP address needs to be configured.
- When a static route is being configured, specifying an Ethernet interface as the outbound interface is not recommended. This is because the Ethernet interface is a broadcast interface. Therefore, if the Ethernet interface is specified as the outbound interface, multiple next hops exist and the system cannot decide which next hop is to be used. In practice, when specifying a broadcast interface (such as an Ethernet interface) or Non-Broadcast Multiple-Access (NBMA) interfaces as the outbound interface, you must specify the associated next-hop address.

- Other attributes

Setting different preferences for static routes helps flexibly apply routing policies. For example, when configuring multiple routes to the same destination address, you can set the same preference for these routes to implement load balancing. You can also set different preferences to implement routing redundancy.

When the **ip route-static** command is run to configure a static route, if the destination address and the mask are set to all 0s (0.0.0.0 0.0.0.0), it indicates that a default route is configured.

Pre-configuration Tasks

Before configuring an IPv4 static route, complete the following task:

- Configuring link layer protocol parameters and IP addresses for interfaces to ensure that the link layer protocol status of the interfaces is Up

Data Preparation

To configure an IPv4 static route, you need the following data.

No.	Data
1	Destination address and mask
2	Outbound interface or next-hop IPv4 address
3	Preference of the IPv4 static route

2.2.2 Configuring an IPv4 Static Route

When configuring an IPv4 static route, you need to correctly configure its destination address, outbound interface, and next hop.

Context

Do as follows on the router to be configured with static route:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip route-static ip-address { mask | mask-length } { nexthop-address | interface-  
type interface-number [ nexthop-address ] | vpn-instance vpn-instance-name nexthop-  
address } [ preference preference | tag tag ] * [ description text ]
```

An IPv4 static route is configured.

By default, no IPv4 static route is configured.

----End

2.2.3 (Optional) Setting the Default Preference for IPv4 Static Routes

Setting the default preference for IPv4 static routes can affect route selection.

Context

Do as follows on the routers that need to be configured with static routes and change the default priority for static routes:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip route-static default-preference preference
```

The default preference is set for static routes.

By default, the preference of static routes is 60.

When a static route is configured, the default preference is used if no preference is explicitly specified for the static route. After a default preference is specified, the new default preference is valid for subsequent rather than existing IPv4 static routes.

---End

2.2.4 (Optional) Configuring Static Route Selection Based on Relay Depth

After static route selection based on relay depths is configured, the static route module selects the static route with the smallest relay depth as the active route and delivers it to the FIB table. The other routes become inactive.

Context

After static routes are configured, multiple static routes with the same prefix and preference but different relay depths exist. After static route selection based on relay depths is configured, the static route module selects the route with the smallest relay depth as the active route and delivers it to the Forwarding Information Base (FIB) table. The other routes become inactive.

Do as follows on the router to be configured with static routes:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip route-static selection-rule relay-depth
```

Static route selection based on relay depths is configured.

By default, static routes are not selected according to relay depths.

---End

2.2.5 (Optional) Configuring Permanent Advertisement of IPv4 Static Routes

Permanent advertisement of static routes provides a low-cost and simple link detection mechanism and improves the compatibility between Huawei devices and non-Huawei devices.

Context

Link connectivity directly affects the stability and availability of a network, and thus link status detection plays an important role in network maintenance. If service traffic needs to be forwarded along a specified path, you can detect the status of the path through a ping operation. In this manner, you can monitor services at a very low cost.

With permanent advertisement of static routes, you can detect link connectivity by pinging the destination addresses of static routes. After permanent advertisement of static routes is configured, static routes always take effect regardless of the outbound interface status. In this case, the system forwards Ping packets along a specified path only. This helps detect the link status of the specified path.

Do as follows on the router where IPv4 static routes need to be configured.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip route-static ip-address { mask | mask-length } { nexthop-address | interface-  
type interface-number [ nexthop-address ] | vpn-instance vpn-instance-name nexthop-  
address } permanent
```

Permanent advertisement of IPv4 static routes is configured.

By default, permanent advertisement of IPv4 static routes is not configured.

----End

2.2.6 Configuring Static IPv4 Routes in a Topology Instance

By properly configuring static IPv4 routes in a simple topology instance, you can improve the network performance and provide the guaranteed bandwidth for important services.

Context

Before configuring multi-topology on a network, you need to create a topology instance. By properly configuring static IPv4 routes in a simple topology instance, you can improve the network performance and provide the guaranteed bandwidth for important services.

Do as follows on the router where static IPv4 routes need to be configured:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run either of the following commands as required:

● Run:

```
ip route-static ip-address { mask | mask-length } { nexthop-address | interface-  
type interface-number [ nexthop-address ] | vpn-instance vpn-instance-name  
nexthop-address } [ preference preference | tag tag ] * [ description text ]
```

Static IPv4 routes are configured in a base topology instance.

- Run:

```
ip route-static topology topology-name ip-address { mask | mask-length }  
{ nexthop-address | interface-type interface-number [ nexthop-address ] }  
[ preference preference | tag tag ] * [ description text ]
```

Static IPv4 routes are configured in another topology instance.

By default, no static IPv4 routes are configured in a topology instance.

----End

2.2.7 Checking the Configuration

After an IPv4 static route is configured, you can check detailed information about the configured IPv4 static route.

Prerequisite

The configurations of an IPv4 static route are complete.

Procedure

- Run the **display ip routing-table** command to check brief information about the IPv4 routing table.
- Run the **display ip routing-table verbose** command to check detailed information about the IPv4 routing table.

----End

2.3 Configuring an IPv6 Static Route

On an IPv6 network, you can accurately control route selection by configuring IPv6 static routes.

2.3.1 Establishing the Configuration Task

Before configuring an IPv6 static route, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

On a small IPv6 network, you can implement network interconnection by configuring IPv6 static routes. Compared with using dynamic routes, using static routes saves the bandwidth.

Pre-configuration Tasks

Before configuring an IPv6 static route, complete the following task:

- Configuring link layer protocol parameters and IP addresses for interfaces to ensure that the link layer protocol status of the interfaces is Up

Data Preparation

To configure an IPv6 static route, you need the following data.

No.	Data
1	Destination address and mask
2	Outbound interface or next-hop IPv6 address
3	Preference of the IPv6 static route

2.3.2 Configuring an IPv6 Static Route

When configuring an IPv6 static route, you need to correctly configure its destination address, outbound interface, and next hop.

Context

Do as follows on the router to be configured with static routes:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ipv6 route-static dest-ipv6-address prefix-length { interface-type interface-  
number | nexthop-ipv6-address } [ preference preference | tag tag ] *  
[ description text ]
```

An IPv6 static route is configured.

When configuring a static route, you need to specify either the outbound interface or the next-hop address according to the actual situation. If the outbound interface is a PPP interface, you can simply specify the outbound interface. If the outbound interface is a non-P2P interface, you must also specify the next-hop address in addition to specifying the outbound interface.

If **preference** is not specified, the default preference is 60.

By default, no IPv6 static route is configured.

---End

2.3.3 (Optional) Setting the Default Preference for IPv6 Static Routes

By setting the default preference for an IPv6 static route, you can change the preference of the static route.

Context

Do as follows on the router that need to be configured with IPv6 static routes and change the default priority for IPv6 static routes:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ipv6 route-static default-preference preference
```

The default preference of IPv6 static routes is set.

By default, the preference of IPv6 static routes is 60.

When an IPv6 static route is configured, the default preference is used if the preference of the static route is not explicitly specified. After the default preference is specified, the default preference is valid for subsequent rather than existing IPv6 static routes.

----End

2.3.4 Configuring Static IPv6 Routes in a Topology Instance

By properly configuring static IPv6 routes in a simple topology instance, you can improve the network performance and provide the guaranteed bandwidth for important services.

Context

Before configuring multi-topology on a network, you need to create a topology instance. By properly configuring static IPv6 routes in a simple topology instance, you can improve the network performance and provide the guaranteed bandwidth for important services.

Do as follows on the router where static IPv6 routes need to be configured:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run either of the following commands as required:

● Run:

```
ipv6 route-static dest-ipv6-address prefix-length { interface-type interface-number [ nexthop-ipv6-address ] | nexthop-ipv6-address } [ preference preference | tag tag ] * [ description text ]
```

Static IPv6 routes are configured in a base topology instance.

● Run:

```
ipv6 route-static topology topology-name dest-ipv6-address prefix-length { interface-type interface-number [ nexthop-ipv6-address ] | nexthop-ipv6-address } [ preference preference | tag tag ] * [ description text ]
```

Static IPv6 routes are configured in another topology instance.

By default, no static IPv6 routes are configured in a topology instance.

----End

2.3.5 Checking the Configuration

After an IPv6 static route is configured, you can check detailed information about the configured route.

Prerequisite

The configurations of an IPv6 static route are complete.

Procedure

- Run the **display ipv6 routing-table** command to check brief information about the IPv6 routing table.
- Run the **display ipv6 routing-table verbose** command to check detailed information about the IPv6 routing table.

---End

2.4 Configuring BFD for IPv4 Static Routes on the Public Network

On an IPv4 network, configuring BFD for IPv4 static routes on the public network can speed up route convergence and improve network reliability.

2.4.1 Establishing the Configuration Task

Before configuring BFD for static routes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

BFD can rapidly detect IPv4 forwarding failures, ensuring QoS for voice, video, and other video-on-demand (VoD) services on an IPv4 network. With BFD, service providers can provide voice over IP (VoIP) and other real-time services with high availability and scalability.

By binding IPv4 static routes to BFD sessions, you can use BFD sessions to provide link detection for IPv4 static routes on the public network. A static route can be bound to a BFD session.

Pre-configuration Tasks

Before configuring BFD for IPv4 static routes on the public network, complete the following task:

- Configuring link layer protocol parameters and IP addresses for interfaces to ensure that the link layer protocol status of the interfaces is Up

Data Preparation

To configure BFD for IPv4 static routes on the public network, you need the following data.

No.	Data
1	Destination address and mask
2	Outbound interface or next-hop IPv4 address
3	IP address of the peer detected by BFD
4	Local discriminator and remote discriminator of a BFD session

2.4.2 Configuring an IPv4 Static Route

When configuring an IPv4 static route, you need to correctly configure its destination address, outbound interface, and next hop.

Context

Do as follows on the router to be configured with static route:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip route-static ip-address { mask | mask-length } { nexthop-address | interface-  
type interface-number [ nexthop-address ] | vpn-instance vpn-instance-name nexthop-  
address } [ preference preference | tag tag ] * [ description text ]
```

An IPv4 static route is configured.

By default, no IPv4 static route is configured.

----End

2.4.3 Configuring a BFD Session

BFD sessions are used to rapidly detect and monitor the connectivity of links on a network.

Background

See the *HUAWEI NetEngine80E/40E Router Configuration Guide - Reliability*.

2.4.4 Binding a Static Route to a BFD Session

When binding a static route to a BFD session, ensure that the static route resides on the same link as the BFD session.

Context

Do as follows on the router to bind a static route to a BFD session:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip route-static ip-address { mask | mask-length } { nexthop-address | interface-  
type interface-number [ nexthop-address ] } [ preference preference | tag tag ] *  
track bfd-session cfg-name [ description text ]
```

A BFD session is bound to the IPv4 static route on the public network.

NOTE

When binding a static route to a BFD session, ensure that the static route resides on the same link as the BFD session.

NOTE

Ensure that the BFD session to which a static route will be bound is not a non-IP BFD session. A non-IP BFD session can be created using one of the following commands:

- `bfd bind ldp-lsp`
- `bfd bind mpls-te`
- `bfd bind pw`
- `bfd bind static-lsp`
- `bfd bind peer-ip default-ip vsi`

----End

2.4.5 Checking the Configuration

After BFD for static route is configured, you can check BFD session information and information about BFD for static route.

Prerequisite

The configurations of BFD for IPv4 static routes are complete.

Procedure

- Run the `display bfd session { all | discriminator discr-value } [verbose] [slot slot-id]` command to check BFD session information.
- Run the `display current-configuration | include bfd` command to check the configuration of BFD for static routes.

You can check information about a BFD session only after parameters of the BFD session are set and the BFD session is established.

If BFD session negotiation succeeds, you can view that the status of the BFD session is Up. You can also view that the BFD session is bound to the static route by running the `display current-configuration | include bfd` command in the system view.

----End

2.5 Configuring BFD for IPv6 Static Routes on the Public Network

On an IPv6 network, you can configure BFD for IPv6 static route on the public network to speed up route convergence and improve network reliability.

2.5.1 Establishing the Configuration Task

Before configuring BFD for static route, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

IPv6 BFD can rapidly detect IPv6 forwarding failures, ensuring QoS for voice, video, and other video-on-demand (VoD) services on an IPv6 network. With IPv6 BFD, service providers can provide voice over IP (VoIP) and other real-time services with high availability and scalability.

By binding IPv6 static routes to BFD sessions, you can use BFD sessions to provide link detection for IPv6 static routes on the public network. A static route can be bound to a BFD session.

Pre-configuration Tasks

Before configuring BFD for IPv6 static routes on the public network, complete the following task:

- Configuring link layer protocol parameters and IPv6 addresses for interfaces to ensure that the link layer protocol status of the interfaces is Up

Data Preparation

To configure BFD for IPv6 static routes on the public network, you need the following data.

No.	Data
1	Destination address and prefix
2	Outbound interface or next-hop IPv6 address
3	Peer IPv6 address to be detected by BFD
4	Local discriminator and remote discriminator of a BFD session

2.5.2 Configuring an IPv6 Static Route

When configuring an IPv6 static route, you need to correctly configure its destination address, outbound interface, and next hop.

Context

Do as follows on the router to be configured with static routes:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ipv6 route-static dest-ipv6-address prefix-length { interface-type interface-  
number | nexthop-ipv6-address } [ preference preference | tag tag ] *  
[ description text ]
```

An IPv6 static route is configured.

When configuring a static route, you need to specify either the outbound interface or the next-hop address according to the actual situation. If the outbound interface is a PPP interface, you can simply specify the outbound interface. If the outbound interface is a non-P2P interface, you must also specify the next-hop address in addition to specifying the outbound interface.

If **preference** is not specified, the default preference is 60.

By default, no IPv6 static route is configured.

----End

2.5.3 Configuring a BFD Session

BFD sessions are used to rapidly detect and monitor the connectivity of links on a network.

Background

For details, see the *HUAWEI NetEngine80E/40E Router Configuration Guide - Reliability*.

2.5.4 Binding a Static Route to a BFD Session

When binding a static route to a BFD session, ensure that the static route resides on the same link as the BFD session.

Context

Do as follows on the router to bind a static route to a BFD session:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ipv6 route-static dest-ipv6-address prefix-length { interface-type interface-  
number [ nexthop-ipv6-address ] | nexthop-ipv6-address } [ preference preference ]  
[ tag tag ] * [ track bfd-session cfg-name ] [ description text ]
```

The IPv6 static route on the public network is bound to a BFD session.

 **NOTE**

When binding a static route to a BFD session, ensure that the static route resides on the same link as the BFD session.

----End

2.5.5 Checking the Configuration

After BFD for static route is configured, you can check BFD session information and information about BFD for static route.

Prerequisite

The configurations of BFD for IPv6 static routes on the public network are complete.

Procedure

- Run the **display bfd session** { **all** | **discriminator** *discr-value* } [**verbose**] [**slot** *slot-id*] command to check BFD session information.
- Run the **display current-configuration** | **include bfd** command to check the configuration of BFD for static routes.

You can view BFD session information only after BFD session parameters are set and a BFD session is established.

If BFD session negotiation succeeds, you can view that the status of the BFD session is Up. You can also view that static routes are bound to BFD sessions by running the **display current-configuration** | **include bfd** command in the system view.

----End

2.6 Configuring NQA for IPv4 Static Routes

On an IPv4 network, if Bidirectional Forwarding Detection (BFD) for static IPv4 routes of the public network cannot be configured because one of communicating devices does not support BFD, Network Quality Analysis (NQA) for static IPv4 routes can be configured to detect faults in links. An NQA test instance is used to detect the link status to allow a fast link switchover after a fault occurs in a link. This prevents long-time service interruption.

2.6.1 Establishing the Configuration Task

Before configuring NQA for static IPv4 routes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This will help you complete the configuration task quickly and accurately.

Applicable Environment

In real world situations, the link status is monitored for network stability. If an active link fails, traffic switches to a standby link to ensure non-stop traffic forwarding. The Address Resolution Protocol (ARP) probe function and BFD are usually used to detect link faults. In addition, Interior Gateway Protocol (IGP) convergence helps reveal link faults. Under certain circumstances, the preceding methods are unsuitable. For example:

- If only one link, not every link, on the network needs to be monitored, the ARP detection is unsuitable.
- If any device on the network does not support BFD, BFD is unavailable.
- If either end of a link is a Layer 2 device, dynamic routing protocols cannot be deployed, and thus no IGP convergence occurs.

In these situations, NQA for static IPv4 routes can be configured to detect link faults. It can be used to detect faults in links where Layer 2 devices reside and take effect even if only one of the two communicating devices supports NQA.

If a fault occurs, an NQA test instance can immediately detect the fault and instruct the system to delete the associated static route from the IP routing table. Traffic is then forwarded along another path.

Pre-configuration Tasks

Before configuring NQA for static IPv4 routes, complete the following task:

- Configuring link layer protocol parameters and IP addresses for interfaces to ensure that the link layer protocol on the interfaces is Up

Data Preparation

To configure NQA for static IPv4 routes, you need the following data.

No.	Data
1	Administrator name and name of an NQA test instance
2	Destination IP address of the NQA test instance
3	Destination network address and mask
4	Next hop IPv4 address or outbound interface for a static route

2.6.2 Configuring an ICMP Type NQA Test Instance

NQA is an effective tool for locating and diagnosing network faults.

Context

NQA measures the performance of different protocols running on a network. With NQA, carriers can collect the operation indexes of networks in real time, for example, total delay of the Hypertext Transfer Protocol (HTTP), delay in the Transfer Control Protocol (TCP) connection, delay in Domain Name Server (DNS) resolution, file transmission rate, delay in the File Transfer Protocol (FTP) connection, and DNS resolution error ratio. To check these performance indexes, you can create NQA test instances.

An NQA test is performed between a client and a server. The client is responsible for initiating an NQA test. After test instances are configured on the client, NQA places these test instances into test instance queues according to their operation types. After the test instances are started, data information about the protocol-related running status can be collected according to the return packets.

An Internet Control Messages Protocol (ICMP) NQA test instance checks whether a route from the NQA client to the destination is reachable. The ICMP NQA test has a similar function as the **ping** command and provides more detailed output:

- By default, the output contains the results of the latest five tests.
- The test result contains information including the average delay, packet loss ratio, and time when the last packet is correctly received.

An ICMP NQA test instance sends packets at a minimum interval of 1 second. This ensures that NQA reports the test results to the system when a link fault is detected and when the link fault is rectified. For details about NQA, see the chapter "NQA Configuration" in the *HUAWEI NetEngine80E/40E Router Configuration Guide - System Management*.

Do as follows on the NQA client:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
nqa test-instance admin-name test-name
```

An NQA test instance is created and the test instance view is displayed.

Step 3 Run:

```
test-type icmp
```

The test type is set to ICMP.

Step 4 Run:

```
destination-address ipv4 ip-address
```

The destination address is specified for the NQA test instance.

Step 5 (Optional) Run:

```
frequency interval
```

The interval for automatically performing an NQA test is set. By default, no interval is set, and only one test is performed.

Step 6 (Optional) Run:

```
probe-count number
```

The number of probes to be sent each time is set for the NQA test instance. By default, three probes are sent each time.

After probes are sent multiple times for the NQA test instance, you can estimate the network quality more accurately based on the collected statistics.

Step 7 Run:

```
start
```

The NQA test instance is started.

Run one of the following commands as required:

- To start an NQA test immediately, run the **start now** [**end** { **at** [*yyyy/mm/dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } }] command.
- To start an NQA test at a specified time, run the **start at** [*yyyy/mm/dd*] *hh:mm:ss* [**end** { **at** [*yyyy/mm/dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } }] command.
- To start an NQA test after a certain period of time, run the **start delay** { **seconds** *second* | *hh:mm:ss* } [**end** { **at** [*yyyy/mm/dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } }] command.

----End

2.6.3 Binding an IPv4 Static Route to an NQA Test Instance

If a static IPv4 route is associated with an NQA test instance, NQA tests the link status periodically. After NQA detects a fault in the link related to the associated static route, the static route is deleted and traffic diverts to another path.

Context

On a network with a simple topology, configuring static routes allows the network to work properly. Static routes can also be configured on a router that cannot run dynamic routing protocols to generate routes to the destination. Unlike dynamic routing protocols, static routes do not have a dedicated detection mechanism. Static routes cannot detect faults in the network, which probably causes traffic loss.

The NQA for static IPv4 routes feature allows static IPv4 routes to be associated with NQA test instances. The ping function of NQA test instances is used to check the status of links through which static routes pass. If a fault occurs in the link for a static route, the system deletes the static route to force traffic transmitted based on this route to divert to another path.

Do as follows on the router that requires NQA for static IPv4 routes:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip route static ip-address { mask | mask-length } { nexthop-address | interface-  
type interface-number [ nexthop-address ] } [ preference preference | tag tag ] *  
track nqa admin-name test-name [ description text ]
```

A static IPv4 route is associated with an NQA test instance.

NOTE

The destination address of an NQA test instance cannot be the destination address of an associated static route.

If the static route associated with one NQA test instance is associated with another NQA test instance, the association between the static route and the former NQA test instance is automatically removed.

----End

2.6.4 Checking the Configuration

After associating an NQA test instance with a static route, you can check NQA test results and information about the association between the static route and the NQA test instance.

Prerequisite

The configurations of NQA for static IPv4 routes are complete.



NOTE

NQA test results cannot be displayed automatically on the terminal. To check NQA test results, run the **display nqa results** command. By default, the command output shows the results of the latest five tests.

Procedure

Step 1 Run the **display current-configuration | include nqa** command to check configurations about NQA for static IPv4 routes.

Step 2 Run the **display nqa results [test-instance admin-name test-name]** command to check NQA test results.

---End

Example

After associating a static route to an NQA test instance, run the **display current-configuration | include nqa** command in the system view. The command output shows that the static route has been associated with the NQA test instance. For example:

```
<HUAWEI> display current-configuration | include nqa
ip route-static 172.16.1.3 255.255.255.255 GigabitEthernet1/0/0 track nqa admin
icmp
nqa test-instance admin icmp
```

Run the **display nqa results** command. If the following information is displayed, it means that the test succeeds:

- testflag is active
- testtype is icmp
- The test is finished
- Completion:success

For example:

```
<HUAWEI> display nqa results test-instance admin icmp
NQA entry(admin, icmp) :testflag is active ,testtype is icmp
1 . Test 206 result The test is finished
Send operation times: 15 Receive response times: 15
Completion:success RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:172.16.1.2
Min/Max/Average Completion Time: 30/50/35
Sum/Square-Sum Completion Time: 530/19900
Last Good Probe Time: 2010-10-25 15:39:57.1
Lost packet ratio: 0 %
```

For an ICMP NQA test, the minimum, maximum, and average time for receiving ICMP Echo-Reply packets are displayed, that is, **Min/Max/Average Completion Time**. In addition, the

NQA test packet loss ratio is displayed, which help determine the link status. In this example, the packet loss ratio is 0, indicating that the link works properly.

2.7 Configuration Examples

Static route configuration examples explain networking requirements, networking diagrams, configuration notes, configuration roadmap, and configuration procedures.

NOTE

Examples in this document use interface numbers and link types of the NE40E-X8. In real world situations, the interface numbers and link types may be different from those used in this document.

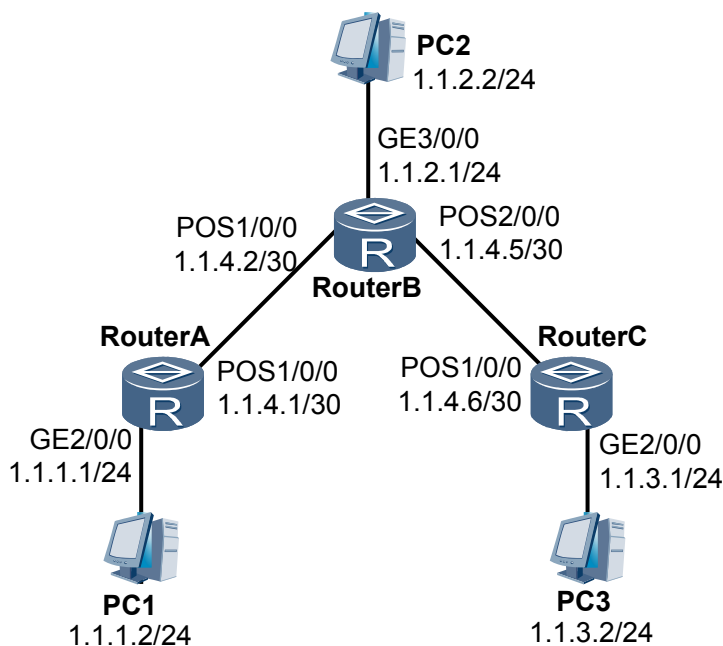
2.7.1 Example for Configuring IPv4 Static Routes

You can configure IPv4 static routes to interconnect any two devices on an IPv4 network.

Networking Requirements

Figure 2-1 shows IP addresses and masks of interfaces and hosts. It is required to interconnect any two hosts in **Figure 2-1**.

Figure 2-1 Networking diagram for configuring IPv4 static routes



Because dynamic routing protocols cannot be configured on PC1, PC2 and PC3 in **Figure 2-1**, so we configure static routes on the routers in this example.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IPv4 address for each interface on each router for interworking.
2. Configure an IPv4 static route and a default route to the destination address on each router.
3. Configure an IPv4 default gateway on each host to make any two hosts communicate.

Data Preparation

To complete the configuration, you need the following data:

- Default route with the next hop being 1.1.4.2 of Router A
- Static route with the destination address and next hop being 1.1.1.0 and 1.1.4.1 respectively of Router B
- Static route with the destination address and next hop being 1.1.3.0, and 1.1.4.6 respectively of Router B
- Default route with the next hop being 1.1.4.5 of Router C
- Default gateway addresses of PC1, PC2, and PC3 being 1.1.1.1, 1.1.2.1, and 1.1.3.1 respectively

Procedure

Step 1 Configure an IP address for each interface.

The configuration details are not described here.

Step 2 Configure static routes.

Configure an IPv4 default route on Router A.

```
[RouterA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
```

Configure two IPv4 static routes on Router B.

```
[RouterB] ip route-static 1.1.1.0 255.255.255.0 1.1.4.1
[RouterB] ip route-static 1.1.3.0 255.255.255.0 1.1.4.6
```

Configure an IPv4 default route on Router C.

```
[RouterC] ip route-static 0.0.0.0 0.0.0.0 1.1.4.5
```

Step 3 Configure hosts.

Set default gateway addresses of PC1, PC2, and PC3 to 1.1.1.1, 1.1.2.1, and 1.1.3.1 respectively.

Step 4 Verify the configuration.

Check the IP routing table of Router A.

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 7          Routes : 7
Destination/Mask    Proto  Pre  Cost  Flags  NextHop          Interface
0.0.0.0/0           Static 60   0      RD     1.1.4.2          Pos1/0/0
1.1.1.0/24          Direct 0     0      D      1.1.1.1          GigabitEthernet2/0/0
1.1.1.1/32          Direct 0     0      D      127.0.0.1        InLoopBack0
1.1.4.0/30          Direct 0     0      D      1.1.4.1          Pos1/0/0
1.1.4.1/32          Direct 0     0      D      127.0.0.1        InLoopBack0
1.1.4.2/32          Direct 0     0      D      1.1.4.2          Pos1/0/0
127.0.0.0/8         Direct 0     0      D      127.0.0.1        InLoopBack0
```

```
127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
```

Run the **ping** command to verify the connectivity.

```
[RouterA] ping 1.1.3.1
PING 1.1.3.1: 56 data bytes, press CTRL_C to break
  Reply from 1.1.3.1: bytes=56 Sequence=1 ttl=254 time=62 ms
  Reply from 1.1.3.1: bytes=56 Sequence=2 ttl=254 time=63 ms
  Reply from 1.1.3.1: bytes=56 Sequence=3 ttl=254 time=63 ms
  Reply from 1.1.3.1: bytes=56 Sequence=4 ttl=254 time=62 ms
  Reply from 1.1.3.1: bytes=56 Sequence=5 ttl=254 time=62 ms
--- 1.1.3.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 62/62/63 ms
```

Run the **tracert** command to verify the connectivity.

```
[RouterA] tracert 1.1.3.1
traceroute to 1.1.3.1(1.1.3.1), max hops: 30 ,packet length: 40,press CTRL_C t o
break
 1 1.1.4.2 31 ms 32 ms 31 ms
 2 1.1.4.6 62 ms 63 ms 62 ms
```

---End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
 interface GigabitEthernet2/0/0
 ip address 1.1.1.1 255.255.255.0
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 1.1.4.1 255.255.255.252
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
#
 return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
 interface GigabitEthernet3/0/0
 ip address 1.1.2.1 255.255.255.0
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 1.1.4.2 255.255.255.252
#
 interface Pos2/0/0
 link-protocol ppp
 ip address 1.1.4.5 255.255.255.252
#
 ip route-static 1.1.1.0 255.255.255.0 1.1.4.1
 ip route-static 1.1.3.0 255.255.255.0 1.1.4.6
#
 return
```

- Configuration file of Router C

```
#
 sysname RouterC
#
```

```

interface GigabitEthernet2/0/0
 ip address 1.1.3.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol ppp
 ip address 1.1.4.6 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0 1.1.4.5
#
return
    
```

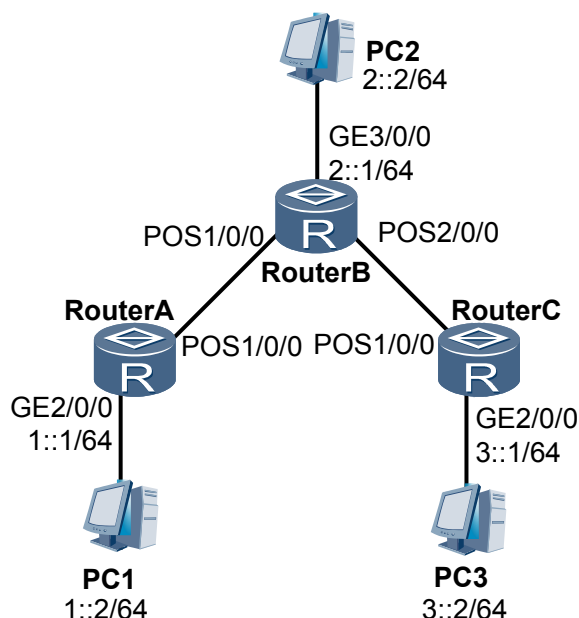
2.7.2 Example for Configuring IPv6 Static Routes

You can configure IPv6 static routes to interconnect any two devices on an IPv6 network.

Networking Requirements

As shown in [Figure 2-2](#), the mask length of all the IPv6 addresses is 64 bits. It is required that every two hosts or routers be interconnected.

Figure 2-2 Networking diagram for configuring IPv6 static routes



Because dynamic routing protocols cannot be configured on PC1, PC2 and PC3 in [Figure 2-2](#), so we configure static routes on the routers in this example. Addresses of POS interfaces on the routers are IPv6 link-local addresses.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IPv6 address for each GE interface on each router for interworking.
2. Configure an IPv6 static route and a default route to the destination address on each router.
3. Configure an IPv6 default gateway on each host to make any two hosts communicate.

Data Preparation

To complete the configuration, you need the following data:

- Default route with the outbound interface being POS 1/0/0 of Router A
- Static route with the destination address and outbound interface being 1:: 64 and POS 1/0/0 respectively of Router B
- Static route with the destination address and outbound interface being 3:: 64 and POS 2/0/0 respectively of Router B
- Default route with the outbound interface being POS 1/0/0 of Router C
- Default gateway addresses of PC1, PC2, and PC3 being 1::1, 2::1, and 3::1 respectively

Procedure

Step 1 Configure an IPv6 address for each interface.

The configuration details are not described here.

Step 2 Configure IPv6 static routes.

Configure an IPv6 default route on Router A.

```
[RouterA] ipv6 route-static :: 0 pos 1/0/0
```

Configure two IPv6 static routes on Router B.

```
[RouterB] ipv6 route-static 1:: 64 pos 1/0/0
```

```
[RouterB] ipv6 route-static 3:: 64 pos 2/0/0
```

Configure an IPv6 default route on Router C.

```
[RouterC] ipv6 route-static :: 0 pos 1/0/0
```

Step 3 Configure host addresses and gateways.

Configure IPv6 addresses for hosts according to the networking diagram, and set default gateway addresses of PC1, PC2, and PC3 to 1::1, 2::1, and 3::1 respectively.

Step 4 Verify the configuration.

Check the IPv6 routing table of Router A.

```
[RouterA] display ipv6 routing-table
```

```
Routing Table : Public
```

```
Destinations : 5          Routes : 5
```

```

Destination : ::
NextHop     : FE80::E0:FCD5:A2BF:401
Cost       : 0
RelayNextHop : ::
Interface  : Pos1/0/0
PrefixLength : 0
Preference : 60
Protocol   : Static
TunnelID   : 0x0
Flags      : D

```

```

Destination : ::1
NextHop     : ::1
Cost       : 0
RelayNextHop : ::
Interface  : InLoopBack0
PrefixLength : 128
Preference : 0
Protocol   : Direct
TunnelID   : 0x0
Flags      : D

```

```

Destination : 1::
NextHop     : 1::1
Cost       : 0
RelayNextHop : ::
Interface  : GigabitEthernet2/0/0
PrefixLength : 64
Preference : 0
Protocol   : Direct
TunnelID   : 0x0
Flags      : D

```

```

Destination : 1::1                PrefixLength : 128
NextHop     : ::1                Preference   : 0
Cost       : 0                  Protocol     : Direct
RelayNextHop : ::                TunnelID    : 0x0
Interface  : InLoopBack0        Flags       : D

Destination : FE80::             PrefixLength : 10
NextHop     : ::                Preference   : 0
Cost       : 0                  Protocol     : Direct
RelayNextHop : ::                TunnelID    : 0x0
Interface  : NULL0             Flags       : D
    
```

Run the **ping** command to verify the connectivity.

```

[RouterA] ping ipv6 3::1
PING 3::1 : 56 data bytes, press CTRL_C to break
  Reply from 3::1
    bytes=56 Sequence=1 hop limit=254 time = 63 ms
  Reply from 3::1
    bytes=56 Sequence=2 hop limit=254 time = 62 ms
  Reply from 3::1
    bytes=56 Sequence=3 hop limit=254 time = 62 ms
  Reply from 3::1
    bytes=56 Sequence=4 hop limit=254 time = 63 ms
  Reply from 3::1
    bytes=56 Sequence=5 hop limit=254 time = 63 ms
--- 3::1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 62/62/63 ms
    
```

Run the **tracert** command to verify the connectivity.

```

[RouterA] tracert ipv6 3::1
traceroute to 3::1 30 hops max,60 bytes packet
 1 FE80::E0:FCD5:86D4:401 11 ms 3 ms 4 ms
 2 3::1 4 ms 3 ms 3 ms
    
```

----End

Configuration Files

- Configuration file of Router A

```

#
 sysname RouterA
#
 ipv6
#
 interface GigabitEthernet2/0/0
  ipv6 address 1::1/64
#
 interface Pos1/0/0
  link-protocol ppp
  ipv6 address auto link-local
#
 ipv6 route-static :: 0 Pos 1/0/0
#
 return
    
```

- Configuration file of Router B

```

#
 sysname RouterB
#
 ipv6
#
 interface GigabitEthernet3/0/0
    
```

```

        ipv6 address 2::1/64
    #
    interface Pos1/0/0
        link-protocol ppp
        ipv6 address auto link-local
    #
    interface Pos2/0/0
        link-protocol ppp
        ipv6 address auto link-local
    #
    ipv6 route-static 1:: 64 Pos1/0/0
    ipv6 route-static 3:: 64 Pos1/0/1
    #
    return
    
```

- Configuration file of Router C

```

    #
    sysname RouterC
    #
    ipv6
    #
    interface GigabitEthernet2/0/0
        ipv6 address 3::1/64
    #
    interface Pos1/0/0
        link-protocol ppp
        ipv6 address auto link-local
    #
    ipv6 route-static :: 0 Pos1/0/0
    #
    return
    
```

2.7.3 Example for Configuring BFD for IPv4 Static Routes

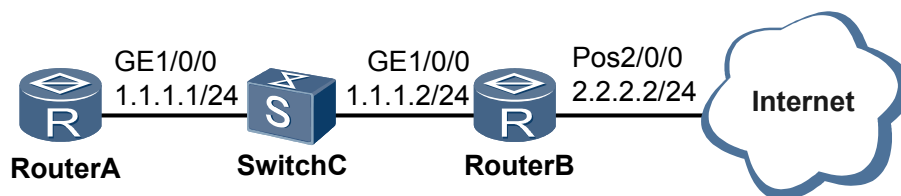
To improve network reliability, you can configure BFD for static route to rapidly detect link faults and speed up route convergence.

Networking Requirements

As shown in [Figure 2-3](#):

- Router A is connected to Router B through Switch C.
- It is required that Router A can communicate with other routers and the network.
- a BFD session is configured between Router A and Router B to detect the link between the two devices.

Figure 2-3 Networking diagram for configuring BFD for IPv4 static routes



Because the network topology is very simple, so static routes can be configured to make Router A communicate with other Routers and the network. By binding BFD sessions to static routes, BFD sessions can detect the link status, which provides the detection mechanism for static routes.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a BFD session between Router A and Router B to detect the link between the two devices.
2. Configure a default static route from Router A to the external network and bind the default static route to the BFD session.

Data Preparation

To complete the configuration, you need the following data:

- Peer IP address to be detected by BFD
- Local discriminator and remote discriminator of a BFD session
- Default values of BFD parameters, including minimum intervals for sending and receiving BFD control packets and local detection multiplier

Procedure

Step 1 Configure an IP address for each interface.

The configuration details are not described here.

Step 2 Configure a BFD session between Router A and Router B.

On Router A, configure a BFD session with Router B.

```
<RouterA> system-view
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd aa bind peer-ip 1.1.1.2
[RouterA-bfd-session-aa] discriminator local 10
[RouterA-bfd-session-aa] discriminator remote 20
[RouterA-bfd-session-aa] commit
[RouterA-bfd-session-aa] quit
```

On Router B, configure a BFD session with Router A.

```
<RouterB> system-view
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd bb bind peer-ip 1.1.1.1
[RouterB-bfd-session-bb] discriminator local 20
[RouterB-bfd-session-bb] discriminator remote 10
[RouterB-bfd-session-bb] commit
[RouterB-bfd-session-bb] quit
```

Step 3 Configure a default static route and bind it to a BFD session.

On Router A, configure a default static route to the external network and bind it to a BFD session named **aa**.

```
[RouterA] ip route-static 0.0.0.0 0 1.1.1.2 track bfd-session aa
```

Step 4 Verify the configuration.

After the configuration, run the **display bfd session all** command on Router A and Router B. The command output shows that a BFD session has been established and is in the Up state. Then, run the **display current-configuration | include bfd** command in the system view. The command output shows that the default static route has been bound to the BFD session.

Take the display on Router A as an example.

```
[RouterA] display bfd session all
-----
Local  Remote PeerIpAddr      State   Type      InterfaceName
-----
10     20     1.1.1.2      Up      S_IP_PEER -
-----
Total UP/DOWN Session Number : 1/0
```

```
[RouterA] display current-configuration | include bfd
bfd
bfd aa bind peer-ip 1.1.1.2
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2 track bfd-session aa
```

Check the IP routing table of Router A. The command output shows that the static route exists in the routing table.

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
Destinations : 3      Routes : 3
Destination/Mask  Proto Pre  Cost   Flags NextHop      Interface
-----
0.0.0.0/0        Static 60   0      RD  1.1.1.2      GigabitEthernet1/0/0
1.1.1.0/24       Direct 0     0      D   1.1.1.1      GigabitEthernet1/0/0
1.1.1.1/32       Direct 0     0      D   127.0.0.1    InLoopBack0
```

Run the **shutdown** command on GE 1/0/0 of Router B to simulate a link fault.

```
[RouterB] interface GigabitEthernet 1/0/0
[RouterB-GigabitEthernet1/0/0] shutdown
```

Check the IP routing table of Router A. The command output shows that default route 0.0.0.0/0 does not exist. This is because the default static route is bound to a BFD session. When BFD detects a link fault, BFD rapidly notifies that the bound static route becomes unavailable. If the static route is not bound to a BFD session, the default route 0.0.0.0/0 will always exist in IP routing table, this may cause traffic loss.

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
Destinations : 2      Routes : 2
Destination/Mask  Proto Pre  Cost   Flags NextHop      Interface
-----
1.1.1.0/24       Direct 0     0      D   1.1.1.1      GigabitEthernet1/0/0
1.1.1.1/32       Direct 0     0      D   127.0.0.1    InLoopBack0
```

----End

Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
bfd
#
interface GigabitEthernet1/0/0
ip address 1.1.1.1 255.255.255.0
#
bfd aa bind peer-ip 1.1.1.2
discriminator local 10
discriminator remote 20
commit
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2 track bfd-session aa
#
```



```

return
● Configuration file of Router B
sysname RouterB
#
bfd
#
interface GigabitEthernet1/0/0
ip address 1.1.1.2 255.255.255.0
#
interface Pos2/0/0
link-protocol ppp
ip address 2.2.2.2 255.255.255.0
#
bfd bb bind peer-ip 1.1.1.1
discriminator local 20
discriminator remote 10
commit
#
return
    
```

2.7.4 Example for Configuring BFD for IPv6 Static Routes

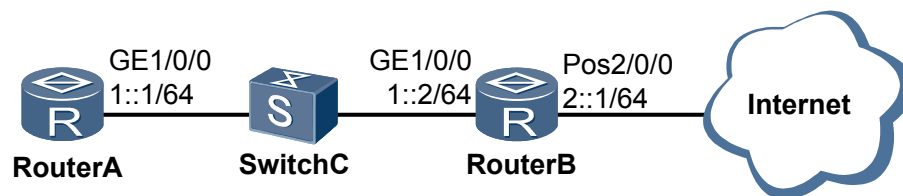
To improve IPv6 network reliability, you can configure BFD for IPv6 static route to rapidly detect link faults and speed up route convergence.

Networking Requirements

As shown in [Figure 2-4](#):

- Router A is connected to Router B through Switch C.
- It is required that Router A can communicate with other routers and the network.
- a BFD session is configured between Router A and Router B to detect the link between the two devices.

Figure 2-4 Networking diagram for configuring BFD for IPv6 static routes



Because the network topology is very simple, so static routes can be configured to make RouterA communicate with other Routers and the network. By binding BFD sessions to static routes, BFD sessions can detect the link status, which provides the detection mechanism for static routes.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a BFD session on Router A and Router B to detect the link between the two devices.

2. Configure a default static route from Router A to the external network and bind the default static route to a BFD session.

Data Preparation

To complete the configuration, you need the following data:

- Peer IPv6 address to be detected by BFD
- Local discriminator and remote discriminator of a BFD session
- Default values of BFD parameters, including minimum intervals for sending and receiving BFD control packets and local detection multiplier

Procedure

- Step 1** Configure an IPv6 address for each interface.

The configuration details are not described here.

- Step 2** Configure a BFD session between Router A and Router B.

On Router A, configure a BFD session with Router B.

```
<RouterA> system-view
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd aa bind peer-ipv6 1::2
[RouterA-bfd-session-aa] discriminator local 10
[RouterA-bfd-session-aa] discriminator remote 20
[RouterA-bfd-session-aa] commit
[RouterA-bfd-session-aa] quit
```

On Router B, configure a BFD session with Router A.

```
<RouterB> system-view
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd bb bind peer-ipv6 1::1
[RouterB-bfd-session-bb] discriminator local 20
[RouterB-bfd-session-bb] discriminator remote 10
[RouterB-bfd-session-bb] commit
[RouterB-bfd-session-bb] quit
```

- Step 3** Configure a default static route and bind it to a BFD session.

On Router A, configure a default static route to the external network and bind it to a BFD session named **aa**.

```
[RouterA] ipv6 route-static 0::0 0 1::2 track bfd-session aa
```

- Step 4** Verify the configuration.

After the configuration, run the **display bfd session all** command on Router A and Router B. The command output shows that a BFD session has been established and is in the Up state. Then, run the **display current-configuration | include bfd** command in the system view. The command output shows that the default static route has been bound to the BFD session.

Take the display on Router A as an example.

```
[RouterA] display bfd session all
-----
Local Remote PeerIpAddr      State   Type      InterfaceName
-----
10     20     1::2
```

```

-----
                        Up          S_IP_PEER          -
-----
Total UP/DOWN Session Number : 1/0
[RouterA] display current-configuration | include bfd
bfd
bfd aa bind peer-ipv6 1::2
ipv6 route-static :: 0 1::2 track bfd-session aa
    
```

Check the IP routing table of Router A. The command output shows that the static route exists in the routing table.

```

[RouterA] display ipv6 routing-table
Routing Table : Public
Destinations : 5          Routes : 5

Destination : ::          PrefixLength : 0
NextHop     : 1::2       Preference   : 60
Cost       : 0           Protocol     : Static
RelayNextHop : ::       TunnelID    : 0x0
Interface  : GigabitEthernet 1/0/0  Flags      : RD

Destination : ::1        PrefixLength : 128
NextHop     : ::1       Preference   : 0
Cost       : 0           Protocol     : Direct
RelayNextHop : ::       TunnelID    : 0x0
Interface  : InLoopBack0  Flags      : D

Destination : 1::        PrefixLength : 64
NextHop     : 1::1      Preference   : 0
Cost       : 0           Protocol     : Direct
RelayNextHop : ::       TunnelID    : 0x0
Interface  : GigabitEthernet 1/0/0  Flags      : D

Destination : 1::1       PrefixLength : 128
NextHop     : ::1       Preference   : 0
Cost       : 0           Protocol     : Direct
RelayNextHop : ::       TunnelID    : 0x0
Interface  : InLoopBack0  Flags      : D

Destination : FE80::     PrefixLength : 10
NextHop     : ::        Preference   : 0
Cost       : 0           Protocol     : Direct
RelayNextHop : ::       TunnelID    : 0x0
Interface  : NULL0       Flags      : D
    
```

Run the **shutdown** command on GE 1/0/0 of Router B to simulate a link fault.

```

[RouterB] interface GigabitEthernet 1/0/0
[RouterB-GigabitEthernet1/0/0] shutdown
    
```

Check the IP routing table of Router A. The command output shows that default route 0::0/0 does not exist. This is because the default static route is bound to a BFD session. When BFD detects a link fault, BFD rapidly notifies that the bound static route becomes unavailable. If the static route is not bound to a BFD session, the default route 0.0.0.0/0 will always exist in IP routing table, this may cause traffic loss.

```

[RouterA] display ipv6 routing-table
Routing Table : Public
Destinations : 1          Routes : 1

Destination : ::1        PrefixLength : 128
NextHop     : ::1       Preference   : 0
Cost       : 0           Protocol     : Direct
RelayNextHop : ::       TunnelID    : 0x0
Interface  : InLoopBack0  Flags      : D
    
```

----End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
 ipv6
#
 bfd
#
 interface GigabitEthernet 1/0/0
  undo shutdown
  ipv6 enable
  ipv6 address 1::1/64
#
 bfd aa bind peer-ipv6 1::2
  discriminator local 10
  discriminator remote 20
  commit
#
 ipv6 route-static :: 0 1::2 track bfd-session aa
#
 return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
 ipv6
#
 bfd
#
 interface GigabitEthernet 1/0/0
  undo shutdown
  shutdown
  ipv6 enable
  ipv6 address 1::2/64
#
 interface Pos2/0/0
  link-protocol ppp
  ipv6 enable
  ipv6 address 2::1/64
#
 bfd bb bind peer-ipv6 1::1
  discriminator local 20
  discriminator remote 10
  commit
#
 return
```

2.7.5 Example for Configuring NQA for IPv4 Static Routes

NQA for static IPv4 routes helps detect network faults rapidly, control the advertisement of static routes, and switch traffic to available paths.

Networking Requirements

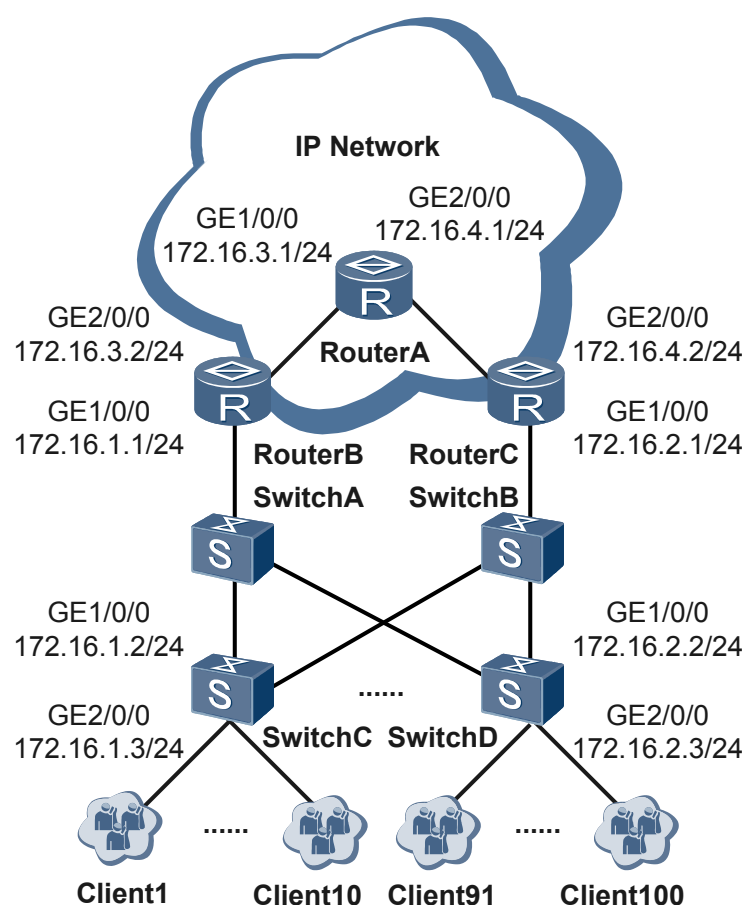
Static routes can be configured on networks with simple topologies or for Routers that cannot generate routes to the destination through dynamic routing protocols. Unlike dynamic routing protocols, static routes do not have a dedicated detection mechanism. After a fault occurs, the corresponding static route cannot be automatically deleted from the IP routing table. The network administrator must delete the corresponding static route to allow traffic to switch to an available path. This delays the link switchover and probably interrupts services for a comparatively long time. BFD for static routes can be deployed to monitor the status of a link, but it requires that

both ends of the link support BFD. If either end of the link does not support BFD, you can configure NQA for static IPv4 routes to monitor the link status.

On the IP MAN shown in **Figure 2-5**, redundant links are used and the following requirements are met:

- Router B and Router C are configured with static routes to the clients. Router B is master and Router C is backup.
- Normally, traffic travels along the active link of Router B → Switch A → Switch C (Switch D).
- If a fault occurs in the active link, traffic switches to the standby link of Router C → Switch B → Switch C (Switch D).

Figure 2-5 Networking diagram for configuring NQA for static IPv4 routes



NOTE

In this example, Switch C and Switch D provide access services for users. In actual networks, Optical Line Terminals (OLTs), Digital Subscriber Line Access Multiplexers (DSLAMs), Multi-service Access Nodes (MSANs), or x Digital Subscriber Line (xDSL) devices can also be used to provide access services for users, and the configuration is similar on Router A, Router B and Router C.

Configuration Roadmap

The configuration roadmap is as follows:

1. Establish an ICMP NQA test instance for the NQA client Router B and the tested device Switch C to test whether the active link of Router B → Switch A → Switch C (Switch D) works properly.
2. Configure static routes on Router B and Router C, and associate the static route on Router B with the NQA test instance. If the NQA test instance detects a link fault, the system deletes the static route from the IP routing table.
3. Configure a dynamic routing protocol on Router A, Router B, and Router C to allow them to learn routes from each other.
4. Configure OSPF on Router B and Router C to import static routes, and set a higher cost for the static route imported to Router C than that imported to Router B. After Router A learns routes from Router B and Router C to the same destination, it prefers the route with a lower cost along the path of Router B → Switch A → Switch C (Switch D).

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface
- Test type, administrator name, and name of an NQA test instance
- Test period and packet sending interval of the NQA test instance
- OSPF area ID (Area 0) where Router A, Router B, and Router C reside

Procedure

Step 1 Configure IP addresses. The configuration is omitted.

Step 2 Configure an NQA test instance on Router B to test the link between Router B and Switch C.

```
<RouterB> system-view
[RouterB] nqa test-instance admin icmp
[RouterB-nqa-admin-icmp] test-type icmp
[RouterB-nqa-admin-icmp] destination-address ipv4 172.16.1.2
[RouterB-nqa-admin-icmp] frequency 3
[RouterB-nqa-admin-icmp] probe-count 1
[RouterB-nqa-admin-icmp] start now
```

Step 3 Configure a static route.

Configure a static route on Router B and associate the static route with an NQA test instance.

```
<RouterB> system-view
[RouterB] ip route-static 172.16.1.3 255.255.255.255 GigabitEthernet 1/0/0 track
nqa admin icmp
```

Configure a static route on Router C.

```
<RouterC> system-view
[RouterC] ip route-static 172.16.1.3 255.255.255.255 GigabitEthernet 1/0/0
permanent
```

Step 4 Configure a dynamic routing protocol on Router A, Router B, and Router C. This example uses OSPF. For detailed configurations, see [5.2 Configuring Basic OSPF Functions](#).

Step 5 Configure OSPF on Router B and Router C to import static routes.

Configure OSPF on Router B to import static routes, and set the cost of each imported static route to 10.

```
<RouterB> system-view
```

```
[RouterB] ospf 1
[RouterB-ospf-1] import-route static cost 10
```

Configure OSPF on Router C to import static routes, and set the cost of each imported static route to 20.

```
<RouterC> system-view
[RouterC] ospf 1
[RouterC-ospf-1] import-route static cost 20
```

Step 6 Verify the configuration.

After completing the configuration, run the **display current-configuration | include nqa** command in the system view on Router B. The command output shows that the static route has been associated with the NQA test instance. Run the **display nqa results** command. The command output shows that the NQA test instance has been established.

Check the configuration of NQA for static IPv4 routes.

```
<RouterB> display current-configuration | include nqa
ip route-static 172.16.1.3 255.255.255.255 GigabitEthernet1/0/0 track nqa admin
icmp
nqa test-instance admin icmp
```

Check NQA test results.

```
<RouterB> display nqa results test-instance admin icmp
NQA entry(admin, icmp) :testflag is active ,testtype is icmp
1 . Test 28 result The test is finished
Send operation times: 1 Receive response times: 1
Completion:success RTD OverThresholds number: 0
Attempts number:1 Drop operation number:0
Disconnect operation number:0 Operation timeout number:0
System busy operation number:0 Connection fail number:0
Operation sequence errors number:0 RTT Stats errors number:0
Destination ip address:172.16.1.2
Min/Max/Average Completion Time: 30/30/30
Sum/Square-Sum Completion Time: 60/900
Last Good Probe Time: 2010-11-14 17:34:20.8
Lost packet ratio: 0 %
```

The information "Lost packet ratio: 0 %" is displayed, indicating that the link works properly.

Check the routing table on Router B. The routing table contains this static route.

```
<RouterB> display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
Destinations : 10 Routes : 10

Destination/Mask Proto Pre Cost Flags NextHop Interface
-----
127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
172.16.1.0/24 Direct 0 0 D 172.16.1.1
GigabitEthernet1/0/0
172.16.1.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
172.16.1.2/32 Direct 0 0 D 172.16.1.2
GigabitEthernet1/0/0
172.16.1.3/32 Static 60 0 D 172.16.1.1
GigabitEthernet1/0/0
172.16.3.0/24 Direct 0 0 D 172.16.3.2
GigabitEthernet2/0/0
172.16.3.1/32 Direct 0 0 D 172.16.3.1
GigabitEthernet2/0/0
172.16.3.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0
172.16.4.0/24 OSPF 10 2 D 172.16.3.1
```

GigabitEthernet2/0/0

Check the routing table on Router A.

```
<RouterA> display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
    Destinations : 9          Routes : 9

Destination/Mask    Proto    Pre  Cost           Flags NextHop           Interface
-----
    127.0.0.0/8      Direct  0    0                D   127.0.0.1           InLoopBack0
    127.0.0.1/32     Direct  0    0                D   127.0.0.1           InLoopBack0
    172.16.1.3/32    O_ASE   150  10              D   172.16.3.2
GigabitEthernet1/0/0
    172.16.3.0/24    Direct  0    0                D   172.16.3.1
GigabitEthernet1/0/0
    172.16.3.1/32    Direct  0    0                D   127.0.0.1           InLoopBack0
    172.16.3.2/32    Direct  0    0                D   172.16.3.2
GigabitEthernet1/0/0
    172.16.4.0/24    Direct  0    0                D   172.16.4.1
GigabitEthernet2/0/0
    172.16.4.1/32    Direct  0    0                D   127.0.0.1           InLoopBack0
    172.16.4.2/32    Direct  0    0                D   172.16.4.2
GigabitEthernet2/0/0
```

The routing table contains a route destined for 172.16.1.3/32 with the next hop of 172.16.3.2 and the cost of 10. Therefore, traffic travels along the path Router B → Switch A → Switch C (Switch D).

Shut down GigabitEthernet 1/0/0 on Router B to simulate a link fault.

```
<RouterB> system-view
[RouterB] interface GigabitEthernet 1/0/0
[RouterB-GigabitEthernet1/0/0] shutdown
```

Check NQA test results.

```
<RouterB> display nqa results test-instance admin icmp

NQA entry(admin, icmp) :testflag is active ,testtype is icmp
1 . Test 608 result The test is finished
  Send operation times: 1                      Receive response times: 0
  Completion:failed                               RTD OverThresholds number: 0
  Attempts number:1                               Drop operation number:1
  Disconnect operation number:0                   Operation timeout number:0
  System busy operation number:0                   Connection fail number:0
  Operation sequence errors number:0               RTT Stats errors number:0
  Destination ip address:172.16.1.2
  Min/Max/Average Completion Time: 0/0/0
  Sum/Square-Sum Completion Time: 0/0
  Last Good Probe Time: 0000-00-00 00:00:00.0
  Lost packet ratio: 100 %
```

The information "Lost packet ratio: 100 %" is displayed, indicating that the link fails.

Check the routing table on Router B. The static route disappears.

```
<RouterB> display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
    Destinations : 7          Routes : 7

Destination/Mask    Proto    Pre  Cost           Flags NextHop           Interface
```



```

        127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
        127.0.0.1/32 Direct  0    0           D   127.0.0.1       InLoopBack0
        172.16.1.3/32 O_ASE  150  20         D   172.16.3.1
GigabitEthernet2/0/0
        172.16.3.0/24 Direct  0    0           D   172.16.3.2
GigabitEthernet2/0/0
        172.16.3.1/32 Direct  0    0           D   172.16.3.1
GigabitEthernet2/0/0
        172.16.3.2/32 Direct  0    0           D   127.0.0.1       InLoopBack0
        172.16.4.0/24 OSPF    10    2         D   172.16.3.1
GigabitEthernet2/0/0
    
```

Check the routing table on Router A.

```

<RouterA> display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
    Destinations : 9          Routes : 9

Destination/Mask    Proto    Pre  Cost           Flags NextHop           Interface
-----
        127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
        127.0.0.1/32 Direct  0    0           D   127.0.0.1       InLoopBack0
        172.16.1.3/32 O_ASE   150  20           D   172.16.4.2
GigabitEthernet2/0/0
        172.16.3.0/24 Direct  0    0           D   172.16.3.1
GigabitEthernet1/0/0
        172.16.3.1/32 Direct  0    0           D   127.0.0.1       InLoopBack0
        172.16.3.2/32 Direct  0    0           D   172.16.3.2
GigabitEthernet1/0/0
        172.16.4.0/24 Direct  0    0           D   172.16.4.1
GigabitEthernet2/0/0
        172.16.4.1/32 Direct  0    0           D   127.0.0.1       InLoopBack0
        172.16.4.2/32 Direct  0    0           D   172.16.4.2
GigabitEthernet2/0/0
    
```

As the static route is associated with the NQA test instance on Router B, after NQA detects the link fault, it immediately notifies Router B that the associated static route is unavailable. Router A cannot learn the route destined for 172.16.1.3/32 from Router B. Router A, however, can learn another route destined for 172.16.1.3/32 from Router C. The next hop of the route is 172.16.4.2, and the cost is 20. Traffic switches to the link of Router C → Switch B → Switch C (Switch D).

----End

Configuration Files

- Configuration file of Router A

```

#
sysname RouterA
#
router id 1.1.1.1
#
interface GigabitEthernet1/0/0
    link-protocol ppp
    undo shutdown
    ip address 172.16.3.1 255.255.255.0
#
interface GigabitEthernet2/0/0
    link-protocol ppp
    undo shutdown
    ip address 172.16.4.1 255.255.255.0
#
    
```

```
ospf 1
import-route static
area 0.0.0.0
network 172.16.3.0 0.0.0.255
network 172.16.4.0 0.0.0.255
#
return
```

● Configuration file of Router B

```
#
sysname RouterB
#
router id 2.2.2.2
#
interface GigabitEthernet1/0/0
link-protocol ppp
undo shutdown
ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
link-protocol ppp
undo shutdown
ip address 172.16.3.2 255.255.255.0
#
ospf 1
import-route static cost 10
area 0.0.0.0
network 172.16.3.0 0.0.0.255
#
ip route-static 172.16.1.3 255.255.255.255 GigabitEthernet1/0/0 track nqa
admin icmp
#
nqa test-instance admin icmp
test-type icmp
destination-address ipv4 172.16.1.2
frequency 3
probe-count 1
start now
#
return
```

● Configuration file of Router C

```
#
sysname RouterC
#
router id 3.3.3.3
#
interface GigabitEthernet1/0/0
link-protocol ppp
undo shutdown
ip address 172.16.2.1 255.255.255.0
#
interface GigabitEthernet2/0/0
link-protocol ppp
undo shutdown
ip address 172.16.4.2 255.255.255.0
#
ospf 1
import-route static cost 20
area 0.0.0.0
network 172.16.4.0 0.0.0.255
#
ip route-static 172.16.1.3 255.255.255.255 GigabitEthernet1/0/0 permanent
#
return
```

2.7.6 Example for Configuring Permanent Advertisement of IPv4 Static Routes

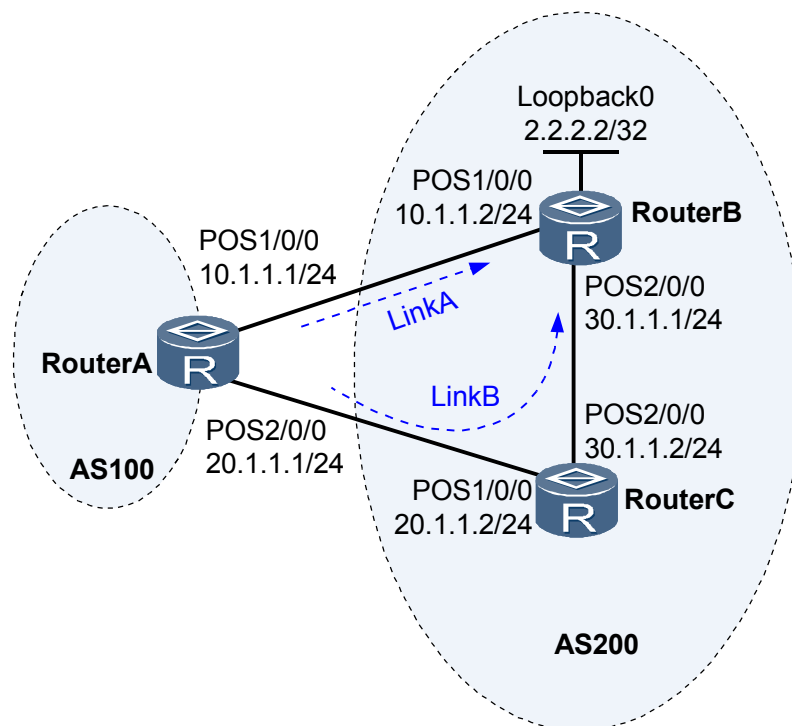
By configuring permanent advertisement of static routes, you can determine the forwarding path of service traffic and provide a low-cost and simple link detection mechanism.

Networking Requirements

If service traffic needs to be forwarded along a specified path, you can detect links of the forwarding path by pinging the destination addresses of static routes. In this manner, you can monitor services at a very low cost.

As shown in **Figure 2-6**, EBGP peer relationships are established between Router A and Router B, and between Router A and Router C by using static routes. There are two links (Link A and Link B) between Router A and Router B. By configuring permanent advertisement of static routes, you can make traffic be forwarded along only Link A regardless of the outbound interface status and detect the status of Link A by periodically pinging the interface address of Router B through the network monitoring system. This thus detects the status of BGP services.

Figure 2-6 Networking diagram for configuring permanent advertisement of IPv4 static routes



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure OSPF on devices in AS 200 to ensure that routes to the address of Loopback0 on Router B are advertised to Router C.

2. Establish EBGP peer relationships between Router A and Router B, and between Router A and Router C.
3. On Router A, configure a static route whose destination address is the address of Loopback0 on Router B and outbound interface is POS 1/0/0 on Router A.
4. On Router A, configure permanent advertisement of the static route to the address of Loopback0 on Router B. In this manner, when POS 1/0/0 on Router A becomes faulty, the static route to the address of Loopback0 on Router B still takes effect.

Data Preparation

To complete the configuration, you need the following data:

- OSPF process IDs of Router B and Router C
- Router IDs and AS numbers of all routers

Procedure

Step 1 Configure an IP address for each interface. The configuration details are not described here.

Step 2 Configure basic OSPF functions on devices in AS 200.

Configure Router B.

```
[RouterB] ospf 1
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

Configure Router C.

```
[RouterC] ospf 1
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

After the preceding configurations, check the routing table of Router C.

```
[RouterC] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 10          Routes : 10

Destination/Mask    Proto    Pre  Cost    Flags NextHop          Interface
-----
      2.2.2.2/32     OSPF     10    1        D   30.1.1.1            Pos2/0/0
      3.3.3.3/32     Direct    0     0        D   127.0.0.1           InLoopBack0
      20.1.1.0/24    Direct    0     0        D   20.1.1.2            Pos1/0/0
      20.1.1.1/32    Direct    0     0        D   20.1.1.1            Pos1/0/0
      20.1.1.2/32    Direct    0     0        D   127.0.0.1           InLoopBack0
      30.1.1.0/24    Direct    0     0        D   30.1.1.2            Pos2/0/0
      30.1.1.1/32    Direct    0     0        D   30.1.1.1            Pos2/0/0
      30.1.1.2/32    Direct    0     0        D   127.0.0.1           InLoopBack0
      127.0.0.0/8     Direct    0     0        D   127.0.0.1           InLoopBack0
      127.0.0.1/32   Direct    0     0        D   127.0.0.1           InLoopBack0
```

The preceding display shows that Router C has learned the OSPF route to 2.2.2.2/32.

Step 3 Configure EBGP connections and establish EBGP peer relationships between Router A and Router B, and between Router A and Router C.

Configure Router A.

```
[RouterA] bgp 100
[RouterA-bgp] peer 10.1.1.2 as-number 200
[RouterA-bgp] peer 20.1.1.2 as-number 200
[RouterA-bgp] quit
```

Configure Router B.

```
[RouterB] bgp 200
[RouterB-bgp] peer 10.1.1.1 as-number 100
[RouterB-bgp] quit
```

Configure Router C.

```
[RouterC] bgp 200
[RouterC-bgp] peer 20.1.1.1 as-number 100
[RouterC-bgp] network 20.1.1.0 255.255.255.0
[RouterC-bgp] import-route ospf 1
[RouterC-bgp] quit
```

After the preceding configurations, check the EBGP connection status of Router A.

```
[RouterA] display bgp peer
BGP local Router ID : 10.1.1.1
Local AS number : 100
Total number of peers : 2                Peers in established state : 2
```

Peer	V	AS	MsgRcvd	MsgSent	OutQ	Up/Down	State	PrefRcv
10.1.1.2	4	200	2	2	0	00:00:28	Established	0
20.1.1.2	4	200	2	2	0	00:00:01	Established	0

The preceding display shows that the status of BGP connections between Router A and Router B, and between Router A and Router C is **Established**. This indicates that EBGP peer relationships have been established.

After the preceding configurations, check the routing table of Router A.

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
1.1.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
2.2.2.2/32	EBGP	255	1	D	20.1.1.2	Pos2/0/0
10.1.1.0/24	Direct	0	0	D	10.1.1.1	Pos1/0/0
10.1.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
10.1.1.2/32	Direct	0	0	D	10.1.1.2	Pos1/0/0
20.1.1.0/24	Direct	0	0	D	20.1.1.1	Pos2/0/0
20.1.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
20.1.1.2/32	Direct	0	0	D	20.1.1.2	Pos2/0/0
30.1.1.0/24	EBGP	255	0	D	20.1.1.2	Pos2/0/0
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0

The preceding display shows that Router A has learned the BGP route to 2.2.2.2/32.

Step 4 On Router A, configure a static route whose destination address is 2.2.2.2/32 and outbound interface is POS 1/0/0.

```
[RouterA] ip route-static 2.2.2.2 32 pos1/0/0 10.1.1.2
```

After the preceding configurations, check the routing table of Router A.

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
    Destinations : 11          Routes : 11

Destination/Mask    Proto  Pre  Cost    Flags NextHop          Interface
-----
    1.1.1.1/32      Direct  0    0        D   127.0.0.1          InLoopBack0
    2.2.2.2/32      Static 60  0        D   10.1.1.2           Pos1/0/0
    10.1.1.0/24     Direct  0    0        D   10.1.1.1           Pos1/0/0
    10.1.1.1/32     Direct  0    0        D   127.0.0.1          InLoopBack0
    10.1.1.2/32     Direct  0    0        D   10.1.1.2           Pos1/0/0
    20.1.1.0/24     Direct  0    0        D   20.1.1.1           Pos2/0/0
    20.1.1.1/32     Direct  0    0        D   127.0.0.1          InLoopBack0
    20.1.1.2/32     Direct  0    0        D   20.1.1.2           Pos2/0/0
    30.1.1.0/24     EBGPF  255  0        D   10.1.1.2           Pos1/0/0
    127.0.0.0/8     Direct  0    0        D   127.0.0.1          InLoopBack0
    127.0.0.1/32   Direct  0    0        D   127.0.0.1          InLoopBack0
```

The preceding display shows that the static route to 2.2.2.2/32 is preferred because the priority of a static route is higher than that of a BGP route.

Step 5 Verify the configuration.

Run the **shutdown** command on POS 1/0/0 of Router A to simulate a link fault.

```
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] shutdown
[RouterA-Pos1/0/0] quit
```

After the preceding configurations, run the **tracert** command on Router A to check the forwarding path of ping packets.

```
<RouterA> tracert 1.1.1.1
tracroute to 1.1.1.1(1.1.1.1), max hops: 30 ,packet length: 40,press CTRL_C t o
break
 1 20.1.1.2 50 ms 30 ms 30 ms
 2 30.1.1.1 < AS=200 > 50 ms 60 ms 60 ms
```

The command output shows that ping packets detour around Link B after Link A becomes faulty. This indicates that the EBGPF route to 2.2.2.2/32 is preferred after the static route to 2.2.2.2/32 becomes inactive. In this case, the status of Link A cannot be detected through a ping operation.

Configure permanent advertisement of static routes on Router A.

```
[RouterA] ip route-static 2.2.2.2 32 pos1/0/0 10.1.1.2 permanent
```

After the preceding configurations, check the routing table of Router A.

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
    Destinations : 8          Routes : 8

Destination/Mask    Proto  Pre  Cost    Flags NextHop          Interface
-----
    1.1.1.1/32      Direct  0    0        D   127.0.0.1          InLoopBack0
    2.2.2.2/32      Static 60  0        D   10.1.1.2          Pos1/0/0
    20.1.1.0/24     Direct  0    0        D   20.1.1.1           Pos2/0/0
    20.1.1.1/32     Direct  0    0        D   127.0.0.1          InLoopBack0
    20.1.1.2/32     Direct  0    0        D   20.1.1.2           Pos2/0/0
    30.1.1.0/24     EBGPF  255  0        D   20.1.1.2           Pos2/0/0
    127.0.0.0/8     Direct  0    0        D   127.0.0.1          InLoopBack0
    127.0.0.1/32   Direct  0    0        D   127.0.0.1          InLoopBack0
```

The preceding display shows that the static route to 2.2.2.2/32 is still valid and the EBGp route to 2.2.2.2/32 is not preferred after the outbound interface of the static route becomes faulty.

Run the **ping** command on Router A to check whether Router A can ping successfully 2.2.2.2/32.

```
[RouterA] ping 2.2.2.2
PING 2.2.2.2: 56 data bytes, press CTRL_C to break
  Request time out
  Request time out
  Request time out
  Request time out
  Request time out

--- 2.2.2.2 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
 100.00% packet loss
```

The preceding command output shows that after permanent advertisement of static routes is configured, ping packets are still forwarded along Link A but not Link B when Link A becomes faulty, and the connectivity of Link A can be detected through a ping operation.

---End

Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 shutdown
 ip address 10.1.1.1 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 20.1.1.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
bgp 100
 peer 10.1.1.2 as-number 200
 peer 20.1.1.2 as-number 200
#
ipv4-family unicast
 undo synchronization
 peer 10.1.1.2 enable
 peer 20.1.1.2 enable
#
 ip route-static 2.2.2.2 255.255.255.255 Pos1/0/0 10.1.1.2 permanent
#
return
```

- Configuration file of Router B

```
#
sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 30.1.1.1 255.255.255.0
```

```
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
bgp 200
 peer 10.1.1.1 as-number 100
#
 ipv4-family unicast
  undo synchronization
  peer 10.1.1.1 enable
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 30.1.1.0 0.0.0.255
#
return
```

● Configuration file of Router C

```
#
 sysname RouterC
#
interface Pos1/0/0
 link-protocol ppp
 ip address 20.1.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 30.1.1.2 255.255.255.0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
bgp 200
 peer 20.1.1.1 as-number 100
#
 ipv4-family unicast
  undo synchronization
  network 20.1.1.0 255.255.255.0
  import-route ospf 1
  peer 20.1.1.1 enable
#
ospf 1
 import-route direct
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
#
return
```


3 RIP Configuration

About This Chapter

RIP can advertise and receive routes to affect the selection of data forwarding paths, and can provide the network management function. RIP is applicable to small-scale networks.

[3.1 Introduction to RIP](#)

RIP is a dynamic routing protocol used on small-scale networks. It is an Interior Gateway Protocol (IGP) and uses the distance-vector routing algorithm.

[3.2 Configuring Basic RIP Functions](#)

To implement RIP features, you need to configure basic RIP functions, including enabling RIP and specifying the network segment where RIP runs, and setting the RIP version.

[3.3 Configuring RIP Route Attributes](#)

In practice, by setting RIP route attributes, you can change RIP routing policies to meet the requirements of complex networks.

[3.4 Controlling the Advertising of RIP Routing Information](#)

To meet the requirements of complex networks, it is required to accurately control the advertising of RIP routing information.

[3.5 Controlling the Receiving of RIP Routing Information](#)

To meet the requirements of complex networks, it is required to accurately control the receiving of RIP routing information.

[3.6 Configuring RIP-2 Features](#)

Different from RIP-1, RIP-2 supports VLSM, CIDR, and authentication, ensuring higher security.

[3.7 Optimizing a RIP Network](#)

You can adjust and optimize the RIP network performance by configuring RIP functions in special network environments, such as configuring RIP timers, setting the interval for sending packets, and setting the maximum number of packets to be sent.

[3.8 Configuring RIP GR](#)

This section describes how to configure RIP GR to avoid incorrect route calculation and packet loss after a RIP router restarts.

[3.9 Configuring the Network Management Function in RIP](#)

By binding RIP to MIBs, you can view and configure RIP through the NMS.

[3.10 Maintaining RIP](#)

This section describes how to reset RIP connections and clear RIP information.

[3.11 Configuration Examples](#)

In actual networking, RIP versions and whether to import external routes will affect which routes can be learned.

3.1 Introduction to RIP

RIP is a dynamic routing protocol used on small-scale networks. It is an Interior Gateway Protocol (IGP) and uses the distance-vector routing algorithm.

3.1.1 Overview of RIP

The implementation of RIP is simple, and its configuration and maintenance are easier than those of OSPF and IS-IS. Therefore, RIP is widely used on small-scale networks.

The Routing Information Protocol (RIP) is a simple Interior Gateway Protocol (IGP). RIP is mainly used on small-scale networks such as campus networks and simple regional networks rather than complex or large-scale networks.

RIP uses the distance-vector routing algorithm and exchanges routing information by using User Datagram Protocol (UDP) packets through the port 520.

RIP employs the hop count to measure the distance to the destination. The distance is called the routing metric. In RIP, the hop count from a router to its directly connected network is 0, and the hop count from a router to a network, which can be reached through another router, is 1. To speed up route convergence, RIP defines the cost as an integer that ranges from 0 to 15. The hop count that is equal to or exceeds 16 is defined as infinity, indicating that the destination network or host is unreachable. This hop limit, however, makes RIP unable to be applied to large-scale networks.

To improve the network performance and prevent routing loops, RIP supports both split horizon and poison reverse.

- The principle of split horizon is that a route learnt by RIP on an interface is not sent to neighbors from the interface. This reduces bandwidth consumption and avoids route loops.
- The principle of poison reverse is that RIP sets the cost of the route learnt from an interface of a neighbor to 16 (specifying the route as unreachable) and then sends the route from the interface back to the neighbor. In this way, RIP can delete useless routes from the routing table of the neighbor.

The implementation of RIP is simple, and its configuration and maintenance is easier than those of Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS). Therefore, RIP is widely used.

RIP has two versions:

- RIPv1
- RIPv2

RIPv1 is a classful routing protocol, whereas RIPv2 is a classless routing protocol. In RIPv2, address 224.0.0.9 is the multicast address of a RIP router.

Compared with RIPv1, RIPv2 has the following advantages:

- It supports route tag and can flexibly control routes on the basis of the tag in the routing policy.
- Its packets contain mask information and support route aggregation and Classless Inter-domain Routing (CIDR).

- It supports the next hop address and can select the optimal next hop address in the broadcast network.
- It uses multicast routes to send update packets. Only RIPv2 routers can receive protocol packets. This reduces the resource consumption.
- To enhance the security, RIPv2 provides two authentication modes to enhance security: plain-text authentication and MD5 authentication.

3.1.2 RIP Features Supported by the NE80E/40E

The RIP features supported by the NE80E/40E include RIPv1, RIPv2, split horizon, poison reverse, and multi-instance.

The NE80E/40E supports the following RIP features:

- RIPv1 and RIPv2
- RIP multi-instance, which functions as an internal routing protocol of VPNs and runs between CEs and PEs in MPLS L3VPN networks

 **NOTE**

For detailed configuration of a VPN instance, see the chapter "BGP MPLS IP VPN Configuration" in the *NE80E/40E Router Configuration Guide - VPN*.

3.2 Configuring Basic RIP Functions

To implement RIP features, you need to configure basic RIP functions, including enabling RIP and specifying the network segment where RIP runs, and setting the RIP version.

3.2.1 Establishing the Configuration Task

Before configuring basic RIP functions, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

Configuring basic RIP functions involves configuring basic RIP features. After the configuration, RIP features are available.

Pre-configuration Tasks

Before configuring basic RIP functions, complete the following tasks:

- Configuring the link layer protocol
- Configuring IP addresses for interfaces to ensure that neighboring nodes are reachable at the network layer

Data Preparation

To configure basic RIP functions, you need the following data.

No.	Data
1	RIP process ID
2	Network segment where the RIP interface resides
3	RIP version number

3.2.2 Enabling RIP

Creating RIP processes is the prerequisite to performing RIP configurations.

Context

If you run RIP-related commands in the interface view before enabling RIP, the configurations take effect only after RIP is enabled.

Do as follows on the router to be enabled with RIP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rip [ process-id ]
```

The RIP is enabled and the RIP view is displayed.

RIP supports multi-instance. To associate RIP processes with VPN instances, you can run the **rip [process-id] vpn-instance vpn-instance-name** command.

 **NOTE**

For easy management and effective control, RIP supports multi-process and multi-instance. The multi-process feature allows a set of interfaces to be associated with a specific RIP process and an interface can be associated with only one RIP process. This ensures that the specific RIP process performs all the protocol operations only on this set of interfaces. Thus, multiple RIP processes can work on a single router and each process is responsible for a unique set of interfaces. In addition, the routing data is independent between RIP processes; however, routes can be imported between processes.

For the routers that support the VPN, each RIP process is associated with a specific VPN instance. In this case, all the interfaces attached to the RIP process should be associated with the RIP-process-related VPN instance.

----End

3.2.3 Enabling RIP on the Specified Network Segment

After enabling RIP, you need to specify the network segment where RIP runs. RIP runs only on the interfaces on the specified network segment. RIP does not receive, send, or forward routes on the interfaces that do not reside on the specified network segment.

Context

By default, after RIP is enabled, it is disabled on all interfaces.

Do as follows on the router to be enabled with RIP.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rip [ process-id ]
```

The RIP process is enabled and the RIP view is displayed.

Step 3 Run:

```
network network-address
```

RIP is enabled on the specified network segment.

network-address specifies the address of a natural network segment.

NOTE

An interface can be associated with only one RIP process.

If any network segment where an interface configured with multiple sub-interface IP addresses resides to a RIP process, the interface cannot be associated with any other RIP processes.

----End

3.2.4 Configuring RIP Version Number

RIP versions include RIPv1 and RIPv2. The two versions have different functions.

Context

Do as follows on the RIP router.

Procedure

- Configuring the Global RIP Version Number

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
rip [ process-id ]
```

The RIP process is enabled and the RIP view is displayed.

3. Run:

```
version { 1 | 2 }
```

The global RIP version number is specified.

- Configuring the RIP Version Number for an Interface

1. Run:
`system-view`
 The system view is displayed.
2. Run:
`interface interface-type interface-number`
 The interface view is displayed.
3. Run:
`rip version { 1 | 2 [broadcast | multicast] }`
 The RIP version number of the packets received by the interface is specified.

 **NOTE**

By default, an interface receives both RIPv1 and RIPv2 packets but sends only RIPv1 packets. When configuring RIPv2 on an interface, you can specify the mode in which the interface sends packets. If no RIP version number is configured in the interface view, the global RIP version is used. The RIP version set on an interface takes precedence over the global RIP version.

----End

3.2.5 Checking the Configuration

After basic RIP functions are successfully configured, you can view the current running status, configuration, and routing information of RIP.

Prerequisite

The configurations of basic RIP functions are complete.

Procedure

- Run `display rip [process-id | vpn-instance vpn-instance-name]` command to check the running status and configuration of RIP.
- Run `display rip process-id route` command to check all activated and inactivated RIP routes.
- Run `display default-parameter rip` command to check the default RIP configuration.
- Run the `display rip process-id statistics interface { all | interface-type interface-number [verbose | neighbor neighbor-ip-address] }` command to check statistics about RIP interfaces.

----End

Example

Run the `display rip [process-id | vpn-instance vpn-instance-name]` command, and you can view the running status and configuration of the enabled RIP process. The command output shows that two VPN instances are running. The first VPN instance is a public network instance; the second VPN instance is named **VPN-Instance-1**.

```
<HUAWEI> display rip
Public VPN-instance
RIP process : 1
RIP version : 1
Preference : 100
Checkzero : Enabled
```

```

    Default-cost : 0
    Summary : Enabled
    Hostroutes : Enabled
    Maximum number of balanced paths : 32
    Update time : 30 sec Age time : 180 sec
    Garbage-collect time : 120 sec
    Graceful restart : Disabled
    Silent interfaces : None
    Default Route : Disabled
    Verify-source : Enabled
    Networks :
    172.4.0.0
    Configured peers : None
    Number of routes in database : 4
    Number of interfaces enabled : 3
    Triggered updates sent : 3
    Number of route changes : 6
    Number of replies to queries : 1
    Number of routes in ADV DB : 6
Private VPN-instance name : VPN-Instance-1
    RIP process : 2
    RIP version : 1
    Preference : 100
    Checkzero : Enabled
    Default-cost : 0
    Summary : Enabled
    Hostroutes : Enabled
    Maximum number of balanced paths : 32
    Update time : 30 sec Age time : 180 sec
    Garbage-collect time : 120 sec
    Graceful restart : Disabled
    Silent interfaces : None
    Default Route : Disabled
    Verify-source : Enabled
    Networks :
    192.4.5.0
    Configured peers : None
    Number of routes in database : 0
    Number of interfaces enabled : 0
    Triggered updates sent : 0
    Number of route changes : 0
    Number of replies to queries : 0
    Number of routes in ADV DB : 6
    Total count for 2 process :
    Number of routes in database : 3
    Number of interfaces enabled : 2
    Number of routes sendable in a periodic update : 6
    Number of routes sent in last periodic update : 4
    
```

Run the **display rip process-id route** command, and you can view all activated and inactivated routes of the specified RIP process.

```

<HUAWEI> display rip 1 route
Route Flags: R - RIP
           A - Aging, G - Garbage-collect
-----
Peer 192.4.5.1 on Pos3/0/1
  Destination/Mask    Nexthop    Cost    Tag    Flags    Sec
  172.4.0.0/16        192.4.5.1    1      0      RA      15
  192.13.14.0/24      192.4.5.1    2      0      RA      15
  192.4.5.0/24        192.4.5.1    1      0      RA      15
    
```

Run the **display default-parameter rip** command, and you can view the default RIP configuration.

```

<HUAWEI> display default-parameter rip
-----
Protocol Level Default Configurations
-----
    
```



```

RIP version      : 1
Preference      : 100
Checkzero       : Enabled
Default-cost    : 0
Auto Summary    : Enabled
Hostroutes      : Enabled
Maximum Balanced Paths : 32
Update time     : 30 sec           Age time : 180 sec
Garbage-collect time : 120 sec
Default Route   : Disabled
Verify-source   : Enabled
Graceful restart : Disabled
    
```

 Interface Level Default Configurations

```

Metricin        : 0
Metricout       : 1
Input Packet Processing : Enabled
Output Packet Processing: Enabled
Poison Reverse  : Disabled
Replay Protect  : Disabled
Split Horizon
  For Broadcast and P2P Interfaces : Enabled
  For NBMA Interfaces               : Disabled
Packet Transmit Interval      : 200 msec
Packet Transmit Number       : 50
RIP Protocol Version          : RIPv1 Compatible (Non-Standard)
    
```

Run the **display rip process-id statistics interface** { **all** | *interface-type interface-number* [**verbose** | **neighbor neighbor-ip-address**] } command, and you can view statistics about the specified RIP interface.

```

<HUAWEI> display rip 1 statistics interface gigabitethernet1/0/0
GigabitEthernet1/0/0(10.0.0.11)
Statistical information          Last min      Last 5 min      Total
-----
Periodic updates sent           5              23              259
Triggered updates sent          5              30              408
Response packet sent            10             34              434
Response packet received        15             38              467
Response packet ignored          0              0                0
Request packet sent              1              3                8
Request packet received          4              20              40
Request packet ignored           0              0                0
Bad packets received            0              0                0
Bad routes received             0              0                0
Packet authentication failed     0              0                0
    
```

3.3 Configuring RIP Route Attributes

In practice, by setting RIP route attributes, you can change RIP routing policies to meet the requirements of complex networks.

3.3.1 Establishing the Configuration Task

RIP route attributes include the RIP preference, additional metrics of an interface, and maximum number of equal-cost routes.

Applicable Environment

In practice, to meet the requirements of a complex network, you can change RIP routing policies by setting RIP route attributes. After performing configuration procedures in this section, you can:

- Affect route selection by changing the additional metric of a RIP interface.
- Change the matching order of by configuring the RIP preference when multiple routing protocols discover routes to the same destination.
- Implement load balancing among multiple equal-cost routes.

Pre-configuration Tasks

Before configuring RIP route attributes, complete the following tasks:

- Configuring IP addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- [Configuring Basic RIP Functions](#)

Data Preparation

To configure RIP route attributes, you need the following data.

No.	Data
1	Additional metric of the interface
2	RIP preference
3	Maximum number of equal-cost routes

3.3.2 Configuring Additional Metrics of an Interface

The additional metric is the metric (hop count) to be added to the original metric of a RIP route. You can set additional metrics for received and sent RIP routes by using different commands.

Context

The additional metric is added to the original metric of the RIP route.

- The [rip metricin](#) command is used to add an additional metric to a received route. After this route is added to the routing table, its metric in the routing table changes. Running this command affects route selection on the local device and other devices on the network.
- The [rip metricout](#) command is used to add an additional metric to a sent route. When this route is advertised, an additional metric is added to this route, but the metric of the route in the routing table does not change. Running this command does not affect route selection on the local device or other devices on the network.

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
rip metricin value
```

The metric added to a received route is set.

Step 4 Run:

```
rip metricout { value | { acl-number | acl-name acl-name | ip-prefix ip-prefix-name } value1 }
```

The metric added to a sent route is set.

 **NOTE**

You can specify the value of the metric to be added to the RIP route that passes the filtering policy by specifying *value1* through an ACL or an IP prefix list. If a RIP route does not pass the filtering, its metric is increased by 1.

---End

3.3.3 Configuring RIP Preference

When there are routes discovered by multiple routing protocols on the same Router, you can make the Router prefer RIP routes by setting the RIP preference.

Context

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rip [ process-id ]
```

The RIP process is enabled and the RIP view is displayed.

Step 3 Run:

```
preference { preference | route-policy route-policy-name } *
```

The RIP preference is set.

By default, the RIP preference is 100.

---End

3.3.4 Setting the Maximum Number of Equal-Cost Routes

By setting the maximum number of equal-cost RIP routes, you can change the number of routes for load balancing.

Context

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rip [ process-id ]
```

The RIP process is enabled and the RIP view is displayed.

Step 3 Run:

```
maximum load-balancing number
```

The maximum number of equal-cost routes is set.

NOTE

The range and default value of the maximum number of equal-cost routes may vary according to products and protocols. You can change the range and default value after purchasing the license.

---End

3.3.5 Checking the Configuration

After RIP route attributes are successfully set, you can view the current running status, configuration, and routing information of RIP.

Prerequisite

The configurations of RIP route attributes are complete.

Procedure

- Run **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*] command to check the running status and configuration of RIP.
- Run **display rip** *process-id* **database** command to check all activated routes in the RIP database.
- Run **display rip** *process-id* **route** command to check all activated and inactivated RIP routes.

---End

Example

Run the **display rip** *process-id* **database** command, and you can view information about the database of the specified RIP process.

```
<HUAWEI> display rip 100 database
 8.0.0.0/8, cost 5, ClassfulSumm
 8.8.8.8/32, cost 5, nexthop 23.1.1.2
 9.0.0.0/8, cost 7, ClassfulSumm
 9.9.9.9/32, cost 7, Imported
```

```
12.0.0.0/8, cost 1, ClassfulSumm
12.1.1.0/24, cost 1, nexthop 23.1.1.2
23.0.0.0/8, cost 0, ClassfulSumm
23.1.1.0/24, cost 0, Rip-interface
```

3.4 Controlling the Advertising of RIP Routing Information

To meet the requirements of complex networks, it is required to accurately control the advertising of RIP routing information.

3.4.1 Establishing the Configuration Task

RIP routing information can be advertised through default routes, Update packets, and imported external routes.

Applicable Environment

In practice, to meet the requirements of a network, you need to control the advertising of RIP routing information accurately. After performing configuration procedures in this section, you can:

- Advertise default routes to neighbors.
- Suppress interfaces from sending RIP Update packets.
- Import external routes from various routing protocols and filter routes to be advertised.

Pre-configuration Tasks

Before configuring the router to control the advertising of RIP routing information, complete the following tasks:

- Configuring IP addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- [Configuring Basic RIP Functions](#)

Data Preparation

To control the advertising of RIP routing information, you need the following data.

No.	Data
1	Metric of the default route to be advertised
2	Number of the interface that is suppressed from sending RIP Update packets
3	Protocol name and process ID of the external route to be imported

3.4.2 Configuring RIP to Advertise Default Routes

A default route is a route destined for 0.0.0.0. By default, RIP does not advertise default routes to its neighbors.

Context

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rip [ process-id ]
```

The RIP process is enabled and the RIP view is displayed.

Step 3 Run:

```
default-route originate [ match default [ avoid-learning ] ] [ cost cost ]
```

RIP is configured to advertise a default route.

You can configure a router to advertise a default route or set the default routes in routing table with the specified metric to its RIP neighbors.

---End

3.4.3 Disabling an Interface from Sending Update Packets

Disabling interfaces from sending Update packets is a method of preventing routing loop and can be implemented in two ways.

Context

Do as follows on the RIP router:

Procedure

- Configuration in a RIP Process (with a High Priority)

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
rip [ process-id ]
```

The RIP process is enabled and the RIP view is displayed.

3. Run the following command as required.

Run:

```
silent-interface all
```

All interfaces are disabled from sending Update packets.

Run:

```
silent-interface interface-type interface-number
```

An interface is disabled from sending Update packets.

You can set an interface to silent so that it only receives Update packets to update its routing table. The **silent-interface** command takes precedence over the **rip output** command in the interface view.

By default, an interface can receive and send Update packets.

- Configuration in the Interface View (with a Low Priority)

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
undo rip output
```

The interface is disabled from sending RIP Update packets.

By running this command, you can specify whether to send RIP Update packets on an interface. The **silent-interface** command takes precedence over the **undo rip output** command. By default, an interface is allowed to send RIP Update packets.

----End

3.4.4 Configuring RIP to Import External Routes

To enrich its routing information, RIP can import the routes learned by other processes or other routing protocols.

Context

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rip [ process-id ]
```

The RIP process is enabled and the RIP view is displayed.

Step 3 (Optional) Run:

```
default-cost cost
```

The default cost of imported routes is set.

If no cost is specified when external routes are imported, the default cost is used.

Step 4 Run:

```
import-route bgp [ cost { cost | transparent } | route-policy route-policy-name ]
* or import-route { { static | direct } | { { rip | ospf | isis } [ process-id ] } }
[ cost cost | route-policy route-policy-name ] *
```

External routes are imported.

Step 5 (Optional) Run:

```
filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name } export
[ protocol [ process-id ] | interface-type interface-number ]
```

The imported routes are filtered when being advertised.

If the routing information to be advertised by RIP contains the routes imported from other routing protocols, you can specify *protocol* to filter the specified routes. If *protocol* is not specified, all the routing information to be advertised will be filtered, including the imported routes and local RIP routes (directly connected routes).

NOTE

The Tag field in RIP is 16 bits in length, whereas the Tag field in other routing protocols is 32 bits in length. If the routes of other routing protocols are imported and the tag is used in the routing policy, ensure that the tag value does not exceed 65535. Otherwise, the routing policy becomes invalid or the matching result is incorrect.

---End

3.4.5 Checking the Configuration

After the function of controlling the advertising of RIP routing information is successfully configured, you can view the current running status, configuration, and routing information of RIP.

Prerequisite

The configurations of controlling the advertising of RIP routing information are complete.

Procedure

- Run the **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*] command to check the running status and configuration of RIP.
- Run the **display rip process-id database** command to check all activated routes in the RIP database.
- Run the **display rip process-id route** command to check all activated and inactivated RIP routes.

---End

Example

Run the **display rip process-id database** command, and you can view information about the database of the specified RIP process.

```
<HUAWEI> display rip 100 database
 8.0.0.0/8, cost 5, ClassfulSumm
 8.8.8.8/32, cost 5, nexthop 23.1.1.2
 9.0.0.0/8, cost 7, ClassfulSumm
 9.9.9.9/32, cost 7, Imported
12.0.0.0/8, cost 1, ClassfulSumm
12.1.1.0/24, cost 1, nexthop 23.1.1.2
23.0.0.0/8, cost 0, ClassfulSumm
23.1.1.0/24, cost 0, Rip-interface
```


3.5 Controlling the Receiving of RIP Routing Information

To meet the requirements of complex networks, it is required to accurately control the receiving of RIP routing information.

3.5.1 Establishing the Configuration Task

You can obtain RIP routing information by receiving Update packets and host routes.

Applicable Environment

In practice, to meet the requirements of a complex network, it is required to control the receiving of RIP routing information accurately. After performing configuration procedures in this section, you can:

- Disable an interface from receiving RIP Update packets.
- Filter the received routing information.
- Import external routes from various routing protocols and filter the imported routes.

Pre-configuration Tasks

Before configuring a router to control the receiving of RIP routing information, complete the following tasks:

- Configuring IP addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- [Configuring Basic RIP Functions](#)

Data Preparation

To control the receiving of RIP routing information, you need the following data.

No.	Data
1	ACL used to filter the routing information

3.5.2 Disabling an Interface from Receiving RIP Update Packets

Disabling interfaces from receiving Update packets is a method of preventing routing loops.

Context

The [undo rip input](#) command can be used to disable an interface from receiving update packets. Its priority is lower than that of the [silent-interface](#) command.

By default, an interface is allowed to receive RIP Update packets.

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
undo rip input
```

The interface is disabled from receiving RIP Update packets.

----End

3.5.3 Disabling RIP from Receiving Host Routes

When you disable RIP from receiving host routes on a router, the router rejects to receive host routes. This prevents the router from receiving a large number of unnecessary routes and thus avoiding wasting network resources.

Context

In certain situations, a router may receive a large number of host routes from the same network segment. These routes are not required in route addressing, but consume many network resources. You can configure the router to refuse to accept host routes by disabling RIP from accepting host routes.

By default, host routes are added to the routing table.

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rip [ process-id ]
```

The RIP process is enabled and the RIP view is displayed.

Step 3 Run:

```
undo host-route
```

RIP is disabled from adding host routes to the routing table.

----End

3.5.4 Configuring RIP to Filter the Received Routes

By specifying ACLs and IP prefix lists, you can configure the inbound policy to filter the routes to be received. You can also configure a router to receive only RIP packets from a specified neighbor.

Context

The router can filter routing information. To filter the imported and advertised routes, you can configure inbound and outbound routing policies by specifying ACLs and IP prefix lists.

You can also configure the router to receive RIP packets only from a specified neighbor.

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rip [ process-id ]
```

The RIP process is enabled and the RIP view is displayed.

Step 3 Run the following commands to configure RIP to filter the received routes as required:

● Run:

```
filter-policy { acl-number | acl-name acl-name } import
```

The learned routing information is filtered based on an ACL.

● Run:

```
filter-policy gateway ip-prefix-name import
```

The routing information advertised by neighbors is filtered based on the IP prefix list.

● Run:

```
filter-policy ip-prefix ip-prefix-name [ gateway ip-prefix-name ] import  
[ interface-type interface-number ]
```

The routes learned by the specified interface are filtered based on the IP prefix list and neighbors.

 **NOTE**

To filter routes to be advertised, run the `filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name } export [protocol [process-id] | interface-type interface-number]` command.

----End

3.5.5 Checking the Configuration

After the function of controlling the receiving of RIP routing information is successfully configured, you can view the current running status, configuration, and routing information of RIP.

Procedure

- Run the **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*] command to check the running status and configuration of RIP.
- Run the **display rip process-id database** [**verbose**] command to check all activated RIP routes in the database.
- Run the **display rip process-id interface** [*interface-type interface-number*] [**verbose**] command to check information about the RIP interface.
- Run the **display rip process-id neighbor** [**verbose**] command to check information about RIP neighbors.
- Run the **display rip process-id route** command to check all activated and inactivated RIP routes.

----End

Example

Run the **display rip process-id database** command, and you can view information about the database of the specified RIP process.

```
<HUAWEI> display rip 100 database
 8.0.0.0/8, cost 5, ClassfulSumm
 8.8.8.8/32, cost 5, nexthop 23.1.1.2
 9.0.0.0/8, cost 7, ClassfulSumm
 9.9.9.9/32, cost 7, Imported
12.0.0.0/8, cost 1, ClassfulSumm
12.1.1.0/24, cost 1, nexthop 23.1.1.2
23.0.0.0/8, cost 0, ClassfulSumm
23.1.1.0/24, cost 0, Rip-interface
```

3.6 Configuring RIP-2 Features

Different from RIP-1, RIP-2 supports VLSM, CIDR, and authentication, ensuring higher security.

3.6.1 Establishing the Configuration Task

Before configuring RIP-2 features, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

RIP-2 is a type of classless routing protocol. A RIP-2 packet carries subnet mask information. Deploying a RIP-2 network saves IP addresses. On a network where the IP addresses of devices are not consecutive, only RIP-2 can be deployed, and RIP-1 cannot be deployed.

RIP-2 features include:

- RIP-2 route summarization
- RIP-2 authentication mode

Pre-configuration Tasks

Before configuring RIP-2 features, complete the following tasks:

- Configuring the link layer protocol
- Configuring IP addresses for interfaces to ensure that neighboring nodes are reachable at the network layer

Data Preparation

To configure RIP-2 features, you need the following data.

No.	Data
1	RIP-2 process ID
2	Network segment where the RIP-2 interface resides

3.6.2 Configuring RIP-2 Route Summarization

Route summarization is enabled in RIP-1 by default, and cannot be manually configured. RIP-2 supports VLSM and CIDR. You can configure route summarization in RIP-2 to improve the flexibility of RIP-2. To broadcast all subnet routes, you can disable route summarization in RIP-2.

Context

Route summarization indicates that multiple subnet routes on the same natural network segment are summarized into one route with the natural mask when being advertised to other network segments. Therefore, route summarization reduces the network traffic and the size of the routing table.

Route summarization does not take effect in RIP-1. RIP-2 supports Variable Length Subnet Mask (VLSM) and Classless Interdomain Routing (CIDR). To broadcast all subnet routes, you can disable automatic route summarization of RIP-2.

Do as follows on the RIP router:

Precautions

Route summarization is invalid when split horizon or poison reverse is configured. When the summarized routes are sent outside the natural network boundary, split horizon or poison reverse in related views needs to be disabled.

Procedure

- Enabling RIP-2 Automatic Route Summarization
 1. Run:
`system-view`
The system view is displayed.
 2. Run:
`rip [process-id]`
The RIP process is enabled and the RIP view is displayed.
 3. Run:
`rip version 2`

RIP-2 is configured.

4. Run:

```
summary
```

RIP-2 automatic route summarization is enabled.

 **NOTE**

The **summary** command is used in the RIP view to enable classful network-based route summarization.

● Configuring RIP-2 to Advertise the Summary Address

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
rip summary-address ip-address mask [ avoid-feedback ]
```

The local summary address of RIP-2 is advertised.

 **NOTE**

The **rip summary-address ip-address mask [avoid-feedback]** command is run in the interface view to enable classless network-based route summarization.

----End

3.6.3 Configuring Packet Authentication of RIP-2

RIP-2 supports the ability to authenticate protocol packets and provides two authentication modes, Simple authentication and Message Digest 5 (MD5) authentication, to enhance security.

Context

RIP-2 supports two authentication modes:

- Simple authentication
- MD5 authentication

In simple authentication mode, the unencrypted authentication key is sent in every RIP-2 packet. Therefore, simple authentication does not guarantee security, and cannot meet the requirements for high security.

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run the following command as required:

- Run:

```
rip authentication-mode simple password
```

Simple authentication in the plain text is configured for RIP-2 packets.

- Run:

```
rip authentication-mode md5 { nonstandard { password-key1 key-id | keychain  
keychain-name } | usual password-key2 }
```

MD5 authentication in the cipher text is configured for RIP-2 packets.

 **NOTE**

The MD5 type must be specified if MD5 authentication is configured. The **usual** type supports IETF standard authentication packets, and the **nonstandard** type supports nonstandard authentication packets. The MD5 authentication password that starts and ends with \$@\$@ is invalid, because \$@\$@ is used to distinguish old and new passwords.

----End

3.6.4 Checking the Configuration

After RIP-2 features are successfully configured, you can view the current running status, configuration, and routing information of RIP.

Prerequisite

The configurations of RIP-2 features are complete.

Procedure

- Run the **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*] command to check the running status and configuration of RIP.
- Run the **display rip process-id database** [**verbose**] command to check all activated RIP routes in the database.
- Run the **display rip process-id route** command to check all activated and inactivated RIP routes.

----End

3.7 Optimizing a RIP Network

You can adjust and optimize the RIP network performance by configuring RIP functions in special network environments, such as configuring RIP timers, setting the interval for sending packets, and setting the maximum number of packets to be sent.

3.7.1 Establishing the Configuration Task

Before adjusting and optimizing the RIP network performance, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

On certain networks, you need to configure RIP features and optimize the performance of a RIP network. After performing configuration procedures in this section, you can:

- Change the convergence speed of the RIP network by adjusting the values of RIP timers.
- Reduce the consumption of device resources and network bandwidth by adjusting the number of packets to be sent by interfaces and the interval at which packets are sent.
- Configure split horizon or poison reverse to prevent routing loops.
- After the replay-protect function is enabled, neighbors can communicate after a RIP process is restarted.
- Check the validity of packets and authenticate packets on a network demanding high security.
- Run RIP on a link that does not support broadcast or multicast packets.

Pre-configuration Tasks

Before optimizing a RIP network, complete the following tasks:

- Configuring IP addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- [Configuring Basic RIP Functions](#)

Data Preparation

To optimize a RIP network, you need the following data.

No.	Data
1	Values of timers
2	Number of Update packets that an interface sends each time and interval for sending an Update packet
3	Maximum number of equal-cost routes
4	Packet authentication mode and password
5	IP addresses of RIP neighbors

3.7.2 Configuring RIP Timers

RIP has three timers: Update timer, Age timer and Garbage-collect timer. Changing the values of the three timers affects the RIP convergence speed.

Context

RIP has three timers: Update timer, Age timer and Garbage-collect timer. Changing the values of the three timers affects the RIP convergence speed. For details on timers, see corresponding description in the chapter "RIP" in the *HUAWEI NetEngine80E/40E Router Feature Description - IP Routing*.

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rip [ process-id ]
```

The RIP process is enabled and the RIP view is displayed.

Step 3 Run:

```
timers rip update age garbage-collect
```

RIP timers are configured.

NOTE

- RIP timers take effect immediately after being changed.
- Route flapping occurs if the values of the times are set improperly. The relationship between the values is as follows: *update* must be smaller than *age* and *update* must be smaller than *garbage-collect*. For example, if the update time is longer than the aging time, and a RIP route changes within the update time, the router cannot inform its neighbors of the change on time.
- You must configure RIP timers based on the network performance and uniformly on all the routers running RIP. This avoids unnecessary network traffic or route flapping.

By default, the Update timer is 30s; the Age timer is 180s; the Garbage-collect timer is four times the Update timer, namely, 120s.

In practice, the Garbage-collect timer is not fixed. If the Update timer is set to 30s, the Garbage-collect timer may range from 90s to 120s.

Before permanently deleting an unreachable route from the routing table, RIP advertises this route (with the metric being set to 16) by periodically sending Update packets four times. Subsequently, all the neighbors know that this route is unreachable. Because a route may not always become unreachable at the beginning of an Update period, the Garbage-collect timer is actually three or four times the Update timer.

----End

3.7.3 Setting the Interval for Sending Packets and the Maximum Number of the Sent Packets

By setting the interval for sending RIP Update packets and the maximum number of Update packets to be sent each time, you can effectively control the memory used by a Router to process RIP Update packets.

Context

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
rip pkt-transmit { interval interval | number pkt-count } *
```

The interval for sending Update packets and the maximum number of packets sent each time are set on the interface.

----End

3.7.4 Configuring Split Horizon and Poison Reverse

You can configure split horizon and poison reverse to prevent routing loops.

Context

If both split horizon and poison reverse are configured, only poison reverse takes effect.

On Non-Broadcast Multi-Access (NBMA) networks such as frame relay (FR) and X.25 networks, if no sub-interface is configured, split horizon needs to be disabled to ensure that routing information is transmitted correctly.

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run the following command as required:

- Run:

```
rip split-horizon
```

Split horizon is enabled.

- Run:

```
rip poison-reverse
```

Poison reverse is enabled.

----End

3.7.5 Enabling replay-protect Function

By enabling the replay-protect function, you can obtain the Identification field in the last RIP packet sent by a RIP interface before it goes Down. This prevents RIP routing information on both ends from being unsynchronized or lost.

Context

If the Identification field in the last RIP packet sent before a RIP interface goes Down is X, after the interface goes Up, the Identification field in the subsequent RIP packet sent by this interface becomes 0. If the remote end does not receive the RIP packet with the Identification field being 0, subsequent RIP packets will be discarded until the remote end receives the RIP packet with the Identification field being X+1. This leads to the unsynchronization and loss of RIP routing information of both ends.

To solve this problem, you need to enable the replay-protect function so that RIP can obtain the Identification field in the last RIP packet sent before the RIP interface goes Down and increase the Identification field in the subsequent RIP packet by one.

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
rip authentication-mode md5 nonstandard
```

RIPv2 is configured to use MD5 authentication, and authentication packets use the nonstandard packet format.

 **NOTE**

Before running the **rip replay-protect** command, run the **rip authentication-mode md5 nonstandard** command in the RIP interface view to configure MD5 authentication packets to use the nonstandard packet format (private standard).

Step 4 Run:

```
rip replay-protect
```

The replay-protect function is enabled.

 **NOTE**

- For details of the Identification field in an IP packet, see *Feature Description - IP Services*.
- If you run the **rip replay-protect** command in the same view multiple times, only the last configuration takes effect.

----End

3.7.6 Configuring RIP to Check the Validity of Update Packets

The check on RIP Update packets includes the check on zero fields in RIPv1 packets and the check on source addresses of RIP Update packets. The two types of check have different functions and applications.

Context

Do as follows on the RIP router:

Procedure

- Configuring the Zero Field Check for RIPv1 Packets

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
rip [ process-id ]
```

The RIP process is enabled and the RIP view is displayed.

3. Run:

```
checkzero
```

The zero field check is configured for RIPv1 packets.

Certain fields in a RIPv1 packet must be 0s, and these fields are called zero fields. RIPv1 checks the zero fields on receiving a packet. If the value of any zero field in a RIPv1 packet is not 0, this packet is not processed.

As a RIPv2 packet does not contain any zero field, configuring the zero field check is invalid in RIPv2.

- Configuring the Source Address Check for RIP Update Packets

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
rip [ process-id ]
```

The RIP process is enabled and the RIP view is displayed.

3. Run:

```
verify-source
```

The source address check is configured for RIP Update packets.

When receiving a packet, RIP checks the source address of the packet. If the packet fails in the check, it is not processed.

By default, the source address check is enabled.

----End

3.7.7 Configuring RIP Neighbors

Generally, RIP sends packets by using broadcast or multicast addresses. To run RIP on the links that do not support the forwarding of broadcast or multicast packets, you need to specify RIP neighbors.

Context

Generally, RIP sends packets by using broadcast or multicast addresses. If RIP needs to run on the links that do not support the forwarding of broadcast or multicast packets, you need to configure the devices at both ends of the link as each other's neighbor.

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rip [ process-id ]
```

The RIP process is enabled and the RIP view is displayed.

Step 3 Run:

```
peer ip-address
```

The RIP neighbor is configured.

---End

3.7.8 Checking the Configuration

After the function of adjusting and optimizing the RIP network performance is successfully configured, you can view the current running status, routing information, neighbor information, and interface information of RIP.

Prerequisite

The configurations of optimizing a RIP network are complete.

Procedure

- Run the **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*] command to check the running status and configuration of RIP.
- Run the **display rip** *process-id* **database** [**verbose**] command to check all activated RIP routes in the database.
- Run the **display rip** *process-id* **interface** [*interface-type interface-number*] [**verbose**] command to check information about the RIP interface.
- Run the **display rip** *process-id* **neighbor** [**verbose**] command to check information about RIP neighbors.

- Run the **display rip process-id route** command to check all activated and inactivated RIP routes.

---End

Example

Run the **display rip process-id interface [interface-type interface-number] [verbose]** command, and you can view RIP information about the specified interface. The command output shows that the interface status is Up.

```
<HUAWEI> display rip 1 interface GigabitEthernet1/0/0
-----
Interface          IP Address      State    Protocol          MTU
-----
GE 1/0/0           1.1.1.2         UP      RIPv1 Compatible  500
```

3.8 Configuring RIP GR

This section describes how to configure RIP GR to avoid incorrect route calculation and packet loss after a RIP router restarts.

3.8.1 Establishing the Configuration Task

In practice, you can configure RIP GR on the device with two main control boards to prevent service forwarding from being affected by the fault on one main control board.

Applicable Environment

To avoid traffic interruption and route flapping caused by master/slave switchover, you can enable RIP graceful restart (GR). GR is a technology used to ensure normal traffic forwarding and non-stop forwarding of key services during the restart of routing protocols.

After a RIP process is restarted through GR, the Restarter and the Helper re-establish the neighbor relationship and update the routing table and forwarding table. This ensures non-stop traffic forwarding and stabilizes the network topology. During RIP GR, except the neighbor of the device where master/slave switchover occurs, other routers do not detect the route change.

NOTE

In practice, you can configure RIP GR on the device with two main control boards to prevent service forwarding from being affected by the fault on one main control board.

Pre-configuration Tasks

Before configuring RIP GR, complete the following tasks:

- Configuring IP addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- Configuring basic RIP functions to establish the neighbor relationship successfully

Data Preparation

To configure RIP GR, you need the following data

No.	Data
1	RIP process ID
2	Parameters for establishing a GR session

3.8.2 Enabling RIP GR

To avoid traffic interruption and route flapping caused by master/slave switchover, you can enable RIP GR.

Context

Do as follows on the router to be enabled with GR:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rip [ process-id ]
```

The RIP view is displayed.

Step 3 Run:

```
graceful-restart [ period period | wait-time time | planned-only time ] *
```

RIP GR is enabled.

When most routers on a network do not support RIP GR, setting **wait-time time** to a greater value is recommended. This ensures that the Restarter has enough time to learn correct routes.

----End

Follow-up Procedure

If the Restarter finishes GR within the GR period specified by **period period**, the Restarter automatically exits from GR. Otherwise, the Restarter is forced to exit from GR.

3.8.3 Checking the Configuration

After RIP GR is configured, you can check the RIP GR status.

Prerequisite

The configurations of RIP GR are complete.

Procedure

- Run the **display rip process-id graceful-restart [verbose]** command to check the status of RIP GR.

----End

Example

Run the **display rip 1 graceful-restart** command, and you can view the GR configuration of RIP process 1.

```
<HUAWEI> display rip 1 graceful-restart
Restart mode      : Restarting
Restart status    : In Progress - Waiting for updates
Last complete reason : None
Update progress summary:
-----
Restart capable peers : 0
  Completed: 0   Inprogress: 0
Restart incapable peers: 1
  Completed: 0   Inprogress: 1
Update period finishes in 293 seconds
```

3.9 Configuring the Network Management Function in RIP

By binding RIP to MIBs, you can view and configure RIP through the NMS.

3.9.1 Establishing the Configuration Task

Before binding RIP to MIBs, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

After performing configuration procedures in this section, you can bind RIP to a MIB.

Pre-configuration Tasks

Before configuring the network management function in RIP, complete the following tasks:

- Configuring IP addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- **Configuring Basic RIP Functions**

Data Preparation

None.

3.9.2 Binding RIP to MIBs

Before binding RIP to MIBs, you need to specify the RIP process ID.

Context

Do as follows on the RIP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rip mib-binding process-id
```

RIP is bound to MIBs.

This command is used to bind a RIP process ID to MIBs and specify the ID of the RIP process that accepts Simple Network Management Protocol (SNMP) requests.

---End

3.9.3 Checking the Configuration

After RIP and MIBs are successfully bound, you can view binding information in the current RIP configuration.

Prerequisite

The configurations of the network management function in RIP are complete.

Procedure

Step 1 Run the **display current-configuration** command to check the parameters that take effect on the router.

---End

3.10 Maintaining RIP

This section describes how to reset RIP connections and clear RIP information.

3.10.1 Resetting RIP

Restarting RIP can reset RIP.

Context



CAUTION

The RIP neighbor relationship is deleted after you reset RIP connections with the **reset rip** command. So, confirm the action before you use the command.

To reset RIP connections, run the following **reset** commands in the user view.

Procedure

- Run the **reset rip process-id configuration** command in the user view to reset the parameters of the specified RIP process. When the RIP process starts, all parameters use default values.

----End

3.10.2 Clearing RIP

This section describes how to clear statistics about RIP counters.

Context



CAUTION

RIP information cannot be restored after it is cleared. Exercise caution when running the commands.

To clear RIP information, run the following **reset** command in the user view.

Procedure

- Run the **reset rip process-id statistics [interface [interface-type interface-number [neighbor [neighbor-ip-address]]]]** command in the user view to clear statistics about the counter that is maintained by a specified RIP process.

----End

3.11 Configuration Examples

In actual networking, RIP versions and whether to import external routes will affect which routes can be learned.

NOTE

Examples in this document use interface numbers and link types of the NE40E-X8. In real world situations, the interface numbers and link types may be different from those used in this document.

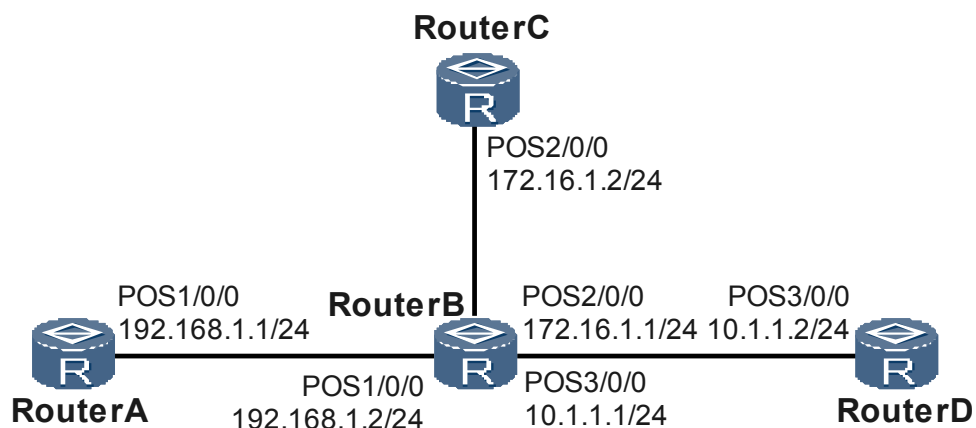
3.11.1 Example for Configuring RIP Version

Before using RIP, you need to configure basic RIP functions and specify a RIP version. You can run commands to view the configuration results.

Networking Requirements

As shown in [Figure 3-1](#), it is required that RIP be enabled on all interfaces of Router A, Router B, Router C, and Router D and the routers interconnect with each other by using RIP-2.

Figure 3-1 Networking diagram for configuring the RIP version number



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IP address for each interface to ensure that neighboring nodes are reachable at the network layer.
2. Enable RIP on each router and configure basic RIP functions.
3. Configure RIP-2 on each router and check information about classless routes.

Data Preparation

To complete the configuration, you need the following data:

- Network segment (192.168.1.0) to be enabled with RIP on Router A
- Network segments (192.168.1.0, 172.16.0.0, and 10.0.0.0) to be enabled with RIP on Router B
- Network segment (172.16.0.0) to be enabled with RIP on Router C
- Network segment (10.0.0.0) to be enabled with RIP on Router D
- RIP-2 on Router A, Router B, Router C, and Router D

Procedure

Step 1 Configure an IP address for each interface.

The configuration details are not described here.

Step 2 Configure basic RIP functions.

Configure Router A.

```
[RouterA] rip
[RouterA-rip-1] network 192.168.1.0
[RouterA-rip-1] quit
```

Configure Router B.

```
[RouterB] rip
```

```
[RouterB-rip-1] network 192.168.1.0
[RouterB-rip-1] network 172.16.0.0
[RouterB-rip-1] network 10.0.0.0
[RouterB-rip-1] quit
```

Configure Router C.

```
[RouterC] rip
[RouterC-rip-1] network 172.16.0.0
[RouterC-rip-1] quit
```

Configure Router D.

```
[RouterD] rip
[RouterD-rip-1] network 10.0.0.0
[RouterD-rip-1] quit
```

Check the RIP routing table of Router A.

```
[RouterA] display rip 1 route
Route Flags: R - RIP, T - TRIP
              A - Aging, G - Garbage-collect
-----
```

Peer	Destination/Mask	Nexthop	Cost	Tag	Flags	Sec
192.168.1.2 on Pos1/0/0	10.1.1.0/24	192.168.1.2	1	0	RA	32
	172.16.1.0/24	192.168.1.2	1	0	RA	32

The preceding display shows that the routes advertised by RIP-1 carry natural masks.

Step 3 Configure the RIP version number.

Configure RIP-2 on Router A.

```
[RouterA] rip
[RouterA-rip-1] version 2
[RouterA-rip-1] quit
```

Configure RIP-2 on Router B.

```
[RouterB] rip
[RouterB-rip-1] version 2
[RouterB-rip-1] quit
```

Configure RIP-2 on Router C.

```
[RouterC] rip
[RouterC-rip-1] version 2
[RouterC-rip-1] quit
```

Configure RIP-2 on Router D.

```
[RouterD] rip
[RouterD-rip-1] version 2
[RouterD-rip-1] quit
```

Step 4 Verify the configuration.

Check the RIP routing table of Router A.

```
[RouterA] display rip 1 route
Route Flags: R - RIP
              A - Aging, G - Garbage-collect
-----
```

Peer	Destination/Mask	Nexthop	Cost	Tag	Flags	Sec
192.168.1.2 on Pos1/0/0	10.1.1.0/24	192.168.1.2	1	0	RA	32
	172.16.1.0/24	192.168.1.2	1	0	RA	32

The preceding display shows that the routes advertised by RIPv2 carry subnet masks.

----End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.1 255.255.255.0
#
rip 1
 version 2
 network 192.168.1.0
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 172.16.1.1 255.255.255.0
#
interface Pos3/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
rip 1
 version 2
 network 192.168.1.0
 network 172.16.0.0
 network 10.0.0.0
#
return
```

- Configuration file of Router C

```
#
 sysname RouterC
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 172.16.1.2 255.255.255.0
#
rip 1
 version 2
 network 172.16.0.0
#
return
```

- Configuration file of Router D

```
#
 sysname RouterD
#
interface Pos3/0/0
```

```

link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
rip 1
version 2
network 10.0.0.0
#
return
    
```

3.11.2 Example for Configuring RIP to Import External Routes

To obtain more RIP routing information, you can configure RIP to import external routes. You can run commands to view the configuration results.

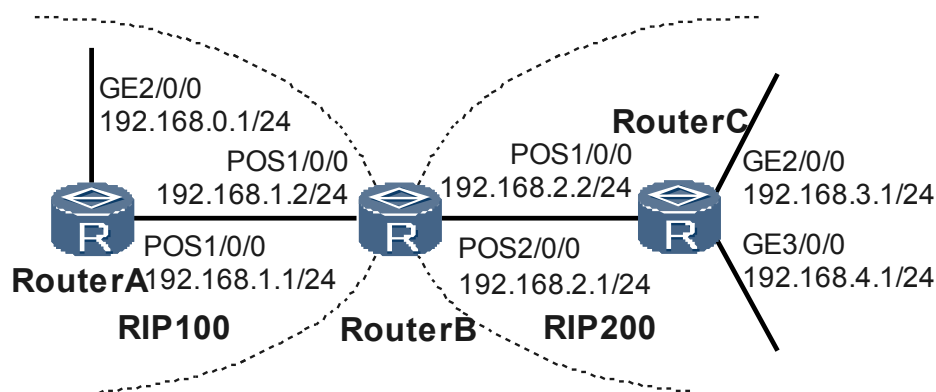
Networking Requirements

As shown in [Figure 3-2](#), two RIP processes, RIP 100 and RIP 200, run on Router B. Router B exchanges routing information with Router A and Router C through RIP 100 and RIP 200 respectively.

It is required that the two RIP processes of Router B import RIP routes from each other. The cost of the routes imported from RIP 200 defaults to 3.

In addition, a filtering policy needs to be configured on Router B to filter out the route 192.168.4.0/24 imported from RIP 200 and prevent it from being advertised to Router A.

Figure 3-2 Networking diagram for configuring RIP to import external routes



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable RIP 100 and RIP 200 on each router and specify network segments.
2. Configure the two RIP processes on Router B to import routes from each other and set the default cost of the routes imported from RIP 200 to 3.
3. Configure an ACL on Router B to filter the routes imported from RIP 200.

Data Preparation

To complete the configuration, you need the following data:

- RIP 100 and network segments (192.168.1.0 and 192.168.0.0) on Router A
- RIP 100, RIP 200, and network segments (192.168.1.0 and 192.168.2.0) on Router B
- RIP 200 and network segments (192.168.2.0, 192.168.3.0, and 192.168.4.0) on Router C
- Default cost of the routes imported by Router B from RIP 200, which is 3
- ACL 2000 that is used to deny the route with the source network segment being 192.168.4.0

Procedure

Step 1 Configure an IP address for each interface.

The configuration details are not described here.

Step 2 Configure basic RIP functions.

Enable RIP process 100 on Router A.

```
[RouterA] rip 100
[RouterA-rip-100] network 192.168.0.0
[RouterA-rip-100] network 192.168.1.0
[RouterA-rip-100] quit
```

Enable two RIP processes, RIP 100 and RIP 200, on Router B.

```
[RouterB] rip 100
[RouterB-rip-100] network 192.168.1.0
[RouterB-rip-100] quit
[RouterB] rip 200
[RouterB-rip-200] network 192.168.2.0
[RouterB-rip-200] quit
```

Enable RIP process 200 on Router C.

```
[RouterC] rip 200
[RouterC-rip-200] network 192.168.2.0
[RouterC-rip-200] network 192.168.3.0
[RouterC-rip-200] network 192.168.4.0
[RouterC-rip-200] quit
```

Check the routing table of Router A.

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 7          Routes : 7
Destination/Mask    Proto Pre  Cost  Flags      NextHop         Interface
127.0.0.0/8         Direct 0     0           D         127.0.0.1       InLoopBack0
127.0.0.1/32        Direct 0     0           D         127.0.0.1       InLoopBack0
192.168.0.0/24      Direct 0     0           D         192.168.0.1     GigabitEthernet2/0/0
192.168.0.1/32      Direct 0     0           D         127.0.0.1       InLoopBack0
192.168.1.0/24      Direct 0     0           D         192.168.1.1     Pos1/0/0
192.168.1.1/32      Direct 0     0           D         127.0.0.1       InLoopBack0
```

Step 3 Configure RIP to import external routes.

Set the default route cost to 3 on Router B and configure the two RIP processes to import routes from each other.

```
[RouterB] rip 100
[RouterB-rip-100] default-cost 3
[RouterB-rip-100] import-route rip 200
[RouterB-rip-100] quit
[RouterB] rip 200
[RouterB-rip-200] import-route rip 100
[RouterB-rip-200] quit
```

Check the routing table of Router A after the routes are imported. The routes to network segments 192.168.2.0/24, 192.168.3.0/24, and 192.168.4.0/24 are imported to RIP.

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
    Destinations : 10          Routes : 10
Destination/Mask    Proto Pre  Cost   Flags      NextHop         Interface
 127.0.0.0/8        Direct 0     0       D         127.0.0.1       InLoopBack0
 127.0.0.1/32       Direct 0     0       D         127.0.0.1       InLoopBack0
192.168.0.0/24      Direct 0     0       D         192.168.0.1     GigabitEthernet2/0/0
192.168.0.1/32     Direct 0     0       D         127.0.0.1       InLoopBack0
192.168.1.0/24     Direct 0     0       D         192.168.1.1     Pos1/0/0
192.168.1.1/32     Direct 0     0       D         127.0.0.1       InLoopBack0
192.168.2.0/24     RIP    100   4       D         192.168.1.2     Pos1/0/0
192.168.3.0/24     RIP    100   4       D         192.168.1.2     Pos1/0/0
192.168.4.0/24     RIP    100   4       D         192.168.1.2     Pos1/0/0
```

Step 4 Configure RIP to filter the imported routes.

Configure an ACL on Router B and set a rule to deny the packets with the source address being 192.168.4.0/24.

```
[RouterB] acl 2000
[RouterB-acl-basic-2000] rule deny source 192.168.4.0 0.0.0.255
[RouterB-acl-basic-2000] rule permit
[RouterB-acl-basic-2000] quit
```

Filter out the route 192.168.4.0/24 imported from RIP 200 on Router B according to the ACL rule.

```
[RouterB] rip 100
[RouterB-rip-100] filter-policy 2000 export
```

Step 5 Verify the configuration.

Check the routing table of Router A after the filtering. The route to 192.168.4.0/24 does not exist in the routing table. This means that the route is filtered out.

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
    Destinations : 9          Routes : 9
Destination/Mask    Proto Pre  Cost   Flags      NextHop         Interface
 127.0.0.0/8        Direct 0     0       D         127.0.0.1       InLoopBack0
 127.0.0.1/32       Direct 0     0       D         127.0.0.1       InLoopBack0
192.168.0.0/24      Direct 0     0       D         192.168.0.1     GigabitEthernet2/0/0
192.168.0.1/32     Direct 0     0       D         127.0.0.1       InLoopBack0
192.168.1.0/24     Direct 0     0       D         192.168.1.1     Pos1/0/0
192.168.1.1/32     Direct 0     0       D         127.0.0.1       InLoopBack0
192.168.2.0/24     RIP    100   4       D         192.168.1.2     Pos1/0/0
192.168.3.0/24     RIP    100   4       D         192.168.1.2     Pos1/0/0
```

----End

Configuration Files

- Configuration file of Router A


```
#
sysname RouterA
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 192.168.0.1 255.255.255.0
#
```



```
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.1 255.255.255.0
#
rip 100
 network 192.168.0.0
 network 192.168.1.0
#
return
```

● Configuration file of Router B

```
#
 sysname RouterB
#
acl number 2000
 rule 5 deny source 192.168.4.0 0.0.0.255
 rule 10 permit
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.1 255.255.255.0
#
rip 100
 default-cost 3
 network 192.168.1.0
 filter-policy 2000 export
 import-route rip 200
#
rip 200
 network 192.168.2.0
 import-route rip 100
#
return
```

● Configuration file of Router C

```
#
 sysname RouterC
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 192.168.4.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.2 255.255.255.0
#
rip 200
 network 192.168.2.0
 network 192.168.3.0
 network 192.168.4.0
#
return
```

4 RIPng Configuration

About This Chapter

RIPng is an extension of RIP for support of IPv6.

[4.1 Introduction to RIPng](#)

RIPng is the extension of RIPv2 on IPv4 networks. Most RIP concepts apply to RIPng.

[4.2 Configuring Basic RIPng Functions](#)

To implement RIPng features, you need to configure basic RIPng functions, including creating RIPng processes and enabling RIPng on interfaces.

[4.3 Configuring RIPng Route Attributes](#)

By setting RIPng route attributes, you can change RIPng routing policies.

[4.4 Controlling the Advertising of RIPng Routing Information](#)

To meet the requirements of complex networks, it is required to accurately control the advertising of RIPng routing information.

[4.5 Controlling the Receiving of RIPng Routing Information](#)

To meet the requirements of complex networks, it is required to accurately control the receiving of RIPng routing information.

[4.6 Optimizing a RIPng Network](#)

You can adjust and optimize the RIPng network performance by configuring RIPng timers, split horizon, poison reverse, and zero field check.

[4.7 Configuring IPsec Authentication for RIPng](#)

Configuring IPsec authentication for RIPng can improve security of a RIPng network.

[4.8 Configuration Examples](#)

In actual networking, different RIPng features have different applications.

4.1 Introduction to RIPng

RIPng is the extension of RIPv2 on IPv4 networks. Most RIP concepts apply to RIPng.

4.1.1 RIPng Overview

RIPng is a distance-vector routing protocol, which measures the distance to the destination host by the hop count.

The Routing Information Protocol Next Generation (RIPng) protocol is an extension of RIPv2 that is applied to IPv4 networks. Most RIP-related concepts are applicable to RIPng.

Extension of RIP

For IPv6 applications, RIPng extends RIP as follows:

- UDP port number: In RIPng, UDP port number 521 is used to send and receive routing information.
- Multicast group address: In RIPng, FF02::9 is used as the multicast group address of RIPng routers.
- Prefix length: In RIPng, the prefix length of a destination address is 128 bits (the mask length).
- Next-hop address: In RIPng, a next-hop address is a 128-bit IPv6 address.
- Source address: In RIPng, link-local address FE80::/10 is used as the source address to send RIPng Update packets.

Operation Principle of RIPng

RIPng is a distance-vector routing protocol. It exchanges routing information by using User Datagram Protocol (UDP) packets through the port 521.

RIPng employs the hop count to measure the distance to the destination. The distance is called the routing metric. In RIPng, the hop count from the router to its directly connected network is 0, and the hop count from the router to a network, which can be reached through another router, is 1. The hop count that is equal to or exceeds 16 is defined as infinity, indicating that the destination network or host is unreachable.

By default, RIPng sends an Update packet every 30 seconds. If no Update packet is received from a neighbor in 180 seconds, RIPng marks all the routes learned from the neighbor as unreachable. If no Update packet is received from a neighbor in 300 seconds, RIPng deletes the routes of the neighbor from the routing table.

To prevent routing loops, RIPng supports split horizon and poison reverse. In addition, RIPng can import routes from other routing protocols.

Each router running RIPng manages a routing database, which contains routing entries to all accessible destinations on a network. These routing entries contain the following information:

- Destination address: indicates the IPv6 address of a host or network.
- Next-hop address: indicates the address of the next router to the destination.
- Interface: indicates the interface through which an IP packet is forwarded.

- Cost: indicates the hop count to the destination. The value is an integer that ranges from 0 to 16. If the value is 16, it indicates that the destination host or network is unreachable.
- Timer: indicates the time since a routing entry is last updated. The timer is reset to 0 when a routing entry is updated.
- Route tag: indicates a label that differentiates routes of interior routing protocols and those of exterior routing protocols.

4.1.2 RIPng Features Supported by the NE80E/40E

The RIPng features supported by the NE80E/40E include split horizon and poison reverse.

In the NE80E/40E, you can modify the routing policy of RIPng by configuring RIPng route attributes. You can also control the advertising and receiving of RIPng routing information to meet the requirements of a complex network. On certain networks, you can configure RIPng features to optimize the RIPng network performance.

4.2 Configuring Basic RIPng Functions

To implement RIPng features, you need to configure basic RIPng functions, including creating RIPng processes and enabling RIPng on interfaces.

4.2.1 Establishing the Configuration Task

To make a Router learn the routes to the network segment of an interface, ensure that the link status of the interface is Up.

Applicable Environment

The configuration of basic RIPng functions involves the configuration of basic RIPng features. After the configuration, the RIPng features are available.

During the RIPng configuration, you must enable RIPng in the system view first. If you run RIPng-related commands in the interface view, these commands take effect only after RIPng is enabled in the system view.

Pre-configuration Tasks

Before configuring basic RIPng functions, complete the following tasks:

- Enabling IPv6 on the router
- Configuring IPv6 addresses for interfaces to ensure that neighboring nodes are reachable at the network layer

Data Preparation

To configure basic RIPng functions, you need the following data.

No.	Data
1	RIPng process ID
2	Interface to be enabled with RIPng

4.2.2 Enabling RIPng and Entering the RIPng View

Creating RIPng processes is the prerequisite to performing RIPng configurations. When creating RIPng processes, you can also enter the RIPng view to perform configurations.

Context

Do as follows on the router to be enabled with RIPng:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ripng [ process-id ]
```

The RIPng process is enabled and the RIPng view is displayed.

When only one RIPng process runs, *process-id* does not need to be specified. That is, *process-id* defaults to 1.

After the RIPng process is cancelled, the **ripng process-id enable** command needs to be reconfigured on an interface.

---End

4.2.3 Enabling RIPng in the Interface View

After an interface is associated with a RIPng process, routing information on this interface can be exchanged through RIPng.

Context

Do as follows on the router to be enabled with RIPng:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

The interface is at the network side of the router. That is, the router is connected to other devices through this interface. To enable the router to learn routes to the network segment where the interface resides, ensure that the link status of the interface is Up.

Step 3 Run:

```
ripng process-id enable
```

RIPng is enabled on the specified interface.

 **NOTE**

In the interface view, this command cannot be executed if IPv6 is not enabled.
This command is inapplicable to ATM interfaces.

If the router connects to other devices through multiple interfaces, repeatedly perform Step 2 and Step 3.

----End

4.2.4 Checking the Configuration

After basic RIPng functions are successfully configured, you can view the configuration and routing information of RIPng.

Prerequisite

The configurations of basic RIPng functions are complete.

Procedure

- Run the **display ripng** [*process-id* | **vpn-instance** *vpn-instance-name*] command to check the configuration of the RIPng process.
- Run the **display ripng process-id route** command to check all activated and inactivated RIPng routes.
- Run the **display ripng process-id statistics interface** { **all** | *interface-type interface-number* [**verbose** | **neighbor** *neighbor-ipv6-address*] } command to check statistics about RIPng interfaces.

----End

Example

Run the **display ripng** [*process-id* | **vpn-instance** *vpn-instance-name*] command, and you can view the configuration of the specified RIPng process.

```
<HUAWEI> display ripng 100
Public vpn6-instance name :
RIPng process : 100
Preference : 100
Checkzero : Enabled
Default Cost : 0
Maximum number of balanced paths : 32
Update time : 30 sec Age time : 180 sec
Garbage-Collect time : 120 sec
Number of periodic updates sent : 0
Number of trigger updates sent : 1
Number of routes in database : 1
Number of interfaces enabled : 1
Total Number of routes : 0
Total Number of routes in ADV DB is : 0
```

Run the **display ripng process-id route** command, and you can view all activated and inactivated RIPng routes of the specified RIPng process.

```
<HUAWEI> display ripng 100 route
A - Aging, G - Garbage-collect
-----
```

```
Peer FE80::200:5EFF:FE04:B602 on GigabitEthernet2/0/0
Dest 3FFE:C00:C18:1::/64,
    via FE80::200:5EFF:FE04:B602, cost 2, tag 0, A, 34 Sec
Dest 3FFE:C00:C18:2::/64,
    via FE80::200:5EFF:FE04:B602, cost 2, tag 0, A, 34 Sec
Peer FE80::200:5EFF:FE04:B601 on GigabitEthernet2/0/0
Dest 3FFE:C00:C18:1::/64,
    via FE80::200:5EFF:FE04:B601, cost 2, tag 0, A, 13 Sec
Dest 3FFE:C00:C18:3::/64,
    via FE80::200:5EFF:FE04:B601, cost 2, tag 0, A, 13 Sec
Peer FE80::200:5EFF:FE04:3302 on GigabitEthernet2/0/0
Dest 100::/32,
    via FE80::200:5EFF:FE04:3302, cost 2, tag 0, A, 6 Sec
Dest 4000:1::/64,
    via FE80::200:5EFF:FE04:3302, cost 2, tag 0, A, 6 Sec
Dest 4000:2::/64,
    via FE80::200:5EFF:FE04:3302, cost 2, tag 0, A, 6 Sec
Dest 4000:3::/64,
    via FE80::200:5EFF:FE04:3302, cost 2, tag 0, A, 6 Sec
Dest 4000:4::/64,
```

Run the **display default-parameter ripng** command, and you can view the default configuration of the specified RIPng process.

```
<HUAWEI> display default-parameter ripng
-----
Protocol Level Default Configurations:
-----
Preference      : 100
Checkzero       : Enabled
Default-cost    : 0
Maximum number of balanced pathsMaximum Balanced Paths : 32
Update time     : 30 sec  Age time           : 180 sec
Garbage-collect time : 120 sec
-----
Interface Level Default Configurations:
-----
Metricin        : 0
Metricout       : 1
Poison Reverse  : Disabled
Split-Horizon
    For Broadcast and P2P Interfaces : Enabled
    For NBMA Interfaces and LoopBack : Disabled
Default-route   : Disabled
Packet Transmit Interval : 200 msecs
Packet Transmit Number   : 30
```

Run the **display ripng process-id statistics interface** command, and you can view statistics about the specified RIPng interface.

```
<HUAWEI> display ripng 1 statistics interface gigabitethernet 1/0/0
GigabitEthernet1/0/0(10.0.0.11)
Statistical information          Last min      Last 5 min      Total
-----
Periodic updates sent           5              23              259
Triggered updates sent          5              30              408
Response packet sent            10             34              434
Response packet received        15             38              467
Response packet ignored         0              0               0
Request packet sent              1              3               8
Request packet received         4              20              40
Request packet ignored          0              0               0
Bad packets received            0              0               0
Bad routes received             0              0               0
Packet authentication failed    0              0               0
```

4.3 Configuring RIPng Route Attributes

By setting RIPng route attributes, you can change RIPng routing policies.

4.3.1 Establishing the Configuration Task

RIPng route attributes include the RIPng preference and interface metric.

Applicable Environment

In practice, to meet the requirements of a complex network, you can change RIPng routing policies by configuring RIPng route attributes. After performing configuration procedures in this section, you can:

- Affect route selection by changing the additional metric of a RIPng interface.
- Change the matching order of routing protocols by configuring the RIPng preference when multiple routing protocols discover routes to the same destination.
- Implement load balancing among multiple equal-cost routes.

Pre-configuration Tasks

Before configuring RIPng route attributes, complete the following tasks:

- Configuring IPv6 addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- [3.2 Configuring Basic RIP Functions](#)

Data Preparation

To configure RIPng route attributes, you need the following data.

No.	Data
1	Additional metric of the interface
2	RIPng preference
3	Maximum number of equal-cost routes

4.3.2 Configuring the RIPng Preference

When there are routes discovered by multiple routing protocols on the same router, you can make the router prefer RIPng routes by setting the RIPng preference.

Context

Each routing protocol has its preference, according to which a routing policy selects the optimal route. The RIPng preference can be set manually. The greater the value is, the lower the preference is.

Do as follows on the RIPng router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ripng [ process-id ]
```

The RIPng process is enabled and the RIPng view is displayed.

Step 3 Run:

```
preference { preference | route-policy route-policy-name } *
```

The RIPng preference is set.

---End

4.3.3 Configuring Additional Metrics of an Interface

You can set additional metrics for received and sent RIPng routes by using different commands.

Context

- The **ripng metricin** command is used to configure a device to add an additional metric to a received route before the device adds the route to its routing table, causing the metric of the route in the routing table to change. Running this command affects route selection on the device and other devices.
- The **ripng metricout** command is used to configure a device to add an additional metric to a route before the device advertises the route, keeping the metric of the route in the routing table unchanged. Running this command does not affect route selection on the local device but will affect route selection of other devices.

You can specify the value of the metric to be added to the RIPng route that passes the filtering policy by specifying *value1* through an IPv6 ACL or an IPv6 prefix list. If a RIPng route does not pass the filtering, its metric is increased by 1.

Do as follows on the RIPng router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ripng metricin value
```

The metric added to a received route is set.

Step 4 Run:

```
ripng metricout { value | { acl6-number | acl6-name acl6-name | ipv6-prefix ipv6-  
prefix-name } value1 }
```

The metric added to a sent route is set.

 **NOTE**

If the router connects to other RIPng routers through multiple interfaces, repeatedly perform Step 2 to Step 4 until metrics of all links are set.

----End

4.3.4 Configuring the Maximum Number of Equal-Cost Routes

By setting the maximum number of equal-cost RIPng routes, you can change the number of routes for load balancing.

Context

Do as follows on the RIPng router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ripng [ process-id ]
```

The RIPng view is displayed.

Step 3 Run:

```
maximum load-balancing number
```

The maximum number of equal-cost routes is set.

 **NOTE**

The range and default value of the maximum number of equal-cost routes may vary according to products and protocols. You can change the range and default value after purchasing the license.

----End

4.3.5 Checking the Configuration

After RIPng route attributes are successfully set, you can view the configuration and routing information of RIPng.

Prerequisite

The configurations of RIPng route attributes are complete.

Procedure

- Run the **display ripng** [*process-id* | **vpn-instance** *vpn-instance-name*] command to check the configuration of the RIPng process.
- Run the **display ripng** *process-id* **database** command to check routes in the RIPng database.
- Run the **display ripng** *process-id* **route** command to check all activated and inactivated RIPng routes.

---End

4.4 Controlling the Advertising of RIPng Routing Information

To meet the requirements of complex networks, it is required to accurately control the advertising of RIPng routing information.

4.4.1 Establishing the Configuration Task

RIPng routing information can be advertised through route summarization, default routes, and imported external routes.

Applicable Environment

In practice, to meet the requirements of a complex network, you need to control the advertising of RIPng routing information accurately. After performing configuration procedures in this section, you can:

- Advertise default routes to neighbors.
- Suppress interfaces from sending RIPng Update packets.
- Import external routes from various routing protocols and filter routes to be advertised.

Pre-configuration Tasks

Before configuring the router to control the advertising of RIPng routing information, complete the following tasks:

- Configuring IPv6 addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- [3.2 Configuring Basic RIP Functions](#)

Data Preparation

To control the advertising of RIPng routing information, you need the following data.

No.	Data
1	Metric of the default route to be advertised
2	Protocol name and process ID of the external route to be imported

4.4.2 Configuring RIPng Route Summarization

By configuring a RIPng router to advertise the summarized IPv6 address on an interface, you can save the space used by RIPng routes in the routing table. You can also set parameters to prevent an interface from learning the same summarized route.

Context

This configuration is to configure the RIPng router to advertise the summarized IPv6 prefix rather than specific routes on an interface.

Do as follows on the RIPng router:

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`interface interface-type interface-number`
The interface view is displayed.
- Step 3** Run:
`ripng summary-address ipv6-address prefix-length [avoid-feedback]`
RIPng route summarization is configured.
- End

4.4.3 Configuring RIPng to Advertise the Default Routes

There are two methods of advertising RIPng default routes. You can configure a router to advertise RIPng default routes according to the actual networking. Additionally, you can specify the cost of the default routes to be advertised.

Context

Do as follows on the RIPng router:

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`interface interface-type interface-number`
The interface view is displayed.
- Step 3** Run:
`ripng default-route { only | originate } [cost cost]`

RIPng is configured to advertise a default route.

You can configure RIPng to advertise default routes as required:

- **only**: advertises only IPv6 default routes (::/0) and suppresses the advertising of other routes.
- **originate**: advertises IPv6 default routes (::/0) and does not affect the advertising of other routes.

A RIPng default route is forcibly advertised by using an Update packet through a specified interface, regardless of whether this route exists in the IPv6 routing table.

----End

4.4.4 Configuring the Default Cost for External Routes Imported by RIPng

If RIPng imports routes from other routing protocols, but no metric is specified, you can set the default metric for imported external routes.

Context

Do as follows on the RIPng router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ripng [ process-id ]
```

The RIPng view is displayed.

Step 3 Run:

```
default-cost cost
```

The default cost is set for the external routes imported by RIPng.

If no metric is specified, this command can be used to set the default cost for the external routes imported by RIPng from other routing protocols.

----End

4.4.5 Configuring RIPng to Import External Routes

Similar to RIP, RIPng can import external routes to enrich routing information.

Context

Do as follows on the RIPng router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ripng [ process-id ]
```

The RIPng view is displayed.

Step 3 (Optional) Run:

```
default-cost cost
```

The default cost is set for imported external routes.

Step 4 Run:

```
import-route protocol [ process-id ] [ cost cost | route-policy route-policy-name ]  
*
```

External routes are imported.

If no cost is specified for imported routes, the default cost is used.

Step 5 (Optional) Run:

```
filter-policy { acl6-number | acl6-name acl6-name | ipv6-prefix ipv6-prefix-name }  
export [ protocol [ process-id ] ]
```

RIPng is configured to filter the imported routing information.

RIPng can filter the imported routes based on an IPv6 ACL or an IPv6 prefix list. Only the routes that meet the match conditions are advertised to neighbors. If *protocol* is not specified in the command, all the routing information to be advertised will be filtered, including the imported routes and local RIPng routes (directly connected routes).

----End

4.4.6 Checking the Configuration

After the function of controlling the advertising of RIPng routing information is successfully configured, you can view RIPng routing information.

Prerequisite

The configurations of controlling the advertising of RIPng routing information are complete.

Procedure

- Run the **display ripng process-id database** command to check routes in the RIPng database.
- Run the **display ripng process-id route** command to check all activated and inactivated RIPng routes.

----End

4.5 Controlling the Receiving of RIPng Routing Information

To meet the requirements of complex networks, it is required to accurately control the receiving of RIPng routing information.

4.5.1 Establishing the Configuration Task

Before controlling the receiving of RIPng routes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

In practice, to meet the requirements of a complicated networking environment, you need to control the receiving of RIPng routing information accurately. After performing configuration procedures in this section, you can:

- Disable an interface from receiving RIPng Update packets.
- Filter the received routing information.
- Import external routes from various routing protocols and filter the imported routes.

Pre-configuration Tasks

Before configuring the router to control the receiving of RIPng routing information, complete the following tasks:

- Configuring IPv6 addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- [Configuring Basic RIPng Functions](#)

Data Preparation

To control the receiving of RIPng routing information, you need the following data.

No.	Data
1	ACL used to filter routing information

4.5.2 Configuring RIPng to Filter the Received Routes

By configure an IPv6 ACL or an IPv6 prefix list to filter received routes, you can configure a router to selectively receive routes.

Context

Do as follows on the RIPng router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ripng [ process-id ]
```

The RIPng view is displayed.

Step 3 Run:

```
filter-policy { acl6-number | acl6-name acl6-name | ipv6-prefix ipv6-prefix-name }  
import
```

The imported routes are filtered.

You can specify an IPv6 ACL or an IPv6 prefix list to filter the imported routes. Only the routes that pass the filtering can be added to the RIPng routing table.

----End

4.5.3 Checking the Configuration

After the function of controlling the receiving of RIPng routing information is successfully configured, you can view RIPng routing information.

Prerequisite

The configurations of controlling the receiving of RIPng routing information are complete.

Procedure

- Run the **display ripng process-id database** command to check routes in the RIPng database.
- Run the **display ripng process-id route** command to check all activated and inactivated RIPng routes.

----End

4.6 Optimizing a RIPng Network

You can adjust and optimize the RIPng network performance by configuring RIPng timers, split horizon, poison reverse, and zero field check.

4.6.1 Establishing the Configuration Task

Before adjusting and optimizing the RIPng network performance, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

On certain networks, you need to configure RIPng features and optimize the performance of a RIPng network. After performing configuration procedures in this section, you can:

- Change the convergence speed of the RIPng network by adjusting RIPng timers.
- Configure split horizon and poison reverse to prevent routing loops.

Pre-configuration Tasks

Before optimizing a RIPng network, complete the following tasks:

- Configuring IPv6 addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- **Configuring Basic RIPng Functions**

Data Preparation

To optimize a RIPng network, you need the following data.

No.	Data
1	Values of timers

4.6.2 Configuring RIPng Timers

RIPng has three timers: Update timer, Age timer and Garbage-collect timer. If the three RIPng timers are configured improperly, routes become unstable.

Context

 **NOTE**

Route flapping occurs if the values of the four RIPng timers are set improperly. The relationship between the values is as follows: *update < age*, *update < garbage-collect*. For example, if the update time is longer than the aging time, and a RIPng route changes within the update time, the router cannot inform its neighbors of the change on time.

By default, the Update timer is 30s; the Age timer is 180s; the Garbage-collect timer is 120s.

Do as follows on the RIPng router:

Procedure

- Step 1** Run:
`system-view`
 The system view is displayed.
- Step 2** Run:
`ripng [process-id]`
 The RIPng view is displayed.
- Step 3** Run:
`timers ripng update age garbage-collect`
 RIPng timers are configured.
 ----End

4.6.3 Setting the Interval for Sending Update Packets and the Maximum Number of Packets Sent Each Time

By setting the interval for sending packets and the maximum number of packets to be sent each time, you can optimize the RIPng performance.

Context

Do as follows on the RIPng router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ripng pkt-transmit { interval interval | number pkt-count }*
```

The interval for sending RIPng Update packets and the maximum number of packets sent each time are set on the specified interface.

----End

4.6.4 Configuring Split Horizon and Poison Reverse

You can configure split horizon and poison reverse to prevent routing loops.

Context

Split horizon is a method of preventing routing loops by preventing the router from advertising a route back onto the interface from which the route is learned. On NBMA networks such as FR networks and X.25 networks, if no sub-interface is configured, split horizon must be disabled to ensure that routes are advertised correctly.

Poison reverse is another method of preventing routing loops by enabling the router to advertise a route as unreachable back through the interface from which the route is learned.

If both split horizon and poison reverse are configured, only poison reverse takes effect.

Do as follows on the RIPng router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run the following command as required:

● Run:

```
ripng split-horizon
```

Split horizon is enabled.

- Run:

```
ripng poison-reverse
```

Poison reverse is enabled.

----End

4.6.5 Enabling the Zero Field Check for RIPng Packets

In a RIPng packet, there are certain fields whose values must be 0. These fields are called zero fields. If the values of these zero fields in some RIPng packets are not 0s, these RIPng packets are ignored.

Context

Do as follows on the RIPng router:

Procedure

- Step 1** Run:

```
system-view
```

The system view is displayed.

- Step 2** Run:

```
ripng [ process-id ]
```

The RIPng view is displayed.

- Step 3** Run:

```
checkzero
```

The zero field check is configured for RIPng packets.

----End

4.6.6 Checking the Configuration

After the function of adjusting and optimizing the RIPng network performance is successfully configured, you can view routing information, neighbor information, and interface information of RIPng.

Prerequisite

The configurations of adjusting and optimizing the RIPng network performance are complete.

Procedure

- Run the **display ripng** [*process-id* | **vpn-instance** *vpn-instance-name*] command to check the configuration of the RIPng process.
- Run the **display ripng process-id database** [**verbose**] command to check routes in the RIPng database.
- Run the **display ripng process-id interface** [*interface-type interface-number*] [**verbose**] command to check information about the RIPng interface.

- Run the **display ripng process-id neighbor [verbose]** command to check information about RIPng neighbors.
- Run the **display ripng process-id route** command to check all activated and inactivated RIPng routes.

---End

4.7 Configuring IPsec Authentication for RIPng

Configuring IPsec authentication for RIPng can improve security of a RIPng network.

4.7.1 Establishing the Configuration Task

RIPng supports IPsec authentication. Before configuring IPsec authentication for RIPng, familiarize yourself with basic IPsec configurations.

Applicable Environment

As networks develop rapidly, network security has become a major concern. If IPsec authentication is configured on a RIPng network, the sent and received RIPng packets will be authenticated, and those cannot pass authentication will be discarded. This can improve the security of the RIPng network.

There are two methods of configuring IPsec authentication for RIPng:

- One method is to configure IPsec authentication in RIPng processes. If IPsec authentication is enabled in a RIPng process, this configuration takes effect on all interfaces in this RIPng process. This method is recommended if IPsec authentication needs to be applied to all interfaces in a RIPng process.
- The other method is to configure IPsec authentication on RIPng interfaces. This method is recommended if IPsec authentication needs to be applied only to some interfaces in a RIPng process.

Pre-configuration Tasks

Before configuring IPsec authentication for RIPng, complete the following tasks:

- Configuring basic IPsec functions
- **Configuring basic RIPng functions**

Data Preparation

To configure IPsec authentication for RIPng, you need the following data.

No.	Data
1	Name of a security association (SA)

4.7.2 Configuring IPsec Authentication in a RIPng Process

Configuring IPsec authentication in the RIPng view is one of the methods used to configure IPsec authentication for RIPng.

Context

If IPsec authentication is enabled in the RIPng view, all interfaces in the RIPng process will perform IPsec authentication on the RIPng packets received or sent by the interfaces.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ripng [ process-id ]
```

The RIPng view is displayed.

Step 3 Run:

```
ipsec sa sa-name
```

IPsec authentication is enabled, and the name of an SA is specified.

----End

4.7.3 Configuring IPsec Authentication on a RIPng Interface

Configuring IPsec authentication in the interface view is the other method used to configure IPsec authentication for RIPng.

Context

This method is recommended if not all the interfaces in a RIPng process need to perform IPsec authentication on packets.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ripng ipsec sa sa-name
```

IPsec authentication is enabled on the interface, and the name of an SA is specified.

 **NOTE**

The **ripng ipsec sa** command takes precedence over the **ipsec sa** command. If both commands are run in respective views and different SA names are specified, only the configuration of the **ripng ipsec sa** command takes effect.

----End

4.7.4 Checking the Configuration

After IPsec authentication for RIPng is configured, you can check the SA used in IPsec authentication and statistics on the RIPng packets that failed authentication.

Prerequisite

After IPsec authentication is enabled in a RIPng process or on a RIPng interface, the configuration takes effect immediately. There is no need to restart the RIPng process.

Procedure

- Run the **display ripng process-id interface** [*interface-type interface-number*] [**verbose**] command to check the SA used in IPsec authentication.
- Run the **display ripng process-id statistics interface** { **all** | *interface-type interface-number* [**verbose** | **neighbor neighbor-ipv6-address**] } command to check the number of RIPng packets that failed authentication.

----End

Example

Run the **display ripng interface** command, and you can view the name of an SA used in IPsec authentication on a RIPng interface.

```
<Router > display ripng 1 interface GigabitEthernet1/0/0 verbose
GigabitEthernet1/0/0
  FE80::A0A:200:1
  State : UP, Protocol : RIPNG, MTU : 1440
  Metricin      : 0
  Metricout     : 1
  Default Route : Disabled
  Poison Reverse : Disabled
  Split Horizon : Enabled
  Authentication : IPSEC (SA - sa1)
```

Run the **display ripng statistics interface** command, and you can view the number of RIPng packets that failed authentication.

```
<Router > display ripng 1 statistics interface gigabitethernet 1/1/0
GigabitEthernet1/0/0 (FE80::2E0:64FF:FE10:8142)
Statistical information          Last min    Last 5 min    Total
-----
Periodic updates sent           5            23            259
Triggered updates sent          5            30            408
Response packet sent            10           34            434
Response packet received         15           38            467
Response packet ignored          0             0              0
Request packet sent              1             3              8
Request packet received           4            20            40
Request packet ignored            0             0              0
Bad packets received             0             0              0
Routes received                  0             0              0
Routes sent                       0             0              0
```

Bad routes received	0	0	0
Packet send failed	0	0	0
Packet IPSEC6 Auth failed	0	0	2

4.8 Configuration Examples

In actual networking, different RIPng features have different applications.

NOTE

Examples in this document use interface numbers and link types of the NE40E-X8. In real world situations, the interface numbers and link types may be different from those used in this document.

4.8.1 Example for Configuring RIPng to Filter the Received Routes

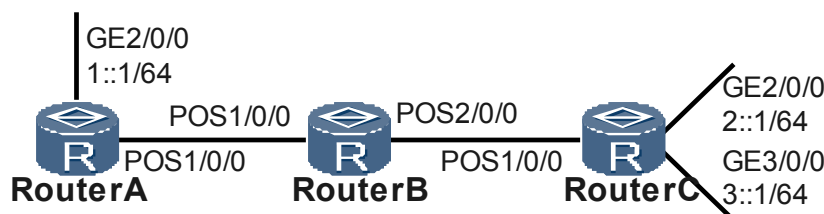
By configuring basic RIPng functions and ACLs, you can enable RIPng to filter received routes. You can run commands to view the configuration results.

Networking Requirements

As shown in [Figure 4-1](#), the prefix length of all the IPv6 addresses is 64, and neighboring routers are connected by using IPv6 link-local addresses.

It is required that all routers learn IPv6 routing information on the network through RIPng. In addition, Router B is required to filter out the route imported from Router C (at 3::/64) so that this route is neither added to the routing table of Router B nor advertised to Router A.

Figure 4-1 Networking diagram for configuring RIPng to filter the received routes



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic RIPng functions on each router to ensure that the routers communicate with each other.
2. Configure an ACL on Router B to filter the imported routes.

Data Preparation

To complete the configuration, you need the following data:

- RIPng process 1 to be enabled on each router
- ACL6 2000 to be configured on Router B to deny routes from network segment 3::/64

Procedure

Step 1 Configure an IPv6 address for each interface.

The configurations details are not described here.

Step 2 Configure basic RIPng functions.

Configure Router A.

```
[RouterA] ripng 1
[RouterA-ripng-1] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ripng 1 enable
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] ripng 1 enable
[RouterA-Pos1/0/0] quit
```

Configure Router B.

```
[RouterB] ripng 1
[RouterB-ripng-1] quit
[RouterB] interface pos 1/0/0
[RouterB-Pos1/0/0] ripng 1 enable
[RouterB-Pos1/0/0] quit
[RouterB] interface pos 2/0/0
[RouterB-Pos2/0/0] ripng 1 enable
[RouterB-Pos2/0/0] quit
```

Configure Router C.

```
[RouterC] ripng 1
[RouterC-ripng-1] quit
[RouterC] interface pos 1/0/0
[RouterC-Pos1/0/0] ripng 1 enable
[RouterC-Pos1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] ripng 1 enable
[RouterC-GigabitEthernet2/0/0] quit
[RouterC] interface gigabitethernet 3/0/0
[RouterC-GigabitEthernet3/0/0] ripng 1 enable
[RouterC-GigabitEthernet3/0/0] quit
```

Check the RIPng routing table of Router B.

```
[RouterB] display ripng 1 route
Route Flags:    A - Aging, G - Garbage-collect
-----
Peer FE80::F54C:0:9FDB:1 on Pos2/0/0
Dest 2::/64,
    via FE80::F54C:0:9FDB:1, cost 1, tag 0, A, 3 Sec
Dest 3::/64,
    via FE80::F54C:0:9FDB:1, cost 1, tag 0, A, 3 Sec
Peer FE80::D472:0:3C23:1 on Pos1/0/0
Dest 1::/64,
    via FE80::D472:0:3C23:1, cost 1, tag 0, A, 4 Sec
```

Check the RIPng routing table of Router A.

```
[RouterA] display ripng 1 route
Route Flags:    A - Aging, G - Garbage-collect
-----
Peer FE80::476:0:3624:1 on Pos1/0/0
Dest 2::/64,
    via FE80::476:0:3624:1, cost 2, tag 0, A, 21 Sec
Dest 3::/64,
    via FE80::476:0:3624:1, cost 2, tag 0, A, 21 Sec
```


Step 3 Configure Router B to filter the imported routes.

```
[RouterB] acl ipv6 number 2000
[RouterB-acl6-basic-2000] rule deny source 3::/64
[RouterB-acl6-basic-2000] rule permit
[RouterB-acl6-basic-2000] quit
[RouterB] ripng 1
[RouterB-ripng-1] filter-policy 2000 import
[RouterB-ripng-1] quit
```

Step 4 Verify the configuration.

Check the RIPng routing table of Router B. The command output shows that the RIPng routing table does not contain the route from network segment 3::/64.

```
[RouterB] display ripng 1 route
Route Flags: A - Aging, G - Garbage-collect
-----
Peer FE80::F54C:0:9FDB:1 on Pos2/0/0
Dest 2::/64,
    via FE80::F54C:0:9FDB:1, cost 1, tag 0, A, 14 Sec
Peer FE80::D472:0:3C23:1 on Pos1/0/0
Dest 1::/64,
    via FE80::D472:0:3C23:1, cost 1, tag 0, A, 25 Sec
[RouterA] display ripng 1 route
Route Flags: A - Aging, G - Garbage-collect
-----
Peer FE80::476:0:3624:1 on Pos1/0/0
Dest 2::/64,
    via FE80::476:0:3624:1, cost 2, tag 0, A, 7 Sec
```

---End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
 ipv6
#
 interface GigabitEthernet2/0/0
 undo shutdown
 ipv6 enable
 ipv6 address 1::1/64
 ripng 1 enable
#
 interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ipv6 enable
 ipv6 address auto link-local
 ripng 1 enable
#
 ripng 1
#
 return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
 ipv6
#
 acl ipv6 number 2000
 rule 0 deny source 3::/64
 rule 1 permit
#
```

```
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ipv6 enable
 ipv6 address auto link-local
 ripng 1 enable
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ipv6 enable
 ipv6 address auto link-local
 ripng 1 enable
#
ripng 1
 filter-policy 2000 import
#
return
```

● Configuration file of Router C

```
#
 sysname RouterC
#
 ipv6
#
interface GigabitEthernet2/0/0
 undo shutdown
 ipv6 enable
 ipv6 address 2::1/64
 ripng 1 enable
#
interface GigabitEthernet3/0/0
 undo shutdown
 ipv6 enable
 ipv6 address 3::1/64
 ripng 1 enable
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ipv6 enable
 ipv6 address auto link-local
 ripng 1 enable
#
ripng 1
#
return
```

5 OSPF Configuration

About This Chapter

OSPF, which is developed by the IETF, is a link-state IGP. OSPF is widely used in access networks and MANs.

[5.1 Introduction to OSPF](#)

By building OSPF networks, you can enable OSPF to discover and calculate routes in ASs. OSPF is applicable to a large-scale network that consists of hundreds of routers.

[5.2 Configuring Basic OSPF Functions](#)

Before building OSPF networks, you need to configure basic OSPF functions.

[5.3 Establishing or Maintaining OSPF Neighbor Relationship](#)

On an OSPF network, all routing information is transmitted and exchanged between neighboring or adjacent routers. By maintaining neighbor relationships or adjacencies, you can stabilize the entire network.

[5.4 Configuring OSPF Stub Areas](#)

By configuring non-backbone areas at the edge of ASs as stub areas, you can reduce the size of the routing table and reduce the number of LSAs to be transmitted.

[5.5 Configuring OSPF NSSA Areas](#)

By configuring non-backbone areas as NSSA areas, external routes can be imported, and a new type of LSA, namely, Type 7 NSSA LSA is introduced.

[5.6 Configuring OSPF Virtual Links](#)

In actual applications, physical connectivity between non-backbone areas and backbone areas may not be ensured due to various limitations. To solve this problem, you can configure OSPF virtual links.

[5.7 Configuring OSPF Attributes in Different Types of Networks](#)

By setting network types for OSPF interfaces and adjusting OSPF attributes, you can build OSPF networks flexibly.

[5.8 Configuring OSPF Route Attributes](#)

By setting OSPF route attributes, you can change OSPF routing policies to meet the requirements of complex networks.

[5.9 Controlling OSPF Routing Information](#)

This section describes how to control the advertising and receiving of OSPF routing information and import routes from other protocols.

[5.10 Optimizing an OSPF Network](#)

By configuring OSPF functions in special network environments, you can adjust and optimize the OSPF network performance.

[5.11 Configuring Local MT](#)

By configuring local MT, you can prevent multicast services from becoming unavailable when both multicast and an MPLS TE tunnel are deployed on a network.

[5.12 Configuring OSPF IP FRR](#)

With OSPF IP FRR, devices can rapidly switch traffic from faulty links to backup links without interrupting traffic. This protects traffic and greatly improves the reliability of OSPF networks.

[5.13 Configuring OSPF GR](#)

To avoid traffic interruption and route flapping caused by the active/standby switchover, you can enable OSPF GR.

[5.14 Configuring BFD for OSPF](#)

If there are high requirements for data transmission, and OSPF convergence needs to be speeded up when the link status changes, you can configure BFD on OSPF links. After detecting a link failure, BFD notifies the routing protocol of the failure, which triggers fast convergence. When the neighbor relationship is Down, the BFD session is deleted dynamically.

[5.15 Configuring the Network Management Function of OSPF](#)

OSPF supports the network management function. You can bind the OSPF MIB to a certain OSPF process, and configure the trap function and log function.

[5.16 Improving Security of an OSPF Network](#)

On a network demanding high security, you can configure OSPF authentication and adopt the GTSM mechanism to improve the security of the OSPF network.

[5.17 Maintaining OSPF](#)

Maintaining OSPF involves resetting OSPF and clearing OSPF statistics.

[5.18 Configuring Examples](#)

This section provides several configuration examples of OSPF together with the configuration flowchart. The configuration examples explain networking requirements, configuration notes, and configuration roadmap.

5.1 Introduction to OSPF

By building OSPF networks, you can enable OSPF to discover and calculate routes in ASs. OSPF is applicable to a large-scale network that consists of hundreds of routers.

5.1.1 OSPF Overview

OSPF is a link-state IGP. At present, OSPFv2 is intended for IPv4.

Defined by the Internet Engineering Task Force (IETF), the Open Shortest Path First (OSPF) protocol is an Interior Gateway Protocol (IGP) implemented on the basis of the link status.

NOTE

In this chapter, OSPF refers to OSPFv2, unless otherwise specified.

OSPF Features

OSPF has the following features:

- **Wide applications**
OSPF is applicable to networks of various sizes and even to the network consisting of hundreds of routers.
- **Fast convergence**
Once the network topology changes, Update packets are transmitted to synchronize the link state databases (LSDBs) of all the routers within the Autonomous System (AS).
- **Loop-free**
According to the collected link status, OSPF calculates routes with the shortest path tree algorithm. This algorithm ensures the generation of loop-free routes.
- **Area division**
An AS can be divided into different areas to facilitate AS management. After the area partition, an LSDB stores routing information only of the local area. The reduce of LSDB size dramatically reduces memory and CPU usage. In addition, less bandwidth is consumed because of the decrease in routing information transmitted within the AS.
- **Equal-cost routes**
OSPF supports multiple equal-cost routes to the same destination.
- **Routing hierarchy**
Four types of routing are available. They are listed in the descending order of priority: intra-area routes, inter-area routes, Type 1 external routes, and Type 2 external routes.
- **Authentication**
Area-based and interface-based packet authentication guarantees the security of packet interaction.
- **Multicast**
Multicast packets are transmitted only on certain types of links to reduce the interference for some devices.

Process of OSPF Route Calculation

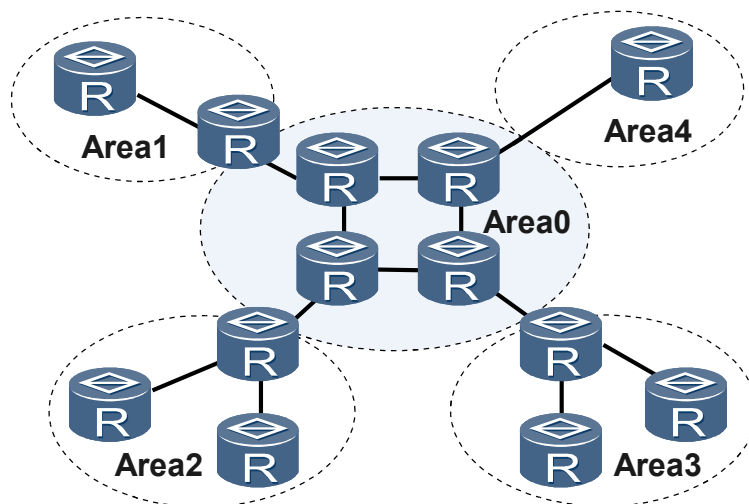
The process of calculating OSPF routes is as follows:

1. Based on the surrounding network topology, each OSPF device originates a Link State Advertisement (LSA). The router then transmits Update packets containing the LSAs to other OSPF devices.
2. Each OSPF device collects the LSAs from other devices, and all these LSAs compose the LSDB. An LSA describes the network topology around a router, whereas an LSDB describes the network topology of the whole AS.
3. OSPF devices transform the LSDB into a weighted directed map. The weighted directed map reflects the topology of the entire network. All routers in the same area have the same map.
4. According to the directed map, each router uses the Shortest Path First (SPF) algorithm to calculate the shortest path tree, regarding itself as the root. The tree displays the routes to each node in the AS.

Area Division

The number of routers increases with the unceasing expansion of the network scale. This leads to a large LSDB on each router. As a result, the load of each router is very heavy. OSPF solves this problem by dividing an AS into different areas. An area is regarded as a device group logically. Each group is identified by an area ID. On the border of an area resides a router rather than a link. A network segment (or a link) belongs to only one area. That is, the area to which each OSPF interface belongs must be specified, as shown in [Figure 5-1](#).

Figure 5-1 OSPF area division



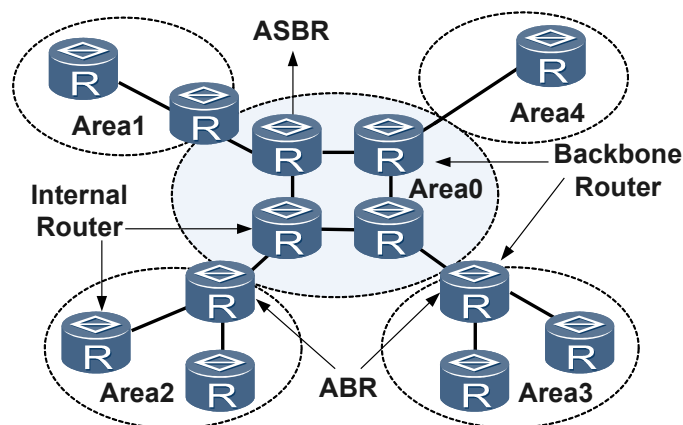
After area division, route aggregation can be performed on border routers to reduce the number of LSAs advertised to other areas. Route aggregation also minimizes the influence caused by changes in the topology.

Router Type

OSPF routers are classified into the following types according to their locations in the AS:

- Internal routers
- Area border routers (ABRs)
- Backbone routers
- AS boundary routers (ASBRs)

Figure 5-2 Types of OSPF routers



OSPF Network Types

OSPF classifies networks into four types according to the link layer protocol:

- Broadcast: If the link layer protocol is Ethernet or FDDI, OSPF defaults the network type to broadcast. In this type of networks, the following situations occur.
 - Hello packets and packets from the Designated Router (DR) are sent in multicast mode (224.0.0.5: indicates the reserved IP multicast addresses for OSPF routers).
 - Link State Update (LSU) packets are sent to the DR in multicast mode (224.0.0.6: indicates the reserved IP multicast address for the OSPF DR), and the DR forwards the LSU packets to destination 224.0.0.5.
 - Database Description (DD) packets, Link State Request (LSR) packets, and all retransmission packets are sent in unicast mode.
 - Link State Acknowledgement (LSAck) packets are usually sent in multicast mode (224.0.0.5). When a router receives repeated LSAs, or the LSAs are deleted due to the timeout of the maximum lifetime, LSAck packets are sent in unicast mode.
- Non-Broadcast Multi-Access (NBMA): If the link layer protocol is Frame Relay, ATM, or X.25, OSPF defaults the network type to NBMA. In this type of networks, protocol packets, such as Hello packets, DD packets, LSR packets, LSU packets, and LSAck packet, are transmitted in unicast mode.
- Point-to-Multipoint (P2MP): A P2MP network must be forcibly changed from other network types. In this type of networks, Hello packets are transmitted in multicast mode (224.0.0.5); DD packets, LSR packets, LSU packets, and LSAck packets are transmitted in unicast mode.
- Point-to-Point (P2P): If the link layer protocol is PPP, HDLC, or LAPB, OSPF defaults the network type to P2P. In this type of networks, protocol packets, such as Hello packets, DD

packets, LSR packets, LSU packets, and LSAck packets, are transmitted in multicast mode (224.0.0.5).

5.1.2 OSPF Features Supported by the NE80E/40E

The NE80E/40E supports various OSPF features, including multi-process, authentication, hot standby, Smart-discover, local MT, GR, TE, DS-TE, VPN multi-instance, sham link, BFD, IGP Shortcut, forwarding adjacency, and GTSM.

Multi-process

OSPF supports multi-process. More than one OSPF process can run on the same router because processes are mutually independent. Route interaction between different OSPF processes is similar to the interaction between different routing protocols.

An interface of a router belongs to only a certain OSPF process.

A typical application of OSPF multi-process is to run OSPF between PEs and CEs in the VPN where OSPF is also adopted in the backbone network. On the PEs, the two OSPF processes are independent of each other.

Authentication

OSPF supports packet authentication. Only the OSPF packets that pass the authentication can be received. If the packets fail to pass the authentication, the neighbor relationship cannot be established.

The NE80E/40E supports two authentication modes:

- Area authentication mode
- Interface authentication mode

If both modes are available, the latter is preferred.

Hot Backup and GR

The router with a distributed structure supports OSPF hot standby (HSB). OSPF backs up necessary information from the active main board (AMB) to the standby main board (SMB). When the AMB fails, the SMB replaces it to ensure the normal operation of OSPF.

OSPF supports two types of HSB:

- Backing up all OSPF data: After the switchover between the AMB and the SMB, OSPF restores its normal work immediately.
- Backing up only the OSPF configuration: After the switchover between the AMB and the SMB, OSPF performs graceful restart (GR), obtains the adjacency relationship from neighbors, and synchronizes the LSDBs.

Smart-discover

Generally, routers periodically send Hello packets through interfaces that run OSPF, routers set up and maintain the neighbor relationship, and elect the DR and the Backup Designated Router (BDR) on the multi-access network (broadcast or NBMA) by exchanging Hello packets. When establishing the neighbor relationship or electing the DR and the BDR on the multi-access network, interfaces can send Hello packets only when the Hello timer expires. This affects the speed for establishing the neighbor relationship and electing the DR and the BDR.

NOTE

- The interval for sending Hello packets on an interface depends on the interval for sending Hello packets set on the interface.
- The default value of the interval for sending Hello packets varies with the network type.

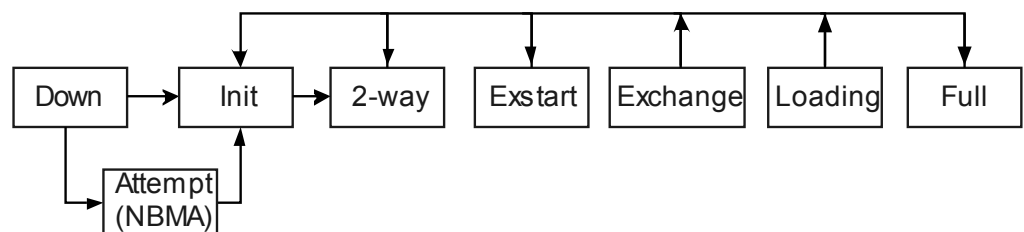
The Smart-discover function can solve the preceding problem.

- In broadcast and NBMA networks, the neighbor relationship can be established rapidly and a DR and a BDR on the networks can be elected rapidly.

When the neighbor status becomes 2-way for the first time, or it returns to Init from the 2-way or higher state as shown in **Figure 5-3**, the interface enabled with the Smart-discover function sends Hello packets to the neighbor without waiting for the timeout of the Hello timer when the interface finds that the status of the neighbor changes.

When the interface status of the DR and the BDR in the multi-access network changes, the interface enabled with the Smart-discover function sends Hello packets to the network segment and takes part in the DR or BDR election.

Figure 5-3 Changes of the neighbor state machine



- On P2P and P2MP networks, the adjacency relationship can be established rapidly. The principle is the same as that in broadcast and NBMA networks.

Local MT

When multicast and a MultiProtocol Label Switching (MPLS) Traffic Engineering (TE) tunnel are deployed in a network simultaneously, services become unavailable because the multicast function may be affected by the TE tunnel. This is because after the TE tunnel is enabled with IGP Shortcut, the outgoing interface of the route calculated by IGP is not the actual physical interface but a TE tunnel interface. According to the unicast route to the multicast source address, a router sends a Join message through a TE tunnel interface. Routers spanned by the TE tunnel cannot sense the Join message, and thus multicast forwarding entries cannot be created. The TE tunnel is unidirectional, so multicast data packets sent by the multicast source are sent to the routers spanned by the TE tunnel through related physical interfaces. The routers, however, do not have multicast forwarding entries. As a result, the multicast data packets are discarded. Services thus become unavailable.

When a network runs the OSPF protocol, you can enable OSPF local Multicast-Topology (MT) to solve the problem of multicast traffic interruption caused by the conflict between multicast and the TE tunnel. After local MT is enabled, multicast packets can be correctly forwarded. If the outgoing interface of the calculated route is a TE tunnel interface of IGP-Shortcut type, a router adds a route of the physical outgoing interface to the MIGP routing table. Multicast uses routes in the MIGP routing table to forward packets.

 **NOTE**

For details of local MT, refer to the chapter "IP Multicast Overview" in the HUAWEI NetEngine80E/40E Router *Feature Description - IP Multicast*.

OSPF GR

When a router restarts or performs the active/standby switchover, it directly ages all routing entries in the Forward Information Base (FIB) table. This results in route interruption. In addition, neighboring routers remove this router from the neighbor list, and notify other routers. This causes the re-calculation of SPF. If this router recovers within a few seconds, the neighbor relationship becomes unstable. This results in route flapping.

After being enabled with OSPF Graceful Restart (GR), a router can ensure continuous packet forwarding if it restarts just for abnormalities. In such a case, route flapping is avoided during the short restart of the router.

 **NOTE**

Unless otherwise specified, "protocol restart" in this document refers to restarting OSPF in GR mode.

When a router restarts OSPF, the GR Restarter does not age the forwarding information. At the same time, the GR Helper keeps the topology information or routes obtained from the GR Restarter for a period. This ensures that traffic forwarding is not interrupted when protocol restart occurs.

OSPF and DS-TE

OSPF TE supports the establishing and maintaining of the Label Switch Path (LSP) of the TE.

When constructing constraint-based routed LSP (CR LSP), MPLS needs information about the traffic attributes of all the links in the area. With the help of the OSPF, MPLS obtains traffic engineering information about the links.

OSPF supports a new type of LSAs called opaque LSA. The opaque LSA can carry TE information. You can use the related commands to configure OSPF to support or not support the originating and handling of the opaque LSA that carries TE information.

Difference service aware TE (DS-TE) is primarily used to optimize and assign network transmission resources, classify the traffic, and specify the percentage of each traffic to the link bandwidth. Traffic engineering is implemented based on each divided class (aggregated class with fine granularity) instead of an aggregated class (aggregated class with coarse granularity). This enhances the performance and utility of the bandwidth.

To support DS-TE in MPLS, OSPF supports Local Overbooking Multiplier TLV and bandwidth constraint (BC) TLV.

 **NOTE**

For details of OSPF TE configurations, refer to the HUAWEI NetEngine80E/40E Router *Configuration Guide - MPLS*.

IGP Shortcut and Forwarding Adjacency

OSPF TE supports either IGP shortcut or Forwarding Adjacency (FA). This two features allow OSPF TE to establish an LSP to reach a specified destination. Without the two features, OSPF cannot use the LSP as an outgoing interface even if the LSP to the destination exists.

The differences between IGP Shortcut and forwarding adjacency are as follows:

- If only forwarding adjacency is enabled, OSPF can reach the destination by using the LSP.
- If only IGP Shortcut is enabled, only the router enabled with IGP Shortcut can use the LSP.

 **NOTE**

For detailed configuration of this feature, refer to the HUAWEI NetEngine80E/40E Router *Configuration Guide - MPLS*.

OSPF VPN Multi-instance

OSPF supports multi-instance, which can run between PEs and CEs in VPN networks.

In BGP MPLS VPN, many sites of one VPN can use OSPF as the internal routing protocol. The sites, however, are handled as being from different ASs. In this way, the OSPF routes learned on one site are transmitted as external routes to another site. This causes a heavy OSPF traffic and some avoidable network management problems.

In the NE80E/40E implementation, you can configure domain IDs on a PE to differentiate the VPNs where different sites reside. Different sites in one VPN consider each other as if they were connected directly. Thus, PEs exchange OSPF routing information as if they were directly connected through a leased line. This improves network management and enhances the validity of the OSPF application.

 **NOTE**

For detailed configuration of this feature, refer to the HUAWEI NetEngine80E/40E Router *Configuration Guide - VPN*.

OSPF Sham Links

OSPF sham links are unnumbered P2P links between two PEs over an MPLS VPN backbone network.

Generally, BGP extended community attributes carry routing information over the MPLS VPN backbone between BGP peers. OSPF running on the remote PE uses this information to generate Type3 summary LSAs from PE to CE. These routes are considered as inter-area routes.

If a router, however, connects to PEs in its own area and establishes an intra-area route (backdoor route) to a particular destination, the VPN traffic always traverses the backdoor route rather than the backbone route. This is because OSPF intra-area routes in the routing table have relatively higher priorities. To prevent this, an unnumbered P2P sham link is configured between the PEs. This provides an intra-area path with a lower cost to the PE.

 **NOTE**

For configurations of OSPF sham links, refer to the HUAWEI NetEngine80E/40E Router *Configuration Guide - VPN*.

BFD for OSPF

By default, in broadcast networks, the interval for OSPF to send Hello packets is 10 seconds; in NBMA networks, the interval for sending Hello packets is 30 seconds, and the period for advertising that the neighbor is Down is four times the interval for sending Hello packets. If the router does not receive the Hello packet from the neighbor before the neighboring router becomes invalid, it deletes the neighbor. That is, the router detects the neighbor faults in seconds. This leads to the loss of a large number of packets in a high-speed network.

To solve the preceding problem in the current detection mechanism, Bidirectional Forwarding Detection (BFD) is developed. BFD can implement detection at the millisecond level. Instead

of replacing the Hello mechanism of OSPF, BFD works with OSPF to fast detect the adjacency fault. BFD is used to notify OSPF of recalculating routes. This can correctly guide the packet forwarding.

Routing Management (RM) module exchanges routing information with the BFD module. Through RM, OSPF notifies BFD of dynamically setting up or deleting BFD sessions. The Event message of BFD is delivered to OSPF through RM.

The process of establishing and deleting a BFD session is as follows:

- Process of establishing a BFD session: If BFD feature is globally configured, BFD is enabled on an interface or a process, and the status of the OSPF neighbor is Full, OSPF uses RM to notify the BFD module of establishing the BFD session and negotiate related parameters of BFD.
- Process of deleting a BFD session: When BFD detects a link fault, BFD generates a Down event and notifies the upper protocol of the fault through RM. OSPF then responds to the event and immediately deletes the adjacency relationship on the link. At this time, the status of the neighbor is not Full. This does not meet the requirements of establishing a BFD session. OSPF then uses RM to notify the BFD module of deleting the BFD session.

OSPF supports dynamically establishing or deleting a BFD session on broadcast, P2P, P2MP, and NBMA links.

Configure BFD according to the actual network environment. If time parameters are set incorrectly, network flapping occurs.

OSPF-BGP

When a new router is connected to the network, or a router restarts, the network traffic may be lost during BGP convergence. This is because the IGP route convergence is quicker than the BGP route convergence.

If the backup link exists, OSPF-BGP linkage makes a router that restarts or a router that is connected to the network start the stub router timer during the OSPF-BGP linkage. During the set linkage period, the router acts as the stub router by increasing the metrics of the links in the LSA generated by the router to 65535. Other OSPF routers are notified of not using the stub router to forward data. This ensures that the router is not used as the spanned router. This avoids traffic loss during traffic switchback because route convergence speed is slower than that of OSPF.

GTSM

The Generalized TTL Security Mechanism (GTSM) refers to the generic TTL security protection mechanism. GTSM protects services of the upper layer over the IP layer by checking whether the TTL value in the IP header is in a pre-defined range. In applications, GTSM is designed to protect the TCP/IP-based control plane (like routing protocols) from CPU-utilization attacks, such as CPU overload attacks.

5.2 Configuring Basic OSPF Functions

Before building OSPF networks, you need to configure basic OSPF functions.

5.2.1 Establishing the Configuration Task

You can run OSPF commands in the interface view regardless of whether OSPF is enabled. When OSPF is disabled, the related commands configured in the interface view still exist.

Applicable Environment

Before configuring OSPF, enable OSPF after specifying the OSPF process and OSPF area ID.

 **NOTE**

When multiple routers are configured in the same area, most configuration data (such as timer, filter, and aggregation) should be kept consistent in the entire area. Wrong configuration may make neighboring routers fail to send messages to each other, and even leads to path congestion or routing loop.

Pre-configuration Tasks

Before configuring basic OSPF functions, complete the following tasks:

- Configuring a link layer protocol
- Configuring IP addresses for interfaces to make neighboring nodes reachable

Data Preparation

To configure basic OSPF functions, you need the following data.

No.	Data
1	Router ID
2	OSPF process ID
3	VPN instance name (if OSPF VPN multi-instance is configured)
4	Areas to which each interface belongs
5	IP address of the network segment where the interface resides

5.2.2 Enabling OSPF and Entering the OSPF View

Creating an OSPF process is a prerequisite for configuring all OSPF features. When creating an OSPF process, you can manually specify the router ID for a router.

Context

To ensure the stability of OSPF, you need to manually set the router ID of each device during network planning. When configuring router IDs for routers, ensure that IDs of any two routers in the AS are different. Generally, you can set the router ID the same as the IP address of a certain interface on the router.

The NE80E/40E supports OSPF multi-processes. When multiple OSPF processes are enabled on the NE80E/40E, you need to specify different process IDs. The OSPF process ID is valid in the local area, which does not affect packet exchange between other NE80E/40Es. Different NE80E/40Es, therefore, can also exchange packets even with different process IDs.

Do as follows on each OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id | router-id router-id ]
```

The OSPF process is enabled and the OSPF view is displayed.

The NE80E/40E supports OSPF multi-instance. To configure OSPF in a VPN instance, run the `ospf [process-id | router-id router-id | vpn-instance vpn-instance-name] *` command. If the VPN instance is specified, the OSPF process belongs to the specified instance. Otherwise, the OSPF process belongs to the global instance.

NOTE

The router ID of each OSPF process must be unique on the entire network; otherwise, the OSPF neighbor relationship cannot be set up and routing information is incorrect. Configuring a unique router ID for each OSPF process on each OSPF device is recommended.

----End

5.2.3 Configuring the Network Segments Included by Each Area

By dividing an AS into different areas, specifying OSPF interfaces, and specifying areas to which these interfaces belong, OSPF can discover and calculate routes in an AS.

Context

A network segment refers to one of the IP addresses of the interfaces that run the OSPF protocol.

A network segment belongs to only one area; that is, you must specify the area for each interface running OSPF.

Do as follows on each OSPF router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
area area-id
```

The OSPF area view is displayed.

Step 4 Run:

```
network ip-address wildcard-mask [ description text ]
```

The network segments in the areas are configured. In the command, **description** is used to configure a description for the specified OSPF network segment.

OSPF can run on an interface only when the following conditions are satisfied:

- Mask length of the IP address of an interface is not shorter than that in the **network** command.
- Master IP address of an interface must belong to the network segment specified by the **network** command.

For a loopback interface, by default, OSPF advertises its IP address in 32-bit host route, regardless of the mask length of the IP address on the interface. To advertise the segment route of the loopback interface, configure the network type as NBMA or broadcast in the interface view. For details, see [5.7.2 Configuring Network Types of OSPF Interfaces](#).

----End

5.2.4 Checking the Configuration

After basic OSPF functions are configured, you can check OSPF statistics, LSDB information, and information about neighbors in each area.

Prerequisite

The configurations of Configuration of Basic OSPF function are complete.

Procedure

- Run the **display ospf [process-id] cumulative** command to check the OSPF statistics.
- Run the **display ospf [process-id] lsdb** command to check LSDB information of OSPF.
- Run the **display ospf [process-id] peer** command to check information about OSPF neighboring routers.
- Run the **display ospf [process-id] routing** command to check information about the OSPF routing table.

----End

Example

Run the **display ospf peer** command. If the status of the OSPF neighbor is Full, it means that OSPF neighbor is correctly established. For example:

```
<HUAWEI> display ospf peer
      OSPF Process 1 with Router ID 10.1.1.2
      Neighbors
Area 0.0.0.0 interface 10.1.1.2(GigabitEthernet1/0/0)'s neighbors
Router ID: 10.1.1.1      Address: 10.1.1.1      GR State: Normal
  State: Full Mode:Nbr is Slave Priority: 1
  DR: 10.1.1.1  BDR: None  MTU: 0
  Dead timer due in 35 sec
  Retrans timer interval: 5
  Neighbor is up for 00:00:05
  Authentication Sequence: [ 0 ]
```

5.3 Establishing or Maintaining OSPF Neighbor Relationship

On an OSPF network, all routing information is transmitted and exchanged between neighboring or adjacent routers. By maintaining neighbor relationships or adjacencies, you can stabilize the entire network.

5.3.1 Establishing the Configuration Task

When setting parameters on an interface, ensure that these parameters are consistent with those on the adjacent router.

Applicable Environment

In actual applications, establishing or maintaining OSPF neighbor relationship is prerequisite to constructing an OSPF network.

Through the following procedures, you can:

- Adjust convergence speed of the OSPF network and network load generated from protocol packets by modifying timers of OSPF packets.
- Enable OSPF to disconnect with the neighbor when the number of times for OSPF to retransmit packets exceeds the threshold by configuring Retransmission Limitation for OSPF (RL-OSPF). This avoids an infinite loop caused by non-stop packet retransmission when the neighbor does not receive packets.
- In the following types of networking, you can speed up the route convergence in the networks by rationally configuring the intervals for updating and receiving LSAs:
 - For the stable networking with high requirements on the route convergence time, you can set the interval for updating or receiving LSAs to 0. In this manner, the change of the topology or routes can be sensed immediately or be advertised to the network through LSAs. This speeds up the route convergence in the network.
 - For the networking with frequent route flapping, you can rationally configure the interval for updating or receiving LSAs, or start an intelligent timer to suppress a large number of LSAs from being updated or received. This prevents OSPF from occupying excessive network bandwidth and router resources.

Pre-configuration Tasks

Before establishing or maintaining OSPF neighbor relationship, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- [Configuring Basic OSPF Functions](#)

Data Preparation

To establish or maintain OSPF neighbor relationship, you need the following data.

No.	Data
1	Number of the interface running OSPF
2	Interval for sending Hello packets and Dead packets.
3	Maximum number of retransmission times
4	Interval for transmitting LSAs
5	Number of update LSAs to be flooded or interval for flooding update LSAs

5.3.2 Configuring the Interval for Sending Hello Packets

By adjusting the Hello interval set on OSPF neighbors, you can change the speed of establishing the neighbor relationship, thus changing the speed of network convergence.

Context

The Hello intervals set on the interfaces connecting two OSPF neighbors need to be the same.
 Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospf timer hello interval
```

The interval for sending Hello packets on the interface is set.

By default, the dead interval on the same interface should be four times the interval for sending Hello packets.

----End

5.3.3 Configuring Smart-discover

After Smart-discover is configured, when the neighbor status of a router changes or the DR or BDR on the multi-address network (broadcast network or NBMA network) changes, a router sends Hello packets to its neighbor immediately without waiting for the Hello timer to expire.

Context

Do as follows on the routers in the area as required:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospf smart-discover
```

The Smart-discover function is enabled on the interface.

---End

5.3.4 Configuring Dead Time of Neighbor Relationship

If a router does not receive a Hello packet from its neighbor within the Holddown time, the router considers the neighbor relationship invalid.

Context

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospf timer dead interval
```

The dead time during which the neighbor relationship becomes invalid is set.

By default, the dead interval on the same interface should be four times the interval for sending Hello packets.

NOTE

Setting the dead interval of an OSPF neighbor to be longer than 20s is recommended. If the dead interval of an OSPF neighbor is shorter than 20s, the session may be closed.

---End

5.3.5 Configuring OSPF Retransmission Limit

By limiting the number of DD packet retransmissions, Update packet retransmissions, or Request packet retransmissions, you can close the neighbor relationship when the number of packet retransmissions reaches the specified value.

Context

The OSPF packet retransmission mechanism is applicable to DD packets, LSU packets, and LSR packets. When the response packets of the three types of packets are not received, the mechanism is used to limit the number of packet retransmission times. When the number of transmission times reaches the specified value, the neighbor relationship is interrupted.

Do as follows on the OSPF router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
retransmission-limit [ max-number ]
```

The OSPF retransmission limit is configured.

By default, the function is disabled.

----End

5.3.6 Configuring the Interval for Updating and Receiving LSAs

You can set the LSA interval according to network connections and router resources.

Context

The OSPF protocol defines that the interval for updating LSAs is 5 seconds. The setting is expected to prevent network connections or frequent routing flapping from occupying excessive bandwidth and router resources.

When the network is stable and fast route convergence is required, you can cancel the interval for updating LSAs by setting the interval to 0. Thus, changes of the topology or routes can be immediately advertised to the network through LSAs. This speeds up route convergence in the network.

Do as follows on the OSPF router.

Procedure

- Configuring the Interval for Updating LSAs

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

3. Run:

```
lsa-originate-interval { 0 | intelligent-timer max-interval start-  
interval hold-interval [ other-type interval ] | other-type interval  
[ intelligent-timer max-interval start-interval hold-interval ] }
```

The interval for updating LSAs is set.

By default, the intelligent timer is enabled. The interval for updating LSAs is expressed in milliseconds. The maximum interval is 5000 milliseconds (ms), the initial interval is 500 ms, and the Holdtime interval is 1000 ms. After an intelligent timer is enabled, the interval for updating LSAs is as follows:

- (1) The initial interval for updating LSAs is specified by the parameter *start-interval*.
- (2) The interval for updating LSAs for the nth ($n \geq 2$) time is equal to *hold-interval* * 2(n-1).
- (3) When the interval specified by *hold-interval* * 2(n-1) reaches the maximum interval specified by *max-interval*, OSPF updates LSAs at the maximum interval for three consecutive times. Then, go back to Step 3.1, and OSPF updates LSAs at the initial interval specified by *start-interval*.

● Configuring the Interval for Receiving LSAs

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

3. Run:

```
lsa-arrival-interval { interval | intelligent-timer max-interval start-  
interval hold-interval }
```

The interval for receiving LSAs is set.

When the network is stable and fast route convergence is required, you can cancel the interval for receiving LSAs by setting it to 0. Routers can thus feel the changes of the topology or routes in time. This speeds up route convergence.

By default, the intelligent timer is enabled. The interval for receiving LSAs is expressed in milliseconds. The maximum interval for receiving LSAs is 1000 ms, the initial interval is 500 ms, and the Holdtime interval is 500 ms. After an intelligent timer is enabled, the interval for receiving LSAs is as follows:

- (1) The initial interval for receiving LSAs is specified by the parameter *start-interval*.

- (2) The interval for receiving LSAs for the n th ($n \geq 2$) time is equal to $hold\text{-}interval * 2^{(n-1)}$.
- (3) When the interval specified by $hold\text{-}interval * 2^{(n-1)}$ reaches the maximum interval specified by $max\text{-}interval$, OSPF receives LSAs at the maximum interval for three consecutive times. Then, go back to Step 3.1, and OSPF receives LSAs at the initial interval specified by $start\text{-}interval$.

----End

5.3.7 Restricting the Flooding of Update LSAs

When many LSAs need to be flooded, a router may be busy processing Update packets and discard the Hello packets that maintain neighbor relationships. By restricting the flooding of update LSAs, you can avoid this problem and maintain neighbor relationships.

Context

When many neighbors exist or many LSAs need to be flooded, a router may receive a large number of Update packets in a short period. If the router is busy processing these Update packets and discards the Hello packets that maintain neighbor relationships, neighbor relationships may be interrupted. During the setup of neighbor relationships, more packets need to be exchanged, which deteriorates the processing of packets. Restricting the flooding of update LSAs is introduced to prevent these problems by maintaining neighbor relationship.

Do as follows on the router that runs OSPF:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
flooding-control [ number transmit-number | timer-interval transmit-interval ] *
```

When the number of neighbors in a process exceeds 256, the flooding of update LSAs is restricted.

By default, a maximum of 50 update LSAs can be flooded every 30 seconds.

NOTE

After the **flooding-control** command is run, the restriction over update LSAs immediately takes effect. If the **flooding-control** command is not configured, restricting the flooding of update LSAs is enabled after the number of OSPF neighbors exceeds 256.

----End

5.3.8 Checking the Configuration

After OSPF neighbor relationships or adjacencies are stable, you can check OSPF statistics and information about neighbors in each area.

Prerequisite

The configurations of Establishing or Maintaining OSPF Neighbor Relationship function are complete.

Procedure

- Run the **display ospf** [*process-id*] **brief** command to check brief information about OSPF.
- Run the **display ospf** [*process-id*] **peer** command to check neighboring Router information about OSPF.
- Run the **display ospf** [*process-id*] **cumulative** command to check the OSPF statistics.
- Run the **display ospf** [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*] command to check the OSPF retransmission queue.

---End

5.4 Configuring OSPF Stub Areas

By configuring non-backbone areas at the edge of ASs as stub areas, you can reduce the size of the routing table and reduce the number of LSAs to be transmitted.

5.4.1 Establishing the Configuration Task

Configuring a stub area is optional. Not all areas can be configured as stub areas. Generally, a stub area, which is located at the AS boundary, is a non-backbone area with only one ABR.

Applicable Environment

To reduce the number of LSAs in the network and enhance OSPF extensibility, define OSPF areas. For some non-backbone areas at the edge of ASs, you can define them as stub areas for further reducing the size of the routing table and the number of LSAs.

This section describes procedures for configuring stub areas.

Pre-configuration Tasks

Before configuring OSPF stub areas, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- **Configuring Basic OSPF Functions**

Data Preparation

To configure OSPF stub areas, you need the following data.

No.	Data
1	Cost of default routes sent to stub areas

5.4.2 Defining the Current Area to be a Stub Area

A stub area is a special area in which ABRs do not flood the received AS external routes. Thus, the number of LSAs is greatly reduced.

Context

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view displayed.

Step 3 Run:

```
area area-id
```

The OSPF area view is displayed.

Step 4 Run:

```
stub [ no-summary ]
```

The current area is configured as a stub area.

The specified parameter **no-summary** takes effect only when the **stub** command is used on the ABR.

For all the routers connected to a stub area, you must configure the area as a stub area by running the **stub** command.

---End

5.4.3 Configuring Metrics of Default Routes Sent to Stub Areas

On a border router connected to a stub area, you can set the cost of the default route to the stub area.

Context

By default, the cost of the Type-3 default route that is transmitted to the stub area by OSPF is 1.

Do as follows on the OSPF router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view displayed.

Step 3 Run:

```
area area-id
```

The OSPF area view is displayed.

Step 4 Run:

```
stub [ no-summary ]
```

The current area is configured as a stub area.

Step 5 Run:

```
default-cost cost
```

The cost of the default route to the stub area is set.

This command is applied to the ABR that is connected to a stub area or an NSSA.

----End

5.4.4 Checking the Configuration

After OSPF stub areas are configured, you can check OSPF LSDB information and routing table information.

Prerequisite

The configurations of the OSPF Stub Areas are complete.

Procedure

- Run the commands as follow to check the LSDB information of OSPF:
 - **display ospf** [process-id] **lsdb** [brief]
 - **display ospf** [process-id] **lsdb** [router | network | summary | asbr | ase | nssa | opaque-link | opaque-area | opaque-as] [link-state-id] [originate-router [advertising-router-id] | self-originate]
- Run the commands as follow to check the information about the OSPF routing table:
 - **display ospf** [process-id] **routing** [ip-address [mask | mask-length]] [interface interface-type interface-number] [nexthop nexthop-address]
 - **display ospf** [process-id] **routing router-id** [router-id]
- Run the **display ospf** [process-id] **abr-asbr** [router-id] command to check the information about the OSPF ABR and ABSR.

----End

5.5 Configuring OSPF NSSA Areas

By configuring non-backbone areas as NSSA areas, external routes can be imported, and a new type of LSA, namely, Type 7 NSSA LSA is introduced.

5.5.1 Establishing the Configuration Task

There can be no Type 5 LSAs in NSSAs. Type 7 LSAs are generated by the ASBR in an NSSA and advertised only in the local NSSA.

Applicable Environment

The concept of NSSA is put forward because stub areas cannot import external routes. An NSSA allows the transmission of Type7 LSAs. Type7 LSAs are generated by an ASBR in an NSSA. When reaching the ABR that is responsible for converting Type 7 LSAs into Type 5 LSAs in the NSSA, Type 7 LSAs with the P-bit being set and the forwarding address being a non-zero address are converted into AS-external LSAs and advertised to other areas.

This section describes procedures for configuring an NSSA.

Pre-configuration Tasks

Before configuring an OSPF NSSA, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- [Configuring Basic OSPF Functions](#)

Data Preparation

To configure an OSPF NSSA, you need the following data.

No.	Data
1	Cost of default routes sent to the NSSA

5.5.2 Defining the Current Area to Be an NSSA Area

Derived from a stub area, an NSSA allows AS external routes to be imported; an ASBR advertises Type 7 NSSA LSAs in the local NSSA.

Context

Do as follows on the OSPF router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
area area-id
```

The OSPF area view is displayed.

Step 4 Run:

```
nssa [ default-route-advertise | flush-waiting-timer interval-value | no-import-route | no-summary | set-n-bit | suppress-forwarding-address | translator-always | translator-interval interval-value | zero-address-forwarding ] *
```

An area is configured as an NSSA.

For all the routers connected to the NSSA, you must configure the area as an NSSA by running the **nssa** command.

The area may be updated after NSSA attributes are configured or deleted. Thus, the NSSA attributes can be re-configured or deleted only after the last update of NSSA attributes is complete.

The parameters are valid only when the **nssa** command is used on specified routers.

By setting the parameter **flush-waiting-timer**, you can set the aging time to a maximum value 3600 seconds to delete invalid Type5 LSAs on other routers. When the ASBR also functions as an ABR, the parameter **flush-waiting-timer** does not take effect. This prevents Type5 LSAs in the non-NSSA from being deleted.

----End

5.5.3 Configuring Metrics of Default Routes Sent to NSSA Areas

On a border router connected to an NSSA, you can set the cost of the default route to the NSSA.

Context

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
area area-id
```

The OSPF area view is displayed.

Step 4 Run:

```
nssa [ default-route-advertise | flush-waiting-timer interval-value | no-import-route | no-summary | set-n-bit | suppress-forwarding-address | translator-always | translator-interval interval-value | zero-address-forwarding ] *
```

An area is configured as an NSSA.

For all the routers connected to the NSSA, you must configure the area as an NSSA by running the **nssa** command.

The optional parameters are valid only when the **nssa** command is used on an ABR.

Step 5 Run:

```
default-cost cost
```

The cost of default Type-3 routes to the NSSA is set.

This command takes effect only when it is configured on the ABR.

----End

5.5.4 Checking the Configuration

After NSSAs are configured, you can check OSPF LSDB information and routing table information.

Prerequisite

The configurations of OSPF NSSA Areas are complete.

Procedure

- Run the commands as follow to check the LSDB information of OSPF:
 - **display ospf** [*process-id*] **lsdb** [**brief**]
 - **display ospf** [*process-id*] **lsdb** [**router** | **network** | **summary** | **asbr** | **ase** | **nssa** | **opaque-link** | **opaque-area** | **opaque-as**] [*link-state-id*] [**originate-router** [*advertising-router-id*]] | **self-originate**]
- Run the commands as follow to check the information about the OSPF routing table:
 - **display ospf** [*process-id*] **routing** [*ip-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]
 - **display ospf** [*process-id*] **routing router-id** [*router-id*]
- Run the **display ospf** [*process-id*] **interface** [**all** | *interface-type interface-number*] [**verbose**] command to check the information about OSPF interfaces.

----End

5.6 Configuring OSPF Virtual Links

In actual applications, physical connectivity between non-backbone areas and backbone areas may not be ensured due to various limitations. To solve this problem, you can configure OSPF virtual links.

5.6.1 Establishing the Configuration Task

A virtual link also functions as a backup link. If the backbone area is partitioned because of a link fault, a virtual link provides the logical connectivity for the backbone area.

Applicable Environment

After OSPF areas are defined, OSPF route update between non-backbone areas is implemented through a backbone area. Then, OSPF requires that all non-backbone areas should maintain the connectivity with the backbone area and the backbone area should maintain its own connectivity.

In actual applications, this requirement may not be met because of some restrictions. To solve this problem, you can configure OSPF virtual links.

This section describes procedures for configuring OSPF virtual links.

Pre-configuration Tasks

Before configuring OSPF virtual links, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- [Configuring Basic OSPF Functions](#)

Data Preparation

To configure OSPF virtual links, you need the following data.

No.	Data
1	ID of the neighboring router on the virtual link
2	Interval for sending Hello packets
3	Retransmission interval and delay interval for LSAs
4	Dead time of routers on the virtual link
5	Authentication mode and password

5.6.2 Configuring OSPF Virtual Links

A virtual link refers to a logical channel established between two ABRs through a non-backbone area.

Context

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
area area-id
```

The OSPF area view is displayed.

Step 4 Run:

```
vlink-peer router-id [ dead dead-interval | hello hello-interval | retransmit
retransmit-interval | smart-discover | trans-delay trans-delay-interval | [ simple
[ [ plain ] plain-text | cipher cipher-text ] | { md5 | hmac-md5 } [ key-id
{ plain plain-text | [ cipher ] cipher-text } ] | authentication-null | keychain
keychain-name ] ] *
```

A virtual link is created and configured.

This command also needs to be used on the other end of the virtual link.

----End

5.6.3 Checking the Configuration

After OSPF virtual links are configured, you can check OSPF LSDB information and routing table information.

Prerequisite

The configurations of OSPF Virtual Links are complete.

Procedure

- Run the commands as follow to check the LSDB information of OSPF.
 - **display ospf** [process-id] **lsdb** [**brief**]
 - **display ospf** [process-id] **lsdb** [**router** | **network** | **summary** | **asbr** | **ase** | **nssa** | **opaque-link** | **opaque-area** | **opaque-as**] [link-state-id] [**originate-router** [advertising-router-id] | **self-originate**]
- Run the commands as follow to check the information about the OSPF routing table.
 - **display ospf** [process-id] **routing** [ip-address [mask | mask-length]] [**interface** interface-type interface-number] [**nexthop** nexthop-address]
 - **display ospf** [process-id] **routing router-id** [router-id]
- Run the **display ospf** [process-id] **vlink** command to check the information about OSPF virtual links.
- Run the **display ospf** [process-id] **interface** [**all** | interface-type interface-number] [**verbose**] command to check the information about OSPF interfaces.

----End

Example

Run the **display ospf vlink** command. If the status of the local virtual link is Full, it means that the virtual link is created successfully. For example:

```
<HUAWEI> display ospf vlink
      OSPF Process 1 with Router ID 1.1.1.1
      Virtual Links
Virtual-link Neighbor-id -> 2.2.2.2, Neighbor-State: Full
Interface: 10.1.1.1 (GigabitEthernet1/0/0)
Cost: 1 State: P-2-P Type: Virtual
Transit Area: 0.0.0.1
Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
GR State: Normal
```

5.7 Configuring OSPF Attributes in Different Types of Networks

By setting network types for OSPF interfaces and adjusting OSPF attributes, you can build OSPF networks flexibly.

5.7.1 Establishing the Configuration Task

OSPF does not support the configuration of network types on Null interfaces.

Applicable Environment

OSPF classifies networks into four types according to the link layer protocol. The NBMA network must be fully connected. That is, any two routers in the network must be directly reachable. In most cases, this requirement cannot be met. Then, you need to change the network type forcibly by running commands.

On a P2MP network, if the mask lengths of devices are different, the OSPF neighbor relationship cannot be established. Through the configuration, you can disable the devices from checking the network mask in Hello packets so that the OSPF neighbor relationship can be established.

In an NBMA network, if no reachable link exists between partial routers, configure the type of the interface to P2MP. If the router has only one peer end in the NBMA network, change the interface type to P2P.

In addition, when configuring a broadcast network or an NBMA network, you can specify the DR priority of each interface to affect the DR/BDR election in the network. Commonly, the router with higher performance and reliability is selected as a DR or BDR.

Pre-configuration Tasks

Before configuring OSPF attributes in different types of networks, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- [Configuring Basic OSPF Functions](#)

Data Preparation

To configure OSPF attributes in different types of networks, you need the following data.

No.	Data
1	Number of the interface running OSPF
2	Network type
3	DR priority of an interface
4	IP address of a neighbor on an NBMA network
5	Poll interval on an NBMA network

5.7.2 Configuring Network Types of OSPF Interfaces

OSPF classifies networks into four types according to link layer protocols. By configuring network types for interfaces, you can change the network types of interfaces.

Context

By default, the network type of an interface is determined by the physical interface. The network type of Ethernet interface is **broadcast**, that of the serial interface and POS interface (encapsulated with PPP or HDLC) is **p2p**, and that of ATM interface and Frame-relay interface is **nbma**.

Do as follows on the OSPF router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospf network-type { broadcast | nbma | p2mp | p2p }
```

Network types are configured for OSPF interfaces.

Configuring the new network type for an interface will cause the OSPF session on the interface to be reestablished.

NOTE

Generally, the network types of two OSPF interfaces on the both ends of the link must be identical. Otherwise, the two interfaces cannot set up the neighbor relationship. Only when the network type of one OSPF interface is broadcast and the network type of the other OSPF interface is P2P, the two interfaces can still set up the neighbor relationship. The broadcast interface can learn the correct OSPF routing information, but the P2P interface cannot learn the OSPF routing information from the peer.

---End

5.7.3 Configuring DR Priorities of OSPF Interfaces

When configuring a broadcast network or an NBMA network, you can specify the DR priority for each interface to change the results of DR/BDR election on the network.

Context

When configuring broadcast networks or NBMA networks, you can specify the DR priority for each interface to affect the DR/BDR election in the network. The greater the value is, the higher the priority is.

By default, the priority of the interface that candidates for the DR is 1.

Do as follows on the OSPF router.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`interface interface-type interface-number`
The interface view is displayed.
- Step 3** Run:
`ospf dr-priority priority`
DR priorities are set for OSPF interfaces.
- End

Follow-up Procedure

After the DR priority is changed, you can re-elect a DR or BDR through the following methods, which, however, will result in the interruption of the OSPF neighbor relationship between routers and therefore are used only when necessary.

- Restarting all routers.
- Running the `shutdown` and `undo shutdown` commands on the interface on which the OSPF neighbor relationship is set up.

5.7.4 Disabling the Function of Checking the Network Mask on a P2MP Network

On a P2MP network, when the mask lengths of devices are different, you can disable devices from checking the network mask so that the OSPF neighbor relationship can be established.

Context

On a P2MP network, when the mask lengths of devices are different, use the `ospf p2mp-mask-ignore` command to ignore the check on the network mask in Hello packets. In this manner, the OSPF neighbor relationship can be established.

Do as follows on the OSPF router:

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`interface interface-type interface-number`
The interface view is displayed.
- Step 3** Run:
`ospf network-type p2mp`

The network type is configured for an OSPF interface.

Step 4 Run:

```
ospf p2mp-mask-ignore
```

The device is configured not to check the network mask on a P2MP network.

----End

5.7.5 Configuring Neighbors for NBMA Networks

An NBMA interface cannot find neighbors by broadcasting Hello packets. Thus, you need to manually specify the IP addresses of neighbors for this interface and set the election rights for these neighbors.

Context

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
peer ip-address [ dr-priority priority ]
```

Neighbors are configured for NBMA networks.

----End

5.7.6 Configuring the Interval for Sending Poll Packets in NBMA Networks

On an NBMA network, after a neighbor becomes invalid, a router sends Hello packets at the set polling interval.

Context

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospf timer poll interval
```

The interval for sending Poll packets on an NBMA interface is set.

----End

5.7.7 Checking the Configuration

After OSPF attributes in different types of network are set, you can check OSPF statistics, LSDB information, neighbor information, and interface information.

Prerequisite

The configurations of OSPF Attributes in Different Types of Networks are complete.

Procedure

- Run the commands as follow to check the LSDB information of OSPF:
 - **display ospf** [process-id] **lsdb** [**brief**]
 - **display ospf** [process-id] **lsdb** [**router** | **network** | **summary** | **asbr** | **ase** | **nssa** | **opaque-link** | **opaque-area** | **opaque-as**] [link-state-id] [**originate-router** [advertising-router-id] | **self-originate**]
- Run the **display ospf** [process-id] **peer** [[interface-type interface-number] neighbor-id | **brief** | **last-nbr-down**] command to check the information about OSPF neighboring nodes.
- Run the **display ospf** [process-id] **nexthop** command to check the information about OSPF next hops.
- Run the commands as follow to check the information about the OSPF routing table:
 - **display ospf** [process-id] **routing** [ip-address [mask | mask-length]] [**interface** interface-type interface-number] [**nexthop** nexthop-address]
 - **display ospf** [process-id] **routing router-id** [router-id]
- Run the **display ospf** [process-id] **interface** [**all** | interface-type interface-number] [**verbose**] command to check the information about OSPF interfaces.

----End

Example

Run the **display ospf interface** command. If OSPF interface types and interface priorities (used for the DR election) are displayed, it means that the configuration succeeds. For example:

```
<HUAWEI> display ospf interface GigabitEthernet2/0/0
      OSPF Process 1 with Router ID 1.1.1.1
      Interfaces
      Interface: 11.1.1.1 (GigabitEthernet2/0/0)
      Cost: 1      State: BDR      Type: Broadcast      MTU: 1500
      Priority: 1
      Designated Router: 11.1.1.2
      Backup Designated Router: 11.1.1.1
      Timers: Hello 10 , Dead 40 , Poll 120 , Retransmit 5 , Transmit Delay 1
```

5.8 Configuring OSPF Route Attributes

By setting OSPF route attributes, you can change OSPF routing policies to meet the requirements of complex networks.

5.8.1 Establishing the Configuration Task

Before configuring OSPF route attributes, familiarize yourself with the applicable environment, complete pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

In actual applications, to meet requirements of a complicated networking environment, you can change OSPF routing policies by configuring OSPF route attributes. Through the following procedures, you can:

- Set the cost of OSPF routes on the interface.
- Change the matching order of routing protocols by configuring the OSPF priority when multiple routing protocols provide routes to the same destination.
- Configure load balancing among multiple equal-cost routes.

Pre-configuration Tasks

Before configuring OSPF route attributes, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- [Configuring Basic OSPF Functions](#)

Data Preparation

To configure OSPF route attributes, you need the following data.

No.	Data
1	Link cost
2	OSPF priority
3	Maximum number of equal-cost routes

5.8.2 Configuring the Link Cost of OSPF

OSPF can automatically calculate the link cost for an interface according to the interface bandwidth. You can also set the link cost for the interface by using the related command.

Context

To configure the cost of an OSPF link, you can directly configure the cost of an OSPF interface.

If you do not set the cost of the OSPF interface directly, OSPF calculates the cost according to the bandwidth of the interface. The calculation formula is as follows: cost of the interface = bandwidth reference value/interface bandwidth. The integer of the calculated result is the cost of the interface. If the result is smaller than 1, the cost value is 1. You can indirectly change the cost of the interface by changing the bandwidth reference value.

By default, the bandwidth reference value is 100 of an OSPF process for an OSPF interface without a set cost. Therefore, interfaces with different bandwidths can obtain different cost values according to the calculation formula.

Do as follows on the OSPF router.

Procedure

- Configuring the Link Cost on an OSPF Interfaces

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
ospf cost cost
```

The cost of OSPF interfaces is set.

- Configuring Bandwidth Reference Value

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

3. Run:

```
bandwidth-reference value
```

The bandwidth reference value is set.

When setting the bandwidth reference value, ensure that the bandwidth reference values of all the routers in the process are consistent.

---End

5.8.3 Configuring OSPF Precedence

When multiple routing protocols discover the routes to the same destination, you can set the OSPF priorities of the routes discovered by these routing protocols.

Context

Multiple dynamic routing protocol may run on a router at the same time. Thus, there is the problem of routing information sharing and routing selection among routing protocols. The

system sets the priority for each routing protocol. When different protocols detect the same route, the route with a higher priority is selected.

After OSPF calculates equal-cost routes, you can run the **nexthop** command to select the route with the highest priority from the equal-cost routes as the next hop. The smaller the weight, the higher the priority of the route. By default, the weight is 255. It indicates that load balancing is carried out among the equal-cost routes without distinguishing their priorities.

Do as follows on the OSPF router:

Procedure

- Configuring OSPF Priority
 1. Run:

```
system-view
```

The system view is displayed.
 2. Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.
 3. Run:

```
preference [ ase ] { preference | route-policy route-policy-name } *
```

The priority of OSPF is set.
- Configuring the Priority for OSPF Equal-Cost Routes
 1. Run:

```
system-view
```

The system view is displayed.
 2. Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.
 3. Run:

```
nexthop ip-address weight value
```

The priority for load balancing of OSPF is set.

----End

5.8.4 Setting the Convergence Priority of OSPF Routes

By setting convergence priorities for OSPF routes, you can set priorities for specific routes so that these routes converge preferentially. This thus shortens the interruption of key services and improves the reliability of the entire network.

Context

With the integration of network services, different services such as data, voice, and video run on the same network infrastructure, and have different requirements for the network. For Video on Demand (VoD) services, the route convergence speed of the multicast source server is the most critical factor that affects multicast services. It is required that the routes to the multicast source should converge rapidly when network faults occur. On the BGP or MPLS VPN bearer

network where OSPF is used to implement the IP connectivity of the backbone network, end-to-end routes between PEs need to be converged rapidly.

You can set priorities for specific routes by setting the convergence priority of OSPF routes so that these routes converge preferentially. This shortens the interruption of key services and improves the reliability of the entire network.

Do as follows on the router that runs OSPF:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF view is displayed.

Step 3 Run:

```
prefix-priority { critical | high | medium } ip-prefix ip-prefix-name
```

The convergence priority of OSPF routes is set.

After the convergence priority of OSPF routes is set, OSPF can calculate and flood LSAs, and synchronize LSDBs according to priorities. This speeds up route convergence. This speeds up route convergence. When an LSA meets multiple priorities, the highest priority takes effect. OSPF calculates LSAs in the sequence of intra-area routes, inter-area routes, and AS external routes. This command makes OSPF calculate the three types of routes separately according to the specified route calculation priorities. Convergence priorities are critical, high, and medium. To speed up the processing of LSAs with the higher priority, during LSA flooding, the LSAs need to be placed into the corresponding critical, high, and medium queues according to priorities.

NOTE

This command takes effect only on the public network.

Step 4 (Optional) Run:

```
quit
```

The system view is displayed.

Step 5 (Optional)Run:

```
ip route prefix-priority-scheduler critical-weight high-weight medium-weight low-weight
```

The scheduling ratio of IPv4 routes by priority is set.

By default, the scheduling ratio of IPv4 routes by priority is 8:4:2:1.

----End

5.8.5 Configuring the Maximum Number of Equal-Cost Routes

You can set the maximum number of intra-area, inter-area, or external routes.

Context

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
maximum load-balancing number
```

The maximum number of equal-cost routes is set.

NOTE

The range and default value of the number of equal-cost routes may vary with products and protocols. You can adjust the range and default value of the number of equal-cost routes after purchasing the License.

----End

5.8.6 Checking the Configuration

After OSPF route attributes are configured, you can check OSPF routing table information, interface information, and next hop information.

Prerequisite

The configurations of OSPF Route Attributes are complete.

Procedure

- Run the **display ospf [process-id] routing [[ip-address [mask | mask-length] | interface interface-type interface-number | nexthop nexthop-address] | router-id [router-id]]** command to check the information about the OSPF routing table.
- Run the **display ospf [process-id] interface [all | interface-type interface-number] [verbose]** command to check the information about OSPF interfaces.

----End

Example

Run the **display ospf [process-id] routing ip-address** command. If the convergence priority of the route is displayed, it means that the configuration succeeds.

```
<HUAWEI> display ospf routing 100.1.1.1

      OSPF Process 1 with Router ID 1.1.1.1

Destination : 100.1.1.0/24
AdverRouter : 100.1.1.2           Area      : 0.0.0.0
Cost        : 1                   Type      : Transit
```

NextHop : 100.1.1.2 Interface : Ethernet3/2/0
 Priority : Low Age : 00h02m43s

5.9 Controlling OSPF Routing Information

This section describes how to control the advertising and receiving of OSPF routing information and import routes from other protocols.

5.9.1 Establishing the Configuration Task

Before controlling OSPF routing information, familiarize yourself with the applicable environment, complete pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

Through the following procedures, you can configure routers to control the advertising and receiving of OSPF routing information and import routes from other protocols.

Pre-configuration Tasks

Before configuring to control OSPF routing information, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- [Configuring Basic OSPF Functions](#)

Data Preparation

To control OSPF routing information, you need the following data.

No.	Data
1	Link costs
2	ACL used to filter routing information
3	Protocol names, process IDs, and default values of the routes to be imported

5.9.2 Configuring OSPF Route Aggregation

After an AS is divided into areas, configuring route aggregation can reduce routing information transmitted between areas, thus reducing the size of the routing table and improving route performance.

Context

Do as follows on the OSPF router.

Procedure

- Configuring ABR Route Aggregation

Do as follows on the OSPF ABR:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

3. Run:

```
area area-id
```

The OSPF area view is displayed.

4. Run:

```
abr-summary ip-address mask [ [ advertise | not-advertise ] | cost cost ]  
*
```

ABR route aggregation of OSPF is configured.

- Configuring ASBR Route Aggregation

Do as follows on the OSPF ASBR:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

3. Run:

```
asbr-summary ip-address mask [ not-advertise | tag tag | cost cost |  
distribute-delay interval ] *
```

ASBR route aggregation of OSPF is configured.

---End

5.9.3 Configuring OSPF to Filter the Received Routes

By configuring filtering conditions for the received routes, you can allow only the routes that pass the filtering to be installed into the routing table.

Context

Do as follows on the OSPF router.

Procedure

- Step 1** Run:

```
system-view
```

The system view is displayed.

- Step 2** Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name } import
```

OSPF is configured to filter the received routes.

OSPF is a dynamic routing protocol based on the link state, and routing information is hidden in the link state. Therefore, the **filter-policy** command cannot be used to filter the advertised and received LSAs. You can then run the **filter-policy** command to filter the routes calculated by OSPF. Only the routes that match the filtering rules are added to the routing table.

The **filter-policy** command is used to filter only the routes that match OSPF and are installed to the local routing table. Routes that do not pass the filtering are neither added to the OSPF routing table nor advertised. Therefore, whether the received routes pass the filtering or not, the LSDB is not affected.

---End

5.9.4 Configuring OSPF to Filter ABR Type3 LSA

By configuring filtering conditions for Type 3 LSAs, you can allow only the routes that pass the filtering to be received or advertised.

Context

Do as follows on the OSPF router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
area area-id
```

The OSPF area view is displayed.

Step 4 Run:

```
filter { acl-number | acl-name acl-name | ip-prefix ip-prefix-name | route-policy route-policy-name } import
```

The received and advertised rule of filtering Type3 LSAs originated by the ABR is configured.

```
filter { acl-number | acl-name acl-name | ip-prefix ip-prefix-name | route-policy route-policy-name } export
```

The rejected received or advertised rule of filtering Type3 LSAs originated by the ABR is configured.

---End

5.9.5 Configuring OSPF to Import External Routes

Importing the routes discovered by other routing protocols can enrich OSPF routing information.

Context

OSPF can ensure loop-free intra-area routes and inter-area routes; however, OSPF cannot prevent external routes from loops. Therefore, you should be cautious when configuring OSPF to import external routes, avoid the loops caused by manual configurations. For detailed information, refer to "OSPF VPN Extension" in the HUAWEI NetEngine80E/40E Router Feature Description - VPN.

Do as follows on the OSPF ASBR.

Procedure

- Configuring OSPF to Import Routes of Other Protocols

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

3. Run:

```
import-route { limit limit-number | protocol [ process-id ] [ cost cost |  
route-policy route-policy-name | tag tag | type type ] * }
```

Routes of other protocols are imported.

4. (Optional)Run:

```
filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-  
name } export [ protocol [ process-id ] ]
```

The routes imported in [Step 3](#) are filtered.

Only the routes that pass the filtering can be advertised.

You can configure OSPF to filter the routing information of a protocol or a process by specifying the parameter *protocol [process-id]*. If *protocol [process-id]* is not specified, OSPF filters all the imported routing information.

 **NOTE**

- The **import-route** command cannot be used to import the default routes of external routes.
- OSPF filters the imported routes; that is, OSPF transforms only eligible external routes to Type5 LSAs and advertises them.

- Configuring OSPF to Import Default Routes

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

3. Run the following commands as required:

- Run:

```
default-route-advertise [ [ always | permit-calculate-other ] | cost
cost | type type | route-policy route-policy-name ] *
```

The default routes are imported to the OSPF process.

To add the imported default routes to the current routing table, ensure that the priority of the configured static default route is lower than that of the default route imported by OSPF if an OSPF router is configured with static default routes.

- Run:

```
default-route-advertise summary cost cost
```

The default cost is specified for Type 3 summary LSAs.

Enable VPN before selecting parameters. Otherwise, this command cannot be configured.

- Configuring Related Parameters for OSPF to Import Routes

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

3. Run:

```
default { cost { cost | inherit-metric } | limit limit | tag tag | type
type } *
```

The default values of the parameters (cost, the upper limit of the imported external routes within the specified period, tag, and type) related to imported routes are set.

When OSPF imports external routes, you can configure the default values for some additional parameters, such as the cost, number of routes, tag, and type. The route tag is used to tag the protocol related information. For example, it is used to differentiate the number of the ASs when OSPF receives BGP.

By default, the metric of the external routes imported by OSPF is 1; a maximum of 2147483647 routes can be imported each time; the type of the imported external routes is Type 2; the default tag value of the imported routes is 1.

NOTE

You can run one of the following commands to set the cost of the imported route. The following commands are listed in the descending order of priorities.

- Run the **apply cost** command to set the cost of a route.
- Run the **import-route** command (OSPF) to set the cost of the imported route.
- Run the **default** command to set the default cost of the imported route.

----End

5.9.6 Checking the Configuration

After OSPF routing information is controlled, you can check OSPF routing table information, interface information, and ASBR route aggregation information.

Prerequisite

The configurations of Controlling OSPF Routing Information are complete.

Procedure

- Run the commands as follow to check the information about the OSPF routing table:
 - **display ospf** [*process-id*] **routing** [*ip-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]
 - **display ospf** [*process-id*] **routing router-id** [*router-id*]
- Run the **display ospf** [*process-id*] **interface** [**all** | *interface-type interface-number*] [**verbose**] command to check the information about OSPF interfaces.
- Run the **display ospf** [*process-id*] **asbr-summary** [*ip-address mask*] command to check the information about OSPF ASBR route aggregation.

----End

Example

Run the **display ospf interface** command. If information about OSPF interfaces is displayed, it means that the configuration succeeds. For example:

```
<HUAWEI> display ospf interface GigabitEthernet2/0/0
      OSPF Process 1 with Router ID 1.1.1.1
          Interfaces
Interface: 11.1.1.1 (GigabitEthernet2/0/0)
Cost: 1          State: BDR          Type: Broadcast      MTU: 1500
Priority: 1
Designated Router: 1.1.1.2
Backup Designated Router: 1.1.1.1
Timers: Hello 10 , Dead 40 , Poll 120 , Retransmit 5 , Transmit Delay 1
```

Run the **display ospf asbr-summary** command. If information about aggregation of the routes imported by the local router is displayed, it means that the configuration succeeds. For example:

```
<HUAWEI> display ospf asbr-summary
      OSPF Process 1 with Router ID 192.168.1.2
          Summary Addresses
Total summary address count: 1
          Summary Address
net          : 10.0.0.0
mask        : 255.0.0.0
tag         : 10
status      : Advertise
Cost        : 0 (Not Configured)
delay       : 0 (Not Configured)
The Count of Route is : 2
Destination  Net Mask      Proto   Process  Type   Metric
10.1.0.0     255.255.0.0   Static  1        2     10
10.2.0.0     255.255.0.0   Static  1        2     10
```

5.10 Optimizing an OSPF Network

By configuring OSPF functions in special network environments, you can adjust and optimize the OSPF network performance.

5.10.1 Establishing the Configuration Task

Before optimizing an OSPF network, familiarize yourself with the applicable environment, complete pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

In some special networking environments, you need to configure OSPF features and optimize the performance of the OSPF network. Through the following procedures, you can:

- Adjust convergence speed of the OSPF network and network load generated from protocol packets by modifying timers of OSPF packets. On some low-speed links, the delay of transmitting LSAs must be considered.
- Avoid resource consumption caused by frequent network changes by adjusting the SPF interval.
- When the backup link exists, you can enable OSPF-BGP linkage on the stub router so that the restarted router or the newly joined router does not use the stub router to forward packets during the linkage of OSPF and BGP. This avoids traffic loss caused by BGP route convergence, which is slower than OSPF route convergence, during traffic switchback.

Pre-configuration Tasks

Before configuring to optimize an OSPF network, complete the configuration tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- [Configuring Basic OSPF Functions](#)

Data Preparation

To optimize an OSPF network, you need the following data.

No.	Data
1	Values of timers of packets
2	MTU carried in DD packets
3	Maximum number of external LSAs in the LSDB
4	Authentication modes and passwords used in authentication

5.10.2 Configuring the Delay for Transmitting LSAs on the Interface

It takes time to transmit OSPF packets on a link. Therefore, a certain delay is added to the aging time of an LSA before the LSA is sent.

Context

By default, the delay is 1 second.

 **NOTE**

On low-speed links, you should focus on this configuration.

Do as follows on the OSPF router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospf trans-delay interval
```

The delay of transmitting LSAs on the interface is set.

---End

5.10.3 Configuring the Interval for Retransmitting LSAs

After a router sends an LSA to its neighbor, the router expects to receive an LSAck packet from its neighbor. If the router does not receive an LSAck packet within the LSA retransmission interval, it retransmits the LSA to the neighbor.

Context

Do as follows on the OSPF router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospf timer retransmit interval
```

The interval for retransmitting LSAs between neighboring routers is set.

By default, the interval for retransmitting LSAs is 5 seconds.

 **NOTE**

Do not set the LSA retransmission interval to a very small value; otherwise, unnecessary retransmission is caused. The retransmission interval must be longer than the time for a packet to be transmitted to and from between two routers.

----End

5.10.4 Configuring the Local Router to Filter the LSAs to Be Sent

When multiple links exist between two routers, you can filter the outgoing LSAs on certain links. This reduces the unnecessary retransmission of LSAs and saves bandwidth resources.

Context

Filtering the LSAs to be sent on the local router can prevent useless LSAs from being sent to neighbors. This can reduce the size of the LSDB of neighbors and speed up the network convergence.

Do as follows on the router that runs OSPF:

Procedure

- Configure the router to filter the LSAs that are sent to the specified neighbors in a P2MP network:
 1. Run:


```
system-view
```

The system view is displayed.
 2. Run:


```
ospf [ process-id ]
```

The OSPF process view is displayed.
 3. Run:


```
filter-lsa-out peer ip-address { all | { summary [ acl { acl-number | acl-name } ] | ase [ acl { acl-number | acl-name } ] | nssa [ acl { acl-number | acl-name } ] } * }
```

In a P2MP network, the local router filters the LSAs to be sent.

By default, the local router does not filter the LSAs to be sent.
- Configure the specified interface enabled with OSPF to filter outgoing LSAs in a broadcast, NBMA, P2P, or P2MP network:
 1. Run:


```
system-view
```

The system view is displayed.
 2. Run:


```
interface interface-type interface-number
```

The interface view is displayed.
 3. Run:


```
ospf filter-lsa-out { all | { summary [ acl { acl-number | acl-name } ] | ase [ acl { acl-number | acl-name } ] | nssa [ acl { acl-number | acl-name } ] } * }
```

The local router filters the LSAs to be sent.

By default, the local router does not filter the LSAs to be sent.

----End

5.10.5 Suppressing the Interface from Receiving and Sending OSPF Packets

By suppressing the OSPF interface from receiving and sending OSPF packets, you can prevent routers on a certain network from obtaining OSPF routing information and prevent the local router from receiving the routing updates advertised by other routers.

Context

To prevent OSPF routing information from being obtained by the routers on a certain network, and prevent the local router from receiving the routing updates advertised by other routers, run the **silent-interface** command to suppress the interface from receiving and sending OSPF packets.

Different processes can suppress the same interface from sending and receiving OSPF packets, but the **silent-interface** command is valid only for the OSPF interface on which the specified process is enabled, and has no effect on the interfaces of other processes.

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
silent-interface { all | interface-type interface-number }
```

An interface is suppressed from receiving and sending OSPF packets.

----End

Follow-up Procedure

After an OSPF interface is set to be in the silent state, the interface can still advertise its direct route. The Hello packets on the interface, however, are blocked, and thus no neighbor relationship can be established on the interface. This can enhance the OSPF capability to adapt to the networking and reduce the consumption of system resources.

5.10.6 Configuring the Interval for SPF Calculation

By setting the interval for SPF calculation, you can reduce resource consumption caused by frequent network changes.

Context

When the OSPF LSDB changes, the shortest path need be recalculated. Frequent network changes occupy many system resources and affect the efficiency of routers. You can configure an intelligent timer and rationally set the interval for the SPF calculation to avoid excessive router memory and bandwidth resources from being occupied.

By default, the intelligent timer is enabled. The interval for the SPF calculation is expressed in milliseconds. The maximum interval for the SPF calculation is 10000 ms, the initial interval is 500 ms, and the Holdtime interval is 1000 ms.

Do as follows on the OSPF router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
spf-schedule-interval { interval1 | intelligent-timer max-interval start-interval  
hold-interval | millisecond interval2 }
```

The interval for the SPF calculation is set.

After an intelligent timer is enabled, the interval for the SPF calculation is as follows:

1. The initial interval for the SPF calculation is specified by the parameter *start-interval*.
2. The interval for the SPF calculation for the *n*th ($n \geq 2$) time is equal to $hold-interval \times 2$ ($n-1$).
3. When the interval specified by $hold-interval \times 2(n-1)$ reaches the maximum interval specified by *max-interval*, OSPF performs the SPF calculation at the maximum interval for three consecutive times. Then, go back to Step 3.1, and OSPF performs the SPF calculation at the initial interval specified by *start-interval*.

----End

5.10.7 Configuring Stub Routers

When a router has a heavy load and cannot forward any other packets, you can configure it as a stub router. After the router is configured as a stub router, other OSPF routers do not use this router to forward data but they can have a route to this stub router.

Context

The metric of the links in the router LSAs generated by the stub router is set to a higher value (65535).

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
stub-router [ on-startup [ interval ] ]
```

A stub router is configured.

By default, the period during which a router keeps being a stub router is 500 seconds.

NOTE

There is no correlation between the stub router configured through this command and the router in the stub area.

---End

5.10.8 Enabling the Mesh-Group Function

When concurrent links exist between a router and its neighbor, you can enable the mesh-group function to reduce the load on the links.

Context

The router ID of a neighbor uniquely identifies a mesh group. Interfaces can belong to the same mesh-group only when the interfaces belong to the same area and OSPF process, the interface statuses are higher than Exchange, and each interface is connected with only one neighbor.

If multiple concurrent links exist between the router and its neighbor that are enabled with the mesh-group function, the router selects a primary link to flood the received LSAs, without performing reverse flooding.

Do as follows on the router that runs OSPF:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
mesh-group enable
```

The mesh-group function is enabled.

By default, the mesh-group function is disabled.

----End

5.10.9 Configuring the MTU in DD Packets

You can configure OSPF to fill in the Interface MTU field of the DD packet with the actual MTU.

Context



CAUTION

After the MTU value in a DD packet is configured, the neighbor relationship is reestablished.

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospf mtu-enable
```

The interface is enabled to fill in the MTU value in a DD packet when sending the DD packets.

Generally, an interface replaces the actual MTU value with 0 when sending DD packets. After this command is configured, the interface fills in the Interface MTU field of the DD packets with the actual MTU value.

----End

5.10.10 Configuring the Maximum Number of External LSAs in the LSDB

By setting the maximum number of external LSAs in the LSDB, you can restrict the number of routes within a proper range.

Context

Do as follows on the OSPF router:

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`ospf [process-id]`
The OSPF process view is displayed.
- Step 3** Run:
`lsdb-overflow-limit number`
The maximum number of external LSAs in the LSDB is set.
- End

5.10.11 Configuring RFC 1583 Compatible External Routing

The routing rule defined in RFC 2328 is different from that in RFC 1583. When the same external route is calculated according to multiple LSAs, the routing rule configured through the `rfc1583 compatible` command is compatible with that defined in RFC 1583.

Context

Do as follows on the OSPF router.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`ospf [process-id]`
The OSPF process view is displayed.
- Step 3** Run:
`rfc1583 compatible`
The external routing rule compatible with RFC 1583 is set.
By default, the routing rule of compatible 1583 is enabled.
- End

5.10.12 Checking the Configuration

After the OSPF network is optimized, you can check OSPF statistics, request and retransmission queues, and brief information about mesh-groups.

Prerequisite

The configurations of Optimizing an OSPF Network are complete.

Procedure

- Run the **display ospf** [*process-id*] **brief** command to check the brief information about OSPF.
- Run the **display ospf** [*process-id*] **cumulative** command to check the OSPF statistics.
- Run the **display ospf** [*process-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*] command to check the OSPF request queue.
- Run the **display ospf** [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*] command to check the OSPF retransmission queue.
- Run the commands as follow to check the OSPF error information:
 - **display ospf** [*process-id*] **error** [*lsa*]
 - **display ospf error** [**packet** [*number*]]
- Run the **display ospf global-statistics** { **process** *process-id* | **vpn-instance** *vpn-instance-name* | **public-instance** | **timewheel** | **brief** } command to check the global statistics information about OSPF.
- Run the **display ospf** [*process-id*] **mesh-group** [**brief**] command to check the brief information about OSPF mesh-groups.

----End

Example

Run the **display ospf brief** command. If details about the OSPF timer and delay in sending LSAs are displayed, it means that the configuration succeeds. For example:

```
<HUAWEI> display ospf brief
      OSPF Process 1 with Router ID 10.1.1.1
      OSPF Protocol Information
RouterID: 10.1.1.1      Border Router: AREA AS NSSA
Route Tag: 0
Multi-VPN-Instance is not enabled
Global DS-TE Mode: Non-Standard IETF Mode
Opaque Capable
Graceful-restart capability: planned and un-planned, totally
Helper support capability : enabled
      filter capability : disabled
      policy capability : strict lsa check, planned and un-planned
Applications Supported: MPLS Traffic-Engineering
Spf-schedule-interval: max 10000ms, start 500ms, hold 1000ms
Default ASE parameters: Metric: 1 Tag: 1 Type: 2
Route Preference: 10
ASE Route Preference: 150
SPF Computation Count: 4
RFC 1583 Compatible
Retransmission limitation is disabled
Area Count: 2 Nssa Area Count: 1
Exchange/Loading Neighbors: 0
Area: 0.0.0.0 (MPLS TE not enabled)
Authtype: MD5 Area flag: Normal
SPF scheduled Count: 4
Exchange/Loading Neighbors: 0
Interface: 10.1.1.1 (Ethernet3/0/0)
Cost: 1 State: Waiting Type: Broadcast MTU: 1500
Priority: 1
Designated Router: 0.0.0.0
Backup Designated Router: 0.0.0.0
Timers: Hello 10 , Dead 40 , Poll 120 , Retransmit 5 , Transmit Delay 1
Area: 0.0.0.6 (MPLS TE not enabled)
Authtype: None Area flag: NSSA
SPF scheduled Count: 0
```

ExChange/Loading Neighbors: 0

5.11 Configuring Local MT

By configuring local MT, you can prevent multicast services from becoming unavailable when both multicast and an MPLS TE tunnel are deployed on a network.

5.11.1 Establishing the Configuration Task

Local MT supports only OSPF processes of the public network instance.

Applicable Environment

If multicast and an MPLS TE tunnel are deployed in a network simultaneously and the TE tunnel is configured with IGP Shortcut, multicast packets are forwarded through the TE tunnel. The routers spanned by the TE tunnel cannot sense the multicast packets, so the routers do not create any multicast forwarding entry. As a result, the multicast service is interrupted. To avoid the preceding problem, local MT is configured. Therefore, the correct multicast routing table can be created to guide the forwarding of multicast packets.

 **NOTE**

- Local MT supports only OSPF processes of the public network instance.
- Local MT does not support forwarding adjacency.

Pre-configuration Tasks

Before configuring local MT, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- [5.2 Configuring Basic OSPF Functions](#)
- Enabling the TE tunnel of the OSPF process

Data Preparation

To configure local MT, you need the following data.

No.	Data
1	Filtering list used to filter OSPF routing information

5.11.2 Enabling Local MT

When both multicast and an MPLS TE tunnel are deployed on a network, you need to enable local MT for multicast packet forwarding.

Context

Do as follows on the router that needs to forward multicast packets and is configured with the TE tunnel that is enabled with IGP Shortcut:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF view is displayed.

Step 3 Run:

```
local-mt enable
```

Local MT is enabled.

----End

5.11.3 (Optional) Controlling the Scale of the MIGP Routing Table

To properly control the size of the MIGP routing table and accelerate the search of the MIGP routing table, you can configure the filtering policy based on multicast source addresses. Only the routes that are destined to multicast source addresses and match the filtering policy are installed into the MIGP routing table.

Context

After creating the MIGP routing table by **Enabling Local MT**, OSPF performs route calculation. When the calculated outgoing interface of the next hop is a TE tunnel interface enabled with IGP shortcut, a router uses the physical interface as the outgoing interface of the next hop and stores it to the MIGP routing table. To make the size of the MIGP routing table reasonable and accelerate the speed for searching the MIGP routing table, you can configure the filtering policy for the multicast source address. Thus, only the routes that head towards the multicast source address and match the policy are added to the MIGP routing table.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF view is displayed.

Step 3 Run:

```
local-mt filter-policy {acl acl-number | ip-prefix ip-prefix-name }
```

The local MT filtering policy of OSPF is configured.

 **NOTE**

You are recommended to configure the routing policy before enabling local MT. This can prevent the excessive routes to the not-multicast source address from being added to the MIGP routing table and thus keeps the number of routes in the MIGP routing table within the upper limit.

----End

5.11.4 Checking the Configuration

After local MT is configured, you can check the OSPF MIGP routing table, routing table, and brief information.

Prerequisite

The configurations of the OSPF Local MT are complete.

Procedure

- Run the **display ospf** [*process-id*] **migp-routing** [*ip-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*] command to check the OSPF MIGP routing table.
- Run the **display ospf** [*process-id*] **routing** command to check the OSPF routing information.
- Run the **display ospf** [*process-id*] **brief** command to check the brief information about OSPF.

----End

5.12 Configuring OSPF IP FRR

With OSPF IP FRR, devices can rapidly switch traffic from faulty links to backup links without interrupting traffic. This protects traffic and greatly improves the reliability of OSPF networks.

5.12.1 Establishing the Configuration Task

Applicable Environment

With the development of networks, Voice over IP (VoIP) and on-line video services require high-quality real-time transmission. Nevertheless, if an OSPF fault occurs, traffic can be switched to a new link only after the following processes: fault detection at the millisecond level, notifying the fault to the routing control plane at the millisecond level, generating and flooding new topology information at the tens of milliseconds level, triggering SPF calculation at the tens of milliseconds level, and notifying and installing a new route at the hundreds-of-milliseconds level. As a result, it takes much more than 50 ms to recovery the link from the fault, which cannot meet the requirement for real-time services on the network.

With OSPF IP FRR that calculates a backup link in advance, devices can fast switch traffic to the backup link without interrupting traffic when the primary link becomes faulty. This protects traffic and thus greatly improves the reliability of OSPF networks.

OSPF IP FRR is applicable to the services that are sensitive to packet delay and packet loss.

Pre-configuration Tasks

Before configuring OSPF IP FRR, complete the following tasks:

- Configuring IP addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- [Configuring Basic OSPF Functions](#)

Data Preparation

To configure OSPF IP FRR, you need the following data.

No.	Data
1	OSPF process ID
2	(Optional) Cost of the interface
3	(Optional) BFD parameters
4	(Optional) Name of the route policy

5.12.2 Enabling OSPF IP FRR

Context

Do as follows on the router that needs the protection for the forwarded traffic:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id | router-id router-id | vpn-instance vpn-instance-name ] *
```

The OSPF process is started, and the OSPF view is displayed.

Step 3 Run:

```
frr
```

The OSPF IP FRR view is displayed.

Step 4 Run:

```
loop-free-alternate
```

OSPF IP FRR is enabled to generate a loop-free backup link.

 **NOTE**

OSPF can generate the loop-free backup link only when the OSPF IP FRR traffic protection inequality is met.

----End

5.12.3 (Optional) Configuring OSPF IP FRR Filtering Policies

Context

After OSPF IP FRR filtering policies are configured, only the OSPF backup routes that match the filtering conditions can be delivered to the forwarding table. To protect the traffic over a specific OSPF route, you can configure a filtering policy that matches the OSPF route to ensure that the route can be added to the forwarding table. When this route becomes faulty, OSPF can fast switch the traffic to a backup link.

Do as follows on the router to be configured with OSPF IP FRR filtering policies:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id | router-id router-id | vpn-instance vpn-instance-name ] *
```

The OSPF process is enabled, and the OSPF view is displayed.

Step 3 Run:

```
frr
```

The OSPF IP FRR view is displayed.

Step 4 Run:

```
frr-policy route route-policy route-policy-name
```

OSPF IP FRR filtering policies are configured.

---End

5.12.4 (Optional) Binding IP FRR and BFD in an OSPF Process

Context

During the configuration of OSPF IP FRR, the lower layer needs to fast respond to the link change so that traffic can be rapidly switched to the backup link in the case of a link failure. By setting the parameter **frr-binding**, you can bind BFD to the link status on an interface so that link faults can be detected rapidly. This ensures that traffic is rapidly switched to the backup link in the case of link failures.

Do as follows on the router where IP FRR needs to be bound to BFD in an OSPF process:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf
```

The OSPF process is enabled, and the OSPF view is displayed.

Step 3 Run:

```
bfd all-interfaces frr-binding
```

IP FRR is bound to BFD in an OSPF process.

---End

5.12.5 (Optional) Binding IP FRR and BFD on a Specified OSPF Interface

Context

During the configuration of OSPF IP FRR, the lower layer needs to fast respond to the link change so that traffic can be rapidly switched to the backup link. By setting the parameter **frr-binding**, you can bind BFD to the link status on an interface so that link faults can be detected rapidly. This ensures that traffic is rapidly switched to the backup link in the case of link failures.

The priority of BFD configured on an interface is higher than that of BFD configured in an OSPF process. If BFD is enabled on an interface, a BFD session is established according to the BFD parameters set on the interface.

Do as follows on the router where IP FRR needs to be bound to BFD on a specified OSPF interface:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
bfd all-interfaces frr-binding
```

IP FRR is bound to BFD on the OSPF interface.

---End

5.12.6 Checking the Configuration

Prerequisite

All OSPF IP FRR configurations are complete.

Procedure

- Run the **display ospf [process-id] routing** command to check information about the primary and backup links after OSPF IP FRR is enabled.

----End

Example

View the routes to the specified OSPF-enabled router, including information about the backup next hop: **Backup NextHop** is address of the backup next hop, **Backup Interface** is outbound interface of the backup next hop, **Backup Type** is type of the backup next hop.

```
<HUAWEI> display ospf routing router-id 2.2.2.2
          OSPF Process 1 with Router ID 1.1.1.1

Destination : 2.2.2.2           Route Type : Intra-area
Area : 0.0.0.0                 AdvRouter : 2.2.2.2
Type : Normal                  Age : 17h03m33s
URT Cost : 1
NextHop : 10.0.0.2             Interface : Ethernet1/0/0
Backup NextHop : 10.0.0.3      Backup Interface : Ethernet0/0/0
Backup Type : LFA LINK-NODE
```

The preceding display shows that a backup route is generated on Router.

5.13 Configuring OSPF GR

To avoid traffic interruption and route flapping caused by the active/standby switchover, you can enable OSPF GR.

5.13.1 Establishing the Configuration Task

In practical applications, you can configure OSPF GR on dual main control boards to prevent service forwarding from being affected by the fault on the main control board.

Applicable Environment

To avoid traffic interruption and route flapping caused by the active/standby switchover, you can enable OSPF GR.

After the OSPF process is restarted through GR, the Restarter and the Helper reestablish the neighbor relationship, exchange routing information, synchronize the LSDB, and update the routing table and forwarding table. These operations ensure the fast convergence of OSPF and the stability the network topology.

NOTE

In practical applications, you can configure OSPF GR on the dual main control boards to avoid service forwarding from being affected by the fault occurred on the main control board.

Pre-configuration Tasks

Before configuring OSPF GR, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- Configuring basic OSPF functions to establish the neighbor relationship successfully

Data Preparation

To configure OSPF GR, you need the following data.

No.	Data
1	OSPF process number
2	Parameters for establishing GR sessions

5.13.2 Enabling the Opaque-LSA of OSPF

The opaque-LSA capability of OSPF needs to be enabled first because OSPF supports GR through Type 9 LSAs.

Context

Do as follows on the router where GR is enabled:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF view is displayed.

Step 3 Run:

```
opaque-capability enable
```

The opaque-LSA function is enabled.

The opaque-LSA feature of OSPF needs to be enabled first because OSPF supports GR through Type 9 LSAs.

----End

5.13.3 Enabling the Default Feature of OSPF GR

This part describes how to enable the default feature of OSPF GR, namely, totally GR.

Context

Do as follows on the router where GR is enabled:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF view is displayed.

Step 3 Run:

```
graceful-restart
```

The OSPF GR feature is enabled.

---End

5.13.4 (Optional) Configuring the GR Session Parameters on the Restarter

This part describes how to set GR session parameters (including GR period, planned GR, and totally GR) on the Restarter.

Context

If you have special requirements for the Restarter, do as follows on the Restarter:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF view is displayed.

Step 3 Run:

```
graceful-restart period period
```

The GR period on the Restarter is set.

By default, the restart time is 120 seconds.

Step 4 Run:

```
graceful-restart planned-only
```

The Restarter supports only the planned GR.

By default, the Restarter supports both the planned GR and unplanned GR.

Step 5 Run:

```
graceful-restart partial
```

The Restarter supports the partial GR.

By default, the Restarter supports the totally GR.

 **NOTE**

If multiple parameters need to be configured at the same time, you can run the `graceful-restart [period period | planned-only | partial] *` command.

----End

5.13.5 (Optional) Configuring GR Session Parameters on the Helper

After an OSPF process is restarted through GR, the Restarter and the Helper reestablish the neighbor relationship, exchange routing information, synchronize the LSDB, and update the routing table and forwarding table. This implements OSPF fast convergence and stabilizes the network topology.

Context

If you have special requirements for the Helper, do as follows on the Helper.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF view is displayed.

Step 3 Run:

```
graceful-restart helper-role { ip-prefix ip-prefix-name | acl-number acl-number |  
acl-name acl-name }
```

The local router can enter the Helper mode only after neighbors pass the filtering policies of **ip-prefix** or **acl**.

Step 4 Run:

```
graceful-restart helper-role ignore-external-lsa
```

The Helper does not check the LSAs outside the AS (AS-external LSA).

By default, the Helper checks the LSAs outside the AS.

Step 5 Run:

```
graceful-restart helper-role planned-only
```

The Helper supports only the planned GR.

By default, the Helper supports both the planned GR and unplanned GR.

 **NOTE**

To configure multiple parameters at the same time, run the `graceful-restart helper-role { [{ ip-prefix ip-prefix-name | acl-number acl-number | acl-name acl-name } | ignore-external-lsa | planned-only] * | never }` command.

----End

5.13.6 (Optional) Configuring the Router not to Enter the Helper Mode

If a router is not expected to enter the Helper mode, you can disable the router from entering the Helper mode.

Context

If a router is not expected to enter the Helper mode, you can do as follows on the router:

Procedure

- Step 1** Run:
`system-view`
- The system view is displayed.
- Step 2** Run:
`ospf [process-id]`
- The OSPF view is displayed.
- Step 3** Run:
`graceful-restart helper-role never`
- The router does not support the Helper mode.
- End

5.13.7 Checking the Configuration

After OSPF GR is configured, you can check the OSPF GR status.

Prerequisite

The configurations of the OSPF GR are complete.

Procedure

- Run the `display ospf graceful-restart [process-id] graceful-restart [verbose]` command to check the restart status of OSPF GR.

----End

Example

Run the `display ospf graceful-restart` command. If the OSPF GR configuration is displayed, it means that the configuration succeeds. For example:

```
<HUAWEI> display ospf graceful-restart
      OSPF Process 1 with Router ID 1.1.1.1
Graceful-restart capability      : enabled
Graceful-restart support        : planned and un-planned, totally
Helper-policy support           : planned and un-planned, strict lsa check
Current GR state                 : normal
Graceful-restart period         : 120 seconds
Number of neighbors under helper:
Normal neighbors                : 0
```

```

Virtual neighbors      : 0
Sham-link neighbors  : 0
Total neighbors       : 0
Number of restarting neighbors : 0
Last exit reason:
  On graceful restart : successful exit
  On Helper           : none
    
```

5.14 Configuring BFD for OSPF

If there are high requirements for data transmission, and OSPF convergence needs to be speeded up when the link status changes, you can configure BFD on OSPF links. After detecting a link failure, BFD notifies the routing protocol of the failure, which triggers fast convergence. When the neighbor relationship is Down, the BFD session is deleted dynamically.

5.14.1 Establishing the Configuration Task

After BFD is enabled, OSPF establishes a BFD session with only the neighbor whose neighbor relationship is in the Full state.

Applicable Environment

To increase the convergence speed of OSPF when the link status changes, you can configure BFD on OSPF links.

Pre-configuration Tasks

Before configuring BFD for OSPF, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- Configuring basic OSPF functions to establish the neighbor relationship successfully
- Enabling BFD globally

Data Preparation

To configure BFD for OSPF, you need the following data.

No.	Data
1	Number of the OSPF process enabled with BFD
2	Type and number of the interface enabled with BFD
3	Values of BFD session parameters

5.14.2 Configuring Global BFD

Before creating a BFD session, you need to enable BFD globally.

Context

To set up a BFD session, you need to enable global BFD first. Do as follows on the router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

Global BFD is enabled.

----End

5.14.3 Configuring BFD for OSPF

On the two routers that need to establish a BFD session, you can configure BFD for all the interfaces in a certain OSPF process.

Context

To configure BFD for all interfaces in an OSPF process, do as follows on the routers at the two ends of the link.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf process-id
```

The OSPF view is displayed.

Step 3 Run:

```
bfd all-interfaces enable
```

BFD for OSPF is enabled to establish a BFD session.

If all the interfaces in a certain process are configured with BFD and neighbors in this process are in the Full state, OSPF sets the default values of BFD parameters for the interfaces.

You can run the **bfd all-interfaces { min-rx-interval receive-interval | min-tx-interval transmit-interval | detect-multiplier multiplier-value } *** command to specify the value for each parameter used to establish a BFD session.

 **NOTE**

If only the **bfd all-interfaces { min-rx-interval receive-interval | min-tx-interval transmit-interval | detect-multiplier multiplier-value } *** command is used and the **bfd all-interfaces enable** command is not used, BFD cannot be enabled.

----End

5.14.4 (Optional) Preventing an Interface from Dynamically Setting Up a BFD Session

To disable BFD on some interfaces, you need to prevent these interfaces from dynamically setting up BFD sessions.

Context

After the **bfd all-interfaces enable** command is used in an OSPF process, BFD sessions are created on all the OSPF interfaces whose neighbor status is Full. If you do not want to enable BFD on an interface, do as follows on the interface:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospf bfd block
```

An interface is prevented from dynamically creating a BFD session.

----End

5.14.5 (Optional) Configuring BFD on the Specified Interface

To configure BFD only on some interfaces and not to enable OSPF BFD globally, or to require some interfaces to fast detect link failures after configuring OSPF BFD on them, you can configure BFD on the specified interface.

Context

To configure BFD on the specified interface and not to enable OSPF BFD, or to require the interface to fast detect link faults after configuring OSPF BFD on the interface, do as follows on the interface.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospf bfd enable
```

BFD is enabled on the interface to establish a BFD session.

When BFD is configured globally and the neighbor status is Full, the default values of BFD parameters used to establish a BFD session are set.

You can run the `ospf bfd { min-rx-interval receive-interval | min-tx-interval transmit-interval | detect-multiplier multiplier-value } *` command to specify the value for each parameter used to establish a BFD session.

 **NOTE**

- The priority of BFD configured on an interface is higher than that of BFD configured in a process. That is, if BFD is enabled on an interface, the parameters of the interface are used to establish BFD sessions.
- If the parameters of a BFD session are set but the `ospf bfd enable` command is not run, BFD cannot be enabled.

----End

5.14.6 Checking the Configuration

After BFD for OSPF is configured, you can check information about the BFD session.

Prerequisite

The configurations of the BFD for OSPF are complete.

Procedure

- Run the `display ospf [process-id] bfd session interface-type interface-number [router-id]` or `display ospf [process-id] bfd session { router-id | all }` command to check the information about the BFD session.

----End

Example

Run the `display ospf bfd session all` command. If a BFD session is correctly established, you can see that the BFD status of the local router is Up. For example:

```
<HUAWEI> display ospf bfd session all
      OSPF Process 1 with Router ID 3.3.3.3
      Area 0.0.0.0 interface 100.2.1.2(GigabitEthernet1/0/0)'s BFD Sessions
NeighborId:2.2.2.2      AreaId:0.0.0.0      Interface:GigabitEthernet1/0/0
BFDState:up           rx      :1000      tx      :100
Multiplier:3         BFD Local Dis:8194      LocalIpAdd:100.2.1.2
RemoteIpAdd:100.2.1.1      Diagnostic Info: Init
```

5.15 Configuring the Network Management Function of OSPF

OSPF supports the network management function. You can bind the OSPF MIB to a certain OSPF process, and configure the trap function and log function.

5.15.1 Establishing the Configuration Task

Before configuring the network management function for OSPF, familiarize yourself with the applicable environment, complete pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

OSPF supports the network management function. You can bind OSPF MIB and a certain OSPF process. In addition, OSPF also supports the trap function and the log function.

Pre-configuration Tasks

Before configuring the network management function of OSPF, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- [Configuring Basic OSPF Functions](#)

Data Preparation

None.

5.15.2 Configuring OSPF MIB Binding

The MIB is a virtual database of the device status maintained by the managed devices.

Context

When multiple OSPF processes are enabled, you can configure OSPF MIB to select the process to be processed, that is, configure OSPF MIB to select the process to which it is bound.

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf mib-binding process-id
```

OSPF MIB binding is configured.

---End

5.15.3 Configuring OSPF Trap

Traps are the notifications sent from a router to inform the NMS of the fault detected by the system.

Context

Do as follows on the OSPF router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
snmp-agent trap enable feature-name ospf { non-excessive all | trap-name  
{ ospfifauthfailure | ospfifconfigerror | ospfifrxbadpacket | ospfifstatechange |  
ospflsdbapproachingoverflow | ospflsdboverflow | ospfmaxagelsa |  
ospfnbrrestarthelperstatuschange | ospfnbrstatechange |  
ospfnssatranslatorstatuschange | ospforiginatelsa | ospfrestartstatuschange |  
ospftxretransmit | ospfvirtifauthfailure | ospfvirtifconfigerror |  
ospfvirtifrxbadpacket | ospfvirtifstatechange | ospfvirtiftxretransmit |  
ospfvirtnbrrestarthelperstatuschange | ospfvirtnbrstatechange } }
```

The trap function for the OSPF module is enabled.

To enable all non-excessive traps of OSPF module, you can run the **non-excessive all** command; to enable the traps of one or more events, you can specify **type-name**.

----End

5.15.4 Configuring OSPF Log

Logs record the operations (such as configuring commands) and specific events (such as the network connection failure) on routers.

Context

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
enable log [ config | error | state | snmp-trap ]
```

The log function is enabled.

----End

5.15.5 Checking the Configuration

After the network management function is configured for OSPF, you can check the contents of the information channel, information recorded in the information center, log buffer, and trap buffer.

Prerequisite

The configurations of the network management function of OSPF are complete.

Procedure

- Run the **display ospf [process-id] brief** command to view information about the binding of OSPF MIBs and OSPF processes.
- Run the **display snmp-agent trap feature-name ospf all** command to view all trap messages of the OSPF module.

----End

5.16 Improving Security of an OSPF Network

On a network demanding high security, you can configure OSPF authentication and adopt the GTSM mechanism to improve the security of the OSPF network.

5.16.1 Establishing the Configuration Task

Before improving the security of an OSPF network, familiarize yourself with the applicable environment, complete pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

In a network demanding high security, you can configure OSPF authentication and adopt the GTSM mechanism to improve the security of the OSPF network.

The GTSM mechanism defends against attacks by checking the TTL value. If an attacker keeps sending packets to a router by simulating real OSPF unicast packets, the router finds itself is the destination of the packets after the interface board receives these packets. The router directly sends the packets to the control plane for OSPF processing without checking the validity of the packets. The router busies itself with processing these "valid" packets. As a result, the system is busy, and the CPU is highly occupied.

The GTSM mechanism protects a router by checking whether the TTL value in the IP packet header is in a pre-defined range to enhance the system security.

NOTE

- NE80E/40E supports IPv4 OSPF GTSM.
- GTSM supports only unicast addresses; therefore, in OSPF, GTSM takes effect on the virtual link and the sham link.

Pre-configuration Tasks

Before improving the security of an OSPF network, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- **Configuring Basic OSPF Functions**

Data Preparation

To improve the security of an OSPF network, you need the following data.

No.	Data
1	OSPF process ID
2	(Optional) Names of VPN instances of OSPF
3	(Optional) TTL value to be checked
4	ID of an OSPF area that needs to be configured with authentication
5	Number of an OSPF interface that needs to be configured with authentication
6	Authentication mode and password

5.16.2 Configuring the OSPF GTSM Functions

The GTSM defends against attacks by checking the TTL value.

Context

To apply GTSM functions, enable GTSM on the two ends of the OSPF connection.

The valid TTL range of the detected packets is $[255 - hops + 1, 255]$.

Do as follows on the GTSM routers on the two ends of the virtual link or sham link.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf valid-ttl-hops hops [ vpn-instance vpn-instance-name ]
```

OSPF GTSM functions are configured.

NOTE

The `ospf valid-ttl-hops` command has two functions:

- Enabling OSPF GTSM
- Configuring the TTL value to be detected

The parameter `vpn-instance` is valid only for the latter function.

Thus, if the private network policy or the public network policy is configured only, it is recommended to set the default action performed on the packets that do not match the GTSM policy as `pass`. This prevents the OSPF packets of other processes from being discarded incorrectly.

----End

5.16.3 Adjusting GTSM

GTSM checks the TTL value of only the packet that matches the GTSM policy. You can enable the log function to record information about the discarded packets for fault location.

Context

GTSM checks the TTL value of only the packet that matches the GTSM policy. For the packets that do not match the GTSM policy, you can set them as "pass" or "drop". If the GTSM default action performed on the packet is set as "drop", you need to configure all the router connections for GTSM. If the packets sent from a router do not match the GTSM policy, they are dropped. The connection thus cannot be established. This ensures security but reduces the ease of use.

You can enable the log function to record the information that the packets are dropped. This is convenient for fault location.

Do as follows on the router configured with GTSM functions.

Procedure

- Setting the GTSM Default Action

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
gtsm default-action { drop | pass }
```

The default action performed on the packets that do not match the GTSM policy is set.

By default, the packets that do not match the GTSM policy can pass the filtering.

 **NOTE**

If the default action is configured but the GTSM policy is not configured, GTSM does not take effect.

---End

5.16.4 Configuring the Area Authentication Mode

OSPF supports packet authentication. Only the packets that pass the authentication can be received. If packets fail to pass the authentication, the neighbor relationship cannot be established.

Context

OSPF supports packet authentication. Only the OSPF packets passing the authentication can be received; otherwise, packets cannot be received and the neighbor relationship cannot be established normally. In area authentication, all the routers in an area must use the same area authentication mode and password. For example, the authentication mode of all devices in Area 0 is simple authentication and the password is abc.

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospf [ process-id ]
```

The OSPF process view is displayed.

Step 3 Run:

```
area area-id
```

The OSPF area view is displayed.

Step 4 Run the following commands to configure the authentication mode of the OSPF area as required:

● Run:

```
authentication-mode simple [ plain plain-text | cipher cipher-text ]
```

The simple authentication is configured for the OSPF area.

● Run:

```
authentication-mode { md5 | hmac-md5 } [ key-id { plain plain-text | cipher cipher-text } ]
```

The MD5 authentication is configured for the OSPF area.

OSPF supports packet authentication. Only the OSPF packets passing the authentication can be received; otherwise, the neighbor relationship cannot be established normally.

All the routers in an area must agree on the same area authentication mode and password. For example, the authentication mode of all routers in area 0 is simple authentication, and the password is abc.

● Run:

```
authentication-mode keychain keychain-name
```

The Keychain authentication is configured for the OSPF area.

 **NOTE**

Before using the Keychain authentication, you need to configure Keychain information in the system view. To establish the OSPF neighbor relationship, you need to ensure that the **key-id**, **algorithm**, and **key-string** of the local ActiveSendKey are the same as those of the remote ActiveRecvKey.

----End

5.16.5 Configuring the Interface Authentication Mode

The interface authentication mode is used among neighbor routers to set the authentication mode and password. Its priority is higher than that of the area authentication mode.

Context

Do as follows on the OSPF router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run the following commands to configure the interface authentication mode as required:

- Run:

```
ospf authentication-mode simple [ plain plain-text | cipher cipher-text ]
```

The simple authentication is configured for the OSPF interface.

- Run:

```
ospf authentication-mode { md5 | hmac-md5 } [ key-id { plain plain-text | cipher cipher-text } ]
```

The MD5 authentication is configured for the OSPF interface.

- Run:

```
ospf authentication-mode null
```

The non-authentication mode is configured for the OSPF interface.

- Run:

```
ospf authentication-mode keychain keychain-name
```

The Keychain authentication is configured for the OSPF area.

 **NOTE**

Before using the Keychain authentication, you need to configure Keychain information in the system view. To establish the OSPF neighbor relationship, you need to ensure that the **key-id**, **algorithm**, and **key-string** of the local ActiveSendKey are the same as those of the remote ActiveRecvKey.

The interface authentication mode is used among neighbor routers to set the authentication mode and password. Its priority is higher than that of the area authentication mode.

The authentication mode and password of interfaces in the same network segment must be consistent except the Keychain authentication mode. If the interfaces are in different network segments, the authentication mode and password of the interfaces can be different.

----End

5.16.6 Checking the Configuration

After OSPF features are configured to improve the stability of an OSPF network, you can check GTSM statistics and brief statistics.

Prerequisite

The configurations of Improving Security of an OSPF Network are complete.

Procedure

- Run the **display gtsm statistics** { slot-id | all } command to check the GTSM statistics.
- Run the **display ospf** [process-id] **request-queue** [interface-type interface-number] [neighbor-id] command to check the OSPF request queue.
- Run the **display ospf** [process-id] **retrans-queue** [interface-type interface-number] [neighbor-id] command to check the OSPF retransmission queue.
- Run the **display ospf** [process-id] **error** [lsa] or **display ospf error** [packet [number]] command to check the OSPF error information.

----End

Example

Run the **display gtsm statistics** command. If the GTSM statistics on each slot, including the total number of OSPF packets, the number of passed packets, and the number of dropped packets, are displayed, it means that the configuration succeeds. For example:

```
<HUAWEI> display gtsm statistics all
GTSM Statistics Table
-----
SlotId  Protocol  Total Counters  Drop Counters  Pass Counters
-----
0       BGP       0               0               0
0       BGPv6    0               0               0
0       OSPF     0               0               0
0       LDP      0               0               0
-----
```

5.17 Maintaining OSPF

Maintaining OSPF involves resetting OSPF and clearing OSPF statistics.

5.17.1 Resetting OSPF

Restarting OSPF can reset OSPF. In addition, you can reset OSPF through GR.

Context



CAUTION

The OSPF neighbor relationship is deleted after you reset OSPF connections with the **reset ospf** command. So, confirm the action before you use the command.

To reset OSPF connections, run the following **reset ospf** commands in the user view.

Procedure

- Run the **reset ospf** [*process-id*] **process** [**flush-waiting-timer** *time*] command in the user view to Restart the OSPF process.
- Run the **reset ospf** [*process-id*] **process** [**graceful-restart**] command in the user view to Restart the OSPF process in GR mode.

----End

5.17.2 Clearing OSPF

This section describes how to clear OSPF statistics, including OSPF counters, imported routes, and GTSM statistics on the board.

Context



CAUTION

OSPF information cannot be restored after you clear it. So, confirm the action before you use the command.

To clear the OSPF information, run the following **reset ospf** commands in the user view.

Procedure

- Run the **reset ospf** [*process-id*] **counters** [**neighbor** [*interface-type interface-number*] [*router-id*]] command in the user view to clear OSPF counters.
- Run the **reset ospf** [*process-id*] **redistribution** command in the user view to clear the routes imported by OSPF.
- Run the **reset gtsm statistics** { *slot-id* | **all** } command in the user view to clear the GTSM statistics on the board.

---End

5.18 Configuring Examples

This section provides several configuration examples of OSPF together with the configuration flowchart. The configuration examples explain networking requirements, configuration notes, and configuration roadmap.

Follow-up Procedure



NOTE

This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.

5.18.1 Example for Configuring Basic OSPF Functions

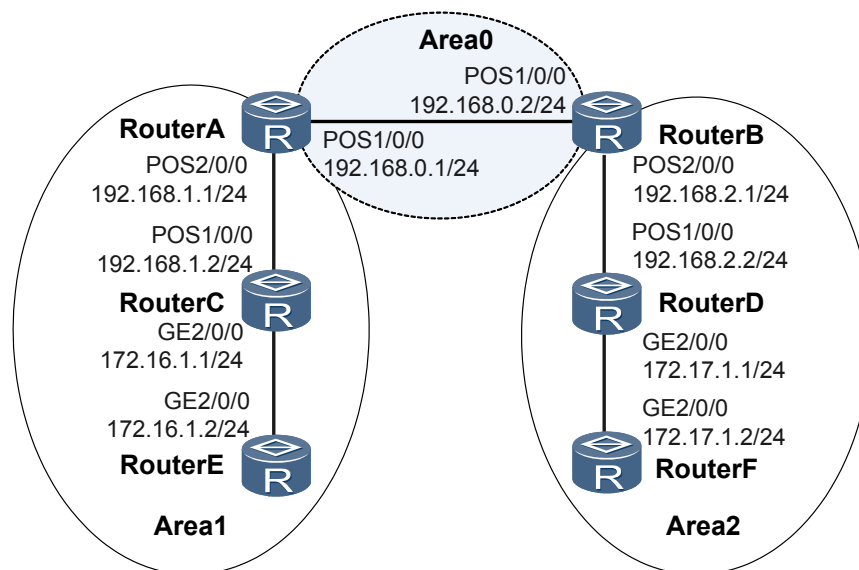
This part provides an example for configuring basic OSPF functions. Detailed operations include enabling OSPF on each router and specifying network segments in different areas.

Networking Requirements

As shown in **Figure 5-4**, all routers run OSPF, and the entire AS is divided into three areas. Router A and Router B serve as ABRs to forward routes between areas.

After the configuration, each router should learn the routes from the AS to all network segments.

Figure 5-4 Networking diagram of configuring basic OSPF functions



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable OSPF on each router, and specify the network segment in different areas.
2. Check the routing list and LSDB.

Data Preparation

To complete the configuration, you need the following data:

- The router ID of Router A is 1.1.1.1, the OSPF process number is 1, the network segment of Area 0 is 192.168.0.0/24, and the network segment of Area 1 is 192.168.1.0/24.
- The router ID of Router B is 2.2.2.2, the OSPF process number is 1, the network segment of Area 0 is 192.168.0.0/24, and the network segment of Area 2 is 192.168.2.0/24.
- The router ID of Router C is 3.3.3.3, the OSPF process number is 1, the network segments of Area 1 are 192.168.1.0/24 and 172.16.1.0/24.
- The router ID of Router D is 4.4.4.4, the OSPF process number is 1, the network segments of Area 2 are 192.168.2.0/24 and 172.17.1.0/24.
- The router ID of Router E is 5.5.5.5, the OSPF process number is 1, the network segment of Area 1 is 172.16.1.0/24.
- The router ID of Router F is 6.6.6.6, the OSPF process number is 1, the network segment of Area 2 is 172.17.1.0/24.

Procedure

Step 1 Configure an IP address for each interface.

The configuration details are not mentioned here.

Step 2 Configure basic OSPF functions.

Configure Router A.

```
[RouterA] router id 1.1.1.1
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.1] quit
```

Configure Router B.

```
[RouterB] router id 2.2.2.2
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] area 2
[RouterB-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.2] quit
```

Configure Router C.

```
[RouterC] router id 3.3.3.3
[RouterC] ospf
[RouterC-ospf-1] area 1
[RouterC-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.1] quit
```

Configure Router D.

```
[RouterD] router id 4.4.4.4
[RouterD] ospf
[RouterD-ospf-1] area 2
[RouterD-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.2] quit
```

Configure Router E.

```
[RouterE] router id 5.5.5.5
[RouterE] ospf
[RouterE-ospf-1] area 1
[RouterE-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.1] quit
```

Configure Router F.

```
[RouterF] router id 6.6.6.6
[RouterF] ospf
[RouterF-ospf-1] area 2
[RouterF-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[RouterF-ospf-1-area-0.0.0.2] quit
```

Step 3 Verify the configuration.

View OSPF neighbors of Router A.

```
[RouterA] display ospf peer
      OSPF Process 1 with Router ID 1.1.1.1
      Neighbors
      Area 0.0.0.0 interface 192.168.0.1(Pos1/0/0)'s neighbors
Router ID: 2.2.2.2      Address: 192.168.0.2
State: Full Mode:Nbr is Master Priority: 1
      DR: 0.0.0.0 BDR: 0.0.0.0 MTU: 0
      Dead timer due in 36 sec
```



```

Retrans timer interval: 5
Neighbor is up for 00:15:04
Authentication Sequence: [ 0 ]
Neighbors
Area 0.0.0.1 interface 192.168.1.1(Pos2/0/0)'s neighbors
Router ID: 3.3.3.3 Address: 192.168.1.2
State: Full Mode:Nbr is Master Priority: 1
DR: 0.0.0.0 BDR: 0.0.0.0 MTU: 0
Dead timer due in 39 sec
Retrans timer interval: 5
Neighbor is up for 00:07:32
Authentication Sequence: [ 0 ]
    
```

View the OSPF routing information of Router A.

```

[RouterA] display ospf routing
OSPF Process 1 with Router ID 1.1.1.1
Routing Tables
Routing for Network
Destination      Cost  Type           NextHop          AdvRouter        Area
172.16.1.0/24   2     Transit        192.168.1.2     3.3.3.3          0.0.0.1
172.17.1.0/24   3     Inter-area     192.168.0.2     2.2.2.2          0.0.0.0
192.168.0.0/24  1     Stub           192.168.0.1     1.1.1.1          0.0.0.0
192.168.1.0/24  1     Stub           192.168.1.1     1.1.1.1          0.0.0.1
192.168.2.0/24  2     Inter-area     192.168.0.2     2.2.2.2          0.0.0.0
Total Nets: 5
Intra Area: 3 Inter Area: 2 ASE: 0 NSSA: 0
    
```

View the LSDB of Router A.

```

[RouterA] display ospf lsdb
OSPF Process 1 with Router ID 1.1.1.1
Link State Database
Area: 0.0.0.0
Type      LinkState ID  AdvRouter      Age Len  Sequence      Metric
Router    2.2.2.2       2.2.2.2        317 48   80000003      1
Router    1.1.1.1       1.1.1.1        316 48   80000002      1
Sum-Net   172.16.1.0    1.1.1.1        250 28   80000001      2
Sum-Net   172.17.1.0    2.2.2.2        203 28   80000001      2
Sum-Net   192.168.2.0   2.2.2.2        237 28   80000002      1
Sum-Net   192.168.1.0   1.1.1.1        295 28   80000002      1
Area: 0.0.0.1
Type      LinkState ID  AdvRouter      Age Len  Sequence      Metric
Router    5.5.5.5       5.5.5.5        214 36   80000004      1
Router    3.3.3.3       3.3.3.3        217 60   80000008      1
Router    1.1.1.1       1.1.1.1        289 48   80000002      1
Network   172.16.1.1    3.3.3.3        670 32   80000001      0
Sum-Net   172.17.1.0    1.1.1.1        202 28   80000001      3
Sum-Net   192.168.2.0   1.1.1.1        242 28   80000001      2
Sum-Net   192.168.0.0   1.1.1.1        300 28   80000001      1
    
```

View the routing table of Router D and test connectivity by using the **ping** command.

```

[RouterD] display ospf routing
OSPF Process 1 with Router ID 4.4.4.4
Routing Tables
Routing for Network
Destination      Cost  Type           NextHop          AdvRouter        Area
172.16.1.0/24   4     Inter-area     192.168.2.1     2.2.2.2          0.0.0.2
172.17.1.0/24   1     Transit        172.17.1.1     4.4.4.4          0.0.0.2
192.168.0.0/24  2     Inter-area     192.168.2.1     2.2.2.2          0.0.0.2
192.168.1.0/24  3     Inter-area     192.168.2.1     2.2.2.2          0.0.0.2
192.168.2.0/24  1     Stub           192.168.2.2     4.4.4.4          0.0.0.2
Total Nets: 5
Intra Area: 2 Inter Area: 3 ASE: 0 NSSA: 0
[RouterD] ping 172.16.1.1
PING 172.16.1.1: 56 data bytes, press CTRL_C to break
Reply from 172.16.1.1: bytes=56 Sequence=1 ttl=253 time=62 ms
Reply from 172.16.1.1: bytes=56 Sequence=2 ttl=253 time=16 ms
Reply from 172.16.1.1: bytes=56 Sequence=3 ttl=253 time=62 ms
    
```

```
Reply from 172.16.1.1: bytes=56 Sequence=4 ttl=253 time=94 ms
Reply from 172.16.1.1: bytes=56 Sequence=5 ttl=253 time=63 ms
--- 172.16.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 16/59/94 ms
```

----End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.0.1 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
router id 2.2.2.2
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.0.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
#
return
```

- Configuration file of Router C

```
#
 sysname RouterC
#
router id 3.3.3.3
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 172.16.1.1 255.255.255.0
#
```

```
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
#
return
```

- Configuration file of Router D

```
#
 sysname RouterD
#
router id 4.4.4.4
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 172.17.1.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.2 255.255.255.0
#
ospf 1
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
return
```

- Configuration file of Router E

```
#
 sysname RouterE
#
router id 5.5.5.5
#
interface GigabitEthernet2/0/0
 ip address 172.16.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.1
  network 172.16.1.0 0.0.0.255
#
return
```

- Configuration file of Router F

```
#
 sysname RouterF
#
router id 6.6.6.6
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 172.17.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.2
  network 172.17.1.0 0.0.0.255
#
return
```

5.18.2 Example for Configuring OSPF Stub Areas

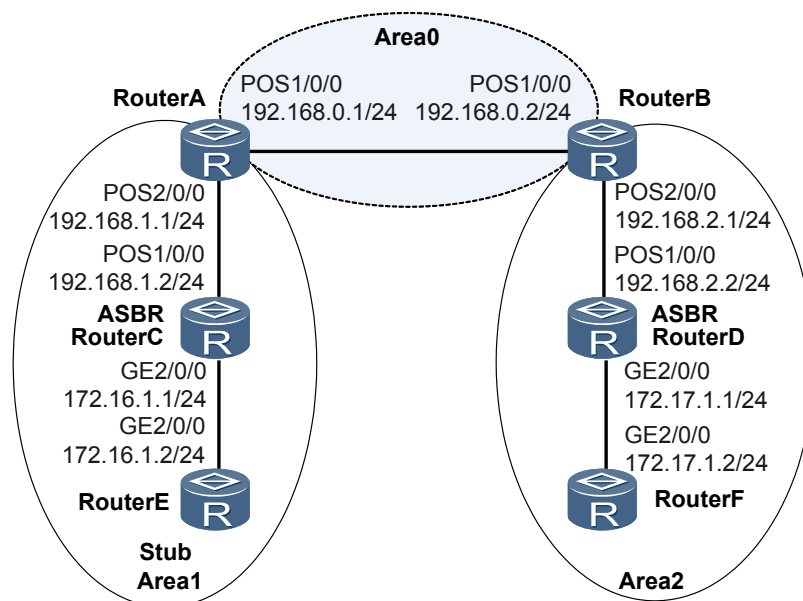
This part provides an example for configuring a stub area that imports static routes to reduce the number of LSAs advertised in this area without affecting the route reachability.

Networking Requirements

As shown in [Figure 5-5](#), all routers run OSPF, and the entire AS is divided into three areas. Router A and Router B serve as ABRs to forward routes between areas. Router D serves as an ASBR to import external routes (static routes).

It is required to configure Area 1 as a stub area to reduce the LSAs advertised to this area without affecting the route reachability.

Figure 5-5 Configuring OSPF stub areas



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable OSPF on each router, and configure basic OSPF functions.
2. Configure static routes on Router D, and import them into OSPF.
3. Configure Area 1 as a stub area, and check the OSPF routing information on Router C.
4. Stop Router A from advertising Type 3 LSAs to the stub area, and check the OSPF routing information on Router C.

Data Preparation

To complete the configuration, you need the following data:

- The router ID of Router A is 1.1.1.1, the process number of OSPF is 1, the network segment of Area 0 is 192.168.0.0/24, and the network segment of Area 1 is 192.168.1.0/24.
- The router ID of Router B is 2.2.2.2, the process number of OSPF is 1, the network segment of Area 0 is 192.168.0.0/24, and the network segment of Area 2 is 192.168.2.0/24.

- The router ID of Router C is 3.3.3.3, the process number of OSPF is 1, and the network segments of Area 1 are 192.168.1.0/24 and 172.16.1.0/24.
- The router ID of Router D is 4.4.4.4, the process number of OSPF is 1, and the network segments of Area 2 are 192.168.2.0/24 and 172.17.1.0/24.
- The router ID of Router E is 5.5.5.5, the process number of OSPF is 1, and the network segment of Area 1 is 172.16.1.0/24.
- The router ID of Router F is 6.6.6.6, the process number of OSPF is 1, and the network segment of Area 2 is 172.17.1.0/24.

Procedure

Step 1 Configure an IP address for each interface.

The configuration details are not mentioned here.

Step 2 Configure basic OSPF functions (see [5.18.1 Example for Configuring Basic OSPF Functions](#)).

Step 3 Configure Router D to import static routes.

```
[RouterD] ip route-static 200.0.0.0 8 null 0
[RouterD] ospf
[RouterD-ospf-1] import-route static type 1
[RouterD-ospf-1] quit
```

View ABR/ASBR information on Router C.

```
[RouterC] display ospf abr-asbr
          OSPF Process 1 with Router ID 3.3.3.3
          Routing Table to ABR and ASBR
```

RtType	Destination	Area	Cost	NextHop	Type
Intra-area	1.1.1.1	0.0.0.1	1	192.168.1.1	ABR
Inter-area	4.4.4.4	0.0.0.1	3	192.168.1.1	ASBR

View the OSPF routing table of Router C.

NOTE

When Router C is in a common area, there are AS external routes in the routing table.

```
[RouterC] display ospf routing
          OSPF Process 1 with Router ID 3.3.3.3
          Routing Tables
```

Destination	Cost	Type	NextHop	AdvRouter	Area
172.16.1.0/24	1	Transit	172.16.1.1	3.3.3.3	0.0.0.1
172.17.1.0/24	4	Inter-area	192.168.1.1	1.1.1.1	0.0.0.1
192.168.0.0/24	2	Inter-area	192.168.1.1	1.1.1.1	0.0.0.1
192.168.1.0/24	1	Stub	192.168.1.2	3.3.3.3	0.0.0.1
192.168.2.0/24	3	Inter-area	192.168.1.1	1.1.1.1	0.0.0.1

```

Routing for ASEs
Destination      Cost      Type      Tag      NextHop      AdvRouter
200.0.0.0/8    4       Type1    1       192.168.1.1 4.4.4.4
Total Nets: 6
Intra Area: 2  Inter Area: 3  ASE: 1  NSSA: 0
```

Step 4 Configure Area 1 as a stub area.

Configure Router A.

```
[RouterA] ospf
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] stub
[RouterA-ospf-1-area-0.0.0.1] quit
```

Configure Router C.

```
[RouterC] ospf
[RouterC-ospf-1] area 1
[RouterC-ospf-1-area-0.0.0.1] stub
[RouterC-ospf-1-area-0.0.0.1] quit
```

Configure Router E.

```
[RouterE] ospf
[RouterE-ospf-1] area 1
[RouterE-ospf-1-area-0.0.0.1] stub
[RouterE-ospf-1-area-0.0.0.1] quit
```

View the routing table of Router C.

NOTE

After the area where Router C resides is configured as a stub area, AS external routes are invisible. Instead, there is a default route.

```
[RouterC] display ospf routing
          OSPF Process 1 with Router ID 3.3.3.3
          Routing Tables

Routing for Network
Destination      Cost  Type      NextHop      AdvRouter      Area
0.0.0.0/0        2    Inter-area 192.168.1.1   1.1.1.1        0.0.0.1
172.16.1.0/24    1    Transit   172.16.1.1   3.3.3.3        0.0.0.1
172.17.1.0/24    4    Inter-area 192.168.1.1   1.1.1.1        0.0.0.1
192.168.0.0/24   2    Inter-area 192.168.1.1   1.1.1.1        0.0.0.1
192.168.1.0/24   1    Stub      192.168.1.2   3.3.3.3        0.0.0.1
192.168.2.0/24   3    Inter-area 192.168.1.1   1.1.1.1        0.0.0.1
Total Nets: 6
Intra Area: 2  Inter Area: 4  ASE: 0  NSSA: 0
```

Step 5 # Stop Router A from advertising Type 3 LSAs to the stub area.

```
[RouterA] ospf
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] stub no-summary
[RouterA-ospf-1-area-0.0.0.1] quit
```

Step 6 Verify the configuration.

View the OSPF routing table of Router C.

```
[RouterC] display ospf routing
          OSPF Process 1 with Router ID 3.3.3.3
          Routing Tables

Routing for Network
Destination      Cost  Type      NextHop      AdvRouter      Area
0.0.0.0/0        2    Inter-area 192.168.1.1   1.1.1.1        0.0.0.1
172.16.1.0/24    1    Transit   172.16.1.1   3.3.3.3        0.0.0.1
192.168.1.0/24   1    Stub      192.168.1.2   3.3.3.3        0.0.0.1
Total Nets: 3
Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

NOTE

After the advertisement of summary LSAs to a stub area is disabled, the routing entries of the stub router are further reduced, and only the default route to a destination outside the AS is reserved.

---End

Configuration Files

NOTE

The configuration files of Router B and Router F are the same as those in the preceding example, and are not mentioned here.

- Configuration file of Router A

```
#
 sysname RouterA
#
router id 1.1.1.1
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.0.1 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  stub no-summary
#
return
```

- Configuration file of Router C

```
#
 sysname RouterC
#
router id 3.3.3.3
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 172.16.1.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
  stub
#
return
```

- Configuration file of Router D

```
#
 sysname RouterD
#
router id 4.4.4.4
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 172.17.1.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.2 255.255.255.0
#
ospf 1
 import-route static type 1
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
ip route-static 200.0.0.0 255.0.0.0 NULL0
#
```

```

return
● Configuration file of Router E
#
sysname RouterE
#
router id 5.5.5.5
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 172.16.1.2 255.255.255.0
#
ospf 1
area 0.0.0.1
network 172.16.1.0 0.0.0.255
stub
#
return

```

5.18.3 Example for Configuring OSPF NSSAs

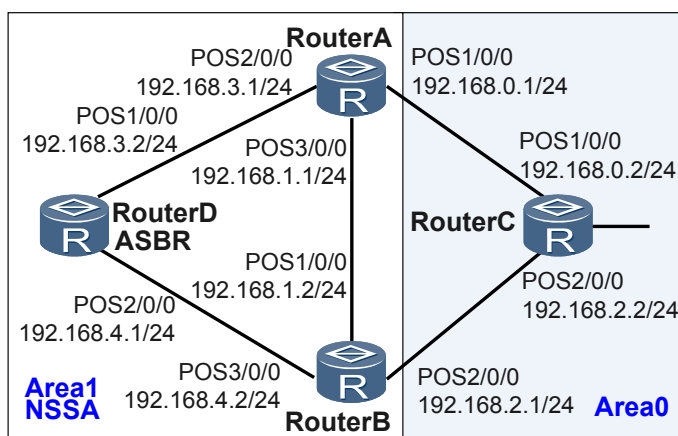
This part provides an example for configuring a translator and an NSSA that imports static routes.

Networking Requirements

As shown in [Figure 5-6](#), all routers run OSPF, and the entire AS is divided into two areas. Router A and Router B serve as ABRs to forward routes between areas. Router D serves as the ASBR to import external routes (static routes).

It is required to configure Area 1 as an NSSA. Configure Router A and Router B as translators in the NSSA, configure Router D as an ASBR to import external routes (static routes) and correctly transmit routing information inside the AS.

Figure 5-6 Configuring an OSPF NSSA



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable OSPF on each router, and configure basic OSPF functions.

2. Configure Area 1 as an NSSA (run the **nssa** command on all routers in Area 1), and check the OSPF routing information and LSDB of Router C.
3. Configure static routes on Router D, and import them into OSPF.
4. Configure translators in the NSSA.

Data Preparation

To complete the configuration, you need the following data:

- The router ID of Router A is 1.1.1.1, the OSPF process number is 1, the network segment of Area 0 is 192.168.0.0/24, and the network segments of Area 1 are 192.168.1.0/24 and 192.168.3.0/24.
- The router ID of Router B is 2.2.2.2, the OSPF process number is 1, the network segment of Area 0 is 192.168.2.0/24, and the network segments of Area 1 are 192.168.1.0/24 and 192.168.4.0/24.
- The router ID of Router C is 3.3.3.3, the OSPF process number is 1, and the network segments of Area 0 are 192.168.0.0/24 and 192.168.2.0/24.
- The router ID of Router D is 4.4.4.4, the OSPF process number is 1, and the network segments of Area 1 are 192.168.3.0/24 and 192.168.4.0/24.

Procedure

Step 1 Configure an IP address for each interface.

The configuration details are not mentioned here.

Step 2 Configure basic OSPF functions (see [5.18.1 Example for Configuring Basic OSPF Functions](#)).

Step 3 Configure Area 1 as an NSSA.

Configure Router A.

```
[RouterA] ospf
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] nssa
[RouterA-ospf-1-area-0.0.0.1] quit
```

Configure Router B.

```
[RouterB] ospf
[RouterB-ospf-1] area 1
[RouterB-ospf-1-area-0.0.0.1] nssa
[RouterB-ospf-1-area-0.0.0.1] quit
```

Configure Router D.

```
[RouterD] ospf
[RouterD-ospf-1] area 1
[RouterD-ospf-1-area-0.0.0.1] nssa
[RouterD-ospf-1-area-0.0.0.1] quit
```

Step 4 Configure Router D to import static routes.

```
[RouterD] ip route-static 100.0.0.0 8 null 0
[RouterD] ospf
[RouterD-ospf-1] import-route static
[RouterD-ospf-1] quit
```

Display the OSPF routing table of Router C.

 **NOTE**

- On Router C, you can view that the router ID of the advertising router that imports AS external routes in the NSSA, that is, the router ID of Router B is 2.2.2.2.
- OSPF selects the ABR with larger router ID as a translator.

```
[RouterC] display ospf routing

      OSPF Process 1 with Router ID 3.3.3.3
      Routing Tables

Routing for Network
Destination      Cost  Type      NextHop      AdvRouter      Area
192.168.3.0/24  2     Inter-area 192.168.0.1  1.1.1.1        0.0.0.0
192.168.4.0/24  2     Inter-area 192.168.2.1  2.2.2.2        0.0.0.0
192.168.0.0/24  1     Stub       192.168.0.2  3.3.3.3        0.0.0.0
192.168.1.0/24  2     Inter-area 192.168.0.1  1.1.1.1        0.0.0.0
192.168.1.0/24  2     Inter-area 192.168.2.1  2.2.2.2        0.0.0.0
192.168.2.0/24  1     Stub       192.168.2.2  3.3.3.3        0.0.0.0

Routing for ASEs
Destination      Cost  Type      Tag      NextHop      AdvRouter
100.0.0.0/8 1 Type2 1 192.168.2.1 2.2.2.2

Total Nets: 7
Intra Area: 2  Inter Area: 4  ASE: 1  NSSA: 0
```

Display the OSPF LSDB of Router C.

```
[RouterC] display ospf lsdb

      OSPF Process 1 with Router ID 3.3.3.3
      Link State Database

Area: 0.0.0.0
Type      LinkState ID      AdvRouter      Age Len  Sequence      Metric
Router    3.3.3.3            3.3.3.3        345 72   80000004      1
Router    2.2.2.2            2.2.2.2        346 48   80000005      1
Router    1.1.1.1            1.1.1.1        193 48   80000006      1
Sum-Net   192.168.4.0        2.2.2.2        393 28   80000001      1
Sum-Net   192.168.4.0        1.1.1.1        189 28   80000001      2
Sum-Net   192.168.3.0        1.1.1.1        189 28   80000002      1
Sum-Net   192.168.3.0        2.2.2.2        192 28   80000002      2
Sum-Net   192.168.1.0        2.2.2.2        393 28   80000001      1
Sum-Net   192.168.1.0        1.1.1.1        189 28   80000002      1

AS External Database
Type      LinkState ID      AdvRouter      Age Len  Sequence      Metric
External  100.0.0.0 2.2.2.2 257 36 80000002 1
```

Step 5 Configure Router A as a translator.

```
[RouterA] ospf
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] nssa default-route-advertise no-summary translator-
always
[RouterA-ospf-1-area-0.0.0.1] quit
[RouterA-ospf-1] quit
```

Step 6 Verify the configuration.

Display the OSPF routing table of Router C.

 **NOTE**

On Router C, an AS external route is imported.

```
[RouterC] display ospf routing

      OSPF Process 1 with Router ID 3.3.3.3
```

Routing Tables

Routing for Network

Destination	Cost	Type	NextHop	AdvRouter	Area
192.168.3.0/24	2	Inter-area	192.168.0.1	1.1.1.1	0.0.0.0
192.168.4.0/24	2	Inter-area	192.168.2.1	2.2.2.2	0.0.0.0
192.168.0.0/24	1	Stub	192.168.0.2	3.3.3.3	0.0.0.0
192.168.1.0/24	2	Inter-area	192.168.2.1	2.2.2.2	0.0.0.0
192.168.1.0/24	2	Inter-area	192.168.0.1	1.1.1.1	0.0.0.0
192.168.2.0/24	1	Stub	192.168.2.2	3.3.3.3	0.0.0.0

Routing for ASEs

Destination	Cost	Type	Tag	NextHop	AdvRouter
100.0.0.0/8	1	Type2	1	192.168.0.1	1.1.1.1

Total Nets: 7
 Intra Area: 2 Inter Area: 4 ASE: 1 NSSA: 0

Display the OSPF LSDB of Router C.

 **NOTE**

- On RouterC, the router ID of the advertising router that imports AS external routes to the NSSA changes to 1.1.1.1. That is, RouterA becomes the translator.
- By default, the new translator, together with the former translator, acts as the translator for 40s. After 40s, only the new translator continues to work as a translator.

[RouterC] **display ospf lsdb**

OSPF Process 1 with Router ID 3.3.3.3
 Link State Database

Area: 0.0.0.0

Type	LinkState ID	AdvRouter	Age	Len	Sequence	Metric
Router	3.3.3.3	3.3.3.3	493	72	80000004	1
Router	2.2.2.2	2.2.2.2	494	48	80000005	1
Router	1.1.1.1	1.1.1.1	341	48	80000006	1
Sum-Net	192.168.4.0	2.2.2.2	541	28	80000001	1
Sum-Net	192.168.4.0	1.1.1.1	337	28	80000001	2
Sum-Net	192.168.3.0	1.1.1.1	337	28	80000002	1
Sum-Net	192.168.3.0	2.2.2.2	340	28	80000002	2
Sum-Net	192.168.1.0	2.2.2.2	541	28	80000001	1
Sum-Net	192.168.1.0	1.1.1.1	337	28	80000002	1

AS External Database

Type	LinkState ID	AdvRouter	Age	Len	Sequence	Metric
External	100.0.0.0	1.1.1.1	248	36	80000001	1

----End

Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
router id 1.1.1.1
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 192.168.0.1 255.255.255.0
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ip address 192.168.3.1 255.255.255.0
#
```

```

interface Pos3/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
 nssa default-route-advertise no-summary translator-always
#
return
    
```

- Configuration file of Router B

```

#
 sysname RouterB
#
router id 2.2.2.2
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.1 255.255.255.0
#
interface Pos3/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.4.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
 nssa
#
return
    
```

- Configuration file of Router C

```

#
 sysname RouterC
#
router id 3.3.3.3
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.0.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
return
    
```

- Configuration file of Router D

```
#
 sysname RouterD
#
router id 4.4.4.4
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.3.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.4.1 255.255.255.0
#
ospf 1
import-route static
 area 0.0.0.1
  network 192.168.3.0 0.0.0.255
  network 192.168.4.0 0.0.0.255
 nssa
#
ip route-static 100.0.0.0 255.0.0.0 NULL0
#
return
```

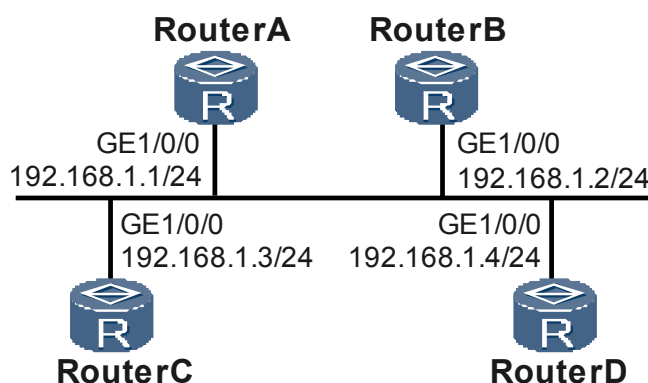
5.18.4 Example for Configuring DR Election of OSPF

This part provides an example for setting the DR priority on an interface for DR election on a broadcast network.

Networking Requirements

As shown in [Figure 5-7](#), Router A has the highest priority (100) in the network and thus is elected as the DR. Router C has the second highest priority, and is elected as the BDR. The priority of Router B is 0, and thus Router B cannot be elected as the DR or BDR. The priority of Router D is not configured and its default value is 1.

Figure 5-7 Configuring DR election of OSPF



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the router ID on each router, enable OSPF, and specify the network segment.
2. Check the DR/BDR status of each router with the default priority.
3. Configure the DR priority of the interface and check the DR/BDR status.

Data Preparation

To complete the configuration, you need the following data:

- The router ID of Router A is 1.1.1.1 and the DR priority is 100.
- The router ID of Router B is 2.2.2.2 and the DR priority is 0.
- The router ID of Router C is 3.3.3.3 and the DR priority is 2.
- The router ID of Router D is 4.4.4.4 and the DR priority is 1.

Procedure

Step 1 Configure an IP address for each interface.

The configuration details are not mentioned here.

Step 2 Configure basic OSPF functions.

Configure Router A.

```
[RouterA] router id 1.1.1.1
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
```

Configure Router B.

```
[RouterB] router id 2.2.2.2
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
```

Configure Router C.

```
[RouterC] router id 3.3.3.3
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
```

Configure Router D.

```
[RouterD] router id 4.4.4.4
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
```

View the DR/BDR status.

```
[RouterA] display ospf peer
      OSPF Process 1 with Router ID 1.1.1.1
        Neighbors
      Area 0.0.0.0 interface 192.168.1.1(GigabitEthernet1/0/0)'s neighbors
      Router ID: 2.2.2.2      Address: 192.168.1.2
      State: Full Mode:Nbr is Master Priority: 1
      DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
      Dead timer due in 32 sec
```

```

Retrans timer interval: 5
Neighbor is up for 00:04:21
Authentication Sequence: [ 0 ]
Router ID: 3.3.3.3      Address: 192.168.1.3
State: Full Mode:Nbr is Master Priority: 1
DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
Dead timer due in 37 sec
Retrans timer interval: 5
Neighbor is up for 00:04:06
Authentication Sequence: [ 0 ]
Router ID: 4.4.4.4      Address: 192.168.1.4
State: Full Mode:Nbr is Master Priority: 1
DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
Dead timer due in 37 sec
Retrans timer interval: 5
Neighbor is up for 00:03:53
Authentication Sequence: [ 0 ]
    
```

View the neighbor information of Router A. You can see the priority of DR and the neighbor status. The Router D is the DR, and Router C is the BDR.

 **NOTE**

When the priority is the same, the router with a higher router ID is elected as the DR. If a new router is added after the DR/BDR election is complete, the new router cannot become the DR even if it has the highest priority.

Step 3 Configure DR priorities on interfaces.

Configure Router A.

```

[RouterA] interface GigabitEthernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ospf dr-priority 100
[RouterA-GigabitEthernet1/0/0] quit
    
```

Configure Router B.

```

[RouterB] interface GigabitEthernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ospf dr-priority 0
[RouterB-GigabitEthernet1/0/0] quit
    
```

Configure Router C.

```

[RouterC] interface GigabitEthernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ospf dr-priority 2
[RouterC-GigabitEthernet1/0/0] quit
    
```

View the DR/BDR status.

```

[RouterD] display ospf peer
OSPF Process 1 with Router ID 4.4.4.4
Neighbors
Area 0.0.0.0 interface 192.168.1.4(GigabitEthernet1/0/0)'s neighbors
Router ID: 1.1.1.1      Address: 192.168.1.1
State: Full Mode:Nbr is Slave Priority: 100
DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
Dead timer due in 31 sec
Retrans timer interval: 5
Neighbor is up for 00:11:17
Authentication Sequence: [ 0 ]
Router ID: 2.2.2.2      Address: 192.168.1.2
State: Full Mode:Nbr is Slave Priority: 0
DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
Dead timer due in 35 sec
Retrans timer interval: 5
Neighbor is up for 00:11:19
Authentication Sequence: [ 0 ]
Router ID: 3.3.3.3      Address: 192.168.1.3
State: Full Mode:Nbr is Slave Priority: 2
    
```

```
DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
Dead timer due in 33 sec
Retrans timer interval: 5
Neighbor is up for 00:11:15
Authentication Sequence: [ 0 ]
```

Step 4 Restart OSPF processes.

In the user view of each router, run the **reset ospf 1 process** command to restart the OSPF process.

Step 5 View the configuration.

View the status of OSPF neighbors.

```
[RouterD] display ospf peer
OSPF Process 1 with Router ID 4.4.4.4
Neighbors
Area 0.0.0.0 interface 192.168.1.4(GigabitEthernet1/0/0)'s neighbors
Router ID: 1.1.1.1 Address: 192.168.1.1
State: Full Mode:Nbr is Slave Priority: 100
DR: 192.168.1.1 BDR: 192.168.1.3 MTU: 0
Dead timer due in 35 sec
Retrans timer interval: 5
Neighbor is up for 00:07:19
Authentication Sequence: [ 0 ]
Router ID: 2.2.2.2 Address: 192.168.1.2
State: Full Mode:Nbr is Master Priority: 0
DR: 192.168.1.1 BDR: 192.168.1.3 MTU: 0
Dead timer due in 35 sec
Retrans timer interval: 5
Neighbor is up for 00:07:19
Authentication Sequence: [ 0 ]
Router ID: 3.3.3.3 Address: 192.168.1.3
State: Full Mode:Nbr is Slave Priority: 2
DR: 192.168.1.1 BDR: 192.168.1.3 MTU: 0
Dead timer due in 37 sec
Retrans timer interval: 5
Neighbor is up for 00:07:17
Authentication Sequence: [ 0 ]
```

View the status of the OSPF interface.

```
[RouterA] display ospf interface
OSPF Process 1 with Router ID 1.1.1.1
Interfaces
Area: 0.0.0.0 (MPLS TE not enabled)
IP Address Type State Cost Pri DR BDR
192.168.1.1 Broadcast DR 1 100 192.168.1.1 192.168.1.3
[RouterB] display ospf interface
OSPF Process 1 with Router ID 2.2.2.2
Interfaces
Area: 0.0.0.0 (MPLS TE not enabled)
IP Address Type State Cost Pri DR BDR
192.168.1.2 Broadcast DROther 1 0 192.168.1.1 192.168.1.3
```

If all neighbors are in the Full state, it indicates that Router A establishes the neighbor relationship with its neighbor. If the neighbor stays "2-Way", it indicates both of them are not the DR or BDR. Thus, they need not exchange LSAs.

If the status of the OSPF interface is DROther, it indicates that it is neither DR nor BDR.

----End

Configuration Files

- Configuration file of Router A


```
#
 sysname RouterA
#
router id 1.1.1.1
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 192.168.1.1 255.255.255.0
 ospf dr-priority 100
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

● Configuration file of Router B

```
#
 sysname RouterB
#
router id 2.2.2.2
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 192.168.1.2 255.255.255.0
 ospf dr-priority 0
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

● Configuration file of Router C

```
#
 sysname RouterC
#
router id 3.3.3.3
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 192.168.1.3 255.255.255.0
 ospf dr-priority 2
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

● Configuration file of Router D

```
#
 sysname RouterD
#
router id 4.4.4.4
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 192.168.1.4 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

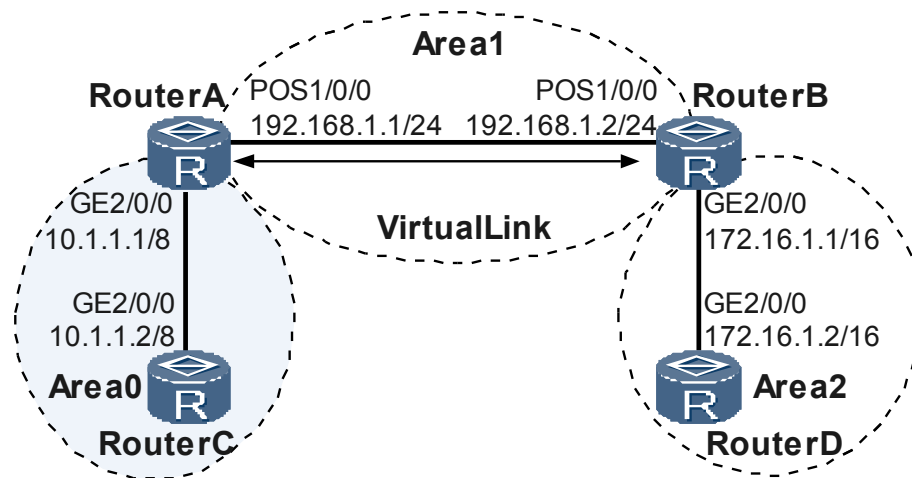
5.18.5 Example for Configuring OSPF Virtual Links

This part provides an example for configuring virtual links to connect non-backbone areas to the backbone area.

Networking Requirements

As shown in [Figure 5-8](#), Area 2 does not connect with the backbone area directly. Area 1 serves as a transit area to connect Area 2 and Area 0. A virtual link is configured between Router A and Router B.

Figure 5-8 Configuring OSPF virtual links



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic OSPF functions on each router.
2. Configure virtual connections on Router A and Router B to connect the backbone area with the non-backbone area.

Data Preparation

To complete the configuration, you need the following data:

- The router ID of Router A is 1.1.1.1, the process number of OSPF is 1, the network segment of Area 1 is 192.168.1.0/24, and the network segment of Area 0 is 10.0.0.0/8.
- The router ID of Router B is 2.2.2.2, the process number of OSPF is 1, the network segment of Area 1 is 192.168.1.0/24, and the network segment of Area 2 is 172.16.0.0/16.
- The router ID of Router C is 3.3.3.3, the process number of OSPF is 1, and the network segment of Area 0 is 10.0.0.0/8.
- The router ID of Router D is 4.4.4.4, the process number of OSPF is 1, and the network segment of Area 2 is 172.16.0.0/16.

Procedure

Step 1 Configure an IP address for each interface.

The configuration details are not mentioned here.

Step 2 Configure basic OSPF functions.

Configure Router A.

```
[RouterA] ospf 1 router-id 1.1.1.1
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.1] quit
```

Configure Router B.

```
[RouterB] ospf 1 router-id 2.2.2.2
[RouterB-ospf-1] area 1
[RouterB-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.1] quit
[RouterB-ospf-1] area 2
[RouterB-ospf-1-area-0.0.0.2] network 172.16.0.0 0.0.255.255
[RouterB-ospf-1-area-0.0.0.2] quit
```

Configure Router C.

```
[RouterC] ospf 1 router-id 3.3.3.3
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[RouterC-ospf-1-area-0.0.0.0] quit
```

Configure Router D.

```
[RouterD] ospf 1 router-id 4.4.4.4
[RouterD-ospf-1] area 2
[RouterD-ospf-1-area-0.0.0.2] network 172.16.0.0 0.0.255.255
[RouterD-ospf-1-area-0.0.0.2] quit
```

View the OSPF routing table of Router A.

NOTE

The routing table of Router A does not contain routes in Area 2 because Area 2 is not directly connected to Area 0.

```
[RouterA] display ospf routing
          OSPF Process 1 with Router ID 1.1.1.1
          Routing Tables

Routing for Network
Destination      Cost  Type      NextHop      AdvRouter     Area
10.0.0.0/8       1    Transit   10.1.1.1     3.3.3.3       0.0.0.0
192.168.1.0/24   1    Stub     192.168.1.1  1.1.1.1       0.0.0.1
Total Nets: 2
Intra Area: 2  Inter Area: 0  ASE: 0  NSSA: 0
```

Step 3 Configure virtual links.

Configure Router A.

```
[RouterA] ospf
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[RouterA-ospf-1-area-0.0.0.1] quit
```

Configure Router B.

```
[RouterB] ospf 1
[RouterB-ospf-1] area 1
[RouterB-ospf-1-area-0.0.0.1] vlink-peer 1.1.1.1
[RouterB-ospf-1-area-0.0.0.1] quit
```

Step 4 Verify the configuration.

View the OSPF routing table of Router A.

```
[RouterA] display ospf routing
          OSPF Process 1 with Router ID 1.1.1.1
          Routing Tables

Routing for Network
Destination      Cost  Type      NextHop      AdvRouter      Area
172.16.0.0/16    2    Inter-area 192.168.1.2   2.2.2.2        0.0.0.0
10.0.0.0/8       1    Transit   10.1.1.1     1.1.1.1        0.0.0.0
192.168.1.0/24   1    Stub     192.168.1.1  1.1.1.1        0.0.0.1
Total Nets: 3
Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

----End

Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.1.1.1 255.0.0.0
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 192.168.1.1 255.255.255.0
#
ospf 1 router-id 1.1.1.1
area 0.0.0.0
network 10.0.0.0 0.255.255.255
area 0.0.0.1
network 192.168.1.0 0.0.0.255
vlink-peer 2.2.2.2
#
return
```

- Configuration file of Router B

```
#
sysname RouterB
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 172.16.1.1 255.255.0.0
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ip address 192.168.1.2 255.255.255.0
#
ospf 1 router-id 2.2.2.2
area 0.0.0.1
network 192.168.1.0 0.0.0.255
vlink-peer 1.1.1.1
area 0.0.0.2
network 172.16.0.0 0.0.255.255
#
return
```

- Configuration file of Router C

```
#
 sysname RouterC
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.1.1.2 255.0.0.0
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.0
  network 10.0.0.0 0.255.255.255
#
return
```
- Configuration file of Router D

```
#
 sysname RouterD
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 172.16.1.2 255.255.0.0
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.2
  network 172.16.0.0 0.0.255.255
#
return
```

5.18.6 Example for Configuring OSPF Load Balancing

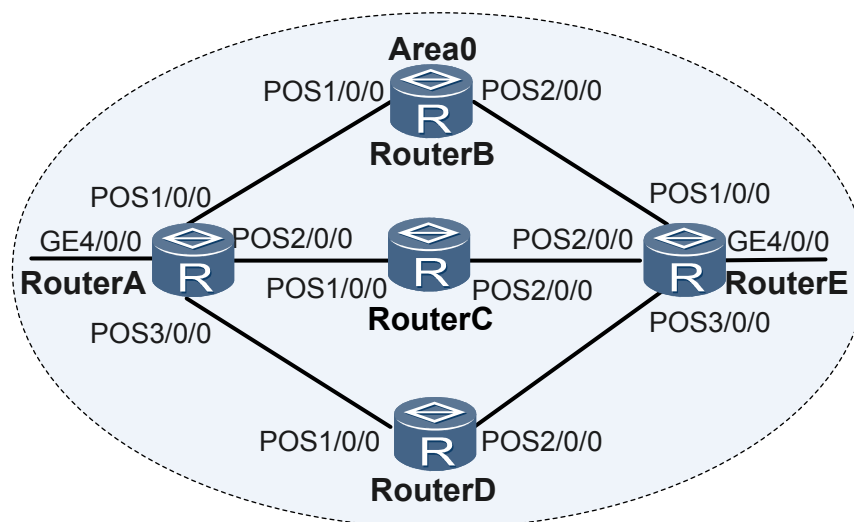
This part provides an example for configuring OSPF load balancing. Detailed operations include enabling load balancing, setting the priority for equal-cost routes, and configuring the load balancing mode.

Networking Requirements

As shown in [Figure 5-9](#):

- Router A, Router B, Router C, Router D, and Router E are interconnected to each other through OSPF.
- Router A, Router B, Router C, Router D, and Router E belong to Area 0.
- Load balancing is required to transmit the traffic of Router A to Router E through Router C and Router D.

Figure 5-9 Networking diagram of configuring OSPF load balancing



Device	Interface	IP Address	Device	Interface	IP Address
RouterA	POS1/0/0	10.1.1.1/24	RouterC	POS1/0/0	10.1.2.2/24
	POS2/0/0	10.1.2.1/24		POS2/0/0	192.168.1.1/24
	POS3/0/0	10.1.3.1/24	RouterD	POS1/0/0	10.1.3.2/24
	GE4/0/0	172.16.1.1/24		POS2/0/0	192.168.2.1/24
RouterB	POS1/0/0	10.1.1.2/24	RouterE	POS1/0/0	192.168.0.2/24
	POS2/0/0	192.168.0.1/24		POS2/0/0	192.168.1.2/24
				POS3/0/0	192.168.2.2/24
				GE4/0/0	172.17.1.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic OSPF functions on each router.
2. Configure load balancing on Router A.
3. Configure the priority for equal-cost routes on Router A.

Data Preparation

To complete the configuration, you need the following data:

- For Router A, the router ID is 1.1.1.1, the OSPF process number is 1, and the network segment of Area 0 is 10.1.1.0/24, 10.1.2.0/24, 10.1.3.0/24, and 172.16.1.0/24.
- For Router B, the router ID is 2.2.2.2, the OSPF process number is 1, and the network segment of Area 0 is 10.1.1.0/8 and 192.168.0.0/8.
- For Router C, the router ID is 3.3.3.3, the OSPF process number is 1, and the network segment of Area 0 is 10.1.2.0/8 and 192.168.1.0/8.

- For Router D, the router ID is 4.4.4.4, the OSPF process number is 1, and the network segment of Area 0 is 10.1.3.0/8 and 192.168.2.0/8.
- For Router E, the router ID is 5.5.5.5, the OSPF process number is 1, and the network segment of Area 0 is 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24, and 172.17.1.0/24.
- The number of load balancing paths on Router A is 2.
- The weight values of the next hop routes from Router A to Router B, Router C, and Router D are 2, 1, and 1 respectively.

Procedure

Step 1 Configure an IP address for each interface.

The configuration details are not mentioned here.

Step 2 Configure basic OSPF functions. The configuration details are not mentioned here.

Step 3 View the routing table of Router A.

As displayed in the routing table, Router A has three valid next hops: 10.1.1.2 (Router B), 10.1.2.2 (Router C), and 10.1.3.2 (RouterD). This is because the default maximum number of equal-cost routes is 6.

```
<RouterA> display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 12          Routes : 14
Destination/Mask    Proto Pre  Cost  Flags      NextHop         Interface
10.1.1.0/24         Direct 0     0      D          10.1.1.1         Pos1/0/0
10.1.1.2/32         Direct 0     0      D          10.1.1.2         Pos1/0/0
10.1.2.0/24         Direct 0     0      D          10.1.2.1         Pos2/0/0
10.1.2.2/32         Direct 0     0      D          10.1.2.2         Pos2/0/0
10.1.3.0/24         Direct 0     0      D          10.1.2.1         Pos3/0/0
10.1.3.2/32         Direct 0     0      D          10.1.2.2         Pos3/0/0
192.168.0.0/24      OSPF   10    2      D          10.1.1.2         Pos1/0/0
192.168.1.0/24      OSPF   10    2      D          10.1.2.2         Pos2/0/0
192.168.2.0/24      OSPF   10    2      D          10.1.2.2         Pos3/0/0
  172.17.1.0/24      OSPF   10    3      D          10.1.1.2         Pos1/0/0
                   OSPF   10    3      D          10.1.2.2         Pos2/0/0
                   OSPF   10    3      D          10.1.3.2         Pos3/0/0
127.0.0.0/8         Direct 0     0      D          127.0.0.1        InLoopBack0
127.0.0.1/32        Direct 0     0      D          127.0.0.1        InLoopBack0
```

NOTE

The maximum number of equal-cost routes varies with products and protocols. You can adjust the maximum number by purchasing the License.

Step 4 Configure a maximum of two routes on Router A to perform load balancing.

```
[RouterA] ospf 1
[RouterA-ospf-1] maximum load-balancing 2
[RouterA-ospf-1] quit
```

View the routing table of Router A. As shown in the routing table, Router A has only two valid next hops, 10.1.1.2 (Router B) and 10.1.2.2 (Router C). This is because the maximum number of equal-cost routes is set to 2.

```
[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 12          Routes : 13
Destination/Mask    Proto Pre  Cost  Flags      NextHop         Interface
10.1.1.0/24         Direct 0     0      D          10.1.1.1         Pos1/0/0
10.1.1.2/32         Direct 0     0      D          10.1.1.2         Pos1/0/0
10.1.2.0/24         Direct 0     0      D          10.1.2.1         Pos2/0/0
10.1.2.2/32         Direct 0     0      D          10.1.2.2         Pos2/0/0
10.1.3.0/24         Direct 0     0      D          10.1.2.1         Pos3/0/0
10.1.3.2/32         Direct 0     0      D          10.1.2.2         Pos3/0/0
192.168.0.0/24      OSPF   10    2      D          10.1.1.2         Pos1/0/0
192.168.1.0/24      OSPF   10    2      D          10.1.2.2         Pos2/0/0
192.168.2.0/24      OSPF   10    2      D          10.1.2.2         Pos3/0/0
  172.17.1.0/24      OSPF   10    3      D          10.1.1.2         Pos1/0/0
                   OSPF   10    3      D          10.1.2.2         Pos2/0/0
                   OSPF   10    3      D          10.1.3.2         Pos3/0/0
127.0.0.0/8         Direct 0     0      D          127.0.0.1        InLoopBack0
127.0.0.1/32        Direct 0     0      D          127.0.0.1        InLoopBack0
```

```

10.1.1.0/24 Direct 0 0 D 10.1.1.1 Pos1/0/0
10.1.1.2/32 Direct 0 0 D 10.1.1.2 Pos1/0/0
10.1.2.0/24 Direct 0 0 D 10.1.2.1 Pos2/0/0
10.1.2.2/32 Direct 0 0 D 10.1.2.2 Pos2/0/0
10.1.3.0/24 Direct 0 0 D 10.1.2.1 Pos3/0/0
10.1.3.2/32 Direct 0 0 D 10.1.2.2 Pos3/0/0
192.168.0.0/24 OSPF 10 2 D 10.1.1.2 Pos1/0/0
192.168.1.0/24 OSPF 10 2 D 10.1.2.2 Pos2/0/0
192.168.2.0/24 OSPF 10 2 D 10.1.2.2 Pos3/0/0
172.17.1.0/24 OSPF 10 3 D 10.1.1.2 Pos1/0/0
OSPF 10 3 D 10.1.2.2 Pos2/0/0
127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
    
```

Step 5 Configure the priority for equal-cost routes on Router A.

```

[RouterA] ospf 1
[RouterA-ospf-1] nexthop 10.1.1.2 weight 2
[RouterA-ospf-1] nexthop 10.1.2.2 weight 1
[RouterA-ospf-1] nexthop 10.1.3.2 weight 1
[RouterA-ospf-1] quit
    
```

View the OSPF routing table of Router A.

```

[RouterA] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 12          Routes : 13
Destination/Mask  Proto Pre  Cost  Flags      NextHop         Interface
10.1.1.0/24      Direct 0     0     D          10.1.1.1        Pos1/0/0
10.1.1.2/32      Direct 0     0     D          10.1.1.2        Pos1/0/0
10.1.2.0/24      Direct 0     0     D          10.1.2.1        Pos2/0/0
10.1.2.2/32      Direct 0     0     D          10.1.2.2        Pos2/0/0
10.1.3.0/24      Direct 0     0     D          10.1.2.1        Pos3/0/0
10.1.3.2/32      Direct 0     0     D          10.1.2.2        Pos3/0/0
192.168.0.0/24   OSPF   10    2     D          10.1.1.2        Pos1/0/0
192.168.1.0/24   OSPF   10    2     D          10.1.2.2        Pos2/0/0
192.168.2.0/24   OSPF   10    2     D          10.1.2.2        Pos3/0/0
172.17.1.0/24   OSPF   10    3     D          10.1.2.2        Pos2/0/0
OSPF   10    3     D          10.1.3.2        Pos3/0/0
127.0.0.0/8      Direct 0     0     D          127.0.0.1       InLoopBack0
127.0.0.1/32     Direct 0     0     D          127.0.0.1       InLoopBack0
    
```

As shown in the display, the priority of the route with the next hops being 10.1.2.2 and 10.1.3.2 is higher than that of the route with the next hop being 10.1.1.2. Thus, Router A has only two valid next hops, 10.1.2.2 (Router C) and 10.1.3.2 (Router D).

----End

Configuration Files

- Configuration file of Router A

```

#
 sysname RouterA
#
interface GigabitEthernet4/0/0
 undo shutdown
 ip address 172.16.1.1 255.255.255.0
#
interface pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
interface pos2/0/0
 link-protocol ppp
 undo shutdown
    
```



```
ip address 10.1.2.1 255.255.255.0
#
interface pos3/0/0
link-protocol ppp
undo shutdown
ip address 10.1.3.1 255.255.255.0
#
ospf 1 router-id 1.1.1.1
maximum load-balancing 2
nexthop 10.1.1.2 weight 2
nexthop 10.1.2.2 weight 1
nexthop 10.1.3.2 weight 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.1.2.0 0.0.0.255
network 10.1.3.0 0.0.0.255
network 172.16.1.0 0.0.0.255
#
return
```

- Configuration file of Router B

```
sysname RouterB
#
interface pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.1.2 255.255.255.0
#
interface pos2/0/0
link-protocol ppp
undo shutdown
ip address 192.168.0.1 255.255.255.0
#
ospf 1 router-id 2.2.2.2
area 0.0.0.0
network 10.1.1.0 0.255.255.255
network 192.168.0.0 0.255.255.255
#
return
```

- Configuration file of Router C

```
#
sysname RouterC
#
interface pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.2.2 255.255.255.0
#
interface pos2/0/0
link-protocol ppp
undo shutdown
ip address 192.168.1.1 255.255.255.0
#
ospf 1 router-id 3.3.3.3
area 0.0.0.0
network 10.1.2.0 0.255.255.255
network 192.168.1.0 0.0.255.255
#
Return
```

- Configuration file of Router D

```
#
sysname RouterD
#
interface pos1/0/0
link-protocol ppp
undo shutdown
ip address 10.1.3.2 255.255.255.0
#
```

```

interface pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.1 255.255.255.0
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.0
  network 10.1.3.0 0.255.255.255
  network 192.168.2.0 0.0.255.255
#
return
    
```

- Configuration file of Router E

```

#
 sysname RouterE
#
interface GigabitEthernet4/0/0
 undo shutdown
 ip address 172.17.1.1 255.255.255.0
#
interface pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.0.2 255.255.255.0
#
interface pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.1.2 255.255.255.0
#
interface pos3/0/0
 link-protocol ppp
 undo shutdown
 ip address 192.168.2.2 255.255.255.0
#
ospf 1 router-id 5.5.5.5
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
return
    
```

5.18.7 Example for Configuring Local MT

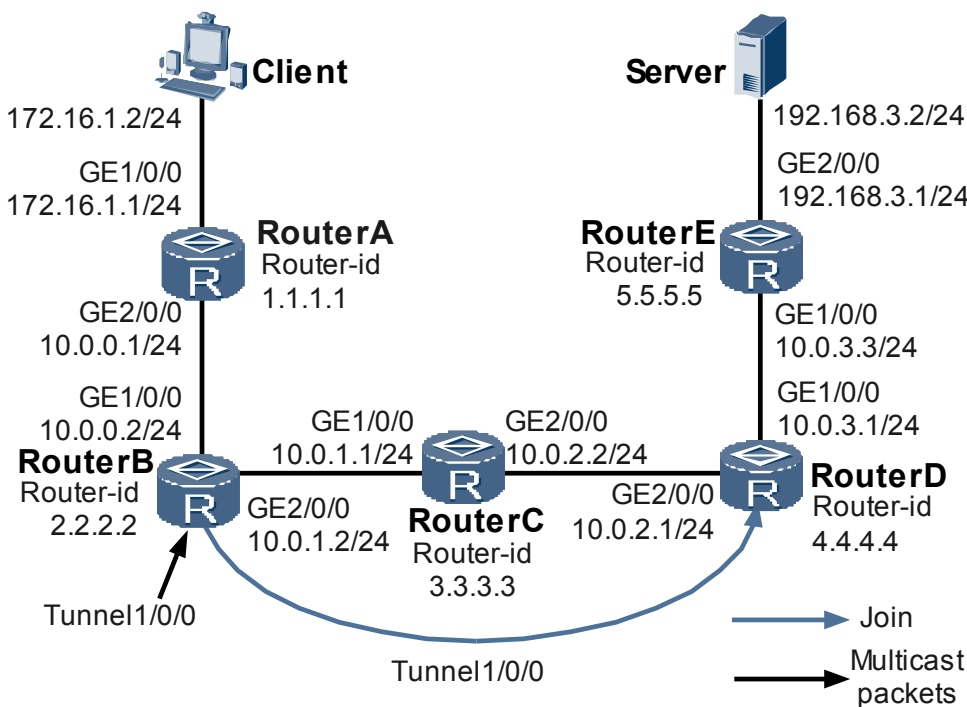
This part provides an example for configuring local MT. When both multicast and an MPLS TE tunnel are deployed on a network, you can build the multicast routing table and guide multicast packet forwarding by configuring local MT.

Networking Requirements

As [Figure 5-10](#) shows:

- Router A, Router B, Router C, Router D, and Router E run OSPF.
- A TE tunnel is established from Router B to Router D.
- IGP Shortcut is enabled on Router B.

Figure 5-10 Networking diagram of configuring OSPF local MT



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic OSPF functions on each router.
2. Configure Protocol Independent Multicast Sparse Mode (PIM-SM).
3. Configure an MPLS Resource Reservation Protocol (RSVP) TE tunnel and enable OSPF IGP Shortcut.
4. Enable local MT.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each router interface, as shown in [Table 5-1](#).
- The tunnel interface is TE tunnel 1/0/0; the tunnel interface borrows the IP address of Loopback 0; the tunnel encapsulation protocol is MPLS TE; the destination address is 4.4.4.4; the tunnel ID is 100; the tunnel signaling protocol is RSVP-TE.

Table 5-1 IP address of Loopback 0

router	IP address of Loopback 0
RouterA	1.1.1.1/32
RouterB	2.2.2.2/32

router	IP address of Loopback 0
RouterC	3.3.3.3/32
RouterD	4.4.4.4/32
RouterE	5.5.5.5/32

Procedure

Step 1 Configure an IP address for each interface and enable OSPF on each interface.

As shown in [Figure 5-10](#), configure an IP address and the mask for each interface and enable OSPF. The configuration details are not mentioned here.

Step 2 Configure PIM-SM.

Enable multicast on all routers and PIM-SM on all interfaces . The configurations on Router B, Router C, Router D, and Router E are similar to those on Router A and are not mentioned here.

```
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] pim sm
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] pim sm
[RouterA-GigabitEthernet1/0/0] quit
```

Enable the Internet Group Management Protocol (IGMP) on the interface connecting Router A and hosts.

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] igmp enable
[RouterA-GigabitEthernet1/0/0] igmp version 3
[RouterA-GigabitEthernet1/0/0] quit
```

Configure the C-BSR and C-RP. Set the service range of the RP on Router D and specify the locations of the C-BSR and C-RP.

```
[RouterD] pim
[RouterD-pim] c-bsr gigabitethernet 1/0/0
[RouterD-pim] c-rp gigabitethernet 1/0/0
[RouterD-pim] quit
```

Run the **display multicast routing-table** command to view the multicast routing table of a router. Take the display of Router C as an example:

```
[RouterC] display multicast routing-table
Multicast routing table of VPN-Instance: public net
Total 3 entries
00001. (192.168.3.8, 224.31.31.31)
    Uptime: 15:03:04
    Upstream Interface: GigabitEthernet2/0/0
    List of 1 downstream interface
        1: GigabitEthernet1/0/0
00002. (192.168.3.9, 224.31.31.31)
    Uptime: 15:03:04
    Upstream Interface: GigabitEthernet2/0/0
    List of 1 downstream interface
        1: GigabitEthernet1/0/0
00003. (192.168.3.10, 224.31.31.31)
```

```
Uptime: 15:03:04
Upstream Interface: GigabitEthernet2/0/0
List of 1 downstream interface
  1: GigabitEthernet1/0/0
```

Step 3 Configure an MPLS RSVP-TE tunnel.

Configure Router B.

```
[RouterB] mpls lsr-id 2.2.2.2
[RouterB] mpls
[RouterB-mpls] mpls te
[RouterB-mpls] mpls rsvp-te
[RouterB-mpls] mpls te cspf
[RouterB-mpls] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] mpls
[RouterB-GigabitEthernet2/0/0] mpls te
[RouterB-GigabitEthernet2/0/0] mpls rsvp-te
[RouterB-GigabitEthernet2/0/0] quit
[RouterB] ospf 1
[RouterB-ospf-1] enable traffic-adjustment
[RouterB-ospf-1] opaque-capability enable
[RouterB-ospf-1] area 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] mpls-te enable
[RouterB-ospf-1-area-0.0.0.0] quit
```

Configure Router C.

```
[RouterC] mpls lsr-id 3.3.3.3
[RouterC] mpls
[RouterC-mpls] mpls te
[RouterC-mpls] mpls rsvp-te
[RouterC-mpls] quit
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] mpls
[RouterC-GigabitEthernet1/0/0] mpls te
[RouterC-GigabitEthernet1/0/0] mpls rsvp-te
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] mpls
[RouterC-GigabitEthernet2/0/0] mpls te
[RouterC-GigabitEthernet2/0/0] mpls rsvp-te
[RouterC-GigabitEthernet2/0/0] quit
[RouterC] ospf 1
[RouterC-ospf-1] opaque-capability enable
[RouterC-ospf-1] area 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] mpls-te enable
[RouterC-ospf-1-area-0.0.0.0] quit
```

Configure Router D.

```
[RouterD] mpls lsr-id 4.4.4.4
[RouterD] mpls
[RouterD-mpls] mpls te
[RouterD-mpls] mpls rsvp-te
[RouterD-mpls] quit
[RouterD] interface gigabitethernet 2/0/0
[RouterD-GigabitEthernet1/0/0] mpls
[RouterD-GigabitEthernet1/0/0] mpls te
[RouterD-GigabitEthernet1/0/0] mpls rsvp-te
[RouterD-GigabitEthernet1/0/0] quit
[RouterD] ospf 1
[RouterD-ospf-1] opaque-capability enable
[RouterD-ospf-1] area 0.0.0.0
[RouterD-ospf-1-area-0.0.0.0] mpls-te enable
[RouterD-ospf-1-area-0.0.0.0] quit
```

Configure an MPLS TE tunnel and enable IGP Shortcut.

Configure an MPLS TE tunnel on Router B and enable IGP Shortcut.

```
[RouterB] interface tunnel 1/0/0
[RouterB-Tunnel1/0/0] ip address unnumbered interface loopback 0
[RouterB-Tunnel1/0/0] tunnel-protocol mpls te
[RouterB-Tunnel1/0/0] destination 4.4.4.4
[RouterB-Tunnel1/0/0] mpls te tunnel-id 100
[RouterB-Tunnel1/0/0] mpls te commit
[RouterB-Tunnel1/0/0] mpls te igp shortcut ospf
[RouterB-Tunnel1/0/0] mpls te igp metric relative -10
[RouterB-Tunnel1/0/0] quit
```

View the OSPF routing table on Router B. You can find that the MPLS TE tunnel is established.

```
[RouterB] display ip routing-table
Routing Tables: Public
    Destinations : 14          Routes : 14
Destination/Mask    Proto Pre  Cost   Flags NextHop         Interface
 2.2.2.2/32         Direct 0     0           D 127.0.0.1       InLoopBack0
 3.3.3.3/32         OSPF   10    1           D 10.0.1.1
GigabitEthernet2/0/0
 4.4.4.4/32         OSPF  10  1 D 2.2.2.2 Tunnel1/0/0 5.5.5.5/32 OSPF 10 2 D 2.2.2.2
Tunnel1/0/0
 10.0.0.0/24        Direct 0     0           D 10.0.0.2
GigabitEthernet1/0/0
 10.0.0.2/32        Direct 0     0           D 127.0.0.1       InLoopBack0
 10.0.1.0/24        Direct 0     0           D 10.0.1.2
GigabitEthernet2/0/0
 10.0.1.2/32        Direct 0     0           D 127.0.0.1       InLoopBack0
 10.0.2.0/24        OSPF   10    2           D 10.0.1.1
GigabitEthernet2/0/0
                   OSPF   10    2           D 10.0.1.1       Tunnel1/0/0
 10.0.3.0/24 OSPF 10 2 D 2.2.2.2 Tunnel1/0/0
 127.0.0.0/8        Direct 0     0           D 127.0.0.1       InLoopBack0
 127.0.0.1/32       Direct 0     0           D 127.0.0.1       InLoopBack0
 172.16.1.0/24      OSPF   10    2           D 10.0.0.1
GigabitEthernet2/0/0
 192.168.3.0/24 OSPF 10 3 D 2.2.2.2 Tunnel1/0/0
```

View the multicast routing table on Router C spanned by the TE tunnel.

```
[RouterC] display multicast routing-table
```

No multicast routing entry is displayed. This indicates that multicast packets are discarded.

Step 4 Configure local MT on Router B.

```
[RouterB] ospf
[RouterB-ospf-1] local-mt enable
[RouterB-ospf-1] quit
```

Step 5 Verify the configuration.

View the multicast routing table on Router C again. You can find that multicast routes are displayed.

```
[RouterC] display multicast routing-table
Multicast routing table of VPN-Instance: public net
Total 3 entries
00001. (192.168.3.8, 224.31.31.31)
    Uptime: 00:00:19
    Upstream Interface: GigabitEthernet2/0/0
    List of 1 downstream interface
        1: GigabitEthernet1/0/0
00002. (192.168.3.9, 224.31.31.31)
    Uptime: 00:00:19
    Upstream Interface: GigabitEthernet2/0/0
    List of 1 downstream interface
        1: GigabitEthernet1/0/0
00003. (192.168.3.10, 224.31.31.31)
```

```

    Uptime: 00:00:19
    Upstream Interface: GigabitEthernet2/0/0
    List of 1 downstream interface
      1: GigabitEthernet1/0/0
    
```

View the MIGP routing table on Router B.

```

[RouterB] display mignp routing-table
Route Flags: R - relied, D - download to fib
-----
Routing Tables: MIGP
    Destinations : 4          Routes : 4
Destination/Mask    Proto  Pre  Cost    Flags  NextHop          Interface
4.4.4.4/32          OSPF   10   2                10.0.1.1
GigabitEthernet2/0/0
5.5.5.5/32          OSPF   10   3                10.0.1.1
GigabitEthernet2/0/0
10.0.3.0/24         OSPF   10   2                10.0.1.1
GigabitEthernet2/0/0
192.168.3.0/24      OSPF   10   3                10.0.1.1          GigabitEthernet2/0/0
    
```

The physical outgoing interface of the next hop of the route with the previous outgoing interface as a TE tunnel interface is calculated in the MIGP routing table.

---End

Configuration Files

- Configuration file of Router A

```

#
sysname RouterA
#
router id 1.1.1.1
#
multicast routing-enable
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.0.0.1 255.255.255.0
pim sm
igmp version 3
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 172.16.1.1 255.255.255.0
pim sm
igmp enable
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
#
ospf 1
area 0.0.0.0
network 172.16.1.0 0.0.0.255
network 10.0.0.0 0.0.0.255
#
return
    
```

- Configuration file of Router B

```

#
sysname RouterB
#
router id 2.2.2.2
#
multicast routing-enable
#
mpls lsr-id 2.2.2.2
mpls
    
```

```

        mpls te
        mpls rsvp-te
        mpls te cspf
    #
    ospf 1
        opaque-capability enable
        enable traffic-adjustment
        local-mt enable
        area 0.0.0.0
            network 10.0.0.0 0.0.0.255
            network 10.0.1.0 0.0.0.255
            network 2.2.2.2 0.0.0.0
        mpls-te enable
    #
    interface GigabitEthernet1/0/0
        undo shutdown
        ip address 10.0.0.2 255.255.255.0
        pim sm
    #
    interface GigabitEthernet2/0/0
        undo shutdown
        ip address 10.0.1.2 255.255.255.0
        pim sm
        mpls
        mpls te
        mpls rsvp-te
    #
    interface LoopBack0
        ip address 2.2.2.2 255.255.255.255
        pim sm
    #
    interface Tunnel1/0/0
        ip address unnumbered interface LoopBack0
        tunnel-protocol mpls te
        destination 4.4.4.4
        mpls te tunnel-id 100
        mpls te igp shortcut ospf
        mpls te igp metric relative -10
        mpls te commit
    #
    pim
        C-BSR LoopBack0
        C-RP LoopBack0
    #
    return
    
```

● Configuration file of Router C

```

    #
    sysname RouterC
    #
    multicast routing-enable
    #
    mpls lsr-id 3.3.3.3
    mpls
        mpls te
        mpls rsvp-te
    #
    ospf 1
        opaque-capability enable
        area 0.0.0.0
            network 10.0.1.0 0.0.0.255
            network 10.0.2.0 0.0.0.255
            network 3.3.3.3 0.0.0.0
        mpls-te enable
    #
    interface GigabitEthernet1/0/0
        undo shutdown
        ip address 10.0.1.1 255.255.255.0
        pim sm
        mpls
    
```



```

        mpls te
        mpls rsvp-te
        #
        interface GigabitEthernet2/0/0
        undo shutdown
        ip address 10.0.2.2 255.255.255.0
        pim sm
        mpls
        mpls te
        mpls rsvp-te
        #
        interface LoopBack0
        ip address 3.3.3.3 255.255.255.255
        #
        return
    
```

● Configuration file of Router D

```

        #
        sysname RouterD
        #
        router id 4.4.4.4
        #
        multicast routing-enable
        #
        mpls lsr-id 4.4.4.4
        mpls
        mpls te
        mpls rsvp-te
        #
        interface GigabitEthernet1/0/0
        undo shutdown
        ip address 10.0.3.1 255.255.255.0
        pim sm
        #
        interface GigabitEthernet2/0/0
        undo shutdown
        ip address 10.0.2.1 255.255.255.0
        pim sm
        mpls
        mpls te
        mpls rsvp-te
        #
        interface LoopBack0
        ip address 4.4.4.4 255.255.255.255
        pim sm
        #
        ospf 1
        opaque-capability enable
        area 0.0.0.0
        network 10.0.2.0 0.0.0.255
        network 10.0.3.0 0.0.0.255
        network 4.4.4.4 0.0.0.0
        mpls-te enable
        #
        pim
        C-BSR GigabitEthernet1/0/0
        C-RP GigabitEthernet1/0/0
        #
        return
    
```

● Configuration file of Router E

```

        #
        sysname RouterE
        #
        router id 5.5.5.5
        #
        multicast routing-enable
        #
        interface GigabitEthernet1/0/0
        undo shutdown
    
```

```

ip address 10.0.3.3 255.255.255.0
pim sm
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 192.168.3.1 255.255.255.0
pim sm
#
interface LoopBack0
ip address 5.5.5.5 255.255.255.255
pim sm
#
ospf 1
area 0.0.0.0
network 10.0.3.0 0.0.0.255
network 192.168.3.0 0.0.0.255
network 5.5.5.5 0.0.0.0
#
return
    
```

5.18.8 Example for Configuring OSPF IP FRR

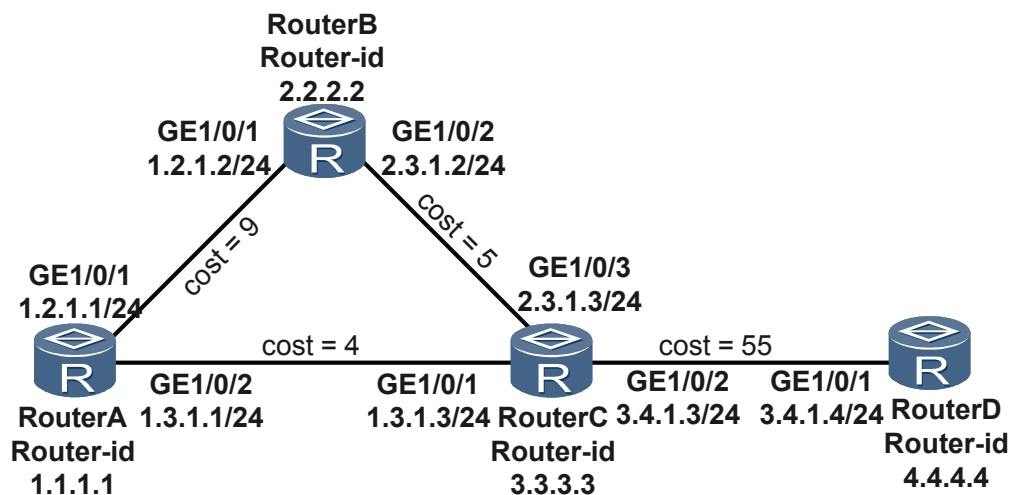
Networking Requirements

When a fault occurs on the network, OSPF IP FRR can fast switch traffic to the backup link without waiting for route convergence. This ensures uninterrupted traffic transmission.

As shown in [Figure 5-11](#):

- OSPF runs on the four routers in the same area.
- If the link between Router A and Router C becomes faulty, the traffic forwarded by Router A is rapidly switched to the backup link and forwarded through Router B.

Figure 5-11 Networking diagram for configuring OSPF IP FRR



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic OSPF functions on each router.

2. Set the cost to ensure that the link from Router A to Router C is preferred.
3. Enable OSPF IP FRR on Router A to protect the traffic forwarded by Router A.

Data Preparation

To complete the configuration, you need the following data:

- Router ID (1.1.1.1), OSPF process ID (1), network segment addresses in Area 1 (1.2.1.0 and 1.3.1.0), and interface cost (as shown in [Figure 5-11](#)) of Router A
- Router ID (2.2.2.2), OSPF process ID (1), network segment addresses in Area 1 (1.2.1.0 and 2.3.1.0), and interface cost (as shown in [Figure 5-11](#)) of Router B
- Router ID (3.3.3.3), OSPF process ID (1), network segment addresses of Area 1 (1.3.1.0, 2.3.1.0, and 3.4.1.0), IP addresses of two loopback interfaces (33.33.33.33 and 33.33.33.30), and interface cost (as shown in [Figure 5-11](#)) of Router C
- Router ID (4.4.4.4), OSPF process ID (1), network segment address in Area 1 (3.4.1.0), IP address of the loopback interface (4.4.4.4), interface cost (as shown in [Figure 5-11](#)), and destination address of the imported static route (160.1.1.1/32) of Router D

Procedure

Step 1 Configure an IP address and the cost for each interface. The configuration details are not mentioned here.

Step 2 Configure basic OSPF functions.

Configure Router A.

```
[RouterA] router id 1.1.1.1
[RouterA] ospf
[RouterA-ospf-1] area 1
[RouterA-ospf-1-area-0.0.0.1] network 1.2.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.1] network 1.3.1.0 0.0.0.255
```

Configure Router B.

```
[RouterB] router id 2.2.2.2
[RouterB] ospf
[RouterB-ospf-1] area 1
[RouterB-ospf-1-area-0.0.0.1] network 2.3.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.1] network 1.2.1.0 0.0.0.255
```

Configure Router C.

```
[RouterC] router id 3.3.3.3
[RouterC] ospf
[RouterC-ospf-1] area 1
[RouterC-ospf-1-area-0.0.0.1] network 2.3.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.1] network 1.3.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.1] network 33.33.33.33 0.0.0.0
[RouterC-ospf-1-area-0.0.0.1] network 33.33.33.30 0.0.0.0
[RouterC-ospf-1-area-0.0.0.1] network 3.4.1.0 0.0.0.255
```

Configure Router D.

```
[RouterD] router id 4.4.4.4
[RouterD] ip route-static 160.1.1.1 255.255.255.255 NULL0
[RouterD] ospf
[RouterD-ospf-1] area 1
[RouterD-ospf-1-area-0.0.0.1] network 3.4.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.1] network 4.4.4.4 0.0.0.0
```

Step 3 Enable OSPF IP FRR and FRR route filtering on Router A.

Enable OSPF IP FRR on Router A.

```
[RouterA] ospf
[RouterA-ospf-1] frr
[RouterA-ospf-1-frr] loop-free-alternate
```

Step 4 Verify the configuration.

View information about the route from Router A to Router D. You can find that OSPF generates a backup route because OSPF IP FRR is enabled.

```
<RouterA> display ospf routing router-id 4.4.4.4

          OSPF Process 1 with Router ID 1.1.1.1

Destination : 4.4.4.4                Route Type : Intra-area
Area        : 0.0.0.1                AdvRouter  : 4.4.4.4
Type        : ASBR                    Age        : 00h31m27s
URT Cost    : 59
NextHop     : 1.3.1.3                Interface  : GigabitEthernet1/0/2
Backup Nexthop : 1.2.1.2            Backup Interface : GigabitEthernet1/0/1
Backup Type  : LFA LINK
```

The preceding display shows that a backup route is generated on Router A.

----End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 1.2.1.1 255.255.255.0
 ospf cost 9
#
interface GigabitEthernet1/0/2
 undo shutdown
 ip address 1.3.1.1 255.255.255.0
 ospf cost 4
#
ospf 1 router-id 1.1.1.1
 frr
  frr-policy route route-policy abc
  loop-free-alternate
 area 0.0.0.1
  network 1.2.1.0 0.0.0.255
  network 1.3.1.0 0.0.0.255
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 1.2.1.2 255.255.255.0
 ospf cost 9
#
interface GigabitEthernet1/0/2
 undo shutdown
 ip address 2.3.1.2 255.255.255.0
```

```

ospf cost 5
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.1
  network 2.3.1.0 0.0.0.255
  network 1.2.1.0 0.0.0.255
#
return

```

- Configuration file of Router C

```

#
sysname RouterC
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 1.3.1.3 255.255.255.0
 ospf cost 4
#
interface GigabitEthernet1/0/2
 undo shutdown
 ip address 3.4.1.3 255.255.255.0
 ospf cost 55
#
interface GigabitEthernet1/0/3
 undo shutdown
 ip address 2.3.1.3 255.255.255.0
 ospf cost 5
#
interface LoopBack0
 ip address 33.33.33.33 255.255.255.255
#
interface LoopBack1
 ip address 33.33.33.30 255.255.255.255
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.1
  network 2.3.1.0 0.0.0.255
  network 1.3.1.0 0.0.0.255
  network 33.33.33.33 0.0.0.0
  network 33.33.33.30 0.0.0.0
  network 3.4.1.0 0.0.0.255
#
return

```

- Configuration file of Router D

```

#
sysname RouterD
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 3.4.1.4 255.255.255.0
 ospf cost 55
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
ospf 1 router-id 4.4.4.4
 import-route static
 area 0.0.0.1
  network 3.4.1.0 0.0.0.255
  network 4.4.4.4 0.0.0.0
#
return

```

5.18.9 Example for Configuring OSPF GR

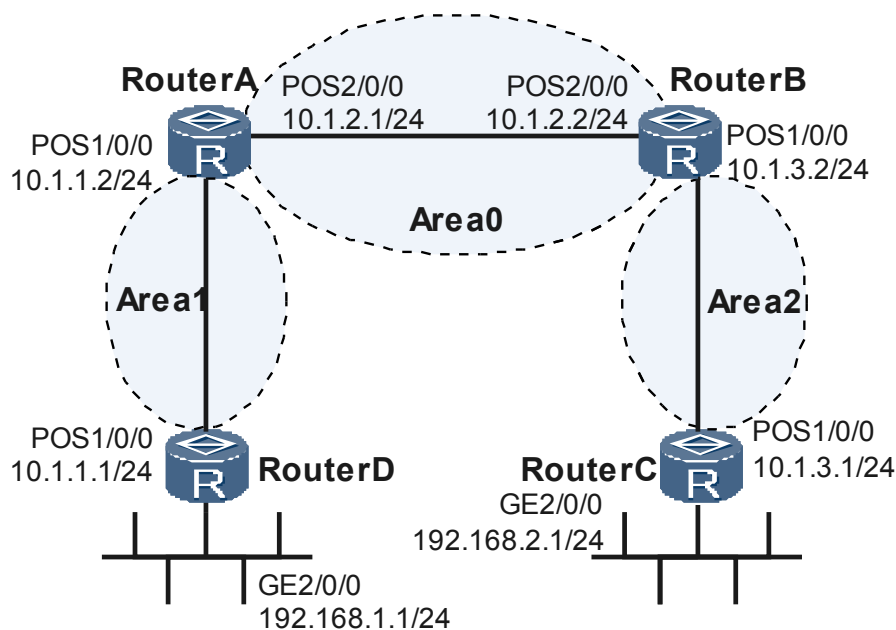
This part provides an example for configuring OSPF GR to ensure nonstop forwarding when an OSPF process restarts through GR or the active/standby switchover is performed.

Networking Requirements

As shown in **Figure 5-12**, Router A, Router B, and Router D are installed with the AMB and SMB that back up each other. The routers interconnect by means of OSPF, and are enabled with GR.

It is required that service forwarding be not interrupted when Router A restarts the OSPF process in GR mode or performs the active/standby switchover.

Figure 5-12 Networking diagram of configuring OSPF GR



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable OSPF to interconnect all routers.
2. Configure GR on RouterA, RouterB and RouterD.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface on the routers
- OSPF process number

Procedure

Step 1 Configure an IP address for each interface.

The detailed configuration procedure is not mentioned here.

Step 2 Configure basic OSPF functions.

Step 3 (Optional) Enable forcible active/standby switchover on Router A and configure the SMB to automatically synchronize information on the AMB.

By default, the forcible active/standby switchover is enabled.

```
[RouterA] slave switchover enable
[RouterA] slave auto-update config
```

Step 4 Enable OSPF GR on Router A, Router B, and Router D.

Configure Router A. The configurations of Router B and Router D are the same as that of Router A, and are not mentioned here.

```
[RouterA] ospf 1
[RouterA-ospf-1] opaque-capability enable
[RouterA-ospf-1] graceful-restart
```

Step 5 Verify the configuration.

Run the **display ospf graceful-restart** command on Router A, Router B, and Router D to check the OSPF GR status. Take the display of Router A as an example. You can find that the value of Graceful-restart capability is **enabled**. This indicates that OSPF GR is enabled on Router A.

```
<RouterA> display ospf 1 graceful-restart
      OSPF Process 1 with Router ID 10.1.1.2
Graceful-restart capability      : enabled
Graceful-restart support        : planned and un-planned, totally
Helper-policy support           : planned and un-planned, strict lsa check
Current GR state                : normal
Graceful-restart period         : 120 seconds
Number of neighbors under helper:
  Normal neighbors              : 0
  Virtual neighbors             : 0
  Sham-link neighbors           : 0
  Total neighbors               : 0
Number of restarting neighbors : 0
Last exit reason:
  On graceful restart           : none
  On Helper                     : none
```

In the user view, run the **reset ospf process graceful-restart** command on Router A to restart OSPF process 1. Run the **display ospf peer** command on Router D to check the OSPF neighbor relationship between Router D and Router A. If the status of the OSPF neighbor relationship is Full, it indicates that the relationship is not interrupted when Router A restarts the OSPF process through GR.

```
<RouterA> reset ospf 1 process graceful-restart
<RouterD> display ospf 1 peer

      OSPF Process 1 with Router ID 192.168.1.1
      Neighbors

Area 0.0.0.1 interface 10.1.1.1(Pos1/0/0)'s neighbors
Router ID: 10.1.1.2      Address: 10.1.1.2      GR State: Doing GR
State: Full Mode:Nbr is Slave Priority: 1
DR: None BDR: None MTU: 0
Dead timer due in 28 sec
Retrans timer interval: 4
Neighbor is up for 00:00:01
Authentication Sequence: [ 0 ]
```

Perform the active/standby switchover on Router A. During the switchover, Router C can ping through Router D, which indicates that service forwarding is not interrupted. Run the **display ospf peer** command on Router D and Router B to check the OSPF neighbor relationship with Router A. The statuses of the OSPF neighbor relationship are displayed as Full.

```
[RouterA] slave switchover
<RouterB> display ospf 1 peer

                OSPF Process 1 with Router ID 10.1.2.2
                  Neighbors

Area 0.0.0.0 interface 10.1.2.2(Pos2/0/0)'s neighbors
Router ID: 10.1.1.2      Address: 10.1.2.1      GR State: Normal
State: Full Mode:Nbr is Slave Priority: 1
DR: None  BDR: None  MTU: 0
Dead timer due in 39 sec
Retrans timer interval: 4
Neighbor is up for 00:01:45
Authentication Sequence: [ 0 ]

                Neighbors

Area 0.0.0.2 interface 10.1.3.2(Pos1/0/1)'s neighbors
Router ID: 10.1.3.1      Address: 10.1.3.1      GR State: Normal
State: Full Mode:Nbr is Master Priority: 1
DR: None  BDR: None  MTU: 0
Retrans timer interval: 4
Dead timer due in 34 sec
Retrans timer interval: 4
Neighbor is up for 00:09:26
Authentication Sequence: [ 0 ]
<RouterC> ping 192.168.1.1
PING 192.168.1.1: 56 data bytes, press CTRL_C to break
  Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=253 time=90 ms
  Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=253 time=30 ms
  Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=253 time=50 ms
  Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=253 time=60 ms
  Reply from 192.168.1.1: bytes=56 Sequence=5 ttl=253 time=70 ms

--- 192.168.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 30/60/90 ms
```

----End

Configuration Files

- Configuration file of Router A


```
#
sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 10.1.2.1 255.255.255.0
#
ospf 1
 opaque-capability enable
 graceful-restart
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
 area 0.0.0.1
  network 10.1.1.0 0.0.0.255
#
return
```
- Configuration file of Router B


```
#
```



```
sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.3.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 10.1.2.2 255.255.255.0
#
ospf 1
 opaque-capability enable
 graceful-restart
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
 area 0.0.0.2
  network 10.1.3.0 0.0.0.255
#
return
```

- Configuration file of Router C

```
#
sysname RouterC
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.3.1 255.255.255.0
#
ospf 1
 area 0.0.0.2
  network 10.1.3.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
return
```

- Configuration file of Router D

```
#
sysname RouterD
#
interface GigabitEthernet2/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.0
#
ospf 1
 opaque-capability enable
 graceful-restart
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```

5.18.10 Example for Configuring BFD for OSPF

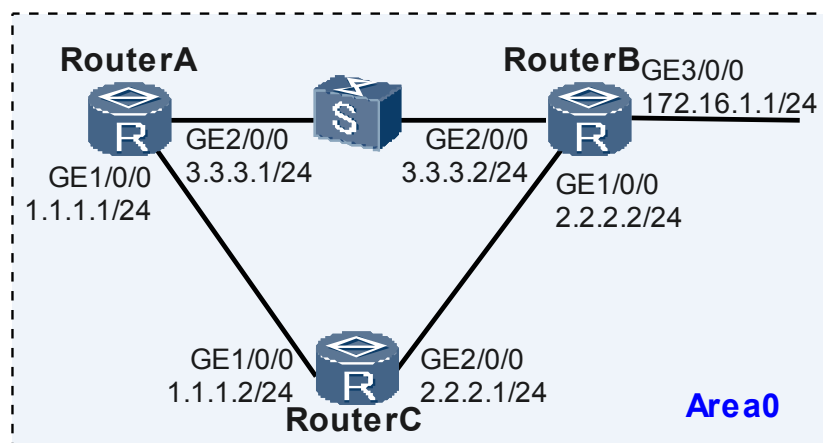
This part provides an example for configuring BFD for OSPF. After BFD for OSPF is configured, BFD can fast detect link faults and report them to OSPF so that service traffic can be transmitted through the backup link.

Networking Requirements

As shown in [Figure 5-13](#), it is required as follows:

- Run OSPF between Router A, Router B, and Router C.
- Enable BFD of the OSPF process on Router A, Router B, and Router C.
- Traffic is transmitted on the active link Router A → Router B. The link Router A → Router C → Router B acts as the standby link.
- BFD of the interface is configured on the link between Router A and Router B. When a fault occurs on the link, BFD can quickly detect the fault and notify OSPF of the fault; therefore, the traffic is transmitted on the standby link.

Figure 5-13 Networking diagram for configuring BFD for OSPF



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the basic OSPF functions on each router.
2. Enable global BFD.
3. Enable the detection mechanism on Router A and Router B.

Data Preparation

To complete the configuration, you need the following data:

- Router ID of Router A is 1.1.1.1, OSPF process number is 1, and the network segments of Area 0 are 3.3.3.0/24 and 1.1.1.0/24.
- Router ID of Router B is 2.2.2.2, OSPF process number is 1, and the network segments of Area 0 are 3.3.3.0/24, 2.2.2.0/24, and 172.16.1.0/24.
- Router ID of Router C is 3.3.3.3, OSPF process number is 1, and the network segments of Area 0 are 1.1.1.0/24 and 2.2.2.0/24.
- Minimum interval for sending the BFD packets, minimum interval for receiving the BFD packets, and local detection multiple on Router A and Router B.

Procedure

Step 1 Assign an IP address to each router interface.

The detailed configuration is not mentioned here.

Step 2 Configure the basic OSPF functions.

Configure Router A.

```
[RouterA] router id 1.1.1.1
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 3.3.3.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

Configure Router B.

```
[RouterB] router id 2.2.2.2
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 3.3.3.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 172.16.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

Configure Router C.

```
[RouterC] router id 3.3.3.3
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 1.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 2.2.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

After the preceding configurations are complete, run the **display ospf peer** command. You can view that the neighboring relationship is set up between Router A and Router B, and that between Router B and Router C. Take the display of Router A as an example:

```
<RouterA> display ospf peer
      OSPF Process 1 with Router ID 1.1.1.1
      Neighbors
Area 0.0.0.0 interface 1.1.1.1(GigabitEthernet1/0/0)'s neighbors
Router ID: 3.3.3.3      Address: 1.1.1.2
State: Full Mode:Nbr is Master Priority: 1
DR: 1.1.1.1 BDR: 1.1.1.2 MTU: 0
Dead timer due in 38 sec
Retrans timer interval: 5
Neighbor is up for 00:00:15
Authentication Sequence: [ 0 ]
      Neighbors
Area 0.0.0.0 interface 3.3.3.1(GigabitEthernet2/0/0)'s neighbors
Router ID: 2.2.2.2      Address: 3.3.3.2
State: Full Mode:Nbr is Master Priority: 1
DR: 3.3.3.1 BDR: 3.3.3.2 MTU: 0
Dead timer due in 25 sec
Retrans timer interval: 5
Neighbor is up for 00:00:59
Authentication Sequence: [ 0 ]
```

Display the information in the OSPF routing table on Router A. You can view the routing entries to Router B and Router C. The next hop address of the route to 172.16.1.0/24 is 3.3.3.2 and traffic is transmitted on the active link Router A → Router B.

```
<RouterA> display ospf routing
      OSPF Process 1 with Router ID 1.1.1.1
      Routing Tables
Routing for Network
```

```
Destination      Cost  Type      NextHop      AdvRouter      Area
172.16.1.1/24  2  Stub  3.3.3.2  2.2.2.2  0.0.0.0
3.3.3.0/24      1      Transit  3.3.3.1      1.1.1.1      0.0.0.0
2.2.2.0/24      2      Transit  3.3.3.2      3.3.3.3      0.0.0.0
2.2.2.0/24      2      Transit  1.1.1.2      3.3.3.3      0.0.0.0
1.1.1.0/24      1      Transit  1.1.1.1      1.1.1.1      0.0.0.0
Total Nets: 5
Intra Area: 5  Inter Area: 0  ASE: 0  NSSA: 0
```

Step 3 Configure OSPF BFD.

Enable global BFD on Router A.

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] ospf
[RouterA-ospf-1] bfd all-interfaces enable
[RouterA-ospf-1] quit
```

Enable global BFD on Router B.

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] ospf
[RouterB-ospf-1] bfd all-interfaces enable
[RouterB-ospf-1] quit
```

Enable global BFD on Router C.

```
[RouterC] bfd
[RouterC-bfd] quit
[RouterC] ospf
[RouterC-ospf-1] bfd all-interfaces enable
[RouterC-ospf-1] quit
```

After the preceding configurations are complete, run the **display ospf bfd session all** command on Router A or Router B. You can view that the status of the BFD session is Up.

Take the display of Router A as an example:

```
[RouterA] display ospf bfd session all
      OSPF Process 1 with Router ID 1.1.1.1
      Area 0.0.0.0 interface 1.1.1.1(GigabitEthernet1/0/0)'s BFD Sessions
NeighborId:3.3.3.3      AreaId:0.0.0.0      Interface:GigabitEthernet1/0/0
BFDState:up           rx      :10      tx      :10
Multiplier:3          BFD Local Dis:8195      LocalIpAdd:1.1.1.1
RemoteIpAdd:1.1.1.2    Diagnostic Info:No diagnostic information
      Area 0.0.0.0 interface 3.3.3.1(GigabitEthernet2/0/0)'s BFD Sessions
NeighborId:2.2.2.2      AreaId:0.0.0.0      Interface:GigabitEthernet2/0/0
BFDState:up           rx      :10      tx      :10
Multiplier:3          BFD Local Dis:8194      LocalIpAdd:3.3.3.1
RemoteIpAdd:3.3.3.2    Diagnostic Info:No diagnostic information
```

Step 4 Configure BFD of the interface.

Configure BFD on GE 2/0/0 of Router A, set the minimum interval for sending the packets and the minimum interval for receiving the packets to 500 ms, and set the local detection time multiple to 4.

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ospf bfd enable
[RouterA-GigabitEthernet2/0/0] ospf bfd min-tx-interval 500 min-rx-interval 500
detect-multiplier 4
[RouterA-GigabitEthernet2/0/0] quit
```

Configure BFD on GE 2/0/0 of Router B, set the minimum interval for sending the packets and the minimum interval for receiving the packets to 500 ms, and set the local detection time multiple to 4.

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] ospf bfd enable
[RouterB-GigabitEthernet2/0/0] ospf bfd min-tx-interval 500 min-rx-interval 500
detect-multiplier 4
[RouterB-GigabitEthernet2/0/0] quit
```

After the preceding configurations are complete, run the **display ospf bfd session all** command on Router A or Router B. You can view that the status of the BFD session is Up.

Take the display of Router B as an example:

```
[RouterB] display ospf bfd session all
      OSPF Process 1 with Router ID 2.2.2.2
      Area 0.0.0.0 interface 3.3.3.2(GigabitEthernet2/0/0)'s BFD Sessions
NeighborId:1.1.1.1      AreaId:0.0.0.0      Interface: GigabitEthernet2/0/0
BFDState:up           rx      :500      tx      :500
Multiplier:4         BFD Local Dis:8198      LocalIpAdd:3.3.3.2
RemoteIpAdd:3.3.3.1   Diagnostic Info:No diagnostic information
      Area 0.0.0.0 interface 2.2.2.2(GigabitEthernet1/0/0)'s BFD Sessions
NeighborId:3.3.3.3      AreaId:0.0.0.0      Interface: GigabitEthernet1/0/0
BFDState:up           rx      :10      tx      :10
Multiplier:3         BFD Local Dis:8199      LocalIpAdd:2.2.2.2
RemoteIpAdd:2.2.2.1   Diagnostic Info:No diagnostic information
```

Step 5 Verify the configuration.

Run the **shutdown** command on GE 2/0/0 of Router B to simulate the active link failure.

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] shutdown
```

Display the routing table on Router A. The standby link Router A → Router C → Router B takes effect after the active link fails. The next hop address of the route to 172.16.1.0/24 becomes 1.1.1.2.

```
<HUAWEI> display ospf routing
      OSPF Process 1 with Router ID 1.1.1.1
      Routing Tables

Routing for Network
Destination      Cost  Type      NextHop      AdvRouter      Area
172.16.1.1/24   2     Stub     1.1.1.2      2.2.2.2        0.0.0.0
3.3.3.0/24      1     Transit  3.3.3.1      1.1.1.1        0.0.0.0
2.2.2.0/24      2     Transit  1.1.1.2      3.3.3.3        0.0.0.0
1.1.1.0/24      1     Transit  1.1.1.1      1.1.1.1        0.0.0.0
Total Nets: 4
Intra Area: 4  Inter Area: 0  ASE: 0  NSSA: 0
```

----End

Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
router id 1.1.1.1
#
bfd
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 3.3.3.1 255.255.255.0
ospf bfd enable
```

```
ospf bfd min-tx-interval 500 min-rx-interval 500 detect-multiplier 4
#
ospf 1
bfd all-interface enable
area 0.0.0.0
network 3.3.3.0 0.0.0.255
network 1.1.1.0 0.0.0.255
#
return
```

- Configuration file of Router B

```
#
sysname RouterB
#
router id 2.2.2.2
#
bfd
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 2.2.2.2 255.255.255.0
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 3.3.3.2 255.255.255.0
ospf bfd enable
ospf bfd min-tx-interval 500 min-rx-interval 500 detect-multiplier 4
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 172.16.1.1 255.255.255.0
#
ospf 1
bfd all-interface enable
area 0.0.0.0
network 3.3.3.0 0.0.0.255
network 2.2.2.0 0.0.0.255
network 172.16.1.0 0.0.0.255
#
return
```

- Configuration file of Router C

```
#
sysname RouterC
#
router id 3.3.3.3
#
bfd
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 1.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 2.2.2.1 255.255.255.0
#
ospf 1
bfd all-interface enable
area 0.0.0.0
network 1.1.1.0 0.0.0.255
network 2.2.2.0 0.0.0.255
#
return
```

5.18.11 Example for Configuring OSPF-BGP

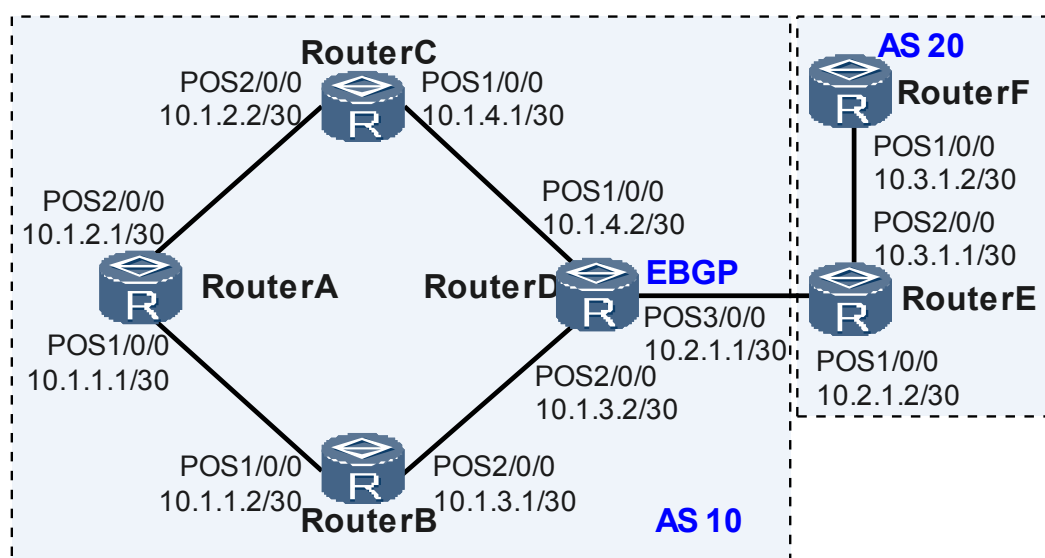
This part provides an example for configuring OSPF-BGP association to prevent network traffic from being interrupted after routers are restarted.

Network Requirements

As shown in [Figure 5-14](#), all routers run BGP. An EBGP connection is established between Router D and Router E. IBGP full connections are established between partial routers in AS 10, and OSPF is used as an IGP protocol.

It is required to enable OSPF-BGP linkage on Router B so that the traffic from Router A to AS 20 is not interrupted after Router B restarts.

Figure 5-14 Networking diagram of configuring OSPF-BGP linkage



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable OSPF on Router A, Router B, Router C, and Router D (except 10.2.1.1/30) and specify the same area for all OSPF interfaces.
2. Establish IBGP full connections between Router A, Router B, Router C, and Router D (except 10.2.1.1/30).
3. Set the OSPF cost on Router C.
4. Establish the EBGP connection between Router D and Router E.
5. Configure the OSPF routes and configure BGP to import directly connected routes on Router D.
6. Configure BGP on Router E.

Data Preparation

To complete the configuration, you need the following data:

- The router ID of Router A is 1.1.1.1, the AS number is 10, the OSPF process number is 1, and the network segments in Area 0 are 10.1.1.0/30 and 10.1.2.0/30.

- The router ID of Router B is 2.2.2.2, the AS number is 10, the OSPF process number is 1, and the network segments in Area 0 are 10.1.1.0/30 and 10.1.3.0/30.
- The router ID of Router C is 3.3.3.3, the AS number is 10, the OSPF process number is 1, and the network segments in Area 0 are 10.1.2.0/30 and 10.1.4.0/30.
- The router ID of Router D is 4.4.4.4, the AS number is 10, the OSPF process number is 1, and the network segments in Area 0 are 10.1.3.0/30 and 10.1.4.0/30.
- The router ID of Router E is 5.5.5.5, and the AS number is 20.

Procedure

Step 1 Configure an IP address for each interface.

The configuration details are not mentioned here.

Step 2 Configure basic OSPF functions.

The configuration details are not mentioned here.

Step 3 Configure an IBGP full connection.

Configure Router A.

```
<RouterA> system-view
[RouterA] interface LoopBack 0
[RouterA-LoopBack0] ip address 1.1.1.1 32
[RouterA-LoopBack0] quit
[RouterA] bgp 10
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 2.2.2.2 as-number 10
[RouterA-bgp] peer 2.2.2.2 connect-interface LoopBack 0
[RouterA-bgp] peer 3.3.3.3 as-number 10
[RouterA-bgp] peer 3.3.3.3 connect-interface LoopBack 0
[RouterA-bgp] peer 4.4.4.4 as-number 10
[RouterA-bgp] peer 4.4.4.4 connect-interface LoopBack 0
[RouterA-bgp] quit
```

Configure Router B.

```
<RouterB> system-view
[RouterB] interface LoopBack 0
[RouterB-LoopBack0] ip address 2.2.2.2 32
[RouterB-LoopBack0] quit
[RouterB] bgp 10
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 1.1.1.1 as-number 10
[RouterB-bgp] peer 1.1.1.1 connect-interface LoopBack 0
[RouterB-bgp] peer 3.3.3.3 as-number 10
[RouterB-bgp] peer 3.3.3.3 connect-interface LoopBack 0
[RouterB-bgp] peer 4.4.4.4 as-number 10
[RouterB-bgp] peer 4.4.4.4 connect-interface LoopBack 0
[RouterB-bgp] quit
```

Configure Router C.

```
<RouterC> system-view
[RouterC] interface LoopBack 0
[RouterC-LoopBack0] ip address 3.3.3.3 32
[RouterC-LoopBack0] quit
[RouterC] bgp 10
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 1.1.1.1 as-number 10
[RouterC-bgp] peer 1.1.1.1 connect-interface LoopBack 0
[RouterC-bgp] peer 2.2.2.2 as-number 10
[RouterC-bgp] peer 2.2.2.2 connect-interface LoopBack 0
[RouterC-bgp] peer 4.4.4.4 as-number 10
```



```
[RouterC-bgp] peer 4.4.4.4 connect-interface LoopBack 0
[RouterC-bgp] quit
```

Configure Router D.

```
<RouterD> system-view
[RouterD] interface LoopBack 0
[RouterD-LoopBack0] ip address 4.4.4.4 32
[RouterD-LoopBack0] quit
[RouterD] bgp 10
[RouterD-bgp] router-id 4.4.4.4
[RouterD-bgp] peer 1.1.1.1 as-number 10
[RouterD-bgp] peer 1.1.1.1 connect-interface LoopBack 0
[RouterD-bgp] peer 2.2.2.2 as-number 10
[RouterD-bgp] peer 2.2.2.2 connect-interface LoopBack 0
[RouterD-bgp] peer 3.3.3.3 as-number 10
[RouterD-bgp] peer 3.3.3.3 connect-interface LoopBack 0
[RouterD-bgp] quit
```

Step 4 Configure an EBGP connection.

Configure Router D.

```
[RouterD] bgp 10
[RouterD-bgp] peer 10.2.1.2 as-number 20
[RouterD-bgp] import-route direct
[RouterD-bgp] import-route ospf 1
[RouterD-bgp] quit
```

Configure Router E.

```
[RouterE] bgp 20
[RouterE-bgp] peer 10.2.1.1 as-number 10
[RouterE-bgp] ipv4-family unicast
[RouterE-bgp-af-ipv4] network 10.3.1.0 30
[RouterE-bgp-af-ipv4] quit
```

Step 5 Set the cost of OSPF on Router C.

```
[RouterC] interface pos 1/0/0
[RouterC-Pos1/0/0] ospf cost 2
[RouterC-Pos1/0/0] quit
[RouterC] interface pos 2/0/0
[RouterC-Pos2/0/0] ospf cost 2
[RouterC-Pos2/0/0] quit
```

NOTE

After the cost of OSPF on Router C is set to 2, Router A chooses only Router B as the intermediate router to the network segment 10.2.1.0. Router C becomes the backup router of Router B.

View the routing table of Router A. As shown in the routing table, the route to the network segment 10.3.1.0 can be learned through BGP, and the outgoing interface is POS 1/0/0.

```
[RouterA] display ip routing-table
Route Flags: R - relied, D - download to fib
```

```
-----
Routing Tables: Public
  Destinations : 16          Routes : 17
Destination/Mask    Proto  Pre  Cost   Flags NextHop         Interface
1.1.1.1/32         Direct  0    0      D    127.0.0.1       InLoopBack0
2.2.2.2/32         OSPF   10   3      D    10.1.1.2        Pos1/0/0
4.4.4.0/24         IBGP   255  0      RD   4.4.4.4         Pos1/0/0
4.4.4.4/32         OSPF   10   3      D    10.1.1.2        Pos1/0/0
5.5.5.0/24         EBGP   255  0      RD   10.2.1.2        Pos1/0/0
10.1.1.0/30        Direct  0    0      D    10.1.1.1        Pos1/0/0
10.1.1.1/32        Direct  0    0      D    127.0.0.1       InLoopBack0
10.1.1.2/32        Direct  0    0      D    10.1.1.2        Pos1/0/0
10.1.2.0/30        Direct  0    0      D    10.1.2.1        Pos2/0/0
10.1.2.1/32        Direct  0    0      D    127.0.0.1       InLoopBack0
```

```

10.1.2.2/32 Direct 0 0 D 10.1.2.2 Pos2/0/0
10.1.3.0/30 OSPF 10 2 D 10.1.1.2 Pos1/0/0
10.1.3.1/32 IBGP 255 0 RD 4.4.4.4 Pos1/0/0
10.1.4.0/30 OSPF 10 3 D 10.1.1.2 Pos1/0/0
OSPF 10 3 D 10.1.2.2 Pos2/0/0
10.1.4.1/32 IBGP 255 0 RD 4.4.4.4 Pos1/0/0
10.2.1.0/30 EBGP 255 0 RD 4.4.4.4 Pos1/0/0
10.2.1.2/32 EBGP 255 0 RD 4.4.4.4 Pos1/0/0
10.3.1.0/30 EBGP 255 0 RD 4.4.4.4 Pos1/0/0

```

View the routing table of Router B.

```
[RouterB] display ip routing-table
```

```
Route Flags: R - relied, D - download to fib
```

```
-----
Routing Tables: Public
```

```

Destinations : 15          Routes : 15
Destination/Mask Proto Pre Cost Flags NextHop Interface
2.2.2.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0
1.1.1.1/32 OSPF 10 2 D 10.1.1.1 Pos1/0/0
4.4.4.0/24 IBGP 255 0 RD 10.1.3.2 Pos2/0/0
4.4.4.4/32 OSPF 10 2 D 10.1.3.2 Pos2/0/0
5.5.5.0/24 EBGP 255 0 RD 10.2.1.2 Pos2/0/0
10.1.1.0/30 Direct 0 0 D 10.1.1.2 Pos1/0/0
10.1.1.1/32 Direct 0 0 D 10.1.1.1 Pos1/0/0
10.1.1.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0
10.1.2.0/30 OSPF 10 2 D 10.1.1.1 Pos1/0/0
10.1.3.0/30 Direct 0 0 D 10.1.3.1 Pos2/0/0
10.1.3.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
10.1.3.2/32 Direct 0 0 D 10.1.3.2 Pos2/0/0
10.1.4.0/30 OSPF 10 2 D 10.1.3.2 Pos2/0/0
10.1.4.1/32 IBGP 255 0 RD 10.1.3.2 Pos2/0/0
10.2.1.0/30 EBGP 255 0 RD 10.1.3.2 Pos2/0/0
10.2.1.2/32 EBGP 255 0 RD 10.1.3.2 Pos2/0/0
10.3.1.0/30 EBGP 255 0 RD 10.1.3.2 Pos2/0/0

```

As shown in the routing table, Router B learns the route to the network segment 10.3.1.0 through BGP, and the outgoing interface is POS 2/0/0. The routes to the network segments 10.1.2.0 and 10.1.4.0 respectively can be learned through OSPF. The costs of the two routes are 2.

Step 6 Enable OSPF-BGP linkage on Router B.

```

[RouterB] ospf 1
[RouterB-ospf-1] stub-router on-startup
[RouterB-ospf-1] quit
[RouterB] quit

```

Step 7 Verify the configuration.

Restart Router B.

 **NOTE**

Confirm the action before you use the command because the command leads to the breakdown of the network in a short time. In addition, when restarting a router, ensure that the configuration file of the router is saved.

```

<RouterB> reboot
System will reboot! Continue?[Y/N] y

```

View the routing table of Router A. As shown in the routing table, the route to the network 10.3.1.0 can be learned through BGP, and the outgoing interface is POS 2/0/0.

```
[RouterA] display ip routing-table
```

```
Route Flags: R - relied, D - download to fib
```

```
-----
Routing Tables: Public
```

```

Destinations : 17          Routes : 17
Destination/Mask Proto Pre Cost Flags NextHop Interface
1.1.1.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0

```

```

2.2.2.2/32 OSPF 10 4 D 10.1.2.2 Pos2/0/0
4.4.4.0/24 IBGP 255 0 RD 4.4.4.4 Pos2/0/0
4.4.4.4/32 OSPF 10 4 D 10.1.2.2 Pos2/0/0
5.5.5.0/24 EBGp 255 0 RD 10.2.1.2 Pos2/0/0
10.1.1.0/30 Direct 0 0 D 10.1.1.1 Pos1/0/0
10.1.1.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
10.1.1.2/32 Direct 0 0 D 10.1.1.2 Pos1/0/0
10.1.2.0/30 Direct 0 0 D 10.1.2.1 Pos2/0/0
10.1.2.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
10.1.2.2/32 Direct 0 0 D 10.1.2.2 Pos2/0/0
10.1.3.0/30 OSPF 10 2 D 10.1.1.2 Pos1/0/0
10.1.3.1/32 IBGP 255 0 RD 4.4.4.4 Pos2/0/0
10.1.4.0/30 OSPF 10 3 D 10.1.2.2 Pos2/0/0
10.1.4.1/32 IBGP 255 0 RD 4.4.4.4 Pos2/0/0
10.2.1.0/30 EBGp 255 0 RD 4.4.4.4 Pos2/0/0
10.2.1.2/32 EBGp 255 0 RD 4.4.4.4 Pos2/0/0
10.3.1.0/30 EBGp 255 0 RD 4.4.4.4 Pos2/0/0
  
```

View the routing table of Router B. As shown in the routing table, only OSPF routes exist in the routing table temporarily and their costs are equal to or greater than 65535. This is because IGP route convergence is faster than BGP route convergence.

```

[RouterB] display ip routing-table
Route Flags: R - relied, D - download to fib
  
```

```

-----
Routing Tables: Public
Destinations : 13          Routes : 13
Destination/Mask Proto Pre Cost Flags NextHop Interface
1.1.1.1/32 OSPF 10 65536 D 10.1.1.1 Pos1/0/0
2.2.2.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0
4.4.4.4/32 OSPF 10 65536 D 10.1.3.2 Pos2/0/0
10.1.1.0/30 Direct 0 0 D 10.1.1.2 Pos1/0/0
10.1.1.1/32 Direct 0 0 D 10.1.1.1 Pos1/0/0
10.1.1.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0
10.1.2.0/30 OSPF 10 65536 D 10.1.1.1 Pos1/0/0
10.1.3.0/30 Direct 0 0 D 10.1.3.1 Pos2/0/0
10.1.3.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
10.1.3.2/32 Direct 0 0 D 10.1.3.2 Pos2/0/0
10.1.4.0/30 OSPF 10 65536 D 10.1.3.2 Pos2/0/0
127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
  
```

View the routing table of Router B.

```

[RouterB] display ip routing-table
Route Flags: R - relied, D - download to fib
  
```

```

-----
Routing Tables: Public
Destinations : 15          Routes : 15
Destination/Mask Proto Pre Cost Flags NextHop Interface
2.2.2.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0
1.1.1.1/32 OSPF 10 2 D 10.1.1.1 Pos1/0/0
4.4.4.0/24 IBGP 255 0 RD 10.1.3.2 Pos2/0/0
4.4.4.4/32 OSPF 10 2 D 10.1.3.2 Pos2/0/0
5.5.5.0/24 EBGp 255 0 RD 10.2.1.2 Pos2/0/0
10.1.1.0/30 Direct 0 0 D 10.1.1.2 Pos1/0/0
10.1.1.1/32 Direct 0 0 D 10.1.1.1 Pos1/0/0
10.1.1.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0
10.1.2.0/30 OSPF 10 2 D 10.1.1.1 Pos1/0/0
10.1.3.0/30 Direct 0 0 D 10.1.3.1 Pos2/0/0
10.1.3.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
10.1.3.2/32 Direct 0 0 D 10.1.3.2 Pos2/0/0
10.1.4.0/30 OSPF 10 2 D 10.1.3.2 Pos2/0/0
10.1.4.1/32 BGP 255 0 RD 10.1.3.2 Pos2/0/0
10.2.1.0/30 BGP 255 0 RD 10.1.3.2 Pos2/0/0
10.2.1.2/32 BGP 255 0 RD 10.1.3.2 Pos2/0/0
10.3.1.0/30 BGP 255 0 RD 10.1.3.2 Pos2/0/0
  
```

As shown in the routing table, after BGP route convergence on Router B is complete, the contents of the routing information are the same as those before the router restarts.

----End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
router id 1.1.1.1
#
 interface Pos1/0/0
  link-protocol ppp
  undo shutdown
  ip address 10.1.1.1 255.255.255.252
#
 interface Pos2/0/0
  link-protocol ppp
  undo shutdown
  ip address 10.1.2.1 255.255.255.252
#
 interface LoopBack0
  ip address 1.1.1.1 255.255.255.255
#
bgp 10
 router-id 1.1.1.1
 peer 2.2.2.2 as-number 10
 peer 2.2.2.2 connect-interface LoopBack 0
 peer 3.3.3.3 as-number 10
 peer 3.3.3.3 connect-interface LoopBack 0
 peer 4.4.4.4 as-number 10
 peer 4.4.4.4 connect-interface LoopBack 0
#
ipv4-family unicast
 undo synchronization
 peer 2.2.2.2 enable
 peer 3.3.3.3 enable
 peer 4.4.4.4 enable
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.1.1.0 0.0.0.3
  network 10.1.2.0 0.0.0.3
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
router id 2.2.2.2
#
 interface Pos1/0/0
  link-protocol ppp
  undo shutdown
  ip address 10.1.1.2 255.255.255.252
#
 interface Pos2/0/0
  link-protocol ppp
  undo shutdown
  ip address 10.1.3.1 255.255.255.252
#
 interface LoopBack0
  ip address 2.2.2.2 255.255.255.255
#
```

```

    bgp 10
      router-id 2.2.2.2
      peer 1.1.1.1 as-number 10
      peer 1.1.1.1 connect-interface LoopBack 0
      peer 3.3.3.3 as-number 10
      peer 3.3.3.3 connect-interface LoopBack 0
      peer 4.4.4.4 as-number 10
      peer 4.4.4.4 connect-interface LoopBack 0
    #
    ipv4-family unicast
      undo synchronization
      peer 1.1.1.1 enable
      peer 3.3.3.3 enable
      peer 4.4.4.4 enable
    #
    ospf 1
      area 0.0.0.0
        network 10.1.1.0 0.0.0.3
        network 10.1.3.0 0.0.0.3
        network 2.2.2.2 0.0.0.0
    #
    return
  
```

● Configuration file of Router C

```

    #
    sysname RouterC
    #
    router id 3.3.3.3
    #
    interface Pos1/0/0
      link-protocol ppp
      undo shutdown
      ip address 10.1.4.1 255.255.255.252
    #
    interface Pos2/0/0
      link-protocol ppp
      undo shutdown
      ip address 10.1.2.2 255.255.255.252
    #
    interface LoopBack0
      ip address 3.3.3.3 255.255.255.255
    #
    bgp 10
      router-id 3.3.3.3
      peer 1.1.1.1 as-number 10
      peer 1.1.1.1 connect-interface LoopBack 0
      peer 2.2.2.2 as-number 10
      peer 2.2.2.2 connect-interface LoopBack 0
      peer 4.4.4.4 as-number 10
      peer 4.4.4.4 connect-interface LoopBack 0
    #
    ipv4-family unicast
      undo synchronization
      peer 1.1.1.1 enable
      peer 2.2.2.2 enable
      peer 4.4.4.4 enable
    #
    ospf 1
      area 0.0.0.0
        network 10.1.2.0 0.0.0.3
        network 10.1.4.0 0.0.0.3
        network 3.3.3.3 0.0.0.0
    #
    return
  
```

● Configuration file of Router D

```

    #
    sysname RouterD
    #
    router id 4.4.4.4
  
```

```
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.4.2 255.255.255.252
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.1.3.2 255.255.255.252
#
interface Pos3/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.2.1.1 255.255.255.252
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
bgp 10
 router-id 4.4.4.4
 peer 10.2.1.2 as-number 20
 peer 1.1.1.1 as-number 10
 peer 1.1.1.1 connect-interface LoopBack 0
 peer 2.2.2.2 as-number 10
 peer 2.2.2.2 connect-interface LoopBack 0
 peer 3.3.3.3 as-number 10
 peer 3.3.3.3 connect-interface LoopBack 0
#
ipv4-family unicast
 undo synchronization
 import-route direct
 import-route ospf 1
 peer 2.2.2.2 enable
 peer 1.1.1.1 enable
 peer 5.5.5.5 enable
 peer 10.2.1.2 enable
#
ospf 1
 area 0.0.0.0
 network 4.4.4.4 0.0.0.0
 network 10.1.3.0 0.0.0.3
 network 10.1.4.0 0.0.0.3
#
return
```

● Configuration file of Router E

```
#
 sysname RouterE
#
router id 5.5.5.5
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.2.1.2 255.255.255.252
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ip address 10.3.1.1 255.255.255.252
#
interface LoopBack0
 ip address 5.5.5.5 255.255.255.255
#
bgp 20
 router-id 5.5.5.5
 peer 10.2.1.1 as-number 10
#
ipv4-family unicast
```

```

undo synchronization
network 10.3.1.0 255.255.255.252
peer 10.2.1.1 enable
#
return

```

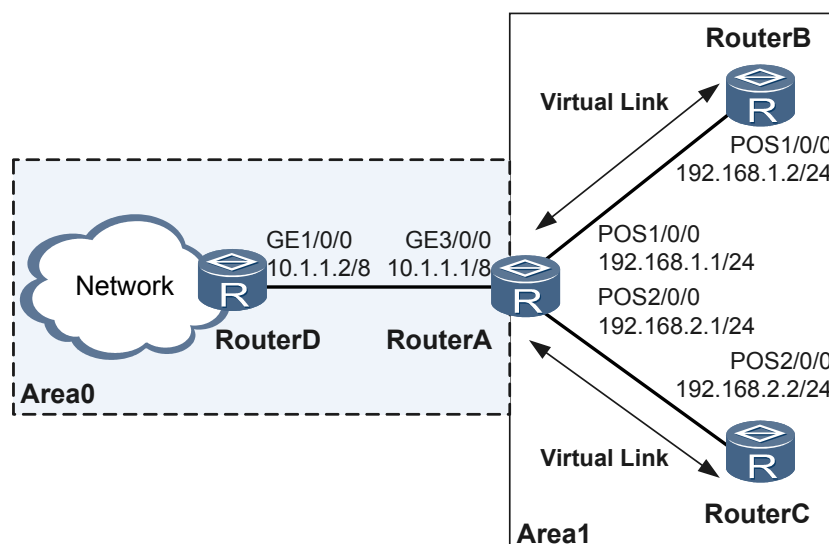
5.18.12 Example for Configuring OSPF GTSM

This part provides an example for configuring OSPF GTSM. Detailed operations include enabling GTSM on each router and specifying the valid TTL range of packets.

Networking Requirements

As shown on the network shown in [Figure 5-15](#), routers run OSPF and GTSM is enabled on Router A, Router B, and Router C.

Figure 5-15 Networking diagram of OSPF GTSM



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure OSPF.
2. Enable GTSM on each router and specify a valid TTL range for packets.

Data Preparation

To complete the configuration, you need the following data:

- OSPF process ID on each router
- Valid TTL range on each router

Procedure

Step 1 Configure an IP address for each interface. The configuration details are not mentioned here.

Step 2 Configure basic OSPF functions. The configuration details are not mentioned here.

Step 3 Configure OSPF GTSM.

On Router A, set the maximum valid TTL range for packets from Router A to other routers is 255 to 255.

```
[RouterA] ospf valid-ttl-hops 1
```

On Router B, set the maximum valid TTL range for packets from Router B to other routers is 254 to 255.

```
[RouterB] ospf valid-ttl-hops 2
```

On Router C, set the maximum valid TTL range for packets from Router C to other routers is 254 to 255.

```
[RouterC] ospf valid-ttl-hops 2
```

Step 4 Verify the configuration.

Check whether OSPF neighbor relationships between routers are successfully established. Take the display on Router C as an example. The neighbor relationship is **Full**, indicating that the neighbor relationship is successfully established.

```
[RouterC] display ospf peer
          OSPF Process 1 with Router ID 3.3.3.3
          Neighbors
          Area 0.0.0.0 interface 192.168.2.2(Pos1/0/0)'s neighbors
Router ID: 1.1.1.1      Address: 192.168.1.2
State: Full  Mode:Nbr is Master  Priority: 1
          DR: None  BDR: None  MTU: 0
          Dead timer due in 36 sec
          Retrans timer interval: 5
          Neighbor is up for 00:15:04
          Authentication Sequence: [ 0 ]
```

On Router C, run the **display gtsm statistics all** command. You can view GTSM statistics on Router C. The default behavior is **pass**, no illegal packets exist, and the number of discarded packets is 0.

```
<RouterC> display gtsm statistics all
GTSM Statistics Table
-----
```

SlotId	Protocol	Total Counters	Drop Counters	Pass Counters
1	BGP	0	0	0
1	BGPv6	0	0	0
1	OSPF	0	0	0
1	LDP	0	0	0
2	BGP	0	0	0
2	BGPv6	0	0	0
2	OSPF	0	0	0
2	LDP	0	0	0
3	BGP	0	0	0
3	BGPv6	0	0	0
3	OSPF	0	0	0
3	LDP	0	0	0
4	BGP	0	0	0
4	BGPv6	0	0	0
4	OSPF	0	0	0
4	LDP	0	0	0
5	BGP	0	0	0

5	BGPv6	0	0	0
5	OSPF	0	0	0
5	LDP	0	0	0
7	BGP	0	0	0
7	BGPv6	0	0	0
7	OSPF	0	0	0
7	LDP	0	0	0

 ----End

Configuration files

- Configuration file of Router A

```
#
 sysname RouterA
#
router id 1.1.1.1
#
 interface GigabitEthernet3/0/0
  undo shutdown
  ip address 10.1.1.1 255.0.0.0
#
 interface Pos1/0/0
  link-protocol ppp
  undo shutdown
  ip address 192.168.1.1 255.255.255.0
#
 interface Pos2/0/0
  link-protocol ppp
  undo shutdown
  ip address 192.168.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  vlink-peer 2.2.2.2
  vlink-peer 3.3.3.3
#
ospf valid-ttl-hops 1
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
router id 2.2.2.2
#
 interface Pos1/0/0
  link-protocol ppp
  undo shutdown
  ip address 192.168.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  vlink-peer 1.1.1.1
#
ospf valid-ttl-hops 2
#
return
```

- Configuration file of Router C

```
#
```

```
sysname RouterC
#
router id 3.3.3.3
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
ip address 192.168.2.2 255.255.255.0
#
ospf 1
 area 0.0.0.1
  network 192.168.2.0 0.0.0.255
  vlink-peer 1.1.1.1
#
ospf valid-ttl-hops 2
#
return
```

- Configuration file of Router D

```
#
sysname RouterD
#
router id 4.4.4.4
#
interface GigabitEthernet1/0/0
 undo shutdown
ip address 10.1.1.2 255.0.0.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.2 0.0.0.255
#
ospf valid-ttl-hops 3
#
return
```

6 OSPFv3 Configuration

About This Chapter

By building Open Shortest Path First Version 3 (OSPFv3) networks, you can enable OSPFv3 to discover and calculate routes in ASs. OSPFv3 is applicable to a large-scale network that consists of hundreds of routers.

[6.1 Introduction to OSPFv3](#)

The OSPFv3 protocol, which is a link-state IGP, runs on IPv6 networks.

[6.2 Configuring Basic OSPFv3 Functions](#)

Before building OSPFv3 networks, you need to configure basic OSPFv3 functions.

[6.3 Establishing or Maintaining OSPFv3 Neighbor Relationship](#)

By establishing and maintaining OSPFv3 neighbor relationships or adjacencies, you can build OSPFv3 networks.

[6.4 Configuring OSPFv3 Areas](#)

OSPFv3 supports stub areas and virtual links, the principle and applicable environment of which are similar to those in OSPFv2.

[6.5 Configuring OSPFv3 NSSA Areas](#)

By configuring areas as NSSA areas, external routes can be imported, and a new type of LSA, namely, Type 7 NSSA LSA is introduced.

[6.6 Configuring OSPFv3 Route Attributes](#)

By setting OSPFv3 route attributes, you can change OSPFv3 routing policies to meet the requirements of complex networks.

[6.7 Controlling OSPFv3 Routing Information](#)

This section describes how to control OSPF routing information. Detailed operations include configuring route aggregation, filtering the received routes, and importing external routes.

[6.8 Optimizing an OSPFv3 Network](#)

By configuring OSPFv3 functions in special network environments, you can adjust and optimize the OSPFv3 network performance.

[6.9 Configuration OSPFv3 GR](#)

By configuring OSPFv3 GR, you can avoid inaccurate route calculation and packet loss after an OSPFv3 router restarts.

6.10 Configuring BFD for OSPFv3

If there are high requirements for data transmission, and OSPFv3 convergence needs to be speeded up when the link status changes, you can configure BFD on OSPFv3 links. After detecting a link failure, BFD notifies the routing protocol of the failure, which triggers fast convergence. When the neighbor relationship is Down, the BFD session is deleted dynamically.

6.11 Configuring OSPFv3 IPsec

OSPFv3 IPsec provides a complete set of IPsec mechanisms to authenticate sent and received OSPFv3 packets, thus protecting devices against forged OSPFv3 packets.

6.12 Configuring the Network Management Function of OSPFv3

OSPFv3 supports the network management function. You can bind the OSPFv3 MIB to a certain OSPFv3 process.

6.13 Maintaining OSPFv3

Maintaining OSPFv3 and Debugging OSPFv3 involve resetting OSPFv3.

6.14 Configuration Examples

This section provides several configuration examples of OSPFv3 together with the configuration flowchart. The configuration examples explain networking requirements, configuration notes, and configuration roadmap.

6.1 Introduction to OSPFv3

The OSPFv3 protocol, which is a link-state IGP, runs on IPv6 networks.

6.1.1 OSPFv3

OSPFv3 uses the same implementation mechanism as OSPFv2 but is not compatible with OSPFv2.

The Open Shortest Path First Version 3.0 (OSPFv3) supports the version 6 of the Internet Protocol (IPv6). OSPFv3 conforms to RFC 2740 (OSPF for IPv6).

OSPFv3 and OSPFv2 have the following in common:

- 32-bit Router ID, Area ID, and Link State Advertisement (LSA) link-state ID
- Five types of packets such as Hello, Database Description (DD), Link State Request (LSR), Link State Update (LSU), and Link State Acknowledgement (LSAck) packets
- Neighbor discovery and adjacency establishment mechanisms
- Flooding and aging mechanisms of LSAs
- LSA types

OSPFv3 and OSPFv2 differ as follows:

- OSPFv3 runs based on a link; OSPFv2 runs based on a network segment.
- OSPFv3 can run multiple instances on the same link.
- The topology of OSPFv3 is independent of IPv6 address prefixes.
- OSPFv3 identifies its neighbors with the IPv6 link-local addresses.
- OSPFv3 has three new types of LSA flooding scopes.

6.1.2 OSPFv3 Features Supported by NE80E/40E

The NE80E/40E supports various OSPFv3 features, including multi-process and GR.

The NE80E/40E supports the following OSPFv3 features:

- Basic features stipulated in RFC 2740
- OSPFv3 stub areas
- OSPFv3 multi-process
- Multiple OSPFv3 processes can run on a router.
- OSPFv3 GR
 - If a router restarts or performs the active/standby switchover, it directly ages all the entries in the Forward Information Base (FIB). This interrupts the routing. The neighboring routers remove the router from the neighbor list and inform other routers of the router failure. Then, SPF needs to be calculated again. If the router recovers after a short period of time, the neighbor relationship becomes unstable. This results in route flapping.
 - If a router restarts because of abnormalities, you can enable OSPFv3 Graceful Restart (GR) to avoid service interruption during the restart of the router.

6.2 Configuring Basic OSPFv3 Functions

Before building OSPFv3 networks, you need to configure basic OSPFv3 functions.

6.2.1 Establishing the Configuration Task

You need to enable OSPFv3 and specify interfaces and area IDs before configuring other functions.

Applicable Environment

Enable the OSPFv3 process and specify its router ID before configuring OSPFv3; otherwise, other functions cannot take effect.

You must enable OSPFv3 and specify the interface and area ID before configuring other functions. OSPFv3 configurations, however, are independent of interface-related features.

Pre-configuration Tasks

Before configuring basic OSPFv3 functions, complete the following tasks:

- Making the network layers of the adjacent nodes accessible
- Enabling IPv6 capabilities

Data Preparation

To configure basic OSPFv3 functions, you need the following data.

No.	Data
1	Router ID
2	OSPFv3 process ID
3	Interfaces on which OSPFv3 needs to be enabled and their areas

6.2.2 Enabling OSPFv3

Creating an OSPFv3 process is a prerequisite for configuring all OSPFv3 features. By creating an OSPFv3 process, you can manually specify the router ID for a router.

Context

OSPFv3 supports multiple processes. Multiple OSPFv3 processes running on one router are differentiated by process IDs. OSPFv3 process ID is set when OSPFv3 is enabled and is only locally valid. It does not affect the packet exchange with other routers.

In the format of an IPv4 address, a router ID is a 32-bit unsigned integer that uniquely identifies a router within an AS. The router ID of OSPFv3 must be manually set. If no router ID is set, OSPFv3 fails to run normally.

When manually setting the router ID, ensure that the router IDs of any two routers in an AS are different. When multiple processes are enabled on a router, it is necessary to specify a unique route ID for each process.

To ensure the stable running of OSPFv3, you need to allocate router IDs and set them in network planning.

Do as follows on the router that runs OSPFv3.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ] [ vpn-instance vpn-instance-name ]
```

OSPFv3 is enabled and the OSPFv3 view is displayed.

Step 3 Run:

```
router-id router-id
```

A Router ID is set.

---End

6.2.3 Enabling OSPFv3 on an Interface

For an interface with multiple instances, you need to specify which instance of the interface is enabled in the OSPFv3 process when enabling OSPFv3 on the interface.

Context

After enabling OSPFv3 in the system view, you need to enable OSPFv3 on the interface.

Because an interface has multiple instances, you need to specify which instance of the interface is enabled in the OSPFv3 process when OSPFv3 is enabled on the interface. If no instance ID is specified, the value defaults to 0. The same instance must be enabled on the interfaces between which the neighbor relationship is set up.

Do as follows on the router that runs OSPFv3.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 (Optional) Run the **ospfv3 network-type** { **broadcast** | **nbma** | **p2mp** [**non-broadcast**] | **p2p** } [**instance** *instance-id*] command to configure the network type of an interface.

When an interface supports multi-instances, you must specify the value of *instance-id* when enabling OSPFv3 on the interface. If the value of *instance-id* is not specified, the default value 0 is adopted. In this case, the configured network type of an interface mismatches the actual network type of the interface. This step is mandatory in such a case.

Step 4 Run:

```
ospfv3 process-id area area-id [ instance instance-id ]
```

OSPFv3 is enabled on the interface.

The area ID can be a decimal integer or in the IPv4 address format, but it is displayed in the IPv4 address format.

----End

6.2.4 Entering the OSPFv3 Area View

By dividing an AS into different areas, specifying OSPFv3 interfaces, and specifying areas to which these interfaces belong, OSPFv3 can discover and calculate routes in an AS.

Context

You must configure the routers in the same area based on the area. Otherwise, the neighbor routers cannot exchange information with each other. The congestion of routing information or routing loop is thus caused.

Do as follows on the router that runs OSPFv3.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

Step 3 Run:

```
area area-id
```

The OSPFv3 area view is displayed.

The area ID can be a decimal integer or in the IPv4 address format, but it is displayed in the IPv4 address format.

An OSPFv3 area cannot be deleted directly. Only after all the configurations in the area view are removed and the status of the related interfaces in this area become Down, this area is automatically removed.

----End

6.2.5 Checking the Configuration

After basic OSPFv3 functions are configured, you can check OSPFv3 brief information, LSDB information, neighbor information, and OSPFv3 routing table.

Prerequisite

The configurations of the Basic OSPFv3 Functions are complete.

Procedure

- Run the **display ospfv3** [*process-id*] command to check the summary information about the OSPFv3 process.
- Run the **display ospfv3** [*process-id*] **interface** [**area** *area-id*] [*interface-type interface-number*] command to check the OSPFv3 interface information.
- Run the commands as follow to check the LSDB information about OSPFv3:
 - **display ospfv3** [*process-id*] **lsdb** [**area** *area-id*] [**originate-router** *advertising-router-id* | **self-originate**] [{ **router** | **network** | **inter-router** [**asbr-router** *asbr-router-id*] | { **inter-prefix** | **nssa** } [*ipv6-address prefix-length*] | **link** | **intra-prefix** | **grace** } [*link-state-id*]]
 - **display ospfv3** [*process-id*] **lsdb** [**originate-router** *advertising-router-id* | **self-originate**] **external** [*ipv6-address prefix-length*] [*link-state-id*]
- Run the **display ospfv3** [*process-id*] [**area** *area-id*] **peer** [*interface-type interface-number* [**verbose**] | *neighbor-id*] command to check the information about the OSPFv3 neighbor.
- Run the commands as follow to check the OSPFv3 routing table:
 - **display ospfv3** [*process-id*] **routing uninstalled**
 - **display ospfv3** [*process-id*] **routing** [**abr-routes** | **asbr-routes** | **statistics** [**uninstalled**] | *ipv6-address prefix-length* | **intra-routes** | **inter-routes** | **ase-routes** | **nssa-routes**]
- Run the **display ospfv3** [*process-id*] **path** command to check the paths to a destination address.
- Run the **display default-parameter ospfv3** command to check the default OSPFv3 configuration.

----End

6.3 Establishing or Maintaining OSPFv3 Neighbor Relationship

By establishing and maintaining OSPFv3 neighbor relationships or adjacencies, you can build OSPFv3 networks.

6.3.1 Establishing the Configuration Task

When setting parameters on an interface, ensure that these parameters are consistent with those on the adjacent router.

Applicable Environment

In applications, establishing or maintaining the OSPFv3 neighbor relationship is a premise for the construction of an OSPFv3 network. After the configuration in this section, you can:

- Adjust the convergence speed of the OSPFv3 network and network load posed by protocol packets by modifying OSPFv3 timers.
- Enable OSPFv3 to be disconnected from its neighbor when the number of OSPFv3 packet retransmissions exceeds the threshold by configuring Retransmission Limitation for OSPF (RL-OSPF) of OSPFv3. This prevents non-stop packet retransmissions if the neighbor does not receive packets.
- Speed up the convergence of an OSPFv3 network by adjusting the intervals for updating and receiving LSAs.

Pre-configuration Tasks

Before establishing or maintaining the OSPFv3 neighbor relationship, complete the following tasks:

- Enabling IPv6 capability
- [Configuring Basic OSPFv3 Functions](#)

Data Preparation

To establish or maintain the OSPFv3 neighbor relationship, you need the following data.

No.	Data
1	Interval for sending Hello packets
2	Dead time of the neighbor relationship
3	Interval for retransmitting LSAs to adjacent routers
4	Delay in sending LSAs

6.3.2 Configuring the Interval for Sending Hello Packets

By adjusting the Hello interval set on OSPFv3 neighbors, you can change the speed of establishing the neighbor relationship, thus changing the speed of network convergence.

Context

Hello packets are periodically sent to the neighbor router to detect and maintain the neighbor relationship and to elect the DR and the BDR. RFC 2328 requires that the Hello timer values of neighbors be consistent. The value of the Hello timer is inversely proportional to the route convergence speed and network load.

Do as follows on the router that runs OSPFv3.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospfv3 timer hello interval [ instance instance-id ]
```

The interval for sending Hello packets is set on the interface.

----End

6.3.3 Configuring Dead Time of Neighbor Relationship

If a router does not receive a Hello packet from its neighbor within the Holddown time, the router considers the neighbor relationship invalid.

Context

If a router does not receive any Hello packet from its neighbor during a specified period, the neighbor router is considered invalid. The specified period is called the dead time of the neighbor relationship. The dead time must be at least four times the Hello interval on an interface.

Do as follows on the router that runs OSPFv3.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospfv3 timer dead interval [ instance instance-id ]
```

The dead time of the neighbor relationship is specified.

----End

6.3.4 Configuring the Interval for Retransmitting LSAs to Neighboring Routers

After a router sends an LSA to its neighbor, the router expects to receive an LSAck packet from its neighbor. If the router does not receive an LSAck packet within the LSA retransmission interval, it retransmits the LSA to the neighbor.

Context

Do as follows on the router that runs OSPFv3.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospfv3 timer retransmit interval [ instance instance-id ]
```

The interval for retransmitting LSAs to the adjacent routers is set.

The value of *seconds* must be greater than the time taken to transmit a packet between two routers.

 **NOTE**

Do not set a value which is too small, for the interval between LSA retransmissions. Otherwise, unnecessary retransmissions may occur.

----End

6.3.5 Configuring the Delay for Transmitting LSAs on the Interface

It takes time to transmit OSPFv3 packets on a link. Therefore, a certain delay is added to the aging time of an LSA before the LSA is sent.

Context

The LSA ages out in the LSDB of a local router instead of in the transmission process. You need to set the delay for an LSA before sending it. For a low-speed network, this configuration is necessary.

Do as follows on the router that runs OSPFv3.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospfv3 trans-delay interval [ instance instance-id ]
```

The delay in transmitting LSAs on the interface is set.

----End

6.3.6 Checking the Configuration

After OSPFv3 neighbor relationships or adjacencies are stable, you can check OSPFv3 interface information and neighbor information.

Prerequisite

The configurations of the Establishing or Maintaining OSPFv3 Neighbor Relationship are complete.

Procedure

- Run the **display ospfv3** [*process-id*] **interface** [**area area-id**] [*interface-type interface-number*] command to check the OSPFv3 interface information.

----End

6.4 Configuring OSPFv3 Areas

OSPFv3 supports stub areas and virtual links, the principle and applicable environment of which are similar to those in OSPFv2.

6.4.1 Establishing the Configuration Task

Configuring a stub area is optional. Not all areas can be configured as stub areas. Generally, a stub area, which is located at the AS boundary, is a non-backbone area with only one ABR.

Applicable Environment

To reduce the number of LSAs in the network and enhance OSPFv3 extensibility, define OSPFv3 areas. For some non-backbone areas at the edge of ASs, you can define them as stub areas for further reducing the size of the routing table and the number of LSAs.

The current NE80E/40E version does not support OSPFv3 NSSA areas.

Pre-configuration Tasks

Before configuring OSPFv3 area attributes, complete the following tasks:

- Enabling IPv6 capability
- [Configuring Basic OSPFv3 Functions](#)

Data Preparation

To configure OSPFv3 area attributes, you need the following data.

No.	Data
1	Areas to be defined as stub areas
2	Metrics of default routes sent to stub areas

6.4.2 Configuring OSPFv3 Stub Areas

A stub area is a special area in which ABRs do not flood the received AS external routes. Thus, the number of LSAs is greatly reduced.

Context

Do as follows on each router that runs OSPFv3 in the stub area:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

Step 3 Run:

```
area area-id
```

The OSPFv3 area view is displayed.

Step 4 Run:

```
stub [ no-summary ]
```

The area is configured as a stub area.

Step 5 (Optional) Run:

```
default-cost cost
```

The cost of the default route sent to the stub area is set.

By default, the cost of the default route sent to the stub area is 1.

This command is configured on the ABR of the stub area only to set the cost of the default route to be sent to the stub area. This command does not need to be configured on other routers in the stub area.

The parameter **no-summary** takes effect only when the **stub** command is configured on the ABR. If this parameter is configured, the ABR only sends the summary-LSA of a default route to the stub area without originating other summary-LSAs. The stub area without AS-external-LSAs or Summary-LSAs is called a totally stub area.

----End

6.4.3 Configuring OSPFv3 Virtual Links

You can establish the logical connectivity between backbone areas and the non-backbone areas that are not physically connected to the backbone area.

Context

After OSPFv3 areas are defined, OSPFv3 route update between non-backbone areas is implemented through a backbone area. Then, OSPFv3 requires that all non-backbone areas

should maintain the connectivity with the backbone area and the backbone area should maintain its own connectivity. In actual applications, this requirement may not be met because of some restrictions. To solve this problem, you can configure OSPFv3 virtual links.

A virtual link must be configured at both ends of the link; otherwise, it does not take effect.

Do as follows on the router that runs OSPFv3.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

Step 3 Run:

```
area area-id
```

The OSPFv3 area view is displayed.

Step 4 Run:

```
vlink-peer router-id [ hello hello-interval | retransmit retransmit-interval |  
trans-delay trans-delay-interval | dead dead-interval | ipsec sa sa-name |  
instance instance-id ] *
```

A virtual link is created and configured.

----End

6.4.4 Checking the Configuration

After OSPFv3 area attributes are configured, you can check the OSPFv3 LSDB, routing table, and virtual links.

Prerequisite

The configurations of the OSPFv3 Areas are complete.

Procedure

- Run the commands as follow to check the LSDB information about OSPFv3:
 - **display ospfv3** [process-id] **lsdb** [area area-id] [originate-router advertising-router-id | self-originate] [{ router | network | inter-router [asbr-router asbr-router-id] | { inter-prefix | nssa } [ipv6-address prefix-length] | link | intra-prefix | grace } [link-state-id]]
 - **display ospfv3** [process-id] **lsdb** [originate-router advertising-router-id | self-originate] **external** [ipv6-address prefix-length] [link-state-id]
- Run the commands as follow to check the OSPFv3 routing table:
 - **display ospfv3** [process-id] **routing uninstalled**

- **display ospfv3** [*process-id*] **routing** [**abr-routes** | **asbr-routes** | **statistics** [**uninstalled**] | *ipv6-address prefix-length* | **intra-routes** | **inter-routes** | **ase-routes** | **nssa-routes**]
- Run the **display ospfv3** [*process-id*] **vlink** command to check the information about OSPFv3 virtual links.

----End

6.5 Configuring OSPFv3 NSSA Areas

By configuring areas as NSSA areas, external routes can be imported, and a new type of LSA, namely, Type 7 NSSA LSA is introduced.

6.5.1 Establishing the Configuration Task

NSSAs are introduced because stub areas cannot import external routes. An NSSA allows the transmission of Type 7 LSAs.

Applicable Environment

An NSSA allows the transmission of Type 7 LSAs, which are generated by ASBRs in an NSSA. The Type 7 LSAs converting into Type 5 LSAs in the NSSA and advertised to other areas.

Pre-configuration Tasks

Before configuring an OSPFv3 NSSA, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- **Configuring basic OSPFv3 functions**

Data Preparation

To configure an OSPFv3 NSSA, you need the following data.

No.	Data
1	Cost of the default route sent to an NSSA

6.5.2 Defining the Current Area to Be an NSSA Area

Derived from a stub area, an NSSA allows AS external routes to be imported; an ASBR advertises Type 7 NSSA LSAs in the local NSSA.

Context

Do as follows on the OSPFv3 router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 process view is displayed.

Step 3 Run:

```
area area-id
```

The OSPFv3 area view is displayed.

Step 4 Run:

```
nssa [ default-route-advertise [ cost cost | type type | tag tag ] * | no-import-  
route | no-summary | translator-always | translator-interval translator-interval |  
set-n-bit ] *
```

An area is configured as an NSSA.

----End

Follow-up Procedure

To connect routers to an NSSA, you need to run the **nssa** command to configure NSSA attributes for the area to which the routers belong.

The area may be updated after NSSA attributes are configured or deleted. Thus, the NSSA attributes can be re-configured or deleted only after the last update of NSSA attributes is complete.

6.5.3 Checking the Configuration

After OSPFv3 NSSAs are configured, you can check OSPFv3 routing table information.

Prerequisite

The configurations of OSPFv3 NSSAs are complete.

Procedure

- Run the **display ospfv3 area** command to check information about OSPFv3 areas.
- Run the commands as follow to check the OSPFv3 routing table.
 - **display ospfv3 [process-id] routing uninstalled**
 - **display ospfv3 [process-id] routing [abr-routes | asbr-routes | statistics [uninstalled] | ipv6-address prefix-length | intra-routes | inter-routes | ase-routes | nssa-routes]**

----End

6.6 Configuring OSPFv3 Route Attributes

By setting OSPFv3 route attributes, you can change OSPFv3 routing policies to meet the requirements of complex networks.

6.6.1 Establishing the Configuration Task

Before configuring OSPFv3 route attributes, familiarize yourself with the applicable environment, complete pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

In actual applications, to meet the requirements of a complicated networking environment, you can change OSPFv3 routing policies by configuring OSPFv3 route attributes. Through the following procedures, you can:

- Set the cost on the OSPFv3 interface.
- Configure load balancing among equal-cost routes.

Pre-configuration Tasks

Before configuring OSPFv3 route attributes, complete the following tasks:

- Enabling IPv6 capability
- [Configuring Basic OSPFv3 Functions](#)

Data Preparation

To configure OSPFv3 route attributes, you need the following data.

No.	Data
1	Link cost
2	Maximum number of equal-cost routes

6.6.2 Setting the Cost of the OSPFv3 Interface

OSPFv3 can automatically calculate the link cost for an interface according to the interface bandwidth. You can also set the link cost for the interface by using the related command.

Context

You can control route calculation by setting the link cost of OSPFv3 on different interfaces.

Do as follows on the router that runs OSPFv3.

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`interface interface-type interface-number`
The interface view is displayed.
- Step 3** Run:
`ospfv3 cost cost [instance instance-id]`
The cost is set on the OSPFv3 interface.
By default, the link cost on an OSPFv3 interface is 1.
----End


6.6.3 Setting the Maximum Number of Equal-Cost Routes

If the destinations and costs of the multiple routes discovered by one routing protocol are the same, load balancing can be performed among these routes.

Context

Do as follows on the router that runs OSPFv3:

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`ospfv3 [process-id]`
The OSPFv3 view is displayed.
- Step 3** Run:
`maximum load-balancing number`
The maximum number of equal-cost routes is set.
The value is an integer ranging from 1 to 3. The default value is 3.
-  **NOTE**
The range and default value of the number of equal-cost routes may vary with products and protocols. You can adjust the range and default value of the number of equal-cost routes after purchasing the License.
- End

6.6.4 Checking the Configuration

After OSPFv3 route attributes are configured, you can check the OSPFv3 interface, LSDB, and routing table.

Prerequisite

The configurations of the OSPFv3 Route Attributes are complete.

Procedure

- Run the **display ospfv3**[*process-id*] **interface** [**area** *area-id*] [*interface-type interface-number*] command to check the OSPFv3 interface information.
- Run the commands as follow to check the LSDB information about OSPFv3:
 - **display ospfv3** [*process-id*] **lsdb** [**area** *area-id*] [**originate-router** *advertising-router-id* | **self-originate**] [{ **router** | **network** | **inter-router** [**asbr-router** *asbr-router-id*] | { **inter-prefix** | **nssa** } [*ipv6-address prefix-length*] | **link** | **intra-prefix** | **grace** } [*link-state-id*]]
 - **display ospfv3** [*process-id*] **lsdb** [**originate-router** *advertising-router-id* | **self-originate**] **external** [*ipv6-address prefix-length*] [*link-state-id*]
- Run the commands as follow to check the OSPFv3 routing table:
 - **display ospfv3** [*process-id*] **routing uninstalled**
 - **display ospfv3** [*process-id*] **routing** [**abr-routes** | **asbr-routes** | **statistics** [**uninstalled**] | *ipv6-address prefix-length* | **intra-routes** | **inter-routes** | **ase-routes** | **nssa-routes**]

---End

6.7 Controlling OSPFv3 Routing Information

This section describes how to control OSPF routing information. Detailed operations include configuring route aggregation, filtering the received routes, and importing external routes.

6.7.1 Establishing the Configuration Task

Before controlling OSPFv3 routing information, familiarize yourself with the applicable environment, complete pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

Through the configuration in this section, you can control the advertising and receiving of OSPFv3 routing information and configure OSPFv3 to import external routes.

Pre-configuration Tasks

Before controlling OSPFv3 routing information, complete the following tasks:

- Enabling IPv6 capability
- **Configuring Basic OSPFv3 Functions**

Data Preparation

To control OSPFv3 routing information, you need the following data.

No.	Data
1	Prefix of IPv6 routes after aggregation
2	Filtering list or name used to filter routing information
3	Link cost on an OSPFv3 interface
4	Maximum number of equal-cost routes
5	Name, process ID, and metric of external routes to be imported

6.7.2 Configuring OSPFv3 Route Aggregation

An ABR can summarize routes with the same prefix into one LSA and advertise the summarized route in other areas. An ASBR can also summarize imported routes with the same prefix into one LSA and then advertise the summarized route to other areas. This can reduce the size of the LSDB in other areas.

Context

If multiple continuous network segments exist in this area, use the **abr-summary** command to summarize them into one network segment. In this way, the ABR only sends an LSA after summarization. No LSA that belongs to the summarization network segment is separately transmitted, thus reducing the LSDB size of other areas.

When a large number of routes are imported, use the **asbr-summary** command to summarize the imported routes and set the delay for advertising the summarized route. In this manner, the summarized route advertised each time contains more valid routing information, and network flapping caused by incorrect routing information is avoided.

Procedure

- Configure route summarization on an ABR.

Do as follows on the ABR that runs OSPFv3:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

3. Run:

```
area area-id
```

The OSPFv3 area view is displayed.

4. Run:

```
abr-summary ipv6-address prefix-length [ cost cost | not-advertise ]*
```

Route summarization is configured in the OSPFv3 area.

cost *cost* set the cost of a summarized route. By default, the cost of a summarized route is the maximum cost among those of routes that are summarized. The value ranges from 1 to 16777214.

If **not-advertise** is set, no routing information of the network segment is advertised.

- Configure route summarization on an ASBR.

Do as follows on the ASBR that runs OSPFv3:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

3. Run:

```
asbr-summary ipv6-address prefix-length [ cost cost | tag tag | not-  
advertise | distribute-delay interval ] *
```

Route summarization is configured on the ASBR.

cost *cost* specifies the cost of a summarized route. By default, the cost of a summarized route is the maximum cost among those of routes that are summarized. The value ranges from 1 to 16777214.

tag *tag* specifies the tag used to control route advertisement. The value of this parameter ranges from 1 to 4294967295.

If **not-advertise** is specified in the command, the summarized IPv6 route that matches a specified IPv6 prefix or prefix length is not advertised.

distribute-delay *interval* specifies the delay for advertising a summarized route.

----End

6.7.3 Configuring OSPFv3 to Filter the Received Routes

By configuring filtering conditions for routing information, you can allow only the routes that pass the filtering to be received or advertised.

Context

After receiving LSAs, OSPFv3 determines whether to add the calculated routes to the local routing table according to the filtering policy.

Do as follows on the router that runs OSPFv3.

Procedure

- Step 1** Run:

```
system-view
```

The system view is displayed.

- Step 2** Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

Step 3 Run:

```
filter-policy { acl6-number | acl6-name acl6-name | ipv6-prefix ipv6-prefix-name }  
import
```

OSPFv3 is configured to filter the imported routes.

----End

6.7.4 Configuring OSPFv3 to Import External Routes

Importing the routes discovered by other routing protocols can enrich OSPFv3 routing information.

Context

Because OSPFv3 is a link state-based routing protocol and cannot directly filter the advertised LSAs, OSPFv3 must filter the routes when importing them. Then, only the routes that pass the filtering can be advertised.

Do as follows on the router that runs OSPFv3.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

Step 3 Run:

```
default { cost cost | tag tag | type type } *
```

The default cost of the imported route is set.

Step 4 Run:

```
import-route protocol [ process-id ] [ cost cost | type type | tag tag | route-  
policy route-policy-name ] *
```

External routes are imported.

Step 5 (Optional) Run:

```
default-route-advertise [ always | cost cost | type type | tag tag | route-policy  
route-policy-name ] *
```

Default routes are advertised to the OSPFv3 route area.

Step 6 (Optional) Run:

```
filter-policy { acl6-number | acl6-name acl6-name | ipv6-prefix ipv6-prefix-name }  
export [ protocol [ process-id ] ]
```

The imported external routes are filtered.

After you run the **import-route** command on an OSPFv3 router to import external routes, the router becomes an ASBR.

You can configure OSPFv3 to filter a certain type of routing information by specifying the *protocol*. If *protocol* is not specified, OSPFv3 filters all the imported routes.

 **NOTE**

The **filter-policy** command takes effect only on the routes imported through the **import-route** command by the ASBR, that is, filters the imported routes. The routes that are filtered out do not generate LSAs and cannot be advertised by OSPFv3. If the **import-route** command is not configured to import other external routes (including OSPFv3 routes in different processes), the **filter-policy** command does not take effect.

----End

6.7.5 Checking the Configuration

After OSPFv3 route attributes are configured, you can check the OSPFv3 interface, LSDB, and routing table.

Prerequisite

The configurations of Controlling OSPFv3 Routing Information are complete.

Procedure

- Run the commands as follow to check the OSPFv3 route aggregation:
 - **display ospfv3** [*process-id*] **abr-summary-list** [*ipv6-address prefix-length*]
 - **display ospfv3** [*process-id*] **asbr-summary** [*ipv6-address prefix-length*] [**verbose**]
- Run the commands as follow to check the LSDB information about OSPFv3:
 - **display ospfv3** [*process-id*] **lsdb** [**area** *area-id*] [**originate-router** *advertising-router-id* | **self-originate**] [{ **router** | **network** | **inter-router** [**asbr-router** *asbr-router-id*] | { **inter-prefix** | **nssa** } [*ipv6-address prefix-length*] | **link** | **intra-prefix** | **grace** } [*link-state-id*]
 - **display ospfv3** [*process-id*] **lsdb** [**originate-router** *advertising-router-id* | **self-originate**] **external** [*ipv6-address prefix-length*] [*link-state-id*]
- Run the commands as follow to check the OSPFv3 routing table:
 - **display ospfv3** [*process-id*] **routing uninstalled**
 - **display ospfv3** [*process-id*] **routing** [**abr-routes** | **asbr-routes** | **statistics** [**uninstalled**] | *ipv6-address prefix-length* | **intra-routes** | **inter-routes** | **ase-routes** | **nssa-routes**]

----End

6.8 Optimizing an OSPFv3 Network

By configuring OSPFv3 functions in special network environments, you can adjust and optimize the OSPFv3 network performance.

6.8.1 Establishing the Configuration Task

Before optimizing an OSPFv3 network, familiarize yourself with the applicable environment, complete pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

By adjusting the OSPFv3 timer, you can change the convergence speed of an OSPFv3 network and the network overload caused by protocol packets. On low-speed links, you need to consider the delay in transmitting LSAs on the interface. By adjusting the SPF calculation interval, you can mitigate resource consumption due to frequent network changes.

You can specify the DR priority of an interface to affect the DR/BDR election in a broadcast network.

Pre-configuration Tasks

Before optimizing an OSPFv3 network, complete the configuration tasks:

- Enabling IPv6 capability
- **Configuring Basic OSPFv3 Functions**

Data Preparation

To optimize an OSPF network, you need the following data.

No.	Data
1	Values of OSPFv3 timers
2	Values of SPF timers
3	DR priority of the interface

6.8.2 Configuring the SPF Timer

By setting the interval for SPF calculation, you can reduce resource consumption caused by frequent network changes.

Context

Whenever the LSDB of OSPFv3 changes, the shortest path should be recalculated. Calculating the shortest path each time the LSDB changes consumes enormous resources and lowers the efficiency of a router.

Adjusting the SPF delay and hold interval can suppress frequent network changes to avoid resource consumption.

Do as follows on the router that runs OSPFv3.

Procedure

- Configure an SPF normal timer.

Do as follows on the router that runs OSPFv3:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

3. Run:

```
spf timers delay-interval hold-interval
```

An SPF normal timer is configured.

- Configure an SPF intelligent timer.

Do as follows on the router that runs OSPFv3:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

3. Run:

```
spf-schedule-interval { delay-interval hold-interval | intelligent-timer  
max-interval start-interval hold-interval }
```

An SPF intelligent timer is configured.

NOTE

An SPF normal timer and an SPF intelligent timer are mutually exclusive.

----End

6.8.3 Setting the Interval for Receiving LSAs

Setting the interval for receiving LSAs prevents unnecessary LSA updates.

Context

When a network is instable, control the minimum interval for receiving the same LSA update. To prevent unnecessary LSA updates caused by network changes, by default, set the interval for receiving the same LSA update to 1000ms.

Do as follows on the router that runs OSPFv3.

Procedure

- Step 1** Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

Step 3 Run:

```
lsa-arrival-interval arrival-interval
```

The interval for receiving LSAs is set.

arrival-interval is an integer ranging from 1 to 10000, in milliseconds. By default, the interval for receiving LSAs is 1000ms.

----End

6.8.4 Configuring an Intelligent Timer for Generating LSAs

Configuring an intelligent timer for generating LSAs speeds up network convergence.

Context

Setting the millisecond-level interval for generating the same LSA speeds up network convergence. When a network becomes instable, reduce the interval for generating the same LSA by using an intelligent timer.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

Step 3 Run:

```
lsa-originate-interval intelligent-timer max-interval start-interval hold-interval
```

The interval for generating the same LSA is set.

max-interval specifies the maximum interval for updating LSAs. The value ranges from 1 to 10000, in milliseconds.

start-interval specifies the initial interval for updating LSAs. The value ranges from 0 to 1000, in milliseconds.

hold-interval specifies the hold interval for updating LSAs. The value ranges from 1 to 5000, in milliseconds.

By default, the maximum interval for updating LSAs is 5000ms, the initial interval for updating LSAs is 0ms, the hold interval for updating LSAs is 5000ms.

----End

6.8.5 Suppressing an Interface from Sending and Receiving OSPFv3 Packets

By suppressing the OSPFv3 interface from receiving and sending OSPFv3 packets, you can prevent routers on a certain network from obtaining OSPFv3 routing information and prevent the local router from receiving routing information from other routers.

Context

To prevent a router from advertising routes to the router on a certain network and from importing the routes of other routers, you can suppress the interface on which OSPFv3 is enabled from receiving and sending OSPFv3 packets.

Do as follows on the router that runs OSPFv3.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

Step 3 Run:

```
silent-interface interface-type interface-number
```

The interface is suppressed from sending and receiving OSPFv3 packets.

----End

Follow-up Procedure

Different processes can suppress the same interface from sending and receiving OSPFv3 packets, but the **silent-interface** command is valid only for the OSPFv3 interface on which the specified process is enabled, and does not take effect on the interface of other processes.

After an OSPFv3 interface is set to be silent, the interface can still advertise its direct routes through the Intra-Area-Prefix-LSA of the same router. No OSPFv3 neighbor relationship can be set up on the interface. Therefore, the OSPFv3 adaptability is enhanced.

6.8.6 Configuring DR Priority of an Interface

When configuring a broadcast network or an NBMA network, you can specify the DR priority for each interface to change the results of DR/BDR election on the network.

Context

The DR priority on a router interface qualifies the interface for the DR election. If the DR priority is 0, the router cannot be elected as a DR or BDR.

Do as follows on the router that runs OSPFv3.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospfv3 dr-priority priority [ instance instance-id ]
```

The DR priority of the interface is set.

---End

Follow-up Procedure

After the DR priority is changed, you can re-elect a DR or BDR through the following methods, which, however, will result in the interruption of the OSPFv3 neighbor relationship between routers and therefore are used only when necessary.

- Restarting all routers.
- Running the **shutdown** and **undo shutdown** commands on the interface on which the OSPFv3 neighbor relationship is set up.

6.8.7 Configuring Stub Routers

When a router has a heavy load and cannot forward any other packets, you can configure it as a stub router. After the router is configured as a stub router, other OSPF routers do not use this router to forward data but they can have a route to this stub router.

Context

A stub router is used to control traffic. It notifies OSPFv3 routers not to forward data by the stub router, but they can have a route to the stub router.

Do as follows on the router that runs OSPFv3:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 process view is displayed.

Step 3 Run:

```
stub-router [ on-startup [ interval ] ]
```

The stub router is configured.

 **NOTE**

There is no correlation between the stub router configured through this command and the router in the stub area.

----End

6.8.8 Ignoring MTU Check on DD Packets

By disabling an interface from checking the MTU field in the received DD packet, you can enable an OSPFv3 router to receive the packet with the MTU field being 0.

Context

Do as follows on the router that runs OSPFv3:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospfv3 mtu-ignore [ instance instance-id ]
```

The MTU check on DD packets is ignored.

After the command is used, the interface does not check the MTU field of a received DD packet.

----End

6.8.9 Checking the Configuration

After an OSPFv3 network is optimized, you can check the OSPFv3 interface, LSDB, and routing table.

Prerequisite

The configurations of Optimizing an OSPFv3 Network are complete.

Procedure

- Run the **display ospfv3** [*process-id*] **interface** [**area** *area-id*] [*interface-type interface-number*] command to check the OSPFv3 interface information.
- Run the commands as follow to check the LSDB information about OSPFv3:
 - **display ospfv3** [*process-id*] **lsdb** [**area** *area-id*] [**originate-router** *advertising-router-id* | **self-originate**] [{ **router** | **network** | **inter-router** [**asbr-router** *asbr-router-id*] | { **inter-prefix** | **nssa** } [*ipv6-address prefix-length*] | **link** | **intra-prefix** | **grace** } [*link-state-id*]]

- **display ospfv3** [*process-id*] **lsdb** [**originate-router** *advertising-router-id* | **self-originate**] **external** [*ipv6-address prefix-length*] [*link-state-id*]
 - Run the commands as follow to check the OSPFv3 routing table:
 - **display ospfv3** [*process-id*] **routing uninstalled**
 - **display ospfv3** [*process-id*] **routing** [**abr-routes** | **asbr-routes** | **statistics** [**uninstalled**] | *ipv6-address prefix-length* | **intra-routes** | **inter-routes** | **ase-routes** | **nssa-routes**]
- End

6.9 Configuration OSPFv3 GR

By configuring OSPFv3 GR, you can avoid inaccurate route calculation and packet loss after an OSPFv3 router restarts.

6.9.1 Establishing the Configuration Task

By default, the OSPFv3 GR capability and Helper capability are disabled.

Applicable Environment

To prevent route flapping and service interruption due to the restart of OSPFv3, you can enable OSPFv3 GR.

After OSPFv3 restarts, the GR restarter and the GR helper keep the neighbor relationship, exchange routing information, synchronize the database, and update the routing table and the forwarding table. OSPFv3 fast convergence is thus realized.

Pre-configuration Tasks

Before configuring OSPFv3 GR, complete the following task:

- [Configuring Basic OSPFv3 Functions](#)

Data Preparation

To optimize an OSPF network, you need the following data.

No.	Data
1	OSPFv3 process ID
2	Filtering rule of the helper mode of OSPFv3 peers

6.9.2 Enabling OSPFv3 GR

After an OSPFv3 process restarts through GR, the Restarter and the Helper reestablish the neighbor relationship, exchange routing information, synchronize the LSDB, and update the routing table and forwarding table. This implements OSPFv3 fast convergence and stabilizes the network topology.

Context

Do as follows on the router that runs OSPFv3:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 process-id
```

The OSPFv3 view is displayed.

Step 3 Run:

```
graceful-restart [ period period | ack-time time | retransmit-interval interval |  
lsa-checking-ignore | planned-only ] *
```

OSPFv3 GR is enabled.

By default, OSPFv3 GR is disabled.

ack-time is optional. After **ack-time** is specified, the restarter can discover more neighbors in the *time* period.

---End

6.9.3 Enabling the Helper of OSPFv3 GR

The GR Helper, which is a neighbor of the GR Restarter, can identify GR signaling, maintain the adjacency with the Restarter during the active/standby switchover of the Restarter, and help the Restarter to restore the network topology.

Context

Do as follows on the router that runs OSPFv3:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 process-id
```

The OSPFv3 view is displayed.

Step 3 Run:

```
helper-role [ { ip-prefix ip-prefix-name | acl-number acl-number | acl-name acl-  
name } | max-grace-period period | planned-only | lsa-checking-ignore ] *
```

The helper of OSPFv3 GR is enabled.

By default, the helper of OSPFv3 GR is disabled.

----End

6.9.4 Check the Configuration

After OSPFv3 GR is configured, you can check GR information.

Prerequisite

The configurations of OSPFv3 GR are complete.

Procedure

- Run the **display ospfv3 [process-id] graceful-restart-information** command to check the status of OSPFv3 GR.

----End

Example

Run the **display ospfv3 graceful-restart-information** command, and you can view that the local router is enabled with GR.

```
<HUAWEI> display ospfv3 graceful-restart-information

      OSPFv3 Router with ID (0.0.0.0) (Process 1)
Graceful-restart capability      : enabled
Graceful-restart support        : planned and unplanned, strict lsa check
Grace-Period Configured         : 120 Sec
Last Restart-exit Reason        : none

Helper capability                : enabled
Helper support                   : planned and unplanned, strict lsa check
Max Grace-Period Configured     : 1800 Sec
Last Helper-exit Reason         : none
```

6.10 Configuring BFD for OSPFv3

If there are high requirements for data transmission, and OSPFv3 convergence needs to be speeded up when the link status changes, you can configure BFD on OSPFv3 links. After detecting a link failure, BFD notifies the routing protocol of the failure, which triggers fast convergence. When the neighbor relationship is Down, the BFD session is deleted dynamically.

6.10.1 Establishing the Configuration Task

Before configuring BFD for OSPFv3, familiarize yourself with the applicable environment, complete pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

To increase the convergence speed of OSPFv3 when the link status changes, you can configure BFD on OSPFv3 links.

BFD keeps track of liveness of network links and detects any faults in the links much faster than the normal keep-alive protocols. When OSPFv3 is associated with BFD sessions, link

failures are notified immediately to OSPFv3 by BFD and OSPFv3 can take actions to perform route calculation and converge in the new network topology.

Pre-configuration Tasks

Before configuring BFD in OSPFv3, complete the following task:

- **Configuring Basic OSPFv3 Functions**

Data Preparation

To configure BFD for OSPFv3, you need the following data.

No.	Data
1	OSPFv3 process ID
2	Minimum Transmission Interval
3	Minimum Receive Interval
4	Detect Multiplier

6.10.2 Enabling BFD for OSPFv3

On the two routers that need to establish a BFD session, you can configure BFD for all the interfaces in a certain OSPFv3 process.

Context

Do as follows on the router that runs OSPFv3:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 process-id
```

The OSPFv3 view is displayed.

Step 3 Run:

```
bfd all-interfaces enable
```

BFD for OSPFv3 is enabled to establish a BFD session.

By default, BFD is disabled at OSPFv3 process level.

----End

6.10.3 Configuring OSPFv3 BFD Parameters at Process Level

After enabling BFD for OSPFv3, you need to configure BFD parameters in the OSPFv3 process.

Context

Do as follows on the router that runs OSPFv3:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 process-id
```

The OSPFv3 view is displayed.

Step 3 Run:

```
bfd all-interfaces { min-transmit-interval min-transmit-value | min-receive-  
interval min-receive-value | detect-multiplier detect-multiplier-value } *
```

OSPFv3 BFD parameters are configured.

By default, BFD parameters are not configured at OSPFv3 process level.

----End

6.10.4 Enabling OSPFv3 BFD at Interface Level

You can configure BFD on a specified interface for fast link failure detection.

Context

Do as follows on the router that runs OSPFv3:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospfv3 bfd enable [ instance instance-id ]
```

OSPFv3 BFD is enabled on the interface.

By default, OSPFv3 BFD is disabled at interface level.

----End

6.10.5 Configuring OSPFv3 BFD Parameters at Interface Level

After enabling BFD for OSPFv3 on an interface, you need to configure BFD parameters on the interface.

Context

Do as follows on the router that runs OSPFv3:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospfv3 bfd { min-transmit-interval min-transmit-value | min-receive-interval min-  
receive-value | detect-multiplier detect-multiplier-value } * [ instance instance-  
id ]
```

OSPFv3 BFD parameters are configured at interface level.

By default, OSPFv3 BFD parameters are not configured.

----End

6.10.6 Checking the Configuration

After BFD for OSPFv3 is configured, you can check information about the BFD session.

Prerequisite

The BFD is enabled and configured for OSPFv3.

Procedure

- Run the **display ospfv3** [*process-id*] **bfd session** [*interface-type interface-number*] [*neighbor-id*] [**verbose**] command to check the BFD session information.

----End

6.11 Configuring OSPFv3 IPsec

OSPFv3 IPsec provides a complete set of IPsec mechanisms to authenticate sent and received OSPFv3 packets, thus protecting devices against forged OSPFv3 packets.

6.11.1 Establishing the Configuration Task

Before configuring OSPFv3 IPsec, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task correctly and quickly.

Applicable Environment

OSPFv3 IPsec uses a complete set of IPsec mechanisms to authenticate sent and received OSPFv3 packets, thus protecting devices against pseudo OSPFv3 packets.

Pre-configuration Tasks

Before configuring OSPFv3 IPsec, complete the following tasks:

- [Configuring Basic OSPFv3 Functions](#)

Data Preparation

To configure OSPFv3 IPsec, you need the following data.

No.	Data
1	Security protocol
2	Authentication algorithms used by AH
3	Authentication algorithm used by ESP
4	Encapsulation algorithm used by ESP
5	AH security parameter indexes used for protecting incoming and outgoing traffic
6	ESP security parameter indexes used for protecting incoming and outgoing traffic
7	AH authentication key (in the format of a string) used for protecting incoming and outgoing traffic
8	ESP authentication key (in the format of a string) used for protecting incoming and outgoing traffic
9	AH authentication key (in the hexadecimal format) used for protecting incoming and outgoing traffic
10	ESP authentication key (in the hexadecimal format) used for protecting incoming and outgoing traffic
11	ESP encapsulation key (in the hexadecimal format) used for protecting incoming and outgoing traffic

6.11.2 Enabling IPsec in an OSPFv3 Process

An SA configured in an OSPFv3 process is used to authenticate packets of the process.

Context

Do as follows on the router that runs OSPFv3:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

Step 3 Run:

```
ipsec sa sa-name
```

An SA is configured in the OSPFv3 process.

An OSPFv3 process can be associated with multiple OSPFv3 areas. An SA applied in the OSPFv3 process can be used in the associated areas.

----End

6.11.3 Enabling IPsec in an OSPFv3 Area

An SA configured in an OSPFv3 area is used to authenticated the packets of the area.

Context

Do as follows on the router that runs OSPFv3:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

Step 3 Run:

```
area area-id
```

The OSPFv3 area view is displayed.

Step 4 Run:

```
ipsec sa sa-name
```

An SA is configured in the OSPFv3 area.

 **NOTE**

The SA configured on an OSPFv3 area takes precedence over that configured in an OSPFv3 process.

----End

6.11.4 Enabling IPsec on an Interface

An SA configured on an interface is used to authenticate the packets sent and received by the interface.

Context

Do as follows on the router that runs OSPFv3:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
ospfv3 ipsec sa sa-name
```

An SA is configured on the interface.

 **NOTE**

The SA configured on an OSPFv3 interface takes precedence over that configured in an OSPFv3 process and an OSPFv3 area.

----End

6.11.5 Enabling IPsec on the Virtual Link

An SA configured on the Virtual Link is used to authenticate the packets sent and received on the Virtual Link.

Context

Do as follows on the router that runs OSPFv3:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ]
```

The OSPFv3 view is displayed.

Step 3 Run:

```
area area-id
```

The OSPFv3 area view is displayed.

Step 4 Run:

```
vlink-peer router-id ipsec sa sa-name
```

An SA is configured to authenticate the packets sent and received on the Virtual Link.



NOTE

The SA configured on a virtual link takes precedence over that configured in an OSPFv3 process and OSPFv3 area 0.

---End

6.11.6 Enabling IPsec on the Sham Link

An SA configured on a sham link is used to authenticate the packets sent and received on the sham link.

Context

Do as follows on the router that runs OSPFv3:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 [ process-id ] vpn-instance [ vpn-instance-name ]
```

The OSPFv3 view is displayed.

Step 3 Run:

```
area area-id
```

The OSPFv3 area view is displayed.

Step 4 Run:

```
sham-link source-address destination-address ipsec sa sa-name
```

An SA is configured on the sham link.



NOTE

The SA configured on a sham link takes precedence over that configured in an OSPFv3 process and OSPFv3 area 0.

---End

6.11.7 Checking the Configuration

After configuring OSPFv3 IPsec, you can view the information about SAs configured in an OSPFv3 process, OSPFv3 area, OSPFv3 interface, OSPFv3 virtual link, and OSPFv3 sham link.

Prerequisite

All configurations of the OSPFv3 IPsec are complete.

Do as follows on the router that runs OSPFv3.

Procedure

- Run the **display ospfv3** [*process-id*] command to view the SA applied in a specified process.
- Run the **display ospfv3** [*process-id*] **interface** command to view the SA applied on a specified interface.
- Run the **display ospfv3** [*process-id*] **area** [*area-id*] command to view the SA applied in a specified area.
- Run the **display ospfv3** [*process-id*] **vlink** command to view the SA applied on the peer end of a virtual link.
- Run the **display ospfv3** [*process-id*] **sham-link** command to view the SA applied on the peer end of a sham link.

----End

Example

Run the **display ospfv3** command, and you can view the SA configured in an OSPFv3 process. For example:

```
<HUAWEI> display ospfv3
Routing Process "OSPFv3 (1)" with ID 0.0.0.0
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
Stub router capability: enabled
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of FULL neighbors 0
Number of Exchange and Loading neighbors 0
Maximum ASE LS ID 1 and Unused list Count 0
Number of LSA originated 0
Number of LSA received 0
SPF Count          : 0
Non Refresh LSA    : 0
Non Full Nbr Count : 0
Number of areas in this router is 1
IP security association configured: sa1
```

Run the **display ospfv3 area** command, and you can view the SA configured in an OSPFv3 area. For example:

```
<HUAWEI> display ospfv3 area
OSPFv3 Process (1)
Area BACKBONE(0) Status: down
Number of interfaces in this area is 0
SPF algorithm executed 0 times
Number of LSA 0. Checksum Sum 0x0000
Number of Unknown LSA 0
Area Bdr Router count: 0
Area ASBdr Router count: 0
IP security association configured: sa1
Area 0.0.0.1 Status: up
Number of interfaces in this area is 1
SPF algorithm executed 3 times
Number of LSA 4. Checksum Sum 0x23AC8
```

```

Number of Unknown LSA 0
Area Bdr Router count: 0
Area ASBdr Router count: 1
IP security association configured: sa4
    
```

Run the **display ospfv3 interface** command, and you can view the SA configured in an OSPFv3 interface. For example:

```

<HUAWEI> display ospfv3 interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 is up, line protocol is up
Interface ID 518
IPv6 Prefixes
FE80::1441:0:E213:1 (Link-Local Address)
2000:1::1
OSPFv3 Process (1), Area 0.0.0.1, Instance ID 0
Router ID 2.2.2.2, Network Type POINTOPOINT, Cost: 1562
Transmit Delay is 1 sec, State Point-To-Point, Priority 1
No designated router on this link
No backup designated router on this link
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
IP security association configured: sa1
IP security association applied: sa1
    
```

Run the **display ospfv3 vlink** command, and you can view the SA configured on an OSPFv3 virtual link. For example:

```

<HUAWEI> display ospfv3 vlink
Virtual Link VLINK1 to router 1.1.1.1 is up
Transit area 0.0.0.1 via interface Pos1/0/0, instance ID 0
Local address 2000:1::1
Remote address 2001:1:1::1
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Adjacency state Full
IP security association configured: sa1
IP security association applied: sa1
    
```

Run the **display ospfv3 sham-link** command, and you can view the SA configured on an OSPFv3 sham link. For example:

```

<HUAWEI> display ospfv3 sham-link
OSPFv3 Process (10)
Sham Link SHAM-LINK1 to router 0.0.0.0 is down
Area 0.0.0.1, via Interface *, Instance ID 0, cost 1
Source address 1::1
Destination address 2::2
Interface ID 0x80000002
Sham-Link Interface Events: 0
Sham-Link Interface LsaCount: 0
Sham-Link Interface Lsa Checksum: 0x0
Transmit Delay is 1 sec, State Down
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:00
Adjacency state Down
IP security association configured: sa1
IP security association applied: sa1
    
```

6.12 Configuring the Network Management Function of OSPFv3

OSPFv3 supports the network management function. You can bind the OSPFv3 MIB to a certain OSPFv3 process.

6.12.1 Establishing the Configuration Task

Before configuring the network management function for OSPFv3, familiarize yourself with the applicable environment, complete pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

OSPFv3 supports the network management function. You can bind OSPFv3 MIB and a certain OSPFv3 process. In addition, OSPFv3 also supports the trap function and the log function.

Pre-configuration Tasks

Before configuring the network management function of OSPFv3, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- [Configuring Basic OSPFv3 Functions](#)

Data Preparation

None.

6.12.2 Configuring OSPFv3 MIB Binding

The MIB is a virtual database of the device status maintained by the managed devices.

Context

When multiple OSPFv3 processes are enabled, you can configure OSPFv3 MIB to select the process to be processed, that is, that is, configure OSPFv3 MIB to select the process to which it is bound.

Do as follows on the OSPFv3 router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ospfv3 mib-binding process-id
```

OSPFv3 MIB binding is configured.

----End

6.12.3 Configuring OSPFv3 Trap

Traps are the notifications sent from a router to inform the NMS of the fault detected by the system.

Context

Do as follows on the OSPFv3 router.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
snmp-agent trap enable feature-name ospfv3 { non-excessive all | trap-name  
{ ifconfigerror | ifrxbadpacket | ifstatechange | nbrrestarthelperstatuschange |  
nbrstatechange | nssatranslatorstatuschange | restartstatuschange |  
virtifconfigerror | virtifrxbadpacket | virtifstatechange |  
virtnbrrestarthelperstatuschange | virtnbrstatechange } }
```

The trap function for the OSPFv3 module is enabled.

To enable all non-excessive traps of OSPFv3 module, you can run the **non-excessive all** command; to enable the traps of one or more events, you can specify **type-name**.

---End

6.12.4 Check the Configuration

After the network management function is configured for OSPFv3, you can check the contents of the information channel, and information recorded in the information center, log buffer, and trap buffer.

Prerequisite

The configurations of the Network Management Function of OSPFv3 are complete.

Procedure

- Run the **display current-configuration** command to check the configuration parameters currently validated on the router.

---End

6.13 Maintaining OSPFv3

Maintaining OSPFv3 and Debugging OSPFv3 involve resetting OSPFv3.

6.13.1 Resetting OSPFv3

Restarting OSPFv3 can reset OSPFv3. In addition, you can reset OSPFv3 through GR.

Context



CAUTION

The OSPFv3 adjacency is removed when you reset the OSPFv3 connection by using the **reset ospfv3** command. So, confirm the action before you use the command.

After modifying the OSPFv3 routing policy or protocol, reset the OSPFv3 connection to validate the modification. To reset OSPFv3 connections, run the following **reset ospfv3** command in the user view.

Procedure

- To validate the new configuration, run the following commands:
 - **reset ospfv3** { *process-id* | **all** } [**graceful-restart** [**extend-period** *period*]]
 - **reset ospfv3** { *process-id* | **all** } **counters** [**neighbor** [*interface-type interface-number*] [*router-id*]]

----End

6.14 Configuration Examples

This section provides several configuration examples of OSPFv3 together with the configuration flowchart. The configuration examples explain networking requirements, configuration notes, and configuration roadmap.

Follow-up Procedure



NOTE

This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.

6.14.1 Example for Configuring OSPFv3 Areas

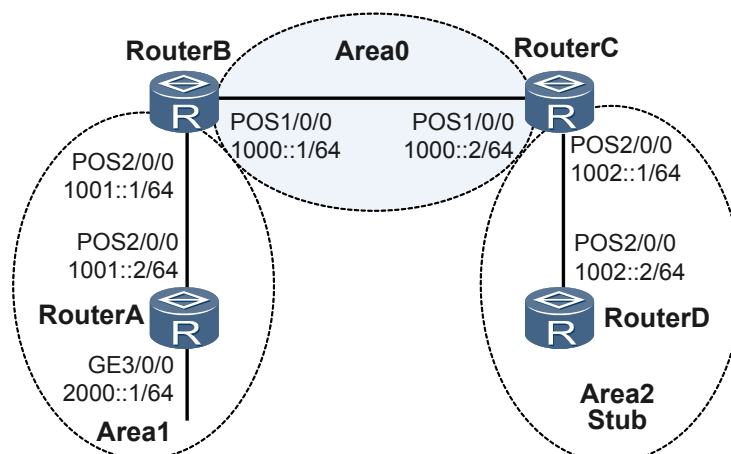
This part provides an example for configuring basic OSPFv3 functions. Detailed operations include enabling OSPFv3 on each router and specifying network segments in different areas.

Networking Requirements

As shown in **Figure 6-1**, all routers run OSPFv3. The entire autonomous system is divided into three areas. Router B and Router C serve as ABRs to forward the inter-area routes.

It is required that Area 2 be configured as a stub area to decrease the LSAs advertised to this area, without affecting route reachability.

Figure 6-1 Networking diagram of configuring OSPFv3 areas



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic OSPFv3 function on each router.
2. Configure Area 2 as a stub area and check the OSPFv3 routing table of Router D.
3. Configure Area 2 as a totally stub area and check the OSPFv3 routing table of Router D.

Data Preparation

To complete the configuration, you need the following data:

- Router ID of Router A as 1.1.1.1 of Area 1
- Router ID of Router B as 2.2.2.2 of Areas 0 and 1
- Router ID of Router C as 3.3.3.3 of Areas 0 and 2
- Router ID of Router D as 4.4.4.4 of Area 2

Procedure

Step 1 Assign an IPv6 address for each interface.

The details are not mentioned here.

Step 2 Configure basic OSPFv3 functions.

Configure Router A.

```
[RouterA] ipv6
[RouterA] ospfv3
[RouterA-ospfv3-1] router-id 1.1.1.1
[RouterA-ospfv3-1] quit
[RouterA] interface GigabitEthernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ospfv3 1 area 1
[RouterA-GigabitEthernet3/0/0] quit
[RouterA] interface pos2/0/0
[RouterA-Pos2/0/0] ospfv3 1 area 1
[RouterA-Pos2/0/0] quit
```

Configure Router B.

```
[RouterB] ipv6
[RouterB] ospfv3
[RouterB-ospfv3-1] router-id 2.2.2.2
[RouterB-ospfv3-1] quit
[RouterB] interface pos1/0/0
[RouterB-Pos1/0/0] ospfv3 1 area 0
[RouterB-Pos1/0/0] quit
[RouterB] interface pos2/0/0
[RouterB-Pos2/0/0] ospfv3 1 area 1
[RouterB-Pos2/0/0] quit
```

Configure Router C.

```
[RouterC] ipv6
[RouterC] ospfv3
[RouterC-ospfv3-1] router-id 3.3.3.3
[RouterC-ospfv3-1] quit
[RouterC] interface pos 1/0/0
[RouterC-Pos1/0/0] ospfv3 1 area 0
[RouterC-Pos1/0/0] quit
[RouterC] interface pos 2/0/0
[RouterC-Pos2/0/0] ospfv3 1 area 2
[RouterC-Pos2/0/0] quit
```

Configure Router D.

```
[RouterD] ipv6
[RouterD] ospfv3
[RouterD-ospfv3-1] router-id 4.4.4.4
[RouterD-ospfv3-1] quit
[RouterD] interface interface pos 2/0/0
[RouterD-Pos2/0/02/0/0] ospfv3 1 area 2
[RouterD-Pos2/0/02/0/0] quit
```

Display the OSPFv3 neighbors of Router B.

```
[RouterB] display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.1)
Neighbor ID      Pri   State           Dead Time   Interface   Instance ID
1.1.1.1          1    Full/ -         00:00:34   PosS2/0/0   0
OSPFv3 Area (0.0.0.0)
Neighbor ID      Pri   State           Dead Time   Interface   Instance ID
3.3.3.3          1    Full/ -         00:00:32   PosS1/0/0   0
```

Display OSPFv3 neighbors of Router C.

```
[RouterC] display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID      Pri   State           Dead Time   Interface   Instance ID
2.2.2.2          1    Full/ -         00:00:37   Pos1/0/0    0
OSPFv3 Area (0.0.0.2)
Neighbor ID      Pri   State           Dead Time   Interface   Instance ID
4.4.4.4          1    Full/ -         00:00:33   Pos2/0/0    0
```

Display the OSPFv3 routing table of Router D.

```
[RouterD] display ospfv3 routing
OSPFv3 Process (1)
Destination                                     Metric
Next-hop
IA 1000::/64                                     2
    via FE80::1572:0:5EF4:1, Pos2/0/0
IA 1001::/64                                     3
    via FE80::1572:0:5EF4:1, Pos2/0/0
1002::/64                                       1
    directly-connected, Pos2/0/0
```

```
IA 2000::/64                                     4
    via FE80::1572:0:5EF4:1, Pos2/0/0
```

Step 3 Configure stub areas.

Configure the stub area of Router D.

```
[RouterD] ospfv3
[RouterD-ospfv3-1] area 2
[RouterD-ospfv3-1-area-0.0.0.2] stub
[RouterD-ospfv3-1-area-0.0.0.2] quit
```

Configure the stub area of Router C, and set the cost of the default route advertised to the stub area to 10.

```
[RouterC] ospfv3
[RouterC-ospfv3-1] area 2
[RouterC-ospfv3-1] stub
[RouterC-ospfv3-1] default-cost 10
[RouterC-ospfv3-1-area-0.0.0.2] quit
```

Display the OSPFv3 routing table of Router D, and you can view a new default route in the routing table. Its cost is the sum of the cost of the directly connected routes and the configured cost.

```
[RouterD] display ospfv3 routing
OSPFv3 Process (1)
  Destination                                     Metric
  Next-hop
IA ::/0                                           11
    via FE80::1572:0:5EF4:1, Pos2/0/0
IA 1000::/64                                       2
    via FE80::1572:0:5EF4:1, Pos2/0/0
IA 1001::/64                                       3
    via FE80::1572:0:5EF4:1, Pos2/0/0
    1002::/64                                       1
    directly-connected, Pos2/0/0
IA 2000::/64                                       4
    via FE80::1572:0:5EF4:1, Pos2/0/0
```

Step 4 Configure totally stub areas.

Configure Router C and configure Area 2 as a totally stub area.

```
[RouterC] ospfv3
[RouterC-ospfv3-1] area 2
[RouterC-ospfv3-1-area-0.0.0.2] stub no-summary
[RouterC-ospfv3-1-area-0.0.0.2] quit
```

Step 5 Verify the configuration.

Display the OSPFv3 routing table of Router D, and you can view that the entries in the routing table decrease; other non-directly connected routes are suppressed; only the default route is reserved.

```
[RouterD] display ospfv3 routing
OSPFv3 Process (1)
  Destination                                     Metric
  Next-hop
IA ::/0                                           11
    via FE80::1572:0:5EF4:1, Pos2/0/0
    1002::/64                                       1
    directly-connected, Pos2/0/0
```

----End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
 ipv6
#
 interface GigabitEthernet3/0/0
  undo shutdown
  ipv6 enable
  ipv6 address 2000::1/64
  ospfv3 1 area 0.0.0.1
#
 interface Pos2/0/0
  link-protocol ppp
  undo shutdown
  ipv6 enable
  ipv6 address 1001::2/64
  ospfv3 1 area 0.0.0.1
#
 ospfv3 1
  router-id 1.1.1.1
  area 0.0.0.1
#
 return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
 ipv6
#
 interface Pos1/0/0
  link-protocol ppp
  undo shutdown
  ipv6 enable
  ipv6 address 1000::1/64
  ospfv3 1 area 0.0.0.0
#
 interface Pos2/0/0
  link-protocol ppp
  undo shutdown
  ipv6 enable
  ipv6 address 1001::1/64
  ospfv3 1 area 0.0.0.1
#
 ospfv3 1
  router-id 2.2.2.2
  area 0.0.0.0
  area 0.0.0.1
#
 return
```

- Configuration file of Router C

```
#
 sysname RouterC
#
 ipv6
#
 interface Pos1/0/0
  link-protocol ppp
  undo shutdown
  ipv6 enable
  ipv6 address 1000::2/64
  ospfv3 1 area 0.0.0.0
#
 interface Pos2/0/0
  link-protocol ppp
```

```

undo shutdown
ipv6 enable
ipv6 address 1002::1/64
ospfv3 1 area 0.0.0.2
#
ospfv3 1
router-id 3.3.3.3
area 0.0.0.0
area 0.0.0.2
stub no-summary
default-cost 10
#
return
    
```

- Configuration file of Router D

```

#
sysname RouterD
#
ipv6
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ipv6 enable
ipv6 address 1002::2/64
ospfv3 1 area 0.0.0.2
#
ospfv3 1
router-id 4.4.4.4
area 0.0.0.2
stub
#
return
    
```

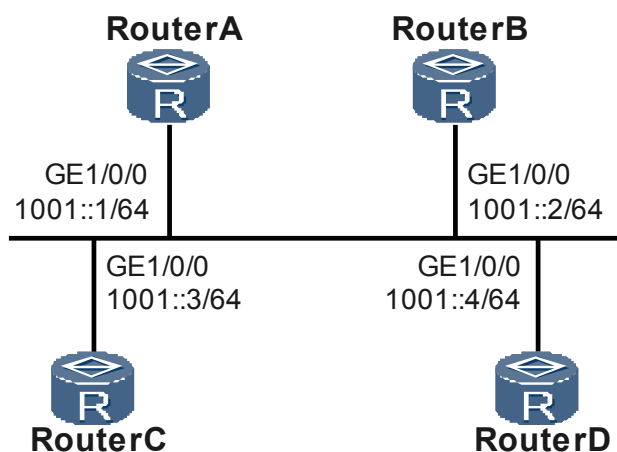
6.14.2 Example for Configuring OSPFv3 DR Election

This part provides an example for setting the DR priority on an interface for DR election on a broadcast network.

Networking Requirements

In [Figure 6-2](#), Router A has a DR priority of 100, which is the highest in the network, so it is elected as the DR. Router C has the second highest priority, so it is elected as the BDR. The priority of Router B is 0 so that it cannot be elected as the DR. Router D does not have a priority and the priority is 1 by default.

Figure 6-2 Networking diagram of configuring OSPFv3 DR election



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the router ID on each router, enable OSPFv3, and specify the network segment.
2. Check the DR/BDR status with the default priority.
3. Configure the DR priority on the interface and check the DR/BDR status.

Data Preparation

To complete the configuration, you need the following data:

- Router ID of Router A as 1.1.1.1; DR priority as 100
- Router ID of Router B as 2.2.2.2; DR priority as 0
- Router ID of Router C as 3.3.3.3; DR priority as 2
- Router ID of Router D as 4.4.4.4; DR priority as 1

Procedure

Step 1 Assign an IPv6 address for each interface.

The details are not mentioned here.

Step 2 Configure basic OSPFv3 functions.

Configure Router A, enable OSPFv3, and set its router ID to 1.1.1.1.

```
[RouterA] ipv6
[RouterA] ospfv3
[RouterA-ospfv3-1] router-id 1.1.1.1
[RouterA-ospfv3-1] quit
[RouterA] interface GigabitEthernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ospfv3 1 area 0
[RouterA-GigabitEthernet1/0/0] quit
```

Configure Router B, enable OSPFv3, and set its Router ID to 2.2.2.2.

```
[RouterB] ipv6
[RouterB] ospfv3
[RouterB-ospfv3-1] router-id 2.2.2.2
[RouterB-ospfv3-1] quit
[RouterB] interface GigabitEthernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ospfv3 1 area 0
[RouterB-GigabitEthernet1/0/0] quit
```

Configure Router C, enable OSPFv3, and set its Router ID to 3.3.3.3.

```
[RouterC] ipv6
[RouterC] ospfv3
[RouterC-ospfv3-1] router-id 3.3.3.3
[RouterC-ospfv3-1] quit
[RouterC] interface GigabitEthernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ospfv3 1 area 0
[RouterC-GigabitEthernet1/0/0] quit
```

Configure Router D, enable OSPFv3, and set its Router ID to 4.4.4.4.

```
[RouterD] ipv6
[RouterD] ospfv3
```

```
[RouterD-ospfv3-1] router-id 4.4.4.4
[RouterD-ospfv3-1] quit
[RouterD] interface GigabitEthernet 1/0/0
[RouterD-GigabitEthernet1/0/0] ospfv3 1 area 0
[RouterD-GigabitEthernet1/0/0] quit
```

Display the neighbors of Router A. You can view the DR priority (its default value is 1) and the neighbor status. Router D is the DR and Router C is the BDR.

 **NOTE**

The router with the greater router ID is the DR when routers have the same priority. If a certain Ethernet interface of a router becomes a DR, the other broadcast interfaces of the router have the highest priority in DR election. That is, the DR router is elected as the DR.

```
[RouterA] display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID      Pri  State                Dead Time  Interface  Instance ID
2.2.2.2          1   2-Way/DROther        00:00:32  GE1/0/0    0
3.3.3.3          1   Full/Backup          00:00:36  GE1/0/0    0
4.4.4.4          1   Full/DR               00:00:38  GE1/0/0    0
```

Display the neighbors of Router D, and you can view that all neighbors of Router D are in the Full state.

```
[RouterD] display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID      Pri  State                Dead Time  Interface  Instance ID
1.1.1.1          1   Full/DROther         00:00:32  GE1/0/0    0
2.2.2.2          1   Full/DROther         00:00:35  GE1/0/0    0
3.3.3.3          1   Full/Backup          00:00:30  GE1/0/0    0
```

Step 3 Set the DR priority of the interface.

Set the DR priority of Router A to 100.

```
[RouterA] interface GigabitEthernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ospfv3 dr-priority 100
[RouterA-GigabitEthernet1/0/0] quit
```

Set the DR priority of Router B to 0.

```
[RouterB] interface GigabitEthernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ospfv3 dr-priority 0
[RouterB-GigabitEthernet1/0/0] quit
```

Set the DR priority of Router C to 2.

```
[RouterC] interface GigabitEthernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ospfv3 dr-priority 2
[RouterC-GigabitEthernet1/0/0] quit
```

Display the neighbors of Router A, and you can view that the DR priority is updated and the DR and BDR remain unchanged.

```
[RouterA] display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID      Pri  State                Dead Time  Interface  Instance ID
2.2.2.2          0   2-Way/DROther        00:00:34  GE1/0/0    0
3.3.3.3          2   Full/Backup          00:00:38  GE1/0/0    0
4.4.4.4          1   Full/DR               00:00:31  GE1/0/0    0
```

Display the neighbors of Router D, and you can view that Router D remains as the DR.

```
[RouterD] display ospfv3 peer
OSPFv3 Process (1)
```

```
OSPFv3 Area (0.0.0.0)
Neighbor ID      Pri   State           Dead Time   Interface   Instance ID
1.1.1.1          100  Full/DROther    00:00:36   GE1/0/0     0
2.2.2.2          0    Full/DROther    00:00:30   GE1/0/0     0
3.3.3.3          2    Full/Backup     00:00:36   GE1/0/0     0
```

Step 4 Re-elect the DR/BDR.

Restart all routers (or run the **shutdown** and **undo shutdown** commands on the interface that establishes the OSPFv3 neighbor relationship), and make OSPFv3 re-elect the DR/BDR.

Step 5 Verify the configuration.

Display the neighbors of Router A, and you can view that Router C is the BDR.

```
[RouterA] display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID      Pri   State           Dead Time   Interface   Instance ID
2.2.2.2          0    Full/DROther    00:00:31   GE1/0/0     0
3.3.3.3          2    Full/Backup     00:00:36   GE1/0/0     0
4.4.4.4          1    Full/DROther    00:00:39   GE1/0/0     0
[RouterA]
```

Display the neighbors of Router D, and you can view that Router A is the DR.

```
[RouterD] display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID      Pri   State           Dead Time   Interface   Instance ID
1.1.1.1          100  Full/DR         00:00:39   GE1/0/0     0
2.2.2.2          0    2-Way/DROther  00:00:35   GE1/0/0     0
3.3.3.3          2    Full/Backup     00:00:39   GE1/0/0     0
```

---End

Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
ipv6
#
interface GigabitEthernet1/0/0
undo shutdown
ipv6 enable
ipv6 address 1001::1/64
ospfv3 1 area 0.0.0.0
ospfv3 dr-priority 100
#
ospfv3 1
router-id 1.1.1.1
area 0.0.0.0
#
return
```

- Configuration file of Router B

```
#
sysname RouterB
#
ipv6
#
interface GigabitEthernet1/0/0
undo shutdown
ipv6 enable
ipv6 address 1001::2/64
ospfv3 1 area 0.0.0.0
```

```

ospfv3 dr-priority 0
#
ospfv3 1
router-id 2.2.2.2
area 0.0.0.0
#
return
    
```

- Configuration file of Router C

```

#
sysname RouterC
#
ipv6
#
interface GigabitEthernet1/0/0
undo shutdown
ipv6 enable
ipv6 address 1001::3/64
ospfv3 1 area 0.0.0.0
ospfv3 dr-priority 2
#
ospfv3 1
router-id 3.3.3.3
area 0.0.0.0
#
return
    
```

- Configuration file of Router D

```

#
sysname RouterD
#
ipv6
#
interface GigabitEthernet1/0/0
undo shutdown
ipv6 enable
ipv6 address 1001::4/64
ospfv3 1 area 0.0.0.0
#
ospfv3 1
router-id 4.4.4.4
area 0.0.0.0
#
return
    
```

6.14.3 Example for Configuring OSPFv3 Virtual Links

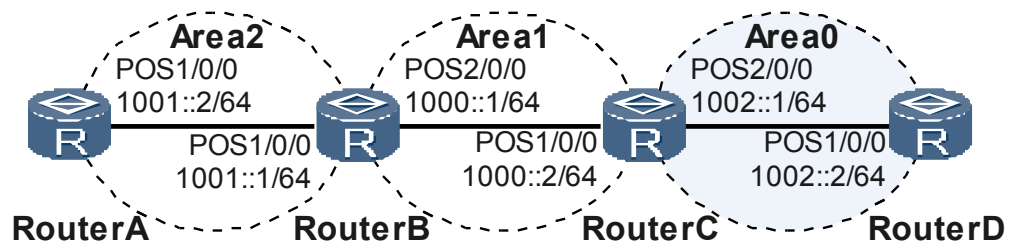
This part provides an example for configuring virtual links to connect non-backbone areas to the backbone area.

Networking Requirements

As shown in [Figure 6-3](#), all the routers run OSPFv3, and the entire autonomous system is divided into three areas. Both Router B and Router C serve as ABRs to forward routes between areas. Area 2 is not connected to the backbone Area 0 directly. Area 1 is the transit area that connects Area 0 and Area 2.

It is required to configure a virtual link in Area 1 on Router B and Router C by the virtual link, making the route from Router A to Router D reachable.

Figure 6-3 Networking diagram of configuring OSPFv3 virtual links



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic OSPFv3 functions on each router.
2. Configure virtual links on Router B and Router C to connect backbone networks to other networks.

Data Preparation

To complete the configuration, you need the following data:

- Router ID of Router A as 1.1.1.1 of Area 2
- Router ID of Router B as 2.2.2.2 of Areas 1 and 2
- Router ID of Router C as 3.3.3.3 of Areas 1 and 0
- Router ID of Router D as 4.4.4.4 of Area 0

Procedure

Step 1 Assign an IP address for each interface.

The details are not mentioned here.

Step 2 Configure basic OSPFv3 functions.

Enable OSPFv3 on Router A and set its Router ID to 1.1.1.1.

```
[RouterA] ipv6
[RouterA] ospfv3
[RouterA-ospfv3-1] router-id 1.1.1.1
[RouterA-ospfv3-1] quit
[RouterA] interface Pos 1/0/0
[RouterA-Pos1/0/0] ospfv3 1 area 2
[RouterA-Pos1/0/0] quit
```

Enable OSPFv3 on Router B and set its Router ID to 2.2.2.2.

```
[RouterB] ipv6
[RouterB] ospfv3
[RouterB-ospfv3-1] router-id 2.2.2.2
[RouterB-ospfv3-1] quit
[RouterB] interface Pos 1/0/0
[RouterB-Pos1/0/0] ospfv3 1 area 2
[RouterB-Pos1/0/0] quit
[RouterB] interface Pos 2/0/0
[RouterB-Pos2/0/0] ospfv3 1 area 1
```

```
[RouterB-Pos2/0/0] quit

# Enable OSPFv3 on Router C and set its Router ID to 3.3.3.3.
```

```
[RouterC] ipv6
[RouterC] ospfv3
[RouterC-ospfv3-1] router-id 3.3.3.3
[RouterC-ospfv3-1] quit
[RouterC] interface Pos 1/0/0
[RouterC-Pos1/0/0] ospfv3 1 area 1
[RouterC-Pos1/0/0] quit
[RouterC] interface Pos 2/0/0
[RouterC-Pos2/0/0] ospfv3 1 area 0
[RouterC-Pos2/0/0] quit
```

```
# Enable OSPFv3 on Router D and set its Router ID to 4.4.4.4.
```

```
[RouterD] ipv6
[RouterD] ospfv3
[RouterD-ospfv3-1] router-id 4.4.4.4
[RouterD-ospfv3-1] quit
[RouterD] interface Pos 1/0/0
[RouterD-Pos1/0/0] ospfv3 1 area 0
[RouterD-Pos1/0/0] quit
```

```
# Display the OSPFv3 routing table of Router C, and you can find that there is no routing information of Area 2 in the routing table.
```

```
[RouterC] display ospfv3 routing
OSPFv3 Process (1)
  Destination                               Metric
  Next-hop
  1000::/64                                  1
    directly-connected, Pos1/0/0
  1002::/64                                  1
    directly-connected, Pos2/0/0
```

Step 3 Configure a virtual link in Area 1 on Router B and Router C.

```
# Configure Router B.
```

```
[RouterB] ospfv3
[RouterB-ospfv3-1] area 1
[RouterB-ospfv3-1-area-0.0.0.1] vlink-peer 3.3.3.3
[RouterB-ospfv3-1-area-0.0.0.1] quit
```

```
# Configure Router C.
```

```
[RouterC] ospfv3
[RouterC-ospfv3-1] area 1
[RouterC-ospfv3-1-area-0.0.0.1] vlink-peer 2.2.2.2
[RouterC-ospfv3-1-area-0.0.0.1] quit
```

Step 4 Verify the configuration.

```
# Display the OSPFv3 routing table of Router C.
```

```
[RouterC] dis ospfv3 routing
OSPFv3 Process (1)
  Destination                               Metric
  Next-hop
  1000::/64                                  1
    directly-connected, Pos1/0/0
  1000::1/128                                1
    via FE80::4D67:0:EB7D:2, Pos1/0/0
  1000::2/128                                1
    directly-connected, Pos1/0/0
  IA 1001::/64                               2
    via FE80::4D67:0:EB7D:2, Pos1/0/0
  1002::/64                                  1
```


directly-connected, Pos2/0/0

 **NOTE**

After a virtual link is configured, Area 2 is connected with Area 0 through the virtual link. So the route to Area 2 is contained in the routing table of Router C.

---End

Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
ipv6
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ipv6 enable
ipv6 address 1001::2/64
ospfv3 1 area 0.0.0.2
#
ospfv3 1
router-id 1.1.1.1
area 0.0.0.2
#
user-interface con 0
user-interface vty 0 4
#
return
```

- Configuration file of Router B

```
#
sysname RouterB
#
ipv6
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ipv6 enable
ipv6 address 1001::1/64
ospfv3 1 area 0.0.0.2
#
interface Pos2/0/0
link-protocol ppp
undo shutdown
ipv6 enable
ipv6 address 1000::1/64
ospfv3 1 area 0.0.0.1
#
ospfv3 1
router-id 2.2.2.2
area 0.0.0.0
area 0.0.0.1
vlink-peer 3.3.3.3
area 0.0.0.2
#
return
```

- Configuration file of Router C

```
#
sysname RouterC
#
ipv6
#
```

```

interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ipv6 enable
 ipv6 address 1000::2/64
 ospfv3 1 area 0.0.0.1
#
interface Pos2/0/0
 link-protocol ppp
 undo shutdown
 ipv6 enable
 ipv6 address 1002::1/64
 ospfv3 1 area 0.0.0.0
#
ospfv3 1
 router-id 3.3.3.3
 area 0.0.0.0
 area 0.0.0.1
  vlink-peer 2.2.2.2
#
user-interface con 0
user-interface vty 0 4
#
return
    
```

- Configuration file of Router D

```

#
sysname RouterD
#
ipv6
#
interface Pos1/0/0
 link-protocol ppp
 undo shutdown
 ipv6 enable
 ipv6 address 1002::2/64
 ospfv3 1 area 0.0.0.0
#
ospfv3 1
 router-id 4.4.4.4
 area 0.0.0.0
#
user-interface con 0
user-interface vty 0 4
#
return
    
```

6.14.4 Example for Configuring OSPFv3 GR

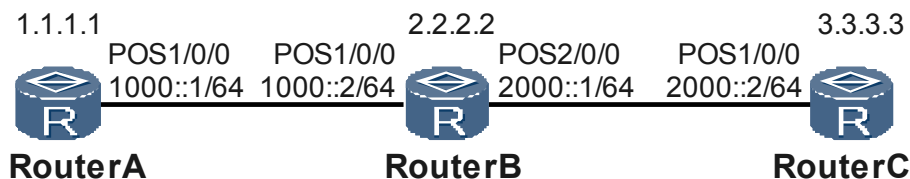
This part provides an example for configuring OSPFv3 GR so that a restarting router can synchronize routing information with its neighbors through GR.

Networking Requirements

As shown in [Figure 6-4](#), Router A, Router B, and Router C are in the same OSPFv3 area. They are interconnected through OSPFv3 and provides GR.

After the OSPFv3 neighbor relationship is set up between Router A, Router B, and Router C, the three routers exchanges routing information. When OSPFv3 on Router A restarts, Router A synchronizes routing information with its neighbors through GR.

Figure 6-4 Networking diagram of configuring OSPFv3 GR



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the OSPFv3 helper in the OSPFv3 view of Router B.
2. Enable OSPFv3 GR in the OSPFv3 view of Router A.

Data Preparation

To complete the configuration, you need the following data:

- IPv6 address of each interface
- OSPFv3 process number

Procedure

Step 1 Assign an IPv6 address for each interface.

The details are not mentioned here.

Step 2 Configure basic OSPF functions.

The details are not mentioned here.

Step 3 Enable OSPFv3 GR on Router A.

```
[RouterA] ospfv3 100
[RouterA-ospfv3-100] graceful-restart
[RouterA-ospfv3-100] quit
```

Step 4 Enable OSPFv3 helper on Router B.

```
[RouterB] ospfv3 100
[RouterB-ospfv3-100] helper-role
[RouterB-ospfv3-100] quit
```

Step 5 Verify the configuration.

Run the **display ipv6 fib 6** command on Router A to display the forwarding information table (FIB).

```
<RouterA> display ipv6 fib 6
FIB Table:
Total number of Routes : 2
Destination:      1000::                               PrefixLength: 64
NextHop          : 1000::1                               Flag           : U
Label            : NULL                                 Tunnel ID      : 0
TimeStamp       : Date- 25:6:2007, Time- 17:31:46      reference     : 1
Interface       : Pos1/0/0
Destination:     2000::                               PrefixLength: 64
NextHop         : FE80::200:1FF:FE00:200                Flag           : DGU
```

```
Label      :      NULL                               Tunnel ID   :   0
TimeStamp  :      Date- 26:6:2007, Time- 14:6:3     reference  :   1
Interface  :      Pos1/0/0
```

Restart OSPFv3 process 100 on Router A in a non-GR mode.

```
<RouterA> reset ospfv3 100
```

Run the **display ipv6 fib 1** command on Router A to view the FIB.

```
<RouterA> display ipv6 fib 1
FIB Table:
Total number of Routes : 1
Destination:      1000::                               PrefixLength :64
NextHop   :      1000::1                               Flag         : U
Label     :      NULL                                   Tunnel ID    : 0
TimeStamp :      Date- 25:6:2007, Time- 17:31:46     reference    : 1
Interface :      Pos1/0/0
```

From the preceding display, you can find that the FIB on Router A changes and services are affected.

Restart OSPFv3 process 100 on Router A in GR mode.

```
<RouterA> reset ospfv3 100 graceful-restart
```

Run the **display ipv6 fib 6** command on Router A to view the FIB and check whether GR works normally. If GR works normally, the FIB does not change and services are not interrupted when Router A restarts the OSPFv3 process in GR mode.

```
<RouterA> display ipv6 fib 6
FIB Table:
Total number of Routes : 2
Destination:      1000::                               PrefixLength : 64
NextHop   :      1000::1                               Flag         : U
Label     :      NULL                                   Tunnel ID    : 0
TimeStamp :      Date- 25:6:2007, Time- 17:31:46     reference    : 1
Interface :      Ethernet3/2/0
Destination:      2000::                               PrefixLength : 64
NextHop   :      FE80::200:1FF:FE00:200               Flag         : DGU
Label     :      NULL                                   Tunnel ID    : 0
TimeStamp :      Date- 26:6:2007, Time- 14:6:3       reference    : 1
Interface :      Ethernet3/2/0
```

From the preceding display, you can find that the FIB on Router A does not change and services are not affected.

----End

Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
ipv6
#
interface Pos1/0/0
link-protocol ppp
undo shutdown
ipv6 enable
ipv6 address 1000::1/64
ospfv3 100 area 0.0.0.0
#
ospfv3 100
router-id 1.1.1.1
graceful-restart
```

```
        area 0.0.0.0
        #
        return
```

- Configuration file of Router B

```
        #
        sysname RouterB
        #
        ipv6
        #
        interface Pos1/0/0
        link-protocol ppp
        undo shutdown
        ipv6 enable
        ipv6 address 1000::2/64
        ospfv3 100 area 0.0.0.0
        #
        interface Pos2/0/0
        link-protocol ppp
        undo shutdown
        ipv6 enable
        ipv6 address 2000::1/64
        ospfv3 100 area 0.0.0.0
        #
        ospfv3 100
        router-id 2.2.2.2
        helper-role
        area 0.0.0.0
        #
        return
```

- Configuration file of Router C

```
        #
        ipv6
        #
        interface Pos2/0/0
        link-protocol ppp
        undo shutdown
        ipv6 enable
        ipv6 address 2000::2/64
        ospfv3 100 area 0.0.0.0
        #
        ospfv3 100
        router-id 3.3.3.3
        area 0.0.0.0
        #
        return
```

6.14.5 Example for Configuring BFD for OSPFv3

This part provides an example for configuring BFD for OSPFv3. After BFD for OSPFv3 is configured, BFD can fast detect link faults and report them to OSPFv3 so that service traffic can be transmitted through the backup link.

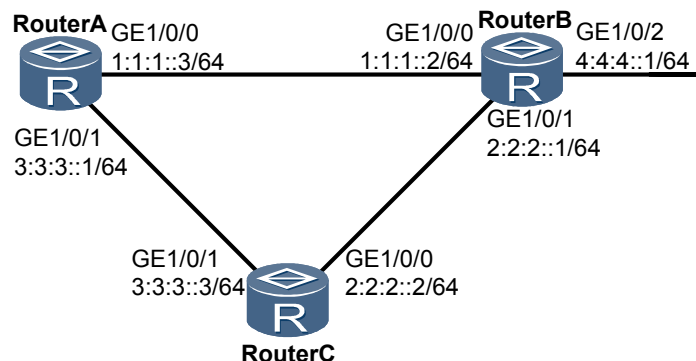
Networking Requirements

As shown in [Figure 6-5](#), it is required as follows:

- Run OSPFv3 between Router A, Router B, and Router C.
- Enable BFD of the OSPFv3 process on Router A, Router B, and Router C.
- Traffic is transmitted on the active link Router A → Router B. The link Router A → Router C → Router B acts as the standby link.

- When a fault occurs on the link, BFD can quickly detect the fault and notify OSPFv3 of the fault; therefore, the traffic is transmitted on the standby link.

Figure 6-5 Networking diagram for configuring BFD for OSPFv3



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the basic OSPFv3 functions on each router.
2. Configuring BFD for OSPFv3.

Data Preparation

To complete the configuration, you need the following data:

- Router ID of Router A is 1.1.1.1.
- Router ID of Router B is 2.2.2.2.
- Router ID of Router C is 3.3.3.3.
- Minimum interval for sending the BFD packets, minimum interval for receiving the BFD packets, and detection multiple on Router A and Router B.

Procedure

Step 1 Assign an IPv6 address to each router interface.

The detailed configuration is not mentioned here.

Step 2 Configure the basic OSPFv3 functions.

Configure Router A.

```
[RouterA] ipv6
[RouterA] ospfv3
[RouterA-ospfv3-1] router-id 1.1.1.1
[RouterA-ospfv3-1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ipv6 enable
[RouterA-GigabitEthernet1/0/0] ospfv3 1 area 0
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ipv6 enable
[RouterA-GigabitEthernet1/0/1] ospfv3 1 area 0.0.0.0
[RouterA-GigabitEthernet1/0/1] quit
```

Configure Router B.

```
[RouterB] ipv6 enable
[RouterB] ospfv3 1
[RouterB-ospfv3-1] router-id 2.2.2.2
[RouterB-ospfv3-1] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ipv6 enable
[RouterB-GigabitEthernet1/0/0] ospfv3 1 area 0.0.0.0
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ipv6 enable
[RouterB-GigabitEthernet1/0/1] ospfv3 1 area 0.0.0.0
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] ipv6 enable
[RouterB-GigabitEthernet1/0/2] ospfv3 1 area 0.0.0.0
```

Configure Router C.

```
[RouterC] ospfv3 1
[RouterC-ospfv3-1] router-id 3.3.3.3
[RouterC-ospfv3-1] quit
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ipv6 enable
[RouterC-GigabitEthernet1/0/0] ospfv3 1 area 0.0.0.0
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] ipv6 enable
[RouterC-GigabitEthernet1/0/1] ospfv3 1 area 0.0.0.0
```

After the preceding configurations are complete, run the **display ospfv3 peer** command. You can view that the neighboring relationship is set up between Router A and Router B, and that between Router B and Router C. Take the display of Router A as an example:

```
[RouterA] display ospfv3 peer verbose
OSPFv3 Process (1)
Neighbor 2.2.2.2 is Full, interface address FE80::E0:CE19:8142:1
  In the area 0.0.0.0 via interface GE1/0/0
  DR Priority is 1 DR is 2.2.2.2 BDR is 1.1.1.1
  Options is 0x000013 (-|R|-|E|V6)
  Dead timer due in 00:00:34
  Neighbour is up for 01:30:52
  Database Summary Packets List 0
  Link State Request List 0
  Link State Retransmission List 0
  Neighbour Event: 6
  Neighbour If Id : 0xe
Neighbor 3.3.3.3 is Full, interface address FE80::E0:9C69:8142:2
  In the area 0.0.0.0 via interface GE1/0/1
  DR Priority is 1 DR is 3.3.3.3 BDR is 1.1.1.1
  Options is 0x000013 (-|R|-|E|V6)
  Dead timer due in 00:00:37
  Neighbour is up for 01:31:18
  Database Summary Packets List 0
  Link State Request List 0
  Link State Retransmission List 0
  Neighbour Event: 6
  Neighbour If Id : 0x9
```

Display the information in the OSPFv3 routing table on Router A. You can view the routing entries to Router B and Router C.

```
[RouterA] display ospfv3 routing
OSPFv3 Process (1)
Destination                                     Next-hop                                     Metric
1:1:1::/64                                       directly connected, GigabitEthernet1/0/0   1
```

```

2:2:2::/64                                     2
  via FE80::E0:9C69:8142:2, GigabitEthernet1/0/1
  via FE80::E0:CE19:8142:1, GigabitEthernet1/0/0
3:3:3::/64                                     1
  directly connected, GigabitEthernet1/0/1
4:4:4::1/64                                    1
  via FE80::E0:CE19:8142:1, GigabitEthernet1/0/0
    
```

As shown in the OSPFv3 routing table, the next hop address of the route to 4:4:4::1/64 is GigabitEthernet1/0/0 and traffic is transmitted on the active link Router A → Router B.

Step 3 Configure OSPFv3 BFD.

Enable global BFD on Router A.

```

[RouterA] bfd
[RouterA-bfd] quit
[RouterA] ospfv3
[RouterA-ospfv3-1] bfd all-interfaces enable min-transmit-interval 100 min-receive-
interval 100 detect-multiplier 4
    
```

Enable global BFD on Router B.

```

[RouterB] bfd
[RouterB-bfd] quit
[RouterB] ospfv3
[RouterB-ospfv3-1] bfd all-interfaces enable min-transmit-interval 100 min-receive-
interval 100 detect-multiplier 4
    
```

Enable global BFD on Router C.

```

[RouterC] bfd
[RouterC-bfd] quit
[RouterC] ospfv3
[RouterC-ospfv3-1] bfd all-interfaces enable min-transmit-interval 100 min-
receive-interval 100 detect-multiplier 4
    
```

After the preceding configurations are complete, run the **display ospfv3 bfd session** command on Router A or Router B. You can view that the status of the BFD session is Up.

Take the display of Router B as an example:

```

<RouterB> display ospfv3 bfd session verbose
* - STALE
OSPFv3 Process (1)
  Neighbor-Id: 1.1.1.1
  BFD Status: Up
  Interface: GE1/0/0
  IPv6-Local-Address: FE80::E0:CE19:8142:1
  IPv6-Remote-Address: FE80::E0:4C3A:143:1
  BFD Module preferred timer values
    Transmit-Interval(ms): 100
    Receive-Interval(ms): 100
    Detect-Multiplier: 3
  OSPFv3 Module preferred timer values
    Transmit-Interval(ms): 100
    Receive-Interval(ms): 100
    Detect-Multiplier: 3
  Configured timer values
    Transmit-Interval(ms): 100
    Receive-Interval(ms): 100
    Detect-Multiplier: 3
  Neighbor-Id: 3.3.3.3
  BFD Status: Down
  Interface: GE1/0/1
  IPv6-Local-Address: FE80::E0:CE19:8142:2
  IPv6-Remote-Address: FE80::E0:9C69:8142:1
  BFD Module preferred timer values
    Transmit-Interval(ms): 2200
    
```



```

    Receive-Interval(ms): 2200
    Detect-Multiplier: 0
    OSPFv3 Module preferred timer values
    Transmit-Interval(ms): 1000
    Receive-Interval(ms): 1000
    Detect-Multiplier: 3
    Configured timer values
    Transmit-Interval(ms): 1000
    Receive-Interval(ms): 1000
    Detect-Multiplier: 3
    
```

Step 4 Verify the configuration.

Run the **shutdown** command on GE 1/0/0 of Router B to simulate the active link failure.

```

[RouterB] interface gigabitethernet1/0/0
[RouterB-GigabitEthernet1/0/0] shutdown
    
```

Display the routing table on Router A. The standby link Router A → Router C → Router B takes effect after the active link fails. The next hop address of the route to 4:4:4:1/64 becomes GigabitEthernet1/0/1.

```

<RouterA> display ospfv3 routing
OSPFv3 Process (1)
Destination                                     Metric
  Next-hop
  1:1:1::/64                                     1
    directly connected, GigabitEthernet1/0/0
  2:2:2::/64                                     2
    via FE80::E0:9C69:8142:2, GigabitEthernet1/0/1
  3:3:3::/64                                     1
    directly connected, GigabitEthernet1/0/1
  4:4:4::1/64                                    2
    via FE80::E0:9C69:8142:2, GigabitEthernet1/0/1
    
```

----End

Configuration Files

- Configuration file of Router A

```

#
 sysname RouterA
#
 ipv6
#
 bfd
#
 ospfv3 1
  router-id 1.1.1.1
  bfd all-interfaces enable min-transmit-interval 100 min-receive-interval 100
  detect-multiplier 4
#
 interface gigabitethernet1/0/0
  ipv6 enable
  ipv6 address 1:1:1::3/64
  ospfv3 1 area 0.0.0.0
#
 interface gigabitethernet1/0/1
  ipv6 enable
  ipv6 address 3:3:3::1/64
  ospfv3 1 area 0.0.0.0
#
 return
    
```

- Configuration file of Router B

```

#
 sysname RouterB
    
```

```
#
ipv6
#
bfd
#
ospfv3 1
router-id 2.2.2.2
bfd all-interfaces enable min-transmit-interval 100 min-receive-interval 100
detect-multiplier 4
#
interface gigabitethernet1/0/0
ipv6 enable
ipv6 address 1:1:1::2/64
ospfv3 1 area 0.0.0.0
#
interface gigabitethernet1/0/1
ipv6 enable
ipv6 address 2:2:2::1/64
ospfv3 1 area 0.0.0.0
#
interface gigabitethernet1/0/2
ipv6 enable
ipv6 address 4:4:4::1/64
ospfv3 1 area 0.0.0.0
#
return
```

- Configuration file of Router C

```
#
sysname RouterC
#
ipv6
#
ospfv3 1
router-id 3.3.3.3
bfd all-interfaces enable min-transmit-interval 100 min-receive-interval 100
detect-multiplier 4
#
interface gigabitethernet1/0/0
ipv6 enable
ipv6 address 2:2:2::2/64
ospfv3 1 area 0.0.0.0
#
interface gigabitethernet1/0/1
ipv6 enable
ipv6 address 3:3:3::3/64
ospfv3 1 area 0.0.0.0
#
return
```

7 IS-IS Configuration

About This Chapter

This chapter describes the basic principle of IS-IS and procedures for configuring IS-IS, and provides configuration examples.

[7.1 Introduction to IS-IS](#)

By building IS-IS networks, you can enable IS-IS to discover and calculate routes in ASs.

[7.2 Configuring Basic IS-IS Functions](#)

IS-IS networks can be built only after basic IS-IS functions are configured.

[7.3 Establishing or Maintaining IS-IS Neighbor Relationships or Adjacencies](#)

This section describes how to configure the parameters that affect the IS-IS neighbor relationship.

[7.4 Configuring IS-IS Attributes in Different Types of Networks](#)

This section describes how to configure IS-IS attributes in different types of networks because IS-IS attributes vary with network types.

[7.5 Configuring IS-IS Route Attributes](#)

Setting IS-IS route attributes affects IS-IS route selection.

[7.6 Controlling the Advertisement of IS-IS Routes](#)

By configuring route leaking and route aggregation and configuring routers to generate default routes, you can control the advertisement of IS-IS routes with different levels in different areas, and control the number of IS-IS routing entries.

[7.7 Controlling the Receiving of IS-IS Routes](#)

By configuring IS-IS to filter routing information, you can control the number of IS-IS routes to be added to the IP routing table and the number of imported routes to be added to the IS-IS routing table.

[7.8 Adjusting and Optimizing an IS-IS Network](#)

By adjusting and optimizing IS-IS, you can enable IS-IS to meet the requirements of complicated networks.

[7.9 Configuring Local MT](#)

By configuring local MT, you can enable multicast packets to be forwarded through TE tunnels on IS-IS networks.

7.10 Configuring IS-IS IPv6

This section describes how to enable the IPv6 capability for IS-IS and adjust IS-IS IPv6 route selection.

7.11 Configuring IS-IS Auto FRR

With IS-IS Auto FRR, traffic on a faulty link can be quickly switched to the backup link of the faulty link. This ensures that the traffic interruption time is within 50 ms and improves the reliability of IS-IS networks.

7.12 Configuring IPv6 IS-IS Auto FRR

With IPv6 IS-IS Auto FRR, traffic on a faulty link can be quickly switched to the backup link of the faulty link. This ensures that the traffic interruption time is within 50 ms and improves the reliability of IS-IS networks.

7.13 Configuring IS-IS GR

By configuring IS-IS GR, you can enable Router to restart gracefully and avoid temporary black holes.

7.14 Configuring Static BFD for IS-IS

BFD can provide channel fault detection featuring light load and high speed (millisecond level). Static BFD needs to be configured manually.

7.15 Configuring Dynamic BFD for IS-IS

BFD can provide channel fault detection featuring light load and high speed (millisecond level). Routing protocols can dynamically trigger the establishment of BFD sessions.

7.16 Configuring Dynamic IPv6 BFD for IS-IS

BFD can provide link failure detection featuring light load and high speed (at the millisecond level). With dynamic BFD, routing protocols can dynamically trigger the establishment of BFD sessions.

7.17 Improving Security of an IS-IS Network

On a network that requires high security, you can configure IS-IS authentication to improve the security of the IS-IS network.

7.18 Configuring IS-IS Multi-Topology (IPv4)

By configuring multi-topology on an IS-IS network, you can properly allocate network resources.

7.19 Configuring IS-IS Multi-Topology (IPv6)

By configuring multi-topology on an IS-IS network, you can properly allocate network resources.

7.20 Maintaining IS-IS

Maintaining IS-IS involves resetting IS-IS and clearing IS-IS statistics.

7.21 Configuration Examples

This section provides several configuration examples of IS-IS together with the configuration flowchart. The configuration examples explain networking requirements, configuration notes, and configuration roadmap.

7.1 Introduction to IS-IS

By building IS-IS networks, you can enable IS-IS to discover and calculate routes in ASs.

7.1.1 Basic Concepts of IS-IS

As an IGP, IS-IS is used inside an AS. IS-IS is a link-state protocol. It uses the SPF algorithm to calculate routes.

The Intermediate System-to-Intermediate System (IS-IS) is a dynamic routing protocol initially issued by the International Organization for Standardization (ISO) for its Connectionless Network Protocol (CLNP).

To support the IP routing, the Internet Engineering Task Force (IETF) extends and modifies IS-IS in RFC 1195. IS-IS can thus be applied to both TCP/IP and OSI environments. This type of IS-IS is called the Integrated IS-IS or Dual IS-IS.

As an Interior Gateway Protocol (IGP), IS-IS is used in Autonomous Systems (ASs). IS-IS is a link-state protocol. It uses the Shortest Path First (SPF) algorithm to calculate routes. It resembles the Open Shortest Path First (OSPF) protocol.

IS-IS Areas

To support the large-scale networks, the IS-IS adopts a two-level structure in a Routing Domain (RD). A large RD is divided into one or more areas. The intra-area routes are managed by the Level-1 routers, whereas the inter-area routes is managed by the Level-2 routers.

Figure 7-1 shows an IS-IS network. Its topology is similar to that of a multi-area OSPF network. Area 1 is a backbone area. All routers in this area are Level-2 routers. The other four areas are non-backbone areas. They are connected to Area 1 through Level-1-2 routers.

Figure 7-1 IS-IS topology

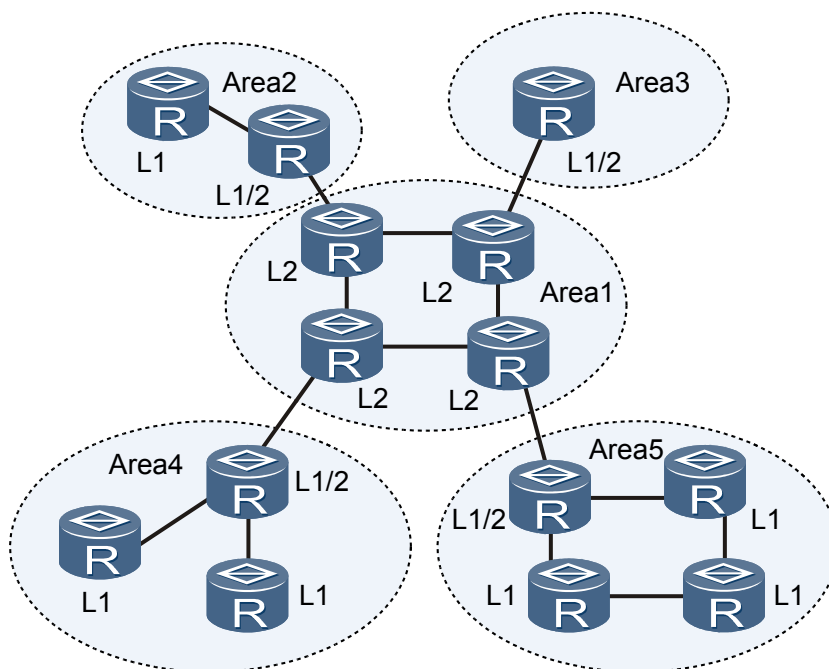
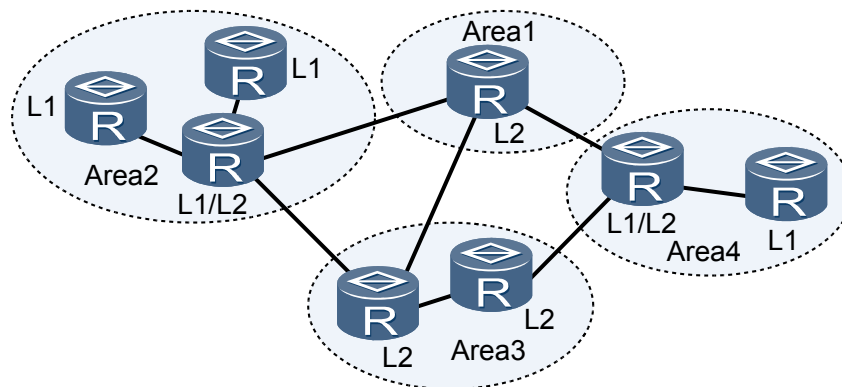


Figure 7-2 shows another type of IS-IS topology. The Level-1-2 routers are used to connect the Level-1 and the Level-2 routers, and are used to establish the backbone network together with the other Level-2 routers. In this topology, no area is specified as a backbone area. All the Level-2 routers constitute an IS-IS backbone network. The devices may belong to different areas, but the areas must be successive.

Figure 7-2 IS-IS topology II



NOTE

The IS-IS backbone network does not refer to a specific area.

This type of networking shows differences between IS-IS and OSPF. For OSPF, the inter-area routes are forwarded by the backbone area, and the SPF algorithm is used in the same area. For IS-IS, both Level-1 routers and Level-2 routers use the SPF algorithm to generate Shortest Path Trees (SPTs).

Network Types

IS-IS supports only two network types, which can be classified as follows according to physical links:

- Broadcast links such as Ethernet and Token-Ring
- Point-to-point links such as PPP and HDLC

NOTE

For a Non-Broadcast Multi-Access (NBMA) network such as ATM, you need to configure sub-interfaces for it. The type of subnets cannot be Point-to-Multipoint (P2MP). IS-IS cannot run on P2MP networks.

7.1.2 IS-IS Features Supported by the NE80E/40E

The NE80E/40E supports various IS-IS features, including multi-instance, multi-process, hot standby, multi-topology, local MT, GR, TE, DS-TE, administrative tags, LSP fragment extension, dynamic hostname exchange, fast convergence, BFD, and 3-way handshake.

Multi-Process and Multi-Instance

For easy management and effective control, IS-IS supports the multi-process and multi-instance features.

- **Multi-Process**
A set of interfaces are associated with a specific IS-IS process. This ensures that the specific IS-IS process performs all the operations only on the set of interfaces. Multiple IS-IS processes then can work on a single Router and each process is responsible for a unique set of interfaces.
- **Multi-Instance**
For a router that supports the Virtual Private Network (VPN), each IS-IS process is associated with a specified VPN-instance. All the interfaces attached to an IS-IS process are associated with the VPN-instance.

IS-IS Hot Standby

Router with distributed architecture support the IS-IS Hot Standby (HSB) feature. IS-IS backs up data from the Active Main Board (AMB) to the Standby Main Board (SMB). When the AMB fails, the SMB becomes active and replaces the AMB. IS-IS can thus work normally.

In the running process of IS-IS HSB, IS-IS configurations on the AMB and SMB must be consistent. When the active/standby switchover occurs, IS-IS on the new AMB performs Graceful Restart (GR). The new AMB resends a request for setting up the neighbor relationship to neighbors to synchronize LSDBs. Traffic, therefore, is not affected.

NOTE

For details of IS-IS HSB and GR, refer to the chapter "HA Configuration" in the HUAWEI NetEngine80E/40E Router *Configuration Guide - Reliability*.

IS-IS Multicast-Topology (MT)

IS-IS IPv6 implementation has the limitation that a mixed topology of IPv4 and IPv6 is considered as an integrated topology during the SPF calculation. This requires that information about all IPv6 topologies and IPv4 topologies be consistent.

The deployment of IPv6 and IPv4 in the network, however, may be inconsistent; therefore, information about all IPv6 topologies and IPv4 topologies may be different. If the SPF calculation is performed in an integrated topology and the same shortest paths are used to forward packets, routers that do not support IPv6 discard received IPv6 packets.

IS-IS Multi-Topology (MT) can be used to solve the preceding problems. IS-IS MT refers to multiple separate IP topologies that are run in an IS-IS AS, such as IPv4 topology and IPv6 topology. Topologies adopt separate SPF calculation. Through MT, the routes are calculated respectively according to the actual IPv4 or IPv6 networks. Thus, network shielding is realized.

Local Multicast-Topology

When multicast and an MPLS TE tunnel are deployed in a network, the multicast function may be affected by the TE tunnel, and the multicast services may become unavailable.

This is because the outgoing interface of the route calculated by an IGP may not be the actual physical interface but a TE tunnel interface, after the TE tunnel is configured with IGP Shortcut. According to the unicast route to the multicast source address, a router sends a Join message through a TE tunnel interface. Router spanned by the TE tunnel cannot sense the Join message. The Router, therefore, do not create any multicast forwarding entry. Because the TE tunnel is unidirectional, multicast data packets sent by the multicast source are sent to the Router spanned by the tunnel through the related physical interfaces. The Router discard the multicast data

packets, because they do not have any multicast forwarding entry. Thus, services become unavailable.

After the local MT is enabled, the separate MIGP routing table can be created for multicast to guide the forwarding of multicast packets.

 **NOTE**

For details of the local MT, refer to the chapter "IS-IS" in the HUAWEI NetEngine80E/40E Router *Feature Description - IP Routing*.

IS-IS GR

Graceful Restart (GR) is a function that is used to restart the Router gracefully. GR ensures uninterrupted traffic forwarding and avoids route flapping during short time Router restart.

If IS-IS does not restart in GR mode, IS-IS sessions are reset and Link State Protocol Data Units (LSPs) are regenerated and flooded. This causes the SPF calculation, route flapping, and forwarding interruption in the entire area. In this case, IETF works out IS-IS GR standards (RFC 3847). The standards deal with protocol restart keeping FIB tables or not keeping FIB tables.

 **NOTE**

For details of IS-IS GR, refer to the chapter "IS-IS" in the HUAWEI NetEngine80E/40E Router *Feature Description - IP Routing*.

IS-IS TE

The IS-IS Traffic Engineering (TE) supports the establishment and maintenance of the Label Switched Path (LSP).

When constructing the Constraint-based Routed (CR) LSP, MPLS needs to learn the traffic attributes of all the links in this area. MPLS can acquire the TE information of the links through IS-IS.

 **NOTE**

For details of the IS-IS TE configurations, refer to the HUAWEI NetEngine80E/40E Router *Configuration Guide - MPLS*.

In this chapter, LSP, excluding the Label Switch Path (LSP) mentioned in this part, is short for the Link State Protocol Data Unit. Note the differences in the two abbreviations.

Administrative Tags

Administrative tags simplify management. IS-IS implements the control function by advertising the prefixes carrying administrative tags. Administrative tags carry administrative information about IP prefixes. They are used to control the route import of different levels and areas, and control the different routing protocols and multiple IS-IS instances running on the same Router. They are also used to carry tags.

Administrative tag values are associated with some attributes. When an IS-IS router advertises an IP prefix with these attributes, the router adds the administrative tag to the TLV in the prefix. In this way, sticking to the prefix, the tag is flooded throughout routing domain.

LSP Fragments Extension

When LSPs to be advertised by IS-IS contain too much information, they are advertised through multiple LSP fragments of the same system. Each LSP fragment is identified by the LSP

identifier field of each LSP. The LSP identifier field is 1 byte long. Thus, the maximum number of fragments that can be generated by any IS-IS router is 256.

The IS-IS LSP fragment extension feature allows an IS-IS router to generate more LSP fragments. To implement this feature, you can configure additional system IDs with the network manager for a Router. Each system ID represents a virtual system that can generate 256 LSP fragments. With more additional system IDs (up to 50 virtual systems), the IS-IS router can generate a maximum of 13056 LSP fragments.

- Related terms

- Originating System

It is a router that runs the IS-IS protocol. As mentioned in this manual, a single IS-IS process can advertise its LSPs as multiple "virtual" Router, and the originating system represents the "real" IS-IS process.

- Normal System ID

It is the system ID of an originating system.

- Additional System ID

Additional system IDs are assigned by the network manager. Each additional system ID can generate up to 256 additional or extended LSP fragments. Like the normal system ID, the additional system ID should be unique in a routing domain.

- Virtual System

The system, identified by an additional system ID, is used to generate extended LSP fragments. These fragments carry the additional system IDs in their LSP IDs.

- Operating modes

A IS-IS router can run the LSP fragment extension feature in the following two modes:

- Mode-1: is used when some older Router in the network do not support this feature.

In this mode, the originating system advertises a link to each of the virtual systems in its LSPs. Similarly, each of the virtual systems advertises a link to the originating system. In this way, the virtual systems look like the actual Router that are connected to the originating system in the network. One restriction in this mode is that only routing information can be advertised through the LSPs of the virtual systems.

- Mode-2: is used when all of the routers in the network support this feature.

In this mode, all the routers in the network know that the LSPs generated by the virtual systems actually belong to the originating system. There is no restriction on the link-state information advertised through the LSPs of the virtual systems.

Dynamic Hostname Exchange Mechanism

To manage and maintain IS-IS networks more conveniently, the dynamic hostname exchange mechanism is introduced. The mechanism provides a mapping service from the hostname to system ID for routers in an IS-IS domain. This dynamic name information is advertised in the form of a dynamic hostname TLV.

The dynamic hostname exchange mechanism also provides a service of associating a hostname with the Designated Intermediate System (DIS) in a broadcast network. This mechanism then advertises this association information through the pseudo node LSP of the router in the form of a dynamic hostname TLV.

The hostname is easier to identify and memorize than the system ID. After this function is configured, the router on which the display command of IS-IS is used displays its hostname rather than system ID.

IS-IS Fast Convergence

- I-SPF

Incremental SPF (I-SPF) calculates only the changed routes at a time rather than all the routes.

In ISO-10589, the Dijkstra algorithm is defined to calculate the routes. When a node changes in the network, this algorithm needs to be used to recalculate all the nodes. Thus, it takes a long time, occupies too many CPU resources, and affects the convergence speed.

I-SPF improves this algorithm. After calculating all the nodes at the first time, it calculates only changed nodes subsequently. The SPT generated at last is the same as that generated through the previous algorithm. This reduces the CPU utilization and speeds up the network convergence.

- PRC

Similar to I-SPF, the Partial Route Calculation (PRC) calculates only changed nodes, but it updates leaves (routes) calculated by I-SPF, instead of calculating the shortest path.

In route calculation, a route represents a leaf, and a router represents a node. If the SPT calculated by I-SPF changes, PRC processes all the leaves on changed nodes. If the SPT remains unchanged, PRC processes only changed leaves.

For example, if only IS-IS is enabled only on an interface of a node, the SPT calculated by I-SPF remains unchanged. In this case, PRC updates only the routes of this interface, thus occupying less CPU.

PRC together with I-SPF further improves the convergence performance of the network. As an improvement of the original SPF algorithm, PRC and I-SPF replace the original algorithm.

 **NOTE**

In the NE80E/40E implementation, only I-SPF and PRC are used to calculate routes.

- LSP fast flooding

When an IS-IS router receives new LSPs from the other Router, it floods out the LSPs in its own LSDB periodically according to the RFC. Thus, the LSDB is synchronized slowly.

LSP fast flooding solves the problem. When a router configured with this feature receives one or more LSPs, it floods out the LSPs less than the specified ones before route calculation. The LSDB can thus be synchronized quickly. This improves the network convergence speed significantly.

- Intelligent timer

Although the route calculation algorithm is improved, the long interval for triggering the route calculation also affects the convergence speed. You can shorten the interval by using a millisecond-level timer. Frequent network changes, however, also occupy too many CPU resources. The SPF intelligent timer solves these problems. It responds to burst events quickly, and avoids the occupation of too many CPU resources.

Generally, an IS-IS network running normally is stable. Too many network changes occur rarely, and an IS-IS router does not calculate routes frequently. Thus, set a short time period (in milliseconds) for the first time for triggering the route calculation. If the network changes frequently, the intelligent timer increases with the calculation times and thus the interval becomes longer. This avoids the occupation of too many CPU resources.

The LSP generation intelligent timer is similar to the SPF intelligent timer. When the LSP generation intelligent timer times out, the system generates a new LSP according to the current topology. The original mechanism adopts a timer with a certain interval, and thus cannot achieve fast convergence and low CPU utilization. Thus, the LSP generation timer

is thus designed as an intelligent timer to respond to the burst events (for example, an interface is Up or Down) quickly and speed up the network convergence. In addition, when the network changes frequently, the interval for the intelligent timer becomes longer automatically to avoid too much CPU occupation.

 **NOTE**

Be cautious to configure the timers according to the practical networks and the Router performances.

BFD for IS-IS

In the NE80E/40E, Bidirectional Forwarding Detection (BFD) is used to detect IS-IS neighbor relationships.

BFD can fast detect the faults on links between IS-IS neighbors and reports them to IS-IS. The fast convergence of IS-IS is thus implemented.

 **NOTE**

BFD detects only the one-hop link between IS-IS neighbors. This is because IS-IS establishes only one-hop neighbors.

- **Static BFD**

Static BFD refers to configuring BFD session parameters manually including local and remote identifiers and delivering BFD session setup requests manually.

The defect of this feature is that BFD sessions are created and deleted manually, which lacks flexibility. In addition, manual configuration errors may be generated. For example, a wrong local or remote identifiers may be configured, therefore, BFD sessions cannot work normally.

- **Dynamic BFD**

Dynamic BFD refers to that routing protocols dynamically trigger the establishment of BFD sessions.

When setting up new neighbor relationship, routing protocols send parameters of neighbors and detection parameters (including source and destination IP addresses) to the BFD module. BFD then sets up sessions according to the received parameters between neighbors. Dynamic BFD is more flexible than static BFD.

Generally, the interval for an IS-IS router to send Hello messages is 10 seconds. The interval for declaring that a neighbor is invalid, that is, the Holddown time for keeping the neighbor relationship, is three times as long as the interval for sending Hello messages. The minimum Holddown time, however, can be only of second level. IS-IS can thus provide only second-level period for sensing the fault of neighbors. As a result, a large number of packets may be lost in the high-speed network environment.

Dynamic BFD can provide channel fault detection of light load and high speed (millisecond level). Dynamic BFD cannot substitute the Hello mechanism of IS-IS. BFD helps IS-IS to detect the faults that occur on neighboring devices or links more quickly, and notifies IS-IS to recalculate routes to correctly guide packet forwarding in time.

On the

 **NOTE**

For details of BFD for IS-IS, refer to the chapter "IS-IS" in the HUAWEI NetEngine80E/40E Router *Feature Description - IP Routing*.

3-Way Handshake

IS-IS needs a reliable data link layer protocol on a P2P link. The 2-Way Handshake defined in ISO 10589 uses Hello messages to establish adjacencies on the P2P interfaces of adjacent

Router. In this mechanism, when a router receives Hello message from a neighbor, the router establish an adjacency with the neighbor and declares that the neighbor is Up.

This mechanism has obvious defects. For example, if the link goes Up and Down frequently after the adjacency is established, CSNPs are lost and the LSDB cannot be synchronized in a full refresh cycle of LSPs; when two or more links exist between two routers, the two routers can still set up an adjacency even if one link is Down but another link is Up. SPF uses parameters of another link for route calculation. As a result, the router that fails to detect fault tries forwarding packets through the link which is down.

The 3-way handshake resolves these issues on P2P links. In this mode, a router declares that its neighbor is Up only when the router knows that its neighbor receives a packet from the router. The extended circuit ID (32 bits) used in the 3-way handshake identifies more links than the local circuit ID (8 bits) that identifies 255 links.

7.2 Configuring Basic IS-IS Functions

IS-IS networks can be built only after basic IS-IS functions are configured.

7.2.1 Establishing the Configuration Task

Before configuring basic IS-IS functions, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

Start an IS-IS process first before configuring IS-IS. Specify an Network Entity Title (NET) and enable IS-IS on related interfaces before configuring the other functions.

Pre-configuration Tasks

Before configuring basic IS-IS functions, complete the following tasks:

- Configuring a link layer protocol
- Configuring IP addresses of interfaces to make neighboring nodes reachable at the network layer

Data Preparation

To configure basic IS-IS functions, you need the following data.

No.	Data
1	Process number
2	NET
3	Levels of routers and interfaces

7.2.2 Starting an IS-IS Process

The first step to configure IS-IS features is to create IS-IS processes.

Context

To enable IS-IS, you should create an IS-IS process and activate it on the interfaces that may be associated with other routers.

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
isis [ process-id ]
```

An IS-IS process is started and the IS-IS view is displayed.

process-id identifies an IS-IS process. If *process-id* is not set, the system uses process 1 by default. To associate the IS-IS process to a VPN instance, you can run the `isis [process-id] [vpn-instance] *` command.

---End

7.2.3 Configuring an NET

The second step to configure IS-IS features is to configure the NET by specifying the area address and system ID.

Context

An NET defines the current IS-IS area address and the system ID of a router. You can configure a maximum of three NETs on a process of a router. The area addresses of the NETs can be different, but their system IDs must be the same.

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

Step 3 Run:

```
network-entity net
```

An NET is configured.



Converting the address of a loopback network to a NET is recommended to ensure that the NET is unique on the network. If a NET is not unique, route flapping may occur. Therefore, plan the network properly.

During the establishment of the Level-2 neighbor relationship, IS-IS does not check whether area addresses are the same. During the establishment of the Level-1 neighbor relationship, area addresses must be the same; otherwise, the Level-1 neighbor relationship cannot be established.

----End

7.2.4 Configuring the Level of a router

By configuring the IS-IS level of a router, you can determine the IS-IS level of the adjacency.

Context

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

Step 3 Run:

```
is-level { level-1 | level-1-2 | level-2 }
```

The level of a router is set.

By default, the level of the router is **level-1-2**.

----End

7.2.5 Enabling IS-IS on a Specified Interface

Before running IS-IS, you need to enable an IS-IS process on a specific interface.

Context

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
isis enable [ process-id ]
```

IS-IS is enabled on a specified interface.

To enable the peer end to learn routes of the network segment where the interface resides, ensure that the status of the interface is Up.

If *process-id* is not specified, an interface is added to IS-IS process 1 by default.

----End

7.2.6 Checking the Configuration

After configuring basic IS-IS functions, you can check information about the IS-IS interface, LSDB, neighbor, routes, and statistics about the IS-IS process.

Prerequisite

The configurations of Basic IS-IS Functions are complete.

Procedure

- Run **display isis interface** [[**verbose** | **traffic-eng**] * | **tunnel**] [*process-id* | **vpn-instance** *vpn-instance-name*] command to check information about the interface enabled with IS-IS.
- Run **display isis lsdb** [{ **level-1** | **level-2** } | **verbose** | { **local** | *lsp-id* | **is-name** *symbolic-name* }] * [*process-id* | **vpn-instance** *vpn-instance-name*] command to check information about the LSDB.
- Run **display isis peer** [**verbose**] [*process-id* | **vpn-instance** *vpn-instance-name*] command to check information about the IS-IS neighbors.
- Run **display isis route** [*process-id* | **vpn-instance** *vpn-instance-name*] [**ipv4**] [**verbose** | [**level-1** | **level-2**] | *ip-address* [*mask* | *mask-length*]] * command to check IS-IS routing information.
- Check the statistics about the IS-IS process:
 - **display isis statistics** [**level-1** | **level-2** | **level-1-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]
 - **display isis statistics packet** [**interface** *interface-type interface-number*]
 - **display isis** *process-id* **statistics** [**level-1** | **level-2** | **level-1-2** | **packet**]

----End

Example

Run the **display isis interface** command. If the IS-IS neighbor relationship is correctly set up, you can find that the IPv4 neighbor of the local router is Up.

```
<HUAWEI> display isis interface
                        Interface information for ISIS (1)
-----
Interface      Id      IPV4.State      IPV6.State      MTU  Type  DIS
GE 1/0/0      001      Up              Down            1497 L1/L2 No/No
```

7.3 Establishing or Maintaining IS-IS Neighbor Relationships or Adjacencies

This section describes how to configure the parameters that affect the IS-IS neighbor relationship.

7.3.1 Establishing the Configuration Task

Before configuring the parameters that affect the IS-IS neighbor relationship, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

This section describes how to establish or maintain the IS-IS neighbor relationship, covering:

- Adjusting timers of various IS-IS packets, including Hello packets, CSNPs, and LSPs
- Adjusting parameters of LSPs

Pre-configuration Tasks

Before establishing or maintaining IS-IS neighbor relationships or adjacencies, complete the following tasks:

- Configuring IP addresses of interfaces to make neighboring nodes reachable
- [7.2 Configuring Basic IS-IS Functions](#)

Data Preparation

To establish or maintain IS-IS neighbor relationships or adjacencies, you need the following data.

No.	Data
1	Parameters of IS-IS timers
2	LSP parameters

7.3.2 Configuring IS-IS Timers for Packets

This part describes how to set the intervals for sending Hello packets, Complete Sequence Number PDUs (CSNPs), and Link State PDUs (LSPs).

Context

Do as follows on the router that runs IS-IS:

Procedure

- Configuring the Interval for Sending Hello Packets

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
isis timer hello hello-interval [ level-1 | level-2 ]
```

The interval for sending the Hello packets is set on an interface.

On a broadcast link, there are Level-1 and Level-2 Hello packets. For different types of packets, you can set different intervals. If no level is specified, both the Level-1 timer and Level-2 timer are configured. On a P2P link, there are only one type of Hello packets. Thus, neither **level-1** nor **level-2** is required.

 **NOTE**

Parameters level-1 and level-2 are configured only on a broadcast interface.

- Configuring the Invalid Number of Hello Packets

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
isis timer holding-multiplier number [ level-1 | level-2 ]
```

The invalid number of Hello packets is set.

If no level is specified, both the Level-1 timer and Level-2 timer are configured.

 **NOTE**

level-1 and **level-2** can be found only on the broadcast interface.

IS-IS maintains neighbor relationships with neighbors through Hello packets. If the local router does not receive any Hello packet from a neighbor within holding time, the local router declares that the neighbor is invalid.

In IS-IS, the period during which the local router and its neighbor keep the neighbor relationship is determined by the invalid number of Hello packets and the interval for sending Hello packets.

- Configuring the Interval for Sending CSNPs

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
isis timer csnp csnp-interval [ level-1 | level-2 ]
```

The interval for sending CSNPs is set.

CSNPs are transmitted by the Designated IS (DIS) to synchronize an LSDB in a broadcast network. If the level is not specified, the timer of the current level is configured.

- Configuring the Interval for Retransmitting LSPs

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
isis timer lsp-retransmit retransmit-interval
```

The interval for retransmitting LSPs on a P2P link is set.

On a P2P link, if the local router does not receive the response within a period of time after it sends an LSP, it considers that the LSP is lost or dropped. To ensure the reliable transmission, the local router retransmits the LSP according to the *retransmit-interval*. By default, the interval for retransmitting the LSP packet on the P2P link is 5 seconds.

The LSPs sent on a broadcast link do not need any response.

- Configuring the Minimum Interval for Sending LSPs

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
isis timer lsp-throttle throttle-interval [ count count ]
```

The minimum interval for sending LSPs is set.

count: specifies the maximum number of LSP packets to be sent within the period specified by *throttle-interval*. The value ranges from 1 to 1000.

You can set the minimum interval for sending LSPs on an IS-IS interface, that is, the delay between two consecutive LSPs. The value is also the interval for sending fragments of a CSNP.

----End

7.3.3 Configuring LSP Parameters

By configuring the LSP generation timer, you can adjust the time that an IS-IS network generates LSPs. Setting the size of the LSP to be generated or received by IS-IS can affect the transmission of LSPs.

Context

Do as follows on the router that runs IS-IS:

Procedure

- Configuring the Interval for Refreshing LSPs

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

3. Run:

```
timer lsp-refresh refresh-time
```

The LSP refreshment period is set.

To synchronize all the LSPs in an area, the routers in the area periodically send all the current LSPs.

By default, the LSP refreshment period is 900 seconds, and the maximum lifetime of an LSP is 1200 seconds. When performing configurations, ensure that the LSP refresh interval is 300 seconds shorter than the maximum LSP Keepalive time. In this way, new LSPs can reach all routers in an area before existing LSPs expire.

NOTE

It is recommended to adjust the difference between the LSP refresh period and the maximum Keepalive time of the LSP depending on the network scale.

- Configuring the Max Lifetime of an LSP

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

3. Run:
`timer lsp-max-age age-time`

The lifetime of an LSP is set.

When a router generates an LSP, it sets the max lifetime for the LSP. After the LSP is received by other routers, its lifetime decreases as time passes. If a router does not receive any updated LSP and the lifetime of this LSP decreases to 0, the lifetime of the LSP lasts 60s. If a new LSP is still not received, this LSP is deleted from the LSDB.

- Configuring the Intelligent Timer Used to Generate LSPs

1. Run:
`system-view`

The system view is displayed.

2. Run:
`isis [process-id]`

The IS-IS view is displayed.

3. Run:
`timer lsp-generation max-interval [init-interval [incr-interval]]
[level-1 | level-2]`

The intelligent timer used to generate LSPs is set.

If no level is configured, both Level-1 and Level-2 are configured.

The initial delay for generating the same LSPs (or LSP fragments) is *init-interval*. The delay for generating the same LSPs (or LSP fragments) secondly is *incr-interval*. When the routes change each time, the delay for generating the same LSPs (or LSP fragments) is twice as the previous value until the delay is up to *max-interval*. After the delay reaches *max-interval* for three times or reset the IS-IS process, the interval is reduced to *init-interval*.

When *incr-interval* is not used and generating the same LSPs (or LSP fragments) for the first time, *init-interval* is used as the initial delay. Then, the delay for generating the same LSPs (or LSP fragments) is *max-interval*. After the delay reaches *max-interval* for three times or the IS-IS process is reset, the interval is reduced to *init-interval*.

When only *max-interval* is used, the intelligent timer changes into a normal one-short timer.

- Configuring the Size of an LSP

1. Run:
`system-view`

The system view is displayed.

2. Run:
`isis [process-id]`

The IS-IS view is displayed.

3. Run:
`lsp-length originate max-size`

The size of an LSP generated by the system is set.

4. Run:
`lsp-length receive max-size`

The size of a received LSP is set.

 **NOTE**

When using *max-size*, ensure that the value of the *max-size* of the generated LSP packet (or the forwarded LSP packet) must be smaller than or equal to that of the received LSP packet.

The value of *max-size* set by using the **lsp-length** command must meet the following conditions.

- The MTU value of an Ethernet interface must be greater than or equal to the sum of *max-size* and 3.
- The MTU value of a P2P interface must be greater than or equal to the value of *max-size*.

● Adding an Interface to a Mesh Group

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
isis mesh-group { mesh-group-number | mesh-blocked }
```

The interface is added to a mesh group.

On the Non Broadcast Multiple Access (NBMA) network, after receiving an LSP, the interface of a router floods the LSP to the other interfaces. In a network with higher connectivity and multiple P2P links, however, the flooding method causes repeated LSP flooding and wastes bandwidth.

To avoid the preceding problem, you can configure several interfaces to form a mesh group. The router in the mesh group does not flood the LSP received from an interface of the group to the other interfaces of the group, but floods it to interfaces of other groups or interfaces that do not belong to any group.

When **mesh-blocked** is configured on an interface, the interface is blocked and cannot flood LSPs outside. All the interfaces added to a mesh group implement global LSDB synchronization through CSNP and PSNP mechanisms.

● Configuring LSP Fragments Extension

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

3. Run:

```
lsp-fragments-extend [ { level-1 | level-2 | level-1-2 } | { mode-1 | mode-2 } ] *
```

LSP fragments extension is enabled in an IS-IS process.

4. Run:

```
virtual-system virtual-system-id
```

A virtual system is configured.

To configure a router to generate extended LSP fragments, you must configure at least one virtual system. The ID of the virtual system must be unique in the domain.

An IS-IS process can be configured with up to 50 virtual system IDs.

If neither the mode nor the level is specified when LSP fragments extension is configured, mode-1 and Level-1-2 are used by default.

----End

7.3.4 Checking the Configuration

After configuring parameters that affect the IS-IS neighbor relationship, you can check information about the IS-IS interface and statistics about the IS-IS process.

Prerequisite

The configurations of Establishing or Maintaining IS-IS Neighbor Relationships or Adjacencies are complete.

Procedure

- Run **display isis interface** [[**verbose** | **traffic-eng**] * | **tunnel**] [*process-id* | **vpn-instance** *vpn-instance-name*] command to check information about the interface enabled with IS-IS.
- Check the statistics of the IS-IS process:
 - **display isis statistics** [**level-1** | **level-2** | **level-1-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]
 - **display isis statistics packet** [**interface** *interface-type interface-number*]
 - **display isis process-id statistics** [**level-1** | **level-2** | **level-1-2** | **packet**]

----End

Example

On GE 1/0/0, set the interval for sending Hello packets to 15, the invalid number of Hello packets to 10, the interval for sending Level-1 CSNPs to 123, and the minimum interval for sending LSPs to 159. Run the **display isis interface verbose** command. The display is as follows:

```
<HUAWEI> display isis interface verbose
Interface information for ISIS(1)
-----
Interface      Id      IPV4.State      IPV6.State      MTU  Type  DIS
GE 1/0/0      001      Up              Down            1497 L1/L2 No/No
Description    : GigabitEthernet1/0/0 Interface
SNPA Address   : 00e0-095b-4201
IP Address     : 123.1.1.1
IPV6 Link Local Address :
IPV6 Global Address(es) :
Csnp Timer Value : L1 123 L2 10
Hello Timer Value : L1 15 L2 15
DIS Hello Timer Value : L1 5 L2 5
Hello Multiplier Value : L1 10 L2 10
LSP-Throttle Timer : L12 159
Cost           : L1 10 L2 10
Ipv6 Cost      : L1 10 L2 10
```

```

Priority                : L1    64  L2    64
Retransmit Timer Value : L12    5
Bandwidth-Value        : Low 100000000 High    0
Static Bfd              : NO
Dynamic Bfd             : NO
Fast-Sense Rpr         : NO
    
```

7.4 Configuring IS-IS Attributes in Different Types of Networks

This section describes how to configure IS-IS attributes in different types of networks because IS-IS attributes vary with network types.

7.4.1 Establishing the Configuration Task

Before configuring IS-IS attributes in different types of networks, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

IS-IS attributes are different in different types of networks. This section describes how to configure IS-IS attributes in different types of networks, covering:

- Simulating a P2P interface on an Ethernet interface by changing the link type of the Ethernet interface to P2P
- Controlling the DIS election
- Checking the OSI network negotiation status on a PPP link
- Enabling two P2P interfaces on two routers in different network segments to establish the neighbor relationship by configuring the interfaces not to perform the IP address check

Pre-configuration Tasks

Before configuring IS-IS attributes in different types of networks, complete the following tasks:

- Configuring IP addresses of interfaces to make neighboring nodes reachable
- [7.2 Configuring Basic IS-IS Functions](#)

Data Preparation

To configure IS-IS attributes in different types of networks, you need the following data.

No.	Data
1	Network type of an interface
2	DIS priority of an interface

7.4.2 Configuring the Network Type of IS-IS Interface

By simulating the network type of an IS-IS interface as P2P, you can ensure that the network types of the two interfaces are the same so that the IS-IS neighbor relationship can be successfully established.

Context

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
isis circuit-type p2p
```

The network type of the interface is set to P2P.

By default, the network type of an interface is determined by the physical interface.

For an interface enabled with IS-IS, when the network type of the interface changes, its related configurations change. Details are as follows:

- After a broadcast interface is simulated as a P2P interface through the **isis circuit-type p2p** command, the interval for sending Hello packets, number of Hello packets that IS-IS does not receive from a neighbor before the neighbor is declared Down, interval for retransmitting LSPs on a P2P link, and various IS-IS authentication modes are restored to the default settings; other configurations such as the DIS priority, DIS name, and interval for sending CSNPs on a broadcast network become invalid.
- After the **undo isis circuit-type** command is run to restore the network type of the interface, the interval for sending Hello packets, number of Hello packets that IS-IS does not receive from a neighbor before the neighbor is declared Down, interval for retransmitting LSPs on a P2P link, various IS-IS authentication modes, DIS priority, and interval for sending CSNPs on a broadcast network are restored to the default settings.

NOTE

Network types of the IS-IS interfaces on both ends of the link must be consistent; otherwise, the neighbor relationship cannot be established.

----End

7.4.3 Configuring the DIS Priority of an Interface

By setting the DIS priority of an interface on a broadcast network, you can control the DIS election on the broadcast network.

Context

Level-1 DISs and the Level-2 DISs are elected respectively, and you can configure different priorities for them. If neither Level-1 nor Level-2 is specified in the command, configure the same priority for Level-1 and Level-2.

The DIS election is based on priorities of interfaces. The interface with the highest priority is elected as the DIS. In the case of the same DIS priority, the interface with the highest MAC address is elected as the DIS. Different from OSPF, an interface with the DIS priority as 0 still takes part in the DIS election in IS-IS.

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
isis dis-priority priority [ level-1 | level-2 ]
```

The DIS priority of the interface is set.

The greater the value is, the higher the priority is.

----End

Follow-up Procedure

NOTE

The DIS priority is valid only to the broadcast network.

If the **isis circuit-type** command is run to emulate the interface as a P2P interface, the **isis dis-priority** command becomes invalid on the interface; after the **undo isis circuit-type** command is run to restore the broadcast interface, the default DIS priority is used.

7.4.4 Configuring the Negotiation Model on a P2P Link

With the 3-way handshake mechanism, you can detect the fault of a unidirectional link and detect the unreliable peer status on P2P interfaces caused by other link faults.

Context

The command is used to specify the negotiation mode for setting up the neighbor relationship on a P2P link. The 3-way handshake mechanism can be used to detect faults on a unidirectional link and detect the unreliable peer status on P2P interfaces of a link with other faults.

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
isis ppp-negotiation { 2-way | 3-way [ only ] }
```

The negotiation model used by the interface is specified.

By default, the 3-way negotiation model is used.

This command is only used to set up the neighbor relationship on a P2P link. For a broadcast link, you can run the **isis circuit-type p2p** command to change the link type to P2P, and then run this command to set the negotiation model.

----End

7.4.5 Configuring OSICP Check on PPP Interfaces

After OSICP negotiation check is configured on PPP interfaces, the OSI network negotiation status of PPP will affect the IS-IS interface status.

Context

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
isis ppp-osicp-check
```

The PPP interface is configured to perform the OSICP status check.

By default, PPP OSCIP status does not affect the status of the IS-IS interface.

This command is applicable only to PPP interfaces, and does not take effect for P2P interfaces on other types of links. For the point-to-point interfaces running other link protocols, this command is invalid.

----End

Follow-up Procedure

After this command is configured, OSI network negotiation status of PPP affects IS-IS interface status. When PPP senses that the OSI network fails to work, the link status of the IS-IS interface turns Down. In this way, IS-IS no longer advertises routes to the network segment where this IS-IS interface resides through LSPs.

7.4.6 Configuring IS-IS Not to Check the IP Address in a Received Hello Packet

By configuring IS-IS not to check the IP addresses in the received Hello packets, you can establish the IS-IS neighbor relationship between the two interfaces that are on the same link but on different network segments.

Context

In general, IS-IS checks the IP address of a received Hello packet. Only the IP address and the local interface that receives the packet belong to the same network segment, the two interfaces can set up the neighbor relationship.

If the IP addresses of the two interfaces are not in the same network segment and the **isis peer-ip-ignore** command is used on the two interfaces, the two interfaces do not check the IP addresses of received Hello packets. The two interfaces then can set up the neighbor relationship normally. The routing table has routes of the two different network segments, but they cannot ping through each other.

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 (Optional) Run:

```
isis circuit-type p2p
```

The network type of the interface is set to P2P.

NOTE

- For broadcast interfaces, you need to run the **isis circuit-type p2p** command in the interface view before running the **isis peer-ip-ignore** command. The **isis circuit-type p2p** command is valid only for broadcast interfaces.
- For P2P and NBMA interfaces, you can directly run the **isis peer-ip-ignore** command without running the **isis circuit-type p2p** command.

Step 4 Run:

```
isis peer-ip-ignore
```

IS-IS does not check the IP address in the Hello packet received by the interface.

----End

7.4.7 Checking the Configuration

After configuring IS-IS attributes in different types of networks, you can check information about the interfaces enabled with IS-IS.

Prerequisite

The configurations of IS-IS Attributes in Different Types of Networks are complete.

Procedure

- Run **display isis interface** [[**verbose** | **traffic-eng**] * | **tunnel**] [*process-id* | **vpn-instance** *vpn-instance-name*] command to check the information about an interface enabled with IS-IS.

----End

Example

On GE 1/0/0, set its network type to BROADCAST and the DIS priority to 100. Run the **display isis interface verbose** command. The display is as follows:

```
<HUAWEI> display isis interface verbose
Interface information for ISIS(1)
-----
Interface      Id      IPV4.State      IPV6.State      MTU  Type  DIS
GE 1/0/0      001      Up              Down            1497 L1/L2 No/No
Description    : GigabitEthernet1/0/0 Interface
SNPA Address   : 00e0-095b-4201
IP Address     : 123.1.1.1
IPV6 Link Local Address :
IPV6 Global Address(es) :
Csnp Timer Value : L1 123 L2 10
Hello Timer Value : L1 15 L2 15
DIS Hello Timer Value : L1 5 L2 5
Hello Multiplier Value : L1 10 L2 10
LSP-Throttle Timer : L12 159
Cost           : L1 10 L2 10
Ipv6 Cost      : L1 10 L2 10
Priority      : L1 100 L2 100
Retransmit Timer Value : L12 5
Bandwidth-Value : Low 100000000 High 0
Static Bfd     : NO
Dynamic Bfd    : NO
Fast-Sense Rpr : NO
Extended-Circuit-Id Value : 0000000001
```

7.5 Configuring IS-IS Route Attributes

Setting IS-IS route attributes affects IS-IS route selection.

7.5.1 Establishing the Configuration Task

Before configuring IS-IS route attributes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

This section describes how to change attributes of routing information, including IS-IS preference, costs of IS-IS interfaces, convergence priorities of IS-IS routes, and configuring load balancing among multiple equal-cost routes.

Pre-configuration Tasks

Before configuring IS-IS route attributes, complete the following tasks:

- Configuring IP addresses of interfaces to make neighboring nodes reachable
- [Configuring Basic IS-IS Functions](#)

Data Preparation

To configure IS-IS route attributes, you need the following data.

No.	Data
1	IS-IS preference
2	Cost of each IS-IS interface
3	Convergence priorities of IS-IS routes

7.5.2 Configuring the Cost of an IS-IS Interface

Setting the cost of an IS-IS interface affects the cost of IS-IS routes and then affects IS-IS route selection.

Context

IS-IS determines the cost of an interface in following three ways in the descending order:

- Interface cost: indicates the link cost configured for a single interface.
- Global cost: indicates the link cost configured for all the interfaces.
- Auto-cost: indicates the link cost calculated automatically based on the interface bandwidth.

If no command is used explicitly, the default cost of an IS-IS interface is 10, and cost type is narrow.

Do as follows on the router that runs IS-IS:

Procedure

- Configuring the IS-IS Cost Type
 1. Run:


```
system-view
```

 The system view is displayed.
 2. Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

3. Run:

```
cost-style { narrow | wide | wide-compatible | { narrow-compatible | compatible } [ relax-spf-limit ] }
```

The IS-IS cost type is configured.

For different cost types, the cost range of an interface is different, and the cost range of the received route is also different:

- If the cost type is narrow, the cost of the interface ranges from 1 to 63. The maximum cost of the received route is 1023.
- If the cost type is narrow-compatible or compatible, the cost of the interface ranges from 1 to 63. The cost of the received route is related to **relax-spf-limit**.
 - If **relax-spf-limit** is not set, the following situations may occur:

If the cost of the route is smaller than or equal to 1023 and the link costs of all interfaces that the route passes through are smaller than or equal to 63, The cost of the route received on the interface adopts the actual cost.

If the cost of the route is smaller than or equal to 1023 but the link costs of the interfaces that the route passes through are greater than 63, the router can learn only the routes of the network segment where the interface resides and the routes imported by the interface. The cost of the route received on the interface adopts the actual cost and then the routes forwarded by the interface are discarded.

If the cost of the route is greater than 1023, the router can learn the routes of the interface whose link cost exceeds 1023 for the first time. The link cost of each interface before this interface is not greater than 63. The routes of the network segment where the interface resides and routes imported by the interface can be learned by the router. The cost of the route received on the interface adopts 1023. The routes forwarded by the interface are discarded.
 - If **relax-spf-limit** is set, there is no limit to the link costs of interfaces and route costs. The cost of the route is the actual one.
- If the cost type is wide or wide-compatible, the cost of the interface ranges from 1 to 16777215. If the cost is 16777215, the Neighbor TLV (cost is 16777215) generated on the link cannot be used for route calculation and can be used only to deliver the information related to TE. The maximum cost of the received route is 0x FFFFFFFF.

● Configuring the Cost of an the IS-IS Interface

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The interface view is displayed.

3. Run:

```
isis cost cost [ level-1 | level-2 ]
```

The cost of the IS-IS interface is set.

You can use the command to configure the cost of a specific interface.

- Configuring IS-IS Global Cost

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

3. Run:

```
circuit-cost cost [ level-1 | level-2 ]
```

The global IS-IS cost is set.

You can use the command to change the costs of all interfaces in a specified process on localrouter at a time.

- Enabling Auto-Cost

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

3. Run:

```
bandwidth-reference value
```

The reference value of the bandwidth is set.

By default, the reference value of the bandwidth is 100.

4. Run:

```
auto-cost enable
```

The interface is configured to automatically calculate the cost of its bandwidth.

The bandwidth reference value configured in Step 3 is valid only when the cost type is wide or wide-compatible. Then, the cost of each interface is calculated through the formula, the cost = (bandwidth-reference/interface bandwidth) × 10.

When the cost type is narrow, narrow-compatible, or compatible, the cost of each interface can be obtained from the following table.

Table 7-1 Relationship between the interface cost and the bandwidth

Cost	Interface Bandwidth Range
60	interface bandwidth ≤ 10Mbit/s
50	10Mbit/s < interface bandwidth ≤ 100Mbit/s
40	100Mbit/s < interface bandwidth ≤ 155Mbit/s
30	155Mbit/s < interface bandwidth ≤ 622Mbit/s

Cost	Interface Bandwidth Range
20	622Mbit/s < interface bandwidth ≤ 2.5Gbit/s
10	2.5Gbit/s < interface bandwidth

 **NOTE**

To change the cost of a loopback interface, run the **isis cost** command in the interface view.

----End

7.5.3 Configuring the Preference of IS-IS

Setting the priorities of IS-IS and IS-IS routes affects IS-IS route selection and route convergence.

Context

Do as follows on the router that runs IS-IS:

Procedure

- Configuring the Preference of IS-IS

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

3. Run:

```
preference preference
```

The preference of IS-IS is set.

This command is used to set the preference for IS-IS. The smaller the value is, the higher the preference is.

By default, the preference of IS-IS is 15.

A router can run multiple routing protocols at the same time. When multiple routing protocols discover routes to the same destination, the protocol with the highest preference takes effect.

- Configuring the Preference of a Specified IS-IS Route

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
isis [ process-id ]
```


The IS-IS view is displayed.

3. Run:

```
preference route-policy route-policy-name
```

The preference of a specified IS-IS route is set according to the routing policy.

- Configuring the Preference of IS-IS Equal-Cost Routes

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

3. Run:

```
nexthop ip-address weight value
```

The preference of IS-IS load balancing is set.

After the equal-cost routes of IS-IS are calculated through the SPF algorithm, you can run the **nexthop** command to choose the route of the highest preference among the equal-cost routes as the next hop. The smaller the weight is, the higher the routing preference is.

By default, the weight is 255. It indicates that the load balancing is performed among the equal-cost routes without distinguishing preferences.

- Configuring the Convergence Priority of IS-IS Routes

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

3. Run:

```
prefix-priority [ level-1 | level-2 ] { critical | high | medium } { ip-  
prefix prefix-name | tag tag-value }
```

Convergence priorities are set for IS-IS routes.

By default, the convergence priority of 32-bit IS-IS host routes is medium and that of other IS-IS routes is low.

The application rule of the convergence priority for IS-IS routes are as follows:

- For the existing IS-IS routes, IS-IS resets the convergence priority for the routes according to the configuration results of the **prefix-priority** command.
- For the new IS-IS routes, IS-IS sets the convergence priority for the routes according to the filtering results of the **prefix-priority** command.
- If an IS-IS route conforms to the matching rules of multiple convergence priorities, the convergence priority of this IS-IS route is the top convergence priority.
- The convergence priority of Level-1 routes is higher than that of Level-2 routes.

- If Level is not specified, IS-IS configured the convergence priority of Level-1 routes and Level-2 routes.

 **NOTE**

This command takes effect only on the public network.

If the convergence priority of IS-IS routes except the 32-bit IS-IS host routes is set by using the **prefix-priority** command, the default convergence priority of 32-bit IS-IS host routes changes from medium to low. The convergence priorities of IS-IS routes are changes with the configuration of the **prefix-priority** command.

4. Run:

quit

The system view is displayed.

5. (Optional) Run:

ip route prefix-priority-scheduler *critical-weight high-weight medium-weight low-weight*

The scheduling ratio of IPv4 routes by priority is set.

By default, the scheduling ratio of IPv4 routes by priority is 8:4:2:1.

----End

7.5.4 Configuring IS-IS Load Balancing

On an IS-IS network where there are multiple equal-cost routes, configuring IS-IS load balancing increases the bandwidth utilization of each link.

Context

If there are redundant links on an IS-IS network, there may be multiple equal-cost routes. Configuring IS-IS load balancing can evenly distribute traffic to each link. This increases the bandwidth utilization of each link and prevents network congestion caused by some overloaded links.

Procedure

- Step 1** Run:

system-view

The system view is displayed.

- Step 2** Run:

isis [*process-id*]

The IS-IS view is displayed.

- Step 3** Run:

maximum load-balancing *number*

The maximum number of equal-cost routes that work in load balancing mode is set.

 **NOTE**

If the value specified by *number* is smaller than the number of existing equal-cost routes on a network, IS-IS selects *number* equal-cost routes from all the equal-cost routes to implement load balancing.

----End

7.5.5 Checking the Configuration

After configuring IS-IS route attributes, you can check the cost of IS-IS interfaces and preferences of IS-IS routes.

Prerequisite

The configurations of IS-IS Route Attributes are complete.

Procedure

- Run **display isis interface** [[**verbose** | **traffic-eng**] * | **tunnel**] [*process-id* | **vpn-instance** *vpn-instance-name*] command to check information about the interface enabled with IS-IS.
- Run **display isis route** [*process-id* | **vpn-instance** *vpn-instance-name*] [**ipv4**] [**verbose** | [**level-1** | **level-2**] | *ip-address* [*mask* | *mask-length*]] * command to check information about the convergence priority of IS-IS routes.

----End

Example

Set IPv4 cost and IPv6 cost to 20 on GE 1/0/0. Run the **display isis interface verbose** command. The display is as follows:

```
<HUAWEI> display isis interface verbose

Interface information for ISIS(1)
-----
Interface      Id      IPV4.State      IPV6.State      MTU  Type  DIS
GE1/0/0        001      Up              Down            1497 L1/L2 No/No
Description    : GE1/0/0 Interface
SNPA Address   : 00e0-c72d-da01
IP Address     : 123.1.1.1
IPV6 Link Local Address :
IPV6 Global Address(es) :
Csnp Timer Value : L1 10 L2 10
Hello Timer Value : L1 10 L2 10
DIS Hello Timer Value : L1 3 L2 3
Hello Multiplier Value : L1 3 L2 3
LSP-Throttle Timer : L12 50
Cost           : L1 20 L2 20
Ipv6 Cost      : L1 20 L2 20
Priority        : L1 64 L2 64
Retransmit Timer Value : L12 5
Bandwidth-Value : Low 100000000 High 0
Static Bfd     : NO
Dynamic Bfd    : NO
Fast-Sense Rpr : NO
```

Set the convergence priorities of the imported routes 10.10.10.0/24 to **Critical**. The display is as follows:

```
<HUAWEI> display isis route verbose

Route information for ISIS(1)
-----

ISIS(1) Level-2 Forwarding Table
-----

IPV4 Dest : 10.10.10.0/24      Int. Cost : 20      Ext. Cost : NULL
```

```

Admin Tag   : -                               Src Count  : 2                               Flags      : A/-/-/-
Priority    : Critical                       Interface  :                               ExitIndex  :
NextHop    :                               Pos1/0/0                               0x80000001
    1.1.1.2

IPv4 Dest   : 1.1.1.0/24                     Int. Cost  : 10                             Ext. Cost  : NULL
Admin Tag   : -                               Src Count  : 2                               Flags      : D/-/L/-
Priority    : Medium                           Interface  :                               ExitIndex  :
NextHop    :                               Pos1/0/0                               0x00000000
    Direct

IPv4 Dest   : 20.20.20.0/24                  Int. Cost  : 20                             Ext. Cost  : NULL
Admin Tag   : -                               Src Count  : 2                               Flags      : A/-/-/-
Priority    : Low                               Interface  :                               ExitIndex  :
NextHop    :                               Pos1/0/0                               0x80000001
    1.1.1.2

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut
      U-Up/Down Bit Set
    
```

7.6 Controlling the Advertisement of IS-IS Routes

By configuring route leaking and route aggregation and configuring routers to generate default routes, you can control the advertisement of IS-IS routes with different levels in different areas, and control the number of IS-IS routing entries.

7.6.1 Establishing the Configuration Task

Before controlling the advertisement of IS-IS routes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

This section describes how to control the advertisement of IS-IS routing information, such as the advertisement of aggregated routes, generation of default routes, and configurations of route leaking.

Pre-configuration Tasks

Before configuring to control the advertisement of IS-IS routing information, complete the following tasks:

- Configuring IP addresses of interfaces to make neighboring nodes reachable
- [7.2 Configuring Basic IS-IS Functions](#)

Data Preparation

To control the advertisement of IS-IS routing information, you need the following data.

No.	Data
1	Routes to be aggregated
2	Types of route leaking

7.6.2 Configuring IS-IS Route Aggregation

Summarizing multiple routes with the same IP prefix into one route can reduce the number of IS-IS routing entries.

Context

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

Step 3 Run:

```
summary ip-address mask [ avoid-feedback | generate_null0_route | tag tag |  
[ level-1 | level-1-2 | level-2 ]] *
```

IS-IS route aggregation is configured.

----End

7.6.3 Configuring IS-IS to Generate Default Routes

By configuring IS-IS to generate default routes, you can control the advertisement of IS-IS routes.

Context

The level of the router determines the level of the default routes. The default routes generated through this command are advertised only to the routers of the same level. Through the routing policy, you can configure the router to generate a default route forcibly only when there is a route matching the policy in the routing table.

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

Step 3 Run:

```
default-route-advertise [ always | match default | route-policy route-policy-name ]  
[ cost cost | tag tag | [ level-1 | level-1-2 | level-2 ] ] * [ avoid-learning ]
```

IS-IS is configured to generate default routes.

----End

7.6.4 Controlling the Route Leaking from a Level-2 Area to a Level-1 Area

By configuring IS-IS route leaking from a Level-2 area to a Level-1 area, you can leak Level-2 routes and level-1 routes in other areas to a Level-1 area.

Context

After IS-IS route leaking is enabled, a Level-1-2 router can leak its routes that meet the requirements from a Level-2 area to a Level-1 area, and can advertise routing information through Level-1 LSPs.

Do as follows on the Level-1-2 router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

Step 3 Run:

```
import-route isis level-2 into level-1 [ tag tag | filter-policy { acl-number | acl-  
name acl-name | ip-prefix ip-prefix-name | route-policy route-policy-name } ] *
```

IS-IS route leaking is enabled.

Routes of Level-2 area and those of other Level-1 areas can be leaked to the Level-1 area where the router resides.

The command is run on the Level-1-2 router which is connected to external areas. By default, Level-2 routes are not leaked to a Level-1 area.

----End

7.6.5 Controlling the Route Leaking from a Level-1 Area to a Level-2 Area

By configuring IS-IS route leaking from a Level-1 area to a Level-2 area, you can prevent route leaking from a Level-1 area to a Level-2 area, and thus effectively control Level-2 routes.

Context

Do as follows on the Level-1-2 router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

Step 3 Run:

```
import-route isis level-1 into level-2 [ tag tag | filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name | route-policy route-policy-name } ] *
```

The routing policy is configured to prevent route leaking from Level-1 area to Level-2 area.

You can use the **undo import-route isis level-1 into level-2** command to prevent route leaking from Level-1 area to Level-2 area.

This command is run on the Level-1-2 router that is connected to external areas. By default, all the routing information (except information about the default route) leaked from a Level-1 area to a Level-2 area.

----End

7.6.6 Checking the Configuration

After configuring route leaking and route aggregation and configuring routers to generate default routes, you can check the configuration by viewing detailed information about the IS-IS routing table and IS-IS routes.

Prerequisite

The configurations of Controlling the Advertisement of IS-IS Routes are complete.

Procedure

- Run **display isis route** [*process-id*] [**vpn-instance** *vpn-instance-name*] [**ipv4**] [**verbose** | [**level-1** | **level-2**] | *ip-address* [*mask* | *mask-length*] *] command to check the IS-IS routing information.
- Run **display isis lsdb** [{ **level-1** | **level-2** } | **verbose** | { **local** | *lsp-id* | **is-name** *symbolic-name* }] * [*process-id* | **vpn-instance** *vpn-instance-name*] command to check the information about the IS-IS LSDB.

----End

Example

Configure IS-IS process 1 to leak routes from a Level-2 area to a Level-1 area. Run **display isis route** the command. The display is as follows:

```
<HUAWEI> display isis route
                        Route information for ISIS(1)
                        -----
                        ISIS(1) Level-1 Forwarding Table
                        -----
```

IPv4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags
10.10.20.0/24	20	NULL	GE1/0/0	10.10.10.1	A/-/L/-
10.10.10.0/24	10	NULL	GE1/0/0	Direct	D/-/L/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set					
ISIS(1) Level-2 Forwarding Table					
IPv4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags
10.10.20.0/24	20	NULL	GE1/0/0	10.10.10.1	A/-/L/-
10.10.10.0/24	10	NULL	GE1/0/0	Direct	D/-/L/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, U-Up/Down Bit Set					

7.7 Controlling the Receiving of IS-IS Routes

By configuring IS-IS to filter routing information, you can control the number of IS-IS routes to be added to the IP routing table and the number of imported routes to be added to the IS-IS routing table.

7.7.1 Establishing the Configuration Task

Before controlling the receiving of IS-IS routes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

This section describes how to control the receiving of IS-IS routing information, such as filtering of the received routes and importing external routes.

Pre-configuration Tasks

Before controlling the receiving of IS-IS routing information, complete the following tasks:

- Configuring IP addresses of interfaces to make neighboring nodes reachable
- [7.2 Configuring Basic IS-IS Functions](#)

Data Preparation

To control the receiving of IS-IS routing information, you need the following data.

No.	Data
1	Filtering list used to filter routing information
2	Protocol name and the process number of the external routes to be imported

7.7.2 Configuring IS-IS to Filter the Received Routes

By configuring IS-IS to filter the received routes, you can control the number of IS-IS routes to be added to the IP routing table, and thus reduce the size of the IP routing table.

Context

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

Step 3 Run:

```
filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name | route-policy route-policy-name } import
```

IS-IS is configured to filter the received routes to determine which routes are to be added to the IP routing table.

----End

7.7.3 Configuring IS-IS to Import External Routes

By configuring IS-IS to import routes, you can enable IS-IS to learn routing information of other protocols or other IS-IS processes.

Context

IS-IS regards the routes discovered by the other routing protocols or other IS-IS processes as external routes. When routes of other protocols are imported, the default costs of the imported routes can be specified.

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

Step 3 Configuring IS-IS to Import External Routes

If you want to set the cost for the imported route, you can run the **import-route protocol** [process-id] [**cost-type** { external | internal }] [**cost cost**] [**tag tag**] [**route-policy route-policy-name**] [**level-1** | **level-2** | **level-1-2**] * command to import the external routes.

If you want to keep the original cost for the imported route, you can run the **import-route** { { **rip** | **isis** | **ospf** } [*process-id*] | **direct** | **bgp** } **inherit-cost** [**tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] * command to import the external routes.

Step 4 Run:

```
filter-policy
 { acl-number | acl-name acl-name | ip-prefix ip-prefix-name | route-policy route-policy-name } export [ protocol [ process-id ] ]
```

Imported routes are filtered before being advertised.

If no level is specified in the **import-route** command, the routes are imported to the Level-2 routing table by default.

----End

7.7.4 Checking the Configuration

After configuring IS-IS to filter the received routes and the imported external routes, you can check the configuration by viewing the IS-IS routing table and IP routing table.

Prerequisite

The configurations of Controlling the Receiving of IS-IS Routes are complete.

Procedure

- Run **display isis lsdb** [{ **level-1** | **level-2** } | **verbose** | { **local** | *lsp-id* | **is-name** *symbolic-name* }] * [*process-id* | **vpn-instance** *vpn-instance-name*] command to check information about IS-IS LSDB.
- Run **display isis route** [*process-id* | **vpn-instance** *vpn-instance-name*] [**ipv4**] [**verbose** | [**level-1** | **level-2**] | *ip-address* [*mask* | *mask-length*]] * command to check IS-IS routing information.

----End

Example

Run the **display isis route** command. If the IS-IS neighbor relationship is correctly set up, you can find that IS-IS process 1 on the local router imports static route 169.1.1.0/24.

```
<HUAWEI> display isis route
                ISIS(1) Level-2 Forwarding Table
                -----
                IPV4 Destination      IntCost      ExtCost ExitInterface      NextHop      Flags
                -----
                123.1.1.0/24          10           NULL     GE1/0/0              Direct       D/-/L/-
                Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                U-Up/Down Bit Set
                ISIS(1) Level-2 Redistribute Table
                -----
                Type IPV4 Destination      IntCost      ExtCost Tag
                -----
                S    169.1.1.0/24          0           NULL
                Type: D-Direct, I-ISIS, S-Static, O-OSPF, B-BGP, R-RIP, U-UNR
```

7.8 Adjusting and Optimizing an IS-IS Network

By adjusting and optimizing IS-IS, you can enable IS-IS to meet the requirements of complicated networks.

7.8.1 Establishing the Configuration Task

Before adjusting and optimizing IS-IS, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

This section mainly describes the adjustment and optimization of an IS-IS network. The details are as follows:

- Configuring levels of IS-IS interfaces and interface status
- Adjusting SPF parameters
- Configuring the IS-IS dynamic hostname mapping and the authentication functions to meet the requirements of users for security and maintenance

Pre-configuration Tasks

Before adjusting and optimizing an IS-IS network, complete the following tasks:

- Configuring IP addresses of interfaces to make neighboring nodes reachable
- [7.2 Configuring Basic IS-IS Functions](#)

Data Preparation

To adjust and optimize an IS-IS network, you need the following data.

No.	Data
1	Levels of IS-IS interfaces
2	Mapping between a system ID and a hostname

7.8.2 Configuring the Level of an IS-IS Interface

By configuring the level of an IS-IS interface, you can determine the level of the neighbor relationship established between the IS-IS interface and its remote end.

Context

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
isis circuit-level [ level-1 | level-1-2 | level-2 ]
```

The level of the interface is set.

By default, the level of the interface is **level-1-2**.

 **NOTE**

Only the current router is a Level-1-2 router, changing the circuit level of the interface is useful. If the current router is not a Level-1-2 router, the level of the router determines the level of the established adjacency.

----End

7.8.3 Setting the Status of IS-IS Interface to Suppressed

By setting the status of an IS-IS interface to silent, you can enable the interface to advertise only direct routes and not to receive or send IS-IS routes. In this manner, the propagation of unnecessary packets on IS-IS networks is controlled.

Context

When an IS-IS network is connected to other ASs, IS-IS needs to be enabled on the outgoing interface, so that the routers inside the area can learn the routes to other ASs. The interface, however, sends IS-IS Hello packets to the network segment where the interface resides, which is unnecessary. You can then run the **isis silent** command to enable the suppression function on the IS-IS interface.

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
isis silent
```

The status of the IS-IS interface is set to suppressed.

When the status of the IS-IS interface becomes suppressed, the interface does not send or receives any IS-IS packet. The routes of the network segment where the interface resides can still be advertised to other routers inside the AS.

 **NOTE**

If the status of IS-IS protocol on the interfaces in the area is Down, the routers within the area cannot learn the routes to other ASs.

----End

7.8.4 Configuring SPF Parameters

By setting SPF parameters, you can adjust the interval for calculating IS-IS routes, and thus avoid the network flapping caused by frequent route calculation.

Context

Do as follows on the router that runs IS-IS:

Procedure

- Configuring SPF Intelligent Timer

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

3. Run:

```
timer spf max-interval [ init-interval [ incr-interval ] ]
```

The SPF intelligent timer is configured.

The change regularity of the intelligent timer is as follows:

- The delay time for the first SPF calculation is *init-interval*; the delay time for the second SPF calculation is *incr-interval*. Then, each time the route changes, the delay time for SPF calculation is twice as the previous value until the delay time reaches *max-interval*. When the delay time for SPF calculation is *max-interval* for three times, or the ISIS process is restarted, the delay time decreases to *init-interval*.
- When *incr-interval* is unavailable, the delay time of the first SPF calculation is *init-interval*; the delay time of the rest SPF calculation is *max-interval*. When the delay time of SPF calculation is *max-interval* for three times, or the ISIS process is restarted, the delay time decreases to *init-interval*.
- When only *max-interval* is used, the intelligent timer becomes an one-shot triggered timer.

- Configuring the Duration for SPF Calculation

1. Run:

```
system-view
```

The system view is displayed.

2. Run:
`isis [process-id]`
The IS-IS view is displayed.
3. Run:
`spf-slice-size duration-time`

The duration for each SPF calculation is set.

When there are many routing entries (more than 150,000) in a routing table, the SPF calculation occupies the CPU for a long time. To avoid this, you can set the duration for each SPF calculation.

----End

7.8.5 Configuring LSP Fast Flooding

By configuring LSP fast flooding, you can speed up the convergence of IS-IS networks.

Context

Do as follows on the router that runs IS-IS:

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`isis [process-id]`
The IS-IS view is displayed.
- Step 3** Run:
`flash-flood [lsp-count | max-timer-interval interval | [level-1 | level-2]] *`
LSP flash-flood is enabled.

You can run the **flash-flood** command to speed up LSP flooding. The parameter *lsp-count* is used to specify the number of LSPs flooded each time, which is applicable for all interfaces. If the number of the LSPs to be sent is greater than *lsp-count*, the value of *lsp-count* takes effect. You can specify the number of LSPs flooded each time for all the interfaces. If the number of LSPs to be sent exceeds this number, the specified number LSPs are flooded. If the configured timer does not time out before route calculation, the LSPs are flooded immediately; otherwise, the LSPs are sent when the timer times out.

When LSP fast flooding is configured, Level-1 LSPs and Level-2 LSPs are fast flooded if the level is not specified.

----End

7.8.6 Configuring IS-IS Dynamic Hostname Mapping

By configuring IS-IS dynamic hostname mapping, you can improve the maintainability and facilitate the maintenance of IS-IS networks.

Context

Do as follows on the router that runs IS-IS:

Procedure

- Configuring the Hostname for the Local IS
 1. Run:
`system-view`
The system view is displayed.
 2. Run:
`isis [process-id]`
The IS-IS view is displayed.
 3. Run:
`is-name symbolic-name`
The hostname of the local IS is configured.

This command is used to configure a name for the local IS-IS process and to enable the mapping from the system ID to the hostname. The configured name is advertised to the other routers in the area through LSPs.

You must run the `is-name` command before enabling the dynamic hostname mapping for the IS-IS process; otherwise, the display command cannot display the mapping between the system ID and the hostname.
- Configure the hostname for the remote IS.
 1. Run:
`system-view`
The system view is displayed.
 2. Run:
`isis [process-id]`
The IS-IS view is displayed.
 3. Run:
`is-name map system-id symbolic-name`
The hostname for the remote IS is configured.

This command is used to locally configure the name for the remote IS-IS router. Each system ID is corresponding to only one name.

If an IS name is configured on both a local router and a remote router, the local setting overwrites the remote setting.
- Configure the hostname for the DIS.
 1. Run:
`system-view`
The system view is displayed.
 2. Run:
`interface interface-type interface-number`

The interface view is displayed.

3. Run:

```
isis dis-name symbolic-name
```

The hostname of the DIS is configured.

This configuration takes effect only on the DIS. The interface on which **isis dis-name** command is used advertises the configured name to the network connected to the interface through a pseudo-node LSP. The configured name is thus associated with the system ID of a specified router. This command does not take effect on P2P interfaces.

----End

7.8.7 Configuring the LSDB Overload Bit

LSPs with the overload bit are still flooded on the network, but the LSPs are not used when routes that pass through a Router configured with the overload bit are calculated.

Context

Do as follows on the router that runs IS-IS:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
isis [ process-id ]
```

The IS-IS view is displayed.

Step 3 Run:

```
set-overload [ on-startup [ timeout1 | start-from-nbr system-id [ timeout1 [ timeout2 ] ] | wait-for-bgp [ timeout1 ] ] ] [ allow { interlevel | external } * ]
```

The overload bit is configured.

----End

Follow-up Procedure

Though the LSPs configured with the overload bit are flooded in the network, the LSPs are not used when the routes that pass the overload Router are calculated. That is, after a router is configured with the overload flag, other routers ignore the router when performing SPF calculation. The direct routes on the router, however, cannot be ignored.

If a router in an IS-IS domain is faulty, route calculation is incorrect in the entire area. To avoid this problem, you can set the overload bit for this router to isolate it from the IS-IS network temporarily. You can thus locate the fault easily.

7.8.8 Configuring the Output of the Adjacency Status

After the output of the IS-IS adjacency status is enabled, the changes in IS-IS adjacencies are output to the configuration terminal until the output of the adjacency status is disabled.

Context

After the local terminal monitor is enabled and the output of the adjacency status is enabled, the changes of the IS-IS adjacency status are output on the terminal until the output is disabled.

Do as follows on the router that runs IS-IS:

Procedure

- Step 1** Run:
- ```
system-view
```
- The system view is displayed.
- Step 2** Run:
- ```
isis [ process-id ]
```
- The IS-IS view is displayed.
- Step 3** Run:
- ```
log-peer-change
```
- The output of the adjacency status is enabled.
- End

## 7.8.9 Checking the Configuration

After adjusting and optimizing IS-IS, you can check the IS-IS mesh group, dynamic hostname, SPF logs, SPF tree, TE information, and IS-IS statistics.

### Prerequisite

The configurations of Adjusting and Optimizing an IS-IS Network are complete.

### Procedure

- Run **display isis mesh-group** [ *process-id* | **vpn-instance** *vpn-instance-name* ] command to check the IS-IS mesh group.
- Run **display isis name-table** [ *process-id* | **vpn-instance** *vpn-instance-name* ] command to check the mapping table in which the hostname of the local router is mapped to a system ID.
- Run **display isis spf-log** [ *process-id* | **vpn-instance** *vpn-instance-name* ] [ **ipv6** | [ **level-1** | **level-2** ] | **verbose** ] \* command to check SPF logs of IS-IS.
- Run **display isis process-id spf-tree statistics** [ [ **level-1** | **level-2** ] | **ipv6** ] \* or **display isis spf-tree statistics** [ [ **level-1** | **level-2** ] | **ipv6** ] \* [ *process-id* | **vpn-instance** *vpn-instance-name* ] command to check the SPF tree of IS-IS.
- Check the statistics about the Traffic Engineering:

- **display isis traffic-eng advertisements** [ { **level-1** | **level-2** | **level-1-2** } | { *lsp-id* | **local** } ] \* [ *process-id* | **vpn-instance** *vpn-instance-name* ]
  - **display isis traffic-eng link** [ { **level-1** | **level-2** | **level-1-2** } | **verbose** ] \* [ *process-id* | **vpn-instance** *vpn-instance-name* ]
  - **display isis traffic-eng network** [ **level-1** | **level-2** | **level-1-2** ] [ *process-id* | **vpn-instance** *vpn-instance-name* ]
  - **display isis traffic-eng statistics** [ *process-id* | **vpn-instance** *vpn-instance-name* ]
  - **display isis traffic-eng sub-tlvs** [ *process-id* | **vpn-instance** *vpn-instance-name* ]
  - Check the statistics about the IS-IS process:
    - **display isis statistics** [ **level-1** | **level-2** | **level-1-2** ] [ *process-id* | **vpn-instance** *vpn-instance-name* ]
    - **display isis statistics packet** [ **interface** *interface-type interface-number* ]
    - **display isis process-id statistics** [ **level-1** | **level-2** | **level-1-2** | **packet** ]
- End

## Example

Run the **display isis name-table 1** command, and you can find that the IS hostname of the local router is **abc**.

```
<HUAWEI> display isis name-table 1

 Name table information for ISIS(1)

System ID Hostname Type

1111.1111.1111 abc DYNAMIC
```

## 7.9 Configuring Local MT

By configuring local MT, you can enable multicast packets to be forwarded through TE tunnels on IS-IS networks.

### 7.9.1 Establishing the Configuration Task

Before configuring IS-IS local MT, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

If multicast and an MPLS TE tunnel are deployed in a network, multicast packets may be forwarded through the TE tunnel. As a result, the routers spanned by the TE tunnel cannot detect the transmission of multicast packets, and thus the routers cannot create any multicast forwarding entry. You can configure local MT function and enable IGP Shortcut on the TE tunnel to avoid the preceding problem. In this manner, a correct MIGP routing table can be created to guide the forwarding of multicast packets.

#### NOTE

Local MT can be configured only in the IS-IS process of the public network instance. In this case, Forwarding Advertise cannot be configured.

## Pre-configuration Tasks

Before configuring IS-IS local MT, complete the following tasks:

- Configuring IP addresses for interfaces to ensure network connectivity between neighboring nodes
- [Configuring Basic IS-IS Functions](#)

## Data Preparation

To configure local MT, you need the following data.

| No. | Data                                                    |
|-----|---------------------------------------------------------|
| 1   | Filtering list used to filter IS-IS routing information |

## 7.9.2 Enabling Local MT

The nodes along the TE tunnel can detect multicast packets and create multicast forwarding entries only after local MT is enabled.

### Context

Do as follows on the router that needs to forward multicast packets and is configured with the TE tunnel enabled with IGP-Shortcut:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis [process-id]
```

The IS-IS view is displayed.

**Step 3** Run:

```
cost-style { compatible [relax-spf-limit] | wide | wide-compatible }
```

The cost type is configured.

**Step 4** Run:

```
traffic-eng
```

TE is configured.

**Step 5** Run:

```
local-mt enable
```

Local MT is enabled.

----End

## 7.9.3 Controlling the Scale of the MIGP Routing Table

By configuring the filtering policy based on multicast source addresses, you can configure routers to add only the routes destined to the specified multicast source address to the MIGP routing table, thus controlling the size of the MIGP routing table.

### Context

After creating the MIGP routing table by **Enabling Local MT**, IS-IS performs route calculation. When the outgoing interface of the next hop calculated is an interface of the TE tunnel enabled with IGP Shortcut, a router uses the physical interface as the outgoing interface of the next hop and saves it to the MIGP routing table.

To make the scale of the MIGP routing table reasonable and accelerate the speed for searching the MIGP routing table, you can configure the filtering policy based on multicast source addresses. Only the routes to multicast source addresses are added to the MIGP table.

#### NOTE

You can configure the routing policy before enabling local MT. This prevents the routes that are not sent to the multicast source address from being added to the MIGP routing table.

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
isis [process-id]
```

The IS-IS view is displayed.

#### Step 3 Run:

```
local-mt filter-policy { acl { acl-number | acl-name } | ip-prefix ip-prefix-name }
```

The local MT routing policy is configured.

---End

## 7.9.4 Checking the Configuration

After configuring local MT, you can check the MIGP routing table, routing information, SPF tree, and IS-IS statistics.

### Prerequisite

The configurations of Local MT are complete.

### Procedure

- Run **display isis** [ process-id ] **migp-routing** [ ip-address [ mask | mask-length ] | { level-1 | level-2 } ] **verbose** \* command to check the IS-IS MIGP routing table.

- Run **display isis route** [ *process-id* | **vpn-instance** *vpn-instance-name* ] [ **ipv4** ] [ **verbose** | [ **level-1** | **level-2** ] | *ip-address* [ *mask* | *mask-length* ] ] \* command to check the IS-IS routing information.
- Run **display isis** [ *process-id* ] **spf-tree statistics** [ [ **level-1** | **level-2** ] | **ipv6** ] \* [ **vpn-instance** *vpn-instance-name* ] command to check the SPF tree of IS-IS.
- Check the statistics of the IS-IS process.
  - **display isis statistics** [ **level-1** | **level-2** | **level-1-2** ] [ *process-id* | **vpn-instance** *vpn-instance-name* ]
  - **display isis statistics packet** [ **interface** *interface-type interface-number* ]
  - **display isis process-id statistics** [ **level-1** | **level-2** | **level-1-2** | **packet** ]

----End

## Example

Configure the MIGP routing table to allow only the routes to the destination 192.168.3.0/24 to pass. Run the **display isis migp-routing** command. The display is as follows:

```
<HUAWEI> display isis migp-routing
MIGP Route information for ISIS(1)

ISIS(1) Level-2 Forwarding Table

IPV4 Destination IntCost ExtCost ExitInterface NextHop Flags

192.168.3.0/24 40 NULL GE2/0/0 10.0.1.1 A/-
Flags: A-Added to MIGP, U-Up/Down Bit Set
```

## 7.10 Configuring IS-IS IPv6

This section describes how to enable the IPv6 capability for IS-IS and adjust IS-IS IPv6 route selection.

### 7.10.1 Establishing the Configuration Task

Before configuring IS-IS IPv6, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

IS-IS supports multiple types networking layer protocols, including IPv6. In an IPv6 network, you can implement interconnection by configuring IS-IS.

The functions and configurations of most attributes of IS-IS IPv6 routes are similar to those of IS-IS IPv4 routes. This section lists only configuration procedures.

#### Pre-configuration Tasks

Before configure IS-IS IPv6, complete the following tasks:

- Enabling global IPv6 in the system view
- Configuring IPv6 addresses of interfaces to make neighboring nodes reachable

- [7.2.2 Starting an IS-IS Process](#)
- [7.2.3 Configuring an NET](#)

## Data Preparation

To configure IS-IS IPv6, you need the following data.

| No. | Data                                                                                                         |
|-----|--------------------------------------------------------------------------------------------------------------|
| 1   | Preference value of IS-IS                                                                                    |
| 2   | Aggregated IS-IS route                                                                                       |
| 3   | The filtering list that is needed to filter the IS-IS routing information and the name of the routing policy |
| 4   | The name and the process number of the external IPv6 routing protocol to be imported                         |

## 7.10.2 Enabling IPv6 on an IS-IS Process

Before configuring IS-IS IPv6, you need to enable the IPv6 capability of an IS-IS process.

### Context

To enable IS-IS, you must first create an IS-IS process and then enable IPv6.

Do as follows on the router that runs IS-IS:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis [process-id]
```

An IS-IS process is enabled and the IS-IS view is displayed.

**Step 3** Run:

```
ipv6 enable
```

IPv6 is enabled on the IS-IS process.

----End

## 7.10.3 Enabling IPv6 on an IS-IS Interface

Enabling IPv6 for an interface can associate the interface with the IS-IS process ID.

### Context

After IPv6 is enabled in the IS-IS process, you also need to enable IPv6 of a specified IS-IS interface.

Do as follows on the router that runs IS-IS:

## Procedure

- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`interface interface-type interface-number`  
The interface view is displayed.
- Step 3** Run:  
`isis ipv6 enable [ process-id ]`  
IS-IS IPv6 is enabled on the interfaces.  
----End

## 7.10.4 Configuring the IPv6 Route Cost on an Interface

Setting the IPv6 route cost for an interface affects IS-IS route selection.

### Context

Do as follows on the routers that runs IS-IS:

## Procedure

- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`interface interface-type interface-number`  
The interface view is displayed.
- Step 3** Run:  
`isis ipv6 cost cost`  
The IPv6 route cost of the link is set.  
The cost is used for SPF calculation in an IPv6 topology.  
----End

## 7.10.5 Configuring the Attributes of IS-IS IPv6 Routes

Configuring IS-IS IPv6 routing features affects IS-IS route selection.

### Context

To perform IPv6-related configurations, you must enable IPv6.

Do as follows on the router that runs IS-IS:

## Procedure

- Configuring the preference of IS-IS IPv6 routes
  1. Run:  
`system-view`  
The system view is displayed.
  2. Run:  
`isis [ process-id ]`  
The IS-IS view is displayed.
  3. Run:  
`ipv6 preference {route-policy route-policy-name | preference } *`  
The preference of IS-IS IPv6 routes is set.
- Configuring IS-IS IPv6 route aggregation
  1. Run:  
`system-view`  
The system view is displayed.
  2. Run:  
`isis [ process-id ]`  
The IS-IS view is displayed.
  3. Run:  
`ipv6 summary ipv6-address prefix-length [ avoid-feedback | generate_null10_route | tag tag | [ level-1 | level-1-2 | level-2 ] ] *`  
IS-IS IPv6 route aggregation is configured.  
  
If no level is specified during IS-IS route aggregation, Level-2 routes are aggregated by default.
- Configuring IS-IS to generate default IPv6 routes
  1. Run:  
`system-view`  
The system view is displayed.
  2. Run:  
`isis [ process-id ]`  
The IS-IS view is displayed.
  3. Run:  
`ipv6 default-route-advertise [ always | match default | route-policy route-policy-name ] [ cost cost | tag tag | [ level-1 | level-2 | level-1-2 ] ] * [ avoid-learning ]`  
IS-IS is configured to generate default IPv6 routes.  
  
After this command is used, IS-IS generates default IPv6 routes and advertises them to IS-IS routers of related levels.



When IS-IS is configured to generate default IPv6 routes, the level of default IPv6 routes is Level-2 if no level is specified.

- Configuring IS-IS to filter the received routes to determine which routes are to be added to the IP routing table
  1. Run:
 

```
system-view
```

The system view is displayed.
  2. Run:
 

```
isis [process-id]
```

The IS-IS view is displayed.
  3. Run:
 

```
ipv6 filter-policy { acl6-name acl6-name | acl6-number | ipv6-prefix ipv6-prefix-name | route-policy route-policy-name } import
```

IS-IS is configured to filter received IPv6 routes to determine which routes to be added to the IPv6 routing table.
- Configuring IS-IS to import IPv6 routes of other protocols
  1. Run:
 

```
system-view
```

The system view is displayed.
  2. Run:
 

```
isis [process-id]
```

The IS-IS view is displayed.
  3. Configuring IS-IS to import external IPv6 routes
 

If you want to set the cost for the imported IPv6 route, you can run the **ipv6 import-route protocol [ process-id ] [ cost cost ] [ tag tag ] [ route-policy route-policy-name ] [ level-1 | level-2 | level-1-2 ]** command to import the external IPv6 routes.

If you want to keep the original cost for the imported IPv6 route, you can run the **ipv6 import-route { { ripng | isis | ospfv3 } [ process-id ] | direct | bgp } inherit-cost [ tag tag | route-policy route-policy-name ] [ level-1 | level-2 | level-1-2 ] }** command to import the external IPv6 routes.
  4. Run:
 

```
ipv6 filter-policy { acl6-name acl6-name | acl6-number | ipv6-prefix ipv6-prefix-name | route-policy route-policy-name } export [protocol [process-id]]
```

IS-IS is enabled to filter imported IPv6 routes when advertising them to other routers.

The **ipv6 filter-policy export** command usually works with the **ipv6 import-route** command. It filters only imported IPv6 routes to be advertised to other routers. If *protocol* is not specified, the command filters the IPv6 routes imported from all the protocols. If *protocol* is specified, it filters only the IPv6 routes imported from a certain protocol.

If no level is specified in the **ipv6 import-route** command, IPv6 routes are imported to the Level-2 routing table.
- Configuring IS-IS route leaking

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
isis [process-id]
```

The IS-IS view is displayed.

3. Run:

```
ipv6 import-route isis level-2 into level-1 [tag tag | filter-policy
{ acl6-number | acl6-name acl6-name | ipv6-prefix ipv6-prefix-name | route-
policy route-policy-name }] *
```

IS-IS IPv6 route leaking is enabled. IPv6 routes in Level-2 areas and other Level-1 areas can be leaked to the Level-1 area where the Level-1-2 router resides. This command is used on Level-1-2 routers connected to external areas.

 **NOTE**

By default, IS-IS IPv6 routes in Level-1 areas are leaked to Level-2 areas.

- Configuring the convergence priority for IS-IS routes

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
isis [process-id]
```

The IS-IS view is displayed.

3. Run:

```
ipv6 prefix-priority [level-1 | level-2] { critical | high | medium }
{ ip-prefix prefix-name | tag tag-value }
```

The convergence priority is set for IS-IS routes.

By default, the convergence priority of IS-IS host routes and default routes is **medium**, and the convergence priority of the other IS-IS routes is **low**.

After the **ipv6 prefix-priority** is run to set the convergence priority for IS-IS routes, the following situations occur:

- The convergence priority of existing IS-IS routes is re-set according to the configuration of the **ipv6 prefix-priority** command.
- The convergence priority of new IS-IS routes is set according to the filtering result of the **ipv6 prefix-priority** command.
- If an IS-IS route meets the matching rules specified in multiple commands that are used to set convergence priorities, this IS-IS route is of top convergence priority among the set convergence priorities.
- If no level is specified, the convergence priority is set for both Level-1 routes and Level-2 routes according to the configuration of the **ipv6 prefix-priority** command.

 NOTE

The **ipv6 prefix-priority** command takes effect only on the public network.  
 If the **ipv6 prefix-priority** command is run to set the convergence priority for IS-IS routes (including IS-IS host routes and default routes), the convergence priority of all the IS-IS routes that meet the matching rules is changed according to the configuration of the **ipv6 prefix-priority** command, and the convergence priority of the IS-IS routes that do not meet the matching rules is changed to low.

----End

## 7.10.6 Checking the Configuration

After configuring IS-IS IPv6, you can check information about the IS-IS interface, LSDB, neighbor, routes, and statistics about the IS-IS process.

### Prerequisite

The configurations of IS-IS IPv6 are complete.

### Procedure

- Run the **display isis interface** [ [ **verbose** | **traffic-eng** ] \* | **tunnel** ] [ *process-id* | **vpn-instance** *vpn-instance-name* ] command to check information about the IS-IS interface.
- Run the **display isis lsdb** [ { **level-1** | **level-2** } | **verbose** | { **local** | *lsp-id* | **is-name** *symbolic-name* } ] \* [ *process-id* | **vpn-instance** *vpn-instance-name* ] command to check information about the LSDB.
- Run the **display isis peer** [ **verbose** ] [ *process-id* | **vpn-instance** *vpn-instance-name* ] command to check information about the IS-IS neighbor.
- Run the **display isis route** [ *process-id* | **vpn-instance** *vpn-instance-name* ] **ipv6** [ **verbose** | [ **level-1** | **level-2** ] | *ipv6-address* [ *prefix-length* ] ] \* command to check the IS-IS routing information.
- Check statistics about the IS-IS process.
  - **display isis statistics** [ **level-1** | **level-2** | **level-1-2** ] [ *process-id* | **vpn-instance** *vpn-instance-name* ]
  - **display isis statistics packet** [ **interface** *interface-type interface-number* ]
  - **display isis process-id statistics** [ **level-1** | **level-2** | **level-1-2** | **packet** ]

----End

### Example

Run the **display isis interface verbose** command, and you can see that the cost of the IPv6 route on Gigabit Ethernet 1/0/0 is 15.

```
<HUAWEI> display isis interface verbose
 Interface information for ISIS(1)

Interface Id IPV4.State IPV6.State MTU Type DIS
GE1/0/0 001 Down Up 1497 L1/L2 No/No
 Description : GE1/0/0 Interface
 Circuit MT State : Standard
 SNPA Address : 00e0-c72d-da01
 IP Address :
 IPV6 Link Local Address : FF80::FFE0:FFFF:FE2D:DA01
```

```

 IPV6 Global Address(es) : 2001::1/64
 Csnp Timer Value : L1 10 L2 10
 Hello Timer Value : L1 10 L2 10
 DIS Hello Timer Value : L1 3 L2 3
 Hello Multiplier Value : L1 3 L2 3
 LSP-Throttle Timer : L12 50
 Cost : L1 10 L2 10
 Ipv6 Cost : L1 15 L2 15
 Priority : L1 64 L2 64
 Retransmit Timer Value : L12 5
 Bandwidth-Value : Low 100000000 High 0
 Static Bfd : NO
 Dynamic Bfd : NO
 Fast-Sense Rpr : NO

```

Run the **display isis route verbose** command, and you can see that the convergence priority of the route to 20::/64 is **Critical**.

```

<HUAWEI> display isis route ipv6 verbose
Route information for ISIS(100)

ISIS(100) Level-1 Forwarding Table

IPV6 Dest : 30::/64 Cost : 10 Flags: D/L/-
Admin Tag : - Src Count : 3 Priority: -
NextHop : Interface : ExitIndex :
 Direct GE1/0/0 0x00000000

IPV6 Dest : 20::/64 Cost : 20 Flags: A/L/-
Admin Tag : - Src Count : 1 Priority: Critical
NextHop : Interface : ExitIndex :
 FE80::263 GE1/0/0 0x00000003
 FE80::563 GE1/0/0 0x00000009

```

## 7.11 Configuring IS-IS Auto FRR

With IS-IS Auto FRR, traffic on a faulty link can be quickly switched to the backup link of the faulty link. This ensures that the traffic interruption time is within 50 ms and improves the reliability of IS-IS networks.

### 7.11.1 Establishing the Configuration Task

Before configuring IS-IS Auto FRR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

At present, the VoIP and on-line video services require high-quality real-time transmission. Nevertheless, if an IS-IS fault occurs, multiple processes, including fault detection, LSP update, LSP flooding, route calculation, and FIB entry delivery, must be performed to switch the traffic to a new link. As a result, it takes much more than 50 ms to recover the link from the fault, which cannot meet the requirement for real-time services on the network.

IS-IS Auto FRR ensures fast switchover of traffic to the backup link before the network convergence, avoiding traffic interruption. This protects traffic and improves reliability of an IS-IS network. The NE80E/40E supports IPv4 IS-IS Auto FRR.

IS-IS Auto FRR is suitable for IP services that require a low delay and low packet loss ratio.

## Pre-configuration Tasks

Before configuring IS-IS Auto FRR, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable at the network layer
- **Configuring basic IS-IS functions**
- Configuring the link cost to ensure that the backup path is the sub-optimal route.

## Data Preparation

To configure IS-IS Auto FRR, you need the following data.

| No. | Data                                        |
|-----|---------------------------------------------|
| 1   | IS-IS process ID                            |
| 2   | Interface to be enabled with IS-IS Auto FRR |

### 7.11.2 Enabling IS-IS Auto FRR

IS-IS can create the loop-free backup route only when the interface cost is in compliance with the traffic protection inequality of IS-IS Auto FRR.

#### Context

Do as follows on the router that needs the protection for the forwarded traffic:

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis [process-id]
```

The IS-IS process is enabled and the IS-IS view is displayed.

**Step 3** Run:

```
frr
```

The IS-IS FRR view is displayed.

**Step 4** Run:

```
loop-free-alternate
```

IS-IS Auto FRR is enabled and the loop-free backup route is created.

If the IS-IS level is not specified, IS-IS Auto FRR is enabled on Level-1 and Level-2 to create the backup route.

For detailed information about IS-IS Auto FRR, refer to the *Feature Description - IP Routing*.

 **NOTE**

IS-IS can create the loop-free backup route only if the interface cost is in compliance with the traffic protection inequality of IS-IS Auto FRR.

----End

## 7.11.3 Checking the Configuration

After configuring IS-IS Auto FRR, you can check the IS-IS backup route and traffic protection type.

### Prerequisite

All IS-IS Auto FRR configurations are complete.

### Procedure

- Run the **display isis route** [ *process-id* | **vpn-instance** *vpn-instance-name* ] [ **ipv4** ] [ **verbose** | [ **level-1** | **level-2** ] | *ip-address* [ *mask* | *mask-length* ] ] \* command to check information about the primary link and backup link after IS-IS Auto FRR is enabled.
- Run the **display isis spf-tree** [ **systemid** *systemid* | **dname** *dname* ] [ [ **level-1** | **level-2** ] | **ipv6** | **verbose** ] \* [ *process-id* | **vpn-instance** *vpn-instance-name* ] command to check the traffic protection type of IS-IS Auto FRR.

----End

### Example

Enable IS-IS Auto FRR, and then check and find information about the backup outbound interface and the backup next hop of the route with the destination address as 100.1.1.0/24. The following is the check result:

```
<HUAWEI> display isis route 100.1.1.1 verbose

Route information for ISIS(1)

ISIS(1) Level-1 Forwarding Table

IPV4 Dest : 100.1.1.0/24 Int. Cost : 30 Ext. Cost : NULL
Admin Tag : - Src Count : 1 Flags : A-/L/-/-
Priority : Low
NextHop : Interface : ExitIndex :
 1.0.0.2 GE1/0/0 0x00000003
 (B)2.0.0.2 GE2/0/0 0x00000004

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set, C-In Computing

ISIS(1) Level-2 Forwarding Table

IPV4 Dest : 100.1.1.0/24 Int. Cost : 30 Ext. Cost : NULL
Admin Tag : - Src Count : 3 Flags : -/-/-/-
Priority : Low

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set, C-In Computing
```

Enable IS-IS Auto FRR, and then check and find the traffic protection type for the router with the system ID as 0000.0000.0004. The following is the check result:

```
<HUAWEI> display isis spf-tree systemid 0000.0000.0004 verbose

Shortest Path Tree for ISIS(1)

ISIS(1) Level-1 Shortest Path Tree

0000.0000.0004.00
 Distance : 20
 Distance-URT : 20
 Flags : SPT/V6_Islt
 IPv4 Nexthops-URT : 1
 (1) 1.0.0.2 IF:GE1/0/0 NBR:0000.0000.0003.00
 (B) 2.0.0.2 IF:GE2/0/0 NBR:0000.0000.0002.00 TYPE:LOOP-FREE
PROTECT:LINK-NODE
 IPv4 Nexthops-MIGP : 0
 IPv6 Nexthops : 0
 Neighbors: 2 (Children:1 Parents:1 Others:0)
 (1) 0000.0000.0003.02
 Cost : 10
 Flags : Parent
 (2) 0000.0000.0004.03
 Cost : 10
 Flags : Child

ISIS(1) Level-2 Shortest Path Tree

0000.0000.0004.00
 Distance : 20
 Distance-URT : 20
 Flags : SPT/V6_Islt
 IPv4 Nexthops-URT : 1
 (1) 1.0.0.2 IF:GE1/0/0 NBR:0000.0000.0003.00
 (B) 2.0.0.2 IF:GE2/0/0 NBR:0000.0000.0002.00 TYPE:LOOP-FREE
PROTECT:LINK-NODE
 IPv4 Nexthops-MIGP : 0
 IPv6 Nexthops : 0
 Neighbors: 2 (Children:1 Parents:1 Others:0)
 (1) 0000.0000.0003.02
 Cost : 10
 Flags : Parent
 (2) 0000.0000.0004.03
 Cost : 10
 Flags : Child
```

## 7.12 Configuring IPv6 IS-IS Auto FRR

With IPv6 IS-IS Auto FRR, traffic on a faulty link can be quickly switched to the backup link of the faulty link. This ensures that the traffic interruption time is within 50 ms and improves the reliability of IS-IS networks.

### 7.12.1 Establishing the Configuration Task

Before configuring IPv6 IS-IS Auto FRR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

## Applicable Environment

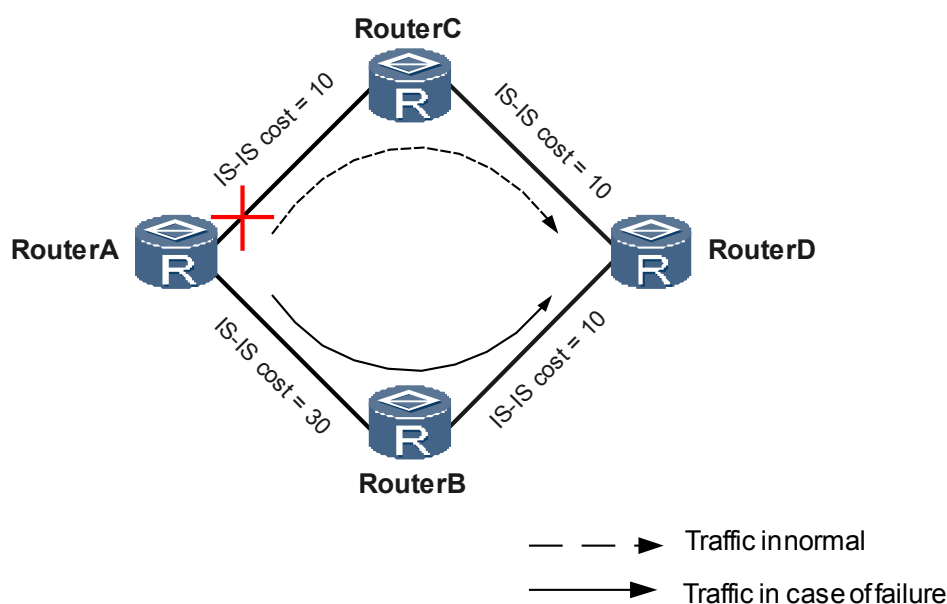
As the network keeps developing, services such as Voice over IP (VoIP) and on-line video services require high-quality real-time transmission. Nevertheless, if an IS-IS fault occurs, traffic can be switched to a new link only after the following processes: fault detection, LSP update, LSP flooding, route calculation, and FIB entry delivery. As a result, traffic is interrupted for much more than 50 ms, which cannot meet the requirement for real-time services on the network.

With IPv6 IS-IS Auto FRR, devices can rapidly switch traffic from faulty links to backup links without interrupting the traffic. This protects traffic and greatly improves the reliability of IS-IS networks. The NE80E/40E supports IPv4 and IPv6 IS-IS Auto FRR.

IPv6 IS-IS Auto FRR is applicable to the services that are very sensitive to packet delay and packet loss.

As shown in **Figure 7-3**, the link cost satisfies the traffic protection inequality, namely,  $\text{Distance\_opt}(B, D) < \text{Distance\_opt}(B, A) + \text{Distance\_opt}(A, D)$ . In this inequality,  $\text{Distance\_opt}(X, Y)$  specifies the shortest path from node X to node Y. After IPv6 IS-IS Auto FRR is configured, when the link between Router A and Router C becomes faulty, traffic forwarded by Router A is rapidly switched to the backup link.

**Figure 7-3** Networking diagram for IPv6 IS-IS Auto FRR (IP protecting IP)



## Pre-configuration Tasks

Before configuring IPv6 IS-IS Auto FRR, complete the following tasks:

- Configuring IP addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- Configuring IPv6 IS-IS.
- Setting costs for links to ensure that the primary link is the optimal path and the backup link is the sub-optimal path.



## Data Preparation

To configure IPv6 IS-IS Auto FRR, you need the following data.

| No. | Data                                             |
|-----|--------------------------------------------------|
| 1   | IS-IS process ID                                 |
| 2   | Interface to be enabled with IPv6 IS-IS Auto FRR |

### 7.12.2 Enabling IPv6 IS-IS Auto FRR

If IPv6 IS-IS Auto FRR is enabled and the traffic protection inequality is satisfied, a backup route can be generated.

#### Context

Do as follows on the router where traffic to be forwarded needs to be protected:

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis [process-id]
```

The IS-IS process is enabled and the IS-IS view is displayed.

**Step 3** Run:

```
ipv6 frr
```

The IPv6 IS-IS FRR view is displayed.

**Step 4** Run:

```
loop-free-alternate [level-1 | level-2 | level-1-2]
```

IPv6 IS-IS Auto FRR is enabled to generate a loop-free backup link.

If no level is specified, IPv6 IS-IS Auto FRR is enabled in Level-1 and Level-2 areas to generate backup routes.

For details of IS-IS Auto FRR, see the *HUAWEI NetEngine80E/40E Router Feature Description - IP Routing*.

 **NOTE**

IS-IS can generate loop-free backup routes only when the traffic protection inequality of IS-IS Auto FRR is satisfied.

----End

## 7.12.3 (Optional) Disabling an Interface from Participating in LFA Calculation

To facilitate network management and fault location, you can prevent certain interfaces from participating in the LFA calculation and specify the interfaces that can function as backup outbound interfaces.

### Context

To disable an interface that is enabled with IPv6 IS-IS from participating in the Loop-Free Alternate (LFA) calculation, you need to do as follows on this interface:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
undo isis ipv6 lfa-backup
```

The interface is disabled from participating in the LFA calculation.

 **NOTE**

By default, an IS-IS interface participates in LFA calculation.

----End

## 7.12.4 Checking the Configuration

After IPv6 IS-IS Auto FRR is configured, you can check backup route information and traffic protection types of IS-IS.

### Prerequisite

The configurations of IPv6 IS-IS Auto FRR are complete.

### Procedure

- Run the **display isis route** [*process-id* | **vpn-instance** *vpn-instance-name*] **ipv6** [**verbose** | [**level-1** | **level-2**] | *ipv6-address* [*prefix-length*]] \* command to check information about the primary and backup links after IPv6 IS-IS Auto FRR is enabled.
- Run the **display isis spf-tree** [**systemid** *systemid* | **dname** *dname*] [[**level-1** | **level-2**] | **ipv6** | **verbose**] \* [*process-id* | **vpn-instance** *vpn-instance-name*] command to check the traffic protection type of IPv6 IS-IS Auto FRR.

----End

## Example

Run the **display isis route** command, and you can view information about the outbound interface and next hop of the backup route. The configuration result is as follows:

```
<HUAWEI> display isis route ipv6 3::3 verbose

Route information for ISIS(100)

ISIS(100) Level-1 Forwarding Table

IPV6 Dest : 3::3/128 Cost : 10 Flags: A/L/-
Admin Tag : - Src Count : 1 Priority: Medium
NextHop : Interface : ExitIndex :
FE80::163 GE0/0/1 0x00000005
(B) FE80::536 GE0/0/0 0x00000007

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set

ISIS(100) Level-2 Forwarding Table

IPV6 Dest : 3::3/128 Cost : 10 Flags: -/-/-
Admin Tag : - Src Count : 2 Priority: Medium

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set
```

Run the **display isis spf-tree** command, and you can view the traffic protection type of a specified device. The configuration result is as follows:

```
<HUAWEI> display isis spf-tree systemid 0000.0000.0004 verbose ipv6

Shortest Path Tree for ISIS(100)

ISIS(100) Level-1 Shortest Path Tree

0000.0000.0004.00
Distance : 10
Distance-URT : 10
Flags : SPT/Direct
IPv4 Nexthops-URT : 2
(1) 30.0.0.3 IF:GE0/0/1 NBR:0000.0000.0004.00
(2) 50.0.0.2 IF:Pos0/0/0 NBR:0000.0000.0004.00
IPv4 Nexthops-MIGP : 0
IPv6 Nexthops : 2
(1) FE80::163 IF:GE0/0/1 NBR:0000.0000.0004.00
(B) FE80::536 IF:Pos0/0/0 NBR:0000.0000.0004.00
TYPE:PRIMARY PROTECT:LINK
(2) FE80::536 IF:Pos0/0/0 NBR:0000.0000.0004.00
(B) FE80::163 IF:GE0/0/1 NBR:0000.0000.0004.00
TYPE:PRIMARY PROTECT:LINK

Neighbors: 3 (Children:1 Parents:2 Others:0)
(1) 0000.0000.0004.02
 Cost : 10
 Flags : Child
(2) >0000.0000.0001.02
 Cost : 10
 Flags : Parent
(3) >0000.0000.0001.00
```

```

Cost : 10
Flags : Parent

ISIS(100) Level-2 Shortest Path Tree

0000.0000.0004.00
 Distance : 10
 Distance-URT : 10
 Flags : SPT/Direct
 IPv4 Nexthops-URT : 2
 (1) 30.0.0.3 IF:GE0/0/1 NBR:0000.0000.0004.00
 (2) 50.0.0.2 IF:Pos0/0/0 NBR:0000.0000.0004.00
 IPv4 Nexthops-MIGP : 0
 IPv6 Nexthops : 2
 (1) FE80::163 IF:GE0/0/1 NBR:0000.0000.0004.00
 (B) FE80::536 IF:Pos0/0/0 NBR:0000.0000.0004.00
 TYPE:PRIMARY PROTECT:LINK
 (2) FE80::536 IF:Pos0/0/0 NBR:0000.0000.0004.00
 (B) FE80::163 IF:GE0/0/1 NBR:0000.0000.0004.00
 TYPE:PRIMARY PROTECT:LINK
 Neighbors: 3 (Children:1 Parents:2 Others:0)
 (1) >0000.0000.0001.02
 Cost : 10
 Flags : Parent
 (2) 0000.0000.0004.02
 Cost : 10
 Flags : Child
 (3) >0000.0000.0001.00
 Cost : 10
 Flags : Parent

```

## 7.13 Configuring IS-IS GR

By configuring IS-IS GR, you can enable Router to restart gracefully and avoid temporary black holes.

### 7.13.1 Establishing the Configuration Task

Before configuring IS-IS GR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

The restart of an IS-IS router causes the temporary interruption of the network, because the adjacency relationship between the router and its neighbor is torn down. The LSPs packets of the router are deleted, which makes route calculation inaccurate. Packets are thus lost.

You can configure IS-IS GR to solve this problem. After IS-IS GR is enabled, the router notifies the neighbor of the restart status, and reestablishes the adjacency relationship with its neighbor without interrupting the forwarding.

The advantages of IS-IS GR are as follows:

- When IS-IS restarts, the router can resend connection requests to its neighbor. The adjacency relationship is not torn down.

- Before LSPs packets are generated, GR minimizes the interference caused by waiting for the database synchronization.
- If the router starts for the first time, the router sets the overload bit in LSPs until the LSDB synchronization is complete. This avoids route black holes.

## Pre-configuration Tasks

Before configuring IS-IS GR, complete the following tasks:

- Configuring IP addresses for interfaces to ensure network connectivity between neighboring nodes
- [Configuring Basic IS-IS Functions](#)

## Data Preparation

To configure IS-IS GR, you need the following data.

| No. | Data                                                                                  |
|-----|---------------------------------------------------------------------------------------|
| 1   | ID of an IS-IS process                                                                |
| 2   | Interval for reestablishing GR sessions                                               |
| 3   | Whether to suppress the advertisement of the adjacency when the GR restarter restarts |

## 7.13.2 Enabling IS-IS GR

Before configuring IS-IS GR, you need to enable the GR capability for IS-IS.

### Context

Do as follows on the router that runs IS-IS:

### Procedure

- Step 1** Run:  
`system-view`  
 The system view is displayed.
- Step 2** Run:  
`isis [ process-id ]`  
 The IS-IS view is displayed.
- Step 3** Run:  
`graceful-restart`  
 IS-IS GR is enabled.  
 By default, IS-IS GR is disabled.
- End

## 7.13.3 Configuring Parameters of an IS-IS GR Session

By setting IS-IS GR parameters, you can avoid temporary black holes on the network.

### Context

The router that starts for the first time does not maintain the forwarding status. If the router restarts, the LSPs generated when the router runs last time may exist in the LSDB of other routers in the network.

The sequence number of an LSP fragment is reinitialized when the router starts. Therefore, the router considers that the previously advertised LSP stored on other routers is newer than the LSP generated locally after the router starts. This leads to the temporary black hole in the network, which lasts until the normal LSDB update process finishes. The router then regenerates its LSPs and advertises the LSPs with the highest sequence number.

When this router starts, if the neighbor of the router suppresses the advertisement of the adjacency until this router advertises the updated LSPs, the preceding case can thus be avoided.

Do as follows on the router that runs IS-IS:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis [process-id]
```

The IS-IS view is displayed.

**Step 3** Run:

```
graceful-restart interval interval-value
```

The interval for reestablishing an IS-IS GR session is set.

The restart interval is set to the Holdtime in an IS-IS Hello PDU. Thus, the adjacency relationship is not torn down when the router restarts. By default, the restart period is 300 seconds.

**Step 4** (Optional) Run:

```
graceful-restart suppress-sa
```

The GR restarter is configured to suppress the Suppress-Advertisement (SA) bit of the restart TLV.

To prevent a router from suppressing the SA bit in a Hello PDU during the active/standby switchover, the administrator can run the **undo graceful-restart suppress-sa** command.

By default, the SA bit is not suppressed.

----End

## 7.13.4 Checking the Configuration

After configuring IS-IS GR, you can check the IS-IS GR status and parameters.

## Prerequisite

The configurations of IS-IS GR are complete.

## Procedure

**Step 1** Run **display isis graceful-restart status [ level-1 | level-2 ] [ process-id | vpn-instance vpn-instance-name ]** command to check the status of IS-IS GR.

---End

## Example

Run the **display isis graceful-restart status** command, and you can find that IS-IS process 1 on the local router is enabled with GR and the default values of all GR parameters are used.

```
<HUAWEI> display isis graceful-restart status
 Restart information for ISIS(1)

IS-IS(1) Level-1 Restart Status
Restart Interval: 300
SA Bit Supported
 Total Number of Interfaces = 1
 Restart Status: RESTART COMPLETE
IS-IS(1) Level-2 Restart Status
Restart Interval: 300
SA Bit Supported
 Total Number of Interfaces = 1
 Restart Status: RESTART COMPLETE
```

## 7.14 Configuring Static BFD for IS-IS

BFD can provide channel fault detection featuring light load and high speed (millisecond level). Static BFD needs to be configured manually.

### 7.14.1 Establishing the Configuration Task

Before configuring static BFD for IS-IS, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

### Applicable Environment

To accelerate IS-IS convergence speed when the link status changes, you can configure BFD on the IS-IS link. To configure a static BFD session, you need to enable BFD and then manually configure the BFD session parameters including local identifier and remote identifier through related commands.

#### NOTE

BFD can only detect one-hop links between IS-IS neighbors because IS-IS can establish only the one-hop neighbor relationship.

### Pre-configuration Tasks

Before configuring static BFD for IS-IS, complete the following tasks:

- Configuring IP addresses of interfaces to make neighboring nodes reachable
- **Configuring Basic IS-IS Functions**

## Data Preparation

To configure static BFD for IS-IS, you need the following data.

| No. | Data                                          |
|-----|-----------------------------------------------|
| 1   | Type and ID of the interface enabled with BFD |

## 7.14.2 Configuring BFD One-hop Detection

Before enabling static BFD for IS-IS, you need to enable BFD globally and on the interface and configure BFD session parameters.

### Context



Configuring BFD one-hop detection before configuring IS-IS fast detection.

Do as follows on the two routers between which a BFD session is established:

### Procedure

- Step 1** Run:  
`system-view`  
 The system view is displayed.
- Step 2** Run:  
`bfd`  
 The global BFD capability is enabled for the node.
- Step 3** Run:  
`quit`  
 Back to the system view.
- Step 4** Run:  
`interface interface-type interface-number`  
 The interface view is displayed.  
 Only physical interface can be enabled with BFD.
- Step 5** Run:  
`isis enable [ process-id ]`  
 IS-IS is enabled on the current interface.
- Step 6** Run:  
`isis bfd static`



Static BFD is enabled on the current interface.

**Step 7** Run:

```
quit
```

Back to the system view.

**Step 8** Run:

```
bfd cfg-name bind peer-ip ip-address [interface interface-type interface-number]
```

BFD binding is created.

If **peer-ip** and **interface** are specified, it indicates that BFD is configured to detect a one-hop link. That is, the fixed route with **interface** as the outgoing interface and **peer-ip** as the next hop is to be detected.

**Step 9** Perform the following to configure identifiers for both nodes;

Run:

```
discriminator local discr-value
```

The local identifier is configured.

And

Run:

```
discriminator remote discr-value
```

The remote identifier is configured.

The corresponding relation between local identifier and remote identifier of devices at the both end of the BFD session should be correct; otherwise, the session cannot be established. After the configuration of local identifier and the remote identifier succeeds, you can not change them.

 **NOTE**

Local identifier of the local router corresponds to the remote identifier of the remote router, and the remote identifier of the local router corresponds to the local identifier of the remote router.

**Step 10** Run:

```
commit
```

The configuration is committed.

----End

## 7.14.3 Enabling IS-IS Fast Detection

IS-IS fast detection is used to process the fault reported by static BFD.

### Context

Do as follows on the router on which IS-IS fast detection need to be enabled:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view of a specified interface is displayed.

**Step 3** Enable IS-IS fast detection as required.

● Run:

```
isis bfd static
```

BFD is configured.

And Run:

```
isis fast-sense rpr
```

RPR fast sense is configured on the specific IS-IS interface.

● Run:

```
isis fast-sense
```

IS-IS fast detection is enabled.

 **NOTE**

- The effect of the **isis fast-sense** command is equal to the effect of the **isis bfd static** command and the **isis fast-sense rpr** command.
- The **isis fast-sense rpr** command is required only on RPR interfaces.

---End

## 7.14.4 Checking the Configuration

After configuring static BFD for IS-IS, you can check BFD session information and static BFD for IS-IS information on an interface.

### Prerequisite

The configurations of Static BFD for IS-IS are complete.

### Procedure

- Run **display isis interface verbose** command to check the BFD for IS-IS configuration on the interface.

---End

### Example

Only after parameters of BFD session are set and the BFD session is established, you can check the information about the BFD session.

If the configurations are correct, you can find that the status of the Fast-Sense field is **YES**.

Run the **display isis interface verbose** command, and you can find that the status of static BFD of IS-IS process 1 is **YES**.

```
<HUAWEI> display isis interface verbose
 Interface information for ISIS(1)

Interface Id IPV4.State IPV6.State MTU Type DIS
GE1/0/0 001 Up Down 1497 L1/L2 No/No
```

```

Description : GE1/0/0 Interface
SNPA Address : 00e0-c72d-da01
IP Address : 123.1.1.1
IPV6 Link Local Address :
IPV6 Global Address(es) :
Csnp Timer Value : L1 10 L2 10
Hello Timer Value : L1 10 L2 10
DIS Hello Timer Value : L1 3 L2 3
Hello Multiplier Value : L1 3 L2 3
LSP-Throttle Timer : L12 50
Cost : L1 20 L2 20
Ipv6 Cost : L1 20 L2 20
Priority : L1 64 L2 64
Retransmit Timer Value : L12 5
Bandwidth-Value : Low 100000000 High 0
Static Bfd : YES
Dynamic Bfd : NO
Fast-Sense Rpr : NO

```

## 7.15 Configuring Dynamic BFD for IS-IS

BFD can provide channel fault detection featuring light load and high speed (millisecond level). Routing protocols can dynamically trigger the establishment of BFD sessions.

### 7.15.1 Establishing the Configuration Task

Before configuring dynamic BFD for IS-IS, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

When the requirement for data transmission is high and IS-IS convergence needs to be speeded up when the link status changes, you can configure dynamic BFD on IS-IS links.

Dynamic BFD should be configured according to the actual network environment. If time parameters are set improperly, network flapping may occur.

#### Pre-configuration Tasks

Before configuring dynamic BFD for IS-IS, complete the following tasks:

- Configuring IP addresses for interfaces to make neighboring nodes reachable
- [7.2 Configuring Basic IS-IS Functions](#)

#### Data Preparation

To configure dynamic BFD for IS-IS, you need the following data.

| No. | Data                                                 |
|-----|------------------------------------------------------|
| 1   | ID of the IS-IS process enabled with BFD             |
| 2   | Type and ID of the interface on which BFD is enabled |
| 3   | Parameters of a BFD session                          |

## 7.15.2 Configuring Global BFD

Before configuring dynamic BFD for IS-IS, you need to enable BFD globally.

### Context

To dynamically set up a BFD session, you need to enable global BFD first. Do as follows on the router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bfd
```

Global BFD is enabled.

---End

## 7.15.3 Configuring Dynamic BFD for an IS-IS Process

By configuring dynamic BFD for an IS-IS process, you can configure parameters for dynamic BFD sessions and enable dynamic BFD for IS-IS on all IS-IS interfaces.

### Context

To configure dynamic BFD on all interfaces of an IS-IS process, do as follows on the two routers on which the BFD session needs to be set up:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis process-id
```

The IS-IS view is displayed.

**Step 3** Run:

```
bfd all-interfaces enable
```

Dynamic BFD of the IS-IS process is enabled to set up a dynamic BFD session.

When global BFD is enabled and the neighbor status is Up, IS-IS sets up BFD sessions on all the interfaces that meet the preceding conditions by using default values of BFD parameters.

**Step 4** (Optional) Run:

```
bfd all-interfaces { min-rx-interval receive-interval | min-tx-interval transmit-interval | detect-multiplier multiplier-value | frr-binding } *
```

The values of BFD parameters used to set up the dynamic BFD session are set.

----End

## 7.15.4 (Optional) Preventing an Interface from Dynamically Setting Up a BFD Session

If you do not want certain IS-IS interfaces to set up dynamic BFD sessions, you can disable these interfaces from dynamically setting up BFD sessions.

### Context

After the **bfd all-interfaces enable** command is used in an IS-IS process, the following situations occur:

- In a P2P network, all IS-IS interfaces whose neighbor status is Up set up dynamic BFD sessions.
- In a broadcast network, all IS-IS interfaces whose neighbor status is Up set up dynamic sessions between DISs and non-DISs.

If you do not want certain interfaces to set up dynamic BFD sessions, do as follows on the interfaces:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
isis bfd block
```

The interface is prevented from dynamically setting up a BFD session.

----End

## 7.15.5 Configuring BFD for a Specified Interface

To configure different dynamic BFD session parameters for certain interfaces, you can configure BFD for the specified interface. The priority of BFD configured on an interface is higher than that of BFD configured in a process.

### Context

To configure BFD only on certain interfaces and not to enable dynamic BFD in an IS-IS process, or to configure the interfaces to fast detect link faults by using different dynamic BFD session parameters after dynamic BFD is configured for the IS-IS process, do as follows on the two interfaces at both ends of the link:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
isis bfd enable
```

BFD is enabled on the interface to dynamically set up a BFD session.

When global BFD is configured and the neighbor status is Up (in the broadcast network, the DIS is in the Up state), the default values of BFD parameters are used to dynamically set up a BFD session.

**Step 4** (Optional) Run:

```
isis bfd { min-rx-interval receive-interval | min-tx-interval transmit-interval |
detect-multiplier multiplier-value | frr-binding } *
```

The values of BFD parameters are set to set up a dynamic BFD session.

 **NOTE**

The priority of BFD configured on an interface is higher than that of BFD configured in a process. That is, if BFD is enabled on an interface, the parameters on the interface are used to set up a BFD session.

----End

## 7.15.6 Checking the Configuration

After configuring dynamic BFD for IS-IS, you can check BFD session information and BFD for IS-IS information on an interface.

### Prerequisite

The configurations of Dynamic BFD for IS-IS are complete.

### Procedure

- Run **display isis** [*process-id* | **vpn-instance** *vpn-instance-name*] **bfd session** { **peer ip-address** | **all** } command to check information about the BFD session.
- Run **display isis** [*process-id*] **bfd interface** command to check the BFD configuration on the interface.

----End

### Example

When the two ends of a link are enabled with BFD, you can find that the BFD status is Up after you run the **display isis** [*process-id* | **vpn-instance** *vpn-instance-name*] **bfd session** { **peer ip-address** | **all** } command. The display is as follows:

```
<HUAWEI> display isis bfd session all
```

```

 BFD session information for ISIS(1)

Peer System ID : 0000.0000.0002 Interface : Pos1/0/0
TX : 1000 BFD State : up Peer IP Address : 1.1.1.2
RX : 1000 LocDis : 8192 Local IP Address: 1.1.1.1
Multiplier : 3 RemDis : 8192 Type : L2
Diag : No diagnostic information

```

Run the **display isis [ process-id ] bfd interface** command, and you can view all the interfaces enabled with BFD and the values of the BFD session parameters on the interface.

```

<HUAWEI> display isis bfd interface
 BFD information of interface for ISIS(1)

Interface BFD.State Min-Tx Min-Rx Mul
Pos1/0/0 enable 1000 1000 3
Total interfaces: 1 Total bfd enabled interfaces: 1

```

## 7.16 Configuring Dynamic IPv6 BFD for IS-IS

BFD can provide link failure detection featuring light load and high speed (at the millisecond level). With dynamic BFD, routing protocols can dynamically trigger the establishment of BFD sessions.

### 7.16.1 Establishing the Configuration Task

Before configuring dynamic IPv6 BFD for IS-IS, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

IPv6 BFD can rapidly detect IPv6 forwarding failures.

Without IPv6 BFD, IS-IS can detect IPv6 link failures only through the Hello mechanism. However, the minimum interval for sending Hello packets is 3s, and a neighbor is declared down after at least three intervals. Therefore, IS-IS provides only second-level neighbor fault detection through the Hello mechanism. This causes the loss of a large amount of data.

IPv6 BFD can provide millisecond-level fault detection. Thus, it can rapidly detect the faults on the protected link or nodes so that traffic can be rapidly switched to the backup path.

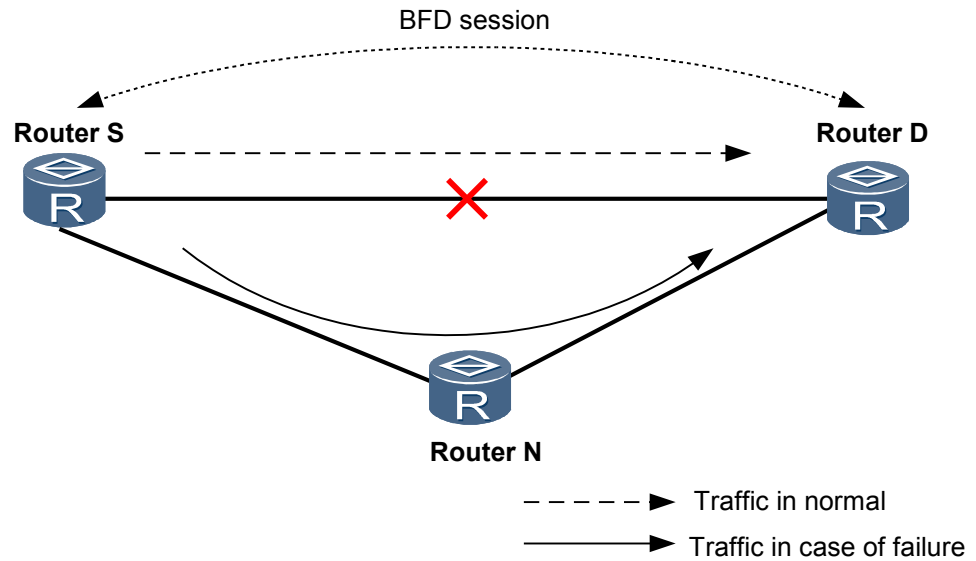
Although smart hello can be configured to set the interval for sending Hello packets to the millisecond-level value, the length of a Hello packet is much longer than a BFD packet. Therefore, within the same detection time, adopting IPv6 BFD for fault detection can reduce the network load. Additionally, IPv6 BFD provides a unified fault detection mechanism, which facilitates network management.

On the NE80E/40E, IPv6 BFD can rapidly detect forwarding failures on the IS-IS IPv6 P2P or broadcast network. This implements rapid convergence of IS-IS IPv6 networks.

- Adopting IPv6 BFD to detect forwarding failures on the IS-IS IPv6 P2P network

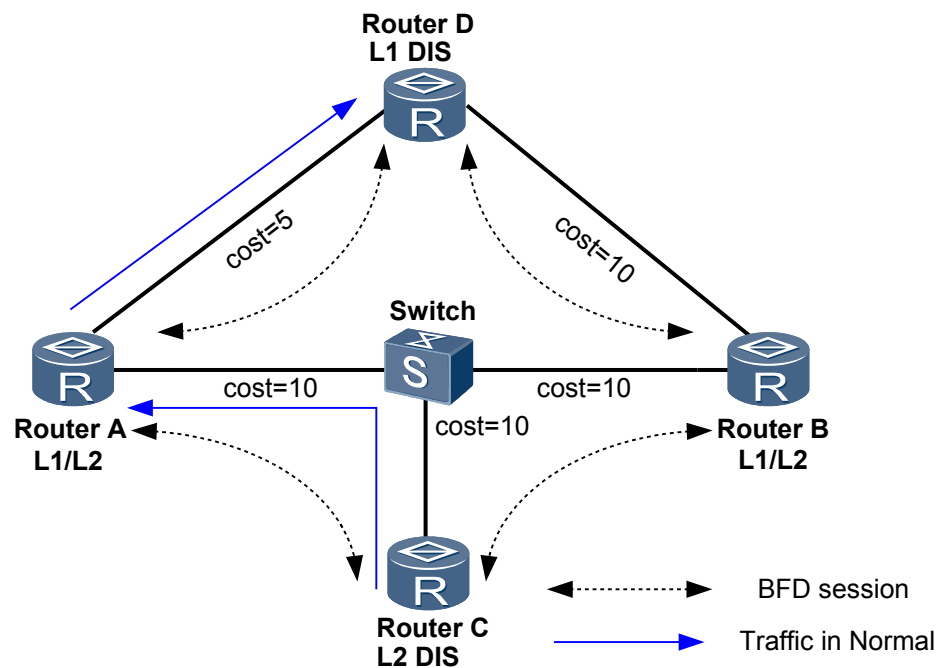
As shown in [Figure 7-4](#), Router S and Router D are IS-IS neighbors. After an IPv6 BFD session is established between Router S and Router D, if the link between Router S and Router D fails, IPv6 BFD can rapidly detect the link failure and notify the upper-layer application of switching traffic to the backup path.

Figure 7-4 IPv6 BFD for IS-IS P2P network



- Adopting IPv6 BFD to detect forwarding failures on the IS-IS IPv6 broadcast network  
 As shown in **Figure 7-5**, after dynamic IPv6 BFD for IS-IS is enabled on the Level-1 node, Level-2 node, and Level-1-2 node, IPv6 BFD sessions are established between the DIS and non-DISs.

Figure 7-5 IPv6 BFD for IS-IS broadcast network

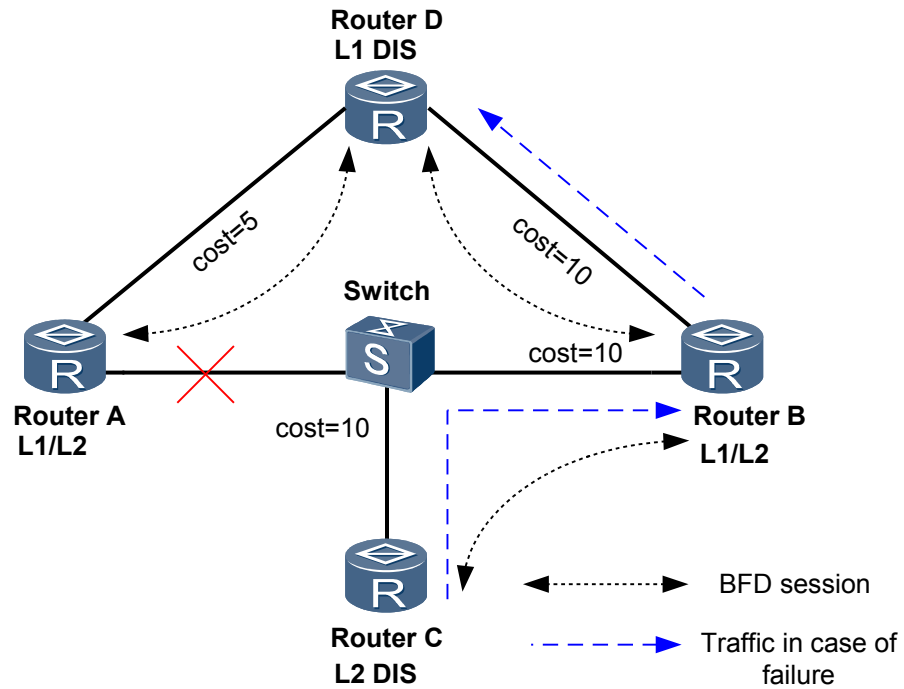


When a forwarding failure occurs on the broadcast network, IPv6 BFD can rapidly detect the failure and notify the upper-layer application of switching traffic to the backup path.



As shown in **Figure 7-6**, when the link between Router A and Router C fails, the Level-2 DIS, namely, Router C, can fast detect the failure, trigger IS-IS to recalculate a route, and then transmit traffic through the backup link.

**Figure 7-6** Traffic switching when the IPv6 BFD for IS-IS broadcast network becomes faulty



## Pre-configuration Tasks

Before configuring dynamic IPv6 BFD for IS-IS, complete the following tasks:

- Configuring IPv6 addresses for interfaces to make neighboring nodes reachable
- **Configuring IS-IS IPv6 Features** to implement IPv6 connectivity between nodes at the network layer

## Data Preparation

To configure dynamic IPv6 BFD for IS-IS, you need the following data.

| No. | Data                                                                                                                    |
|-----|-------------------------------------------------------------------------------------------------------------------------|
| 1   | Nodes to be enabled with IPv6 BFD for IS-IS (You are recommended to enable IPv6 BFD for IS-IS for all the IS-IS nodes.) |
| 2   | ID of the IS-IS process to be enabled with IPv6 BFD                                                                     |
| 3   | Interfaces to be enabled with IPv6 BFD                                                                                  |
| 4   | Minimum interval for sending IPv6 BFD packets                                                                           |

| No. | Data                                                     |
|-----|----------------------------------------------------------|
| 5   | Expected minimum interval for receiving IPv6 BFD packets |
| 6   | IPv6 BFD detection multiplier                            |

## 7.16.2 Enable Global BFD

Before configuring dynamic BFD for IS-IS, you need to enable BFD globally.

### Context

Before configuring dynamic IPv6 BFD for IS-IS, you need to enable BFD globally. Do as follows on the node to be configured with dynamic IPv6 BFD for IS-IS:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bfd
```

BFD is enabled globally.

----End

## 7.16.3 Configuring IPv6 BFD for IS-IS

By configuring IPv6 BFD for IS-IS, you can establish IPv6 BFD sessions.

### Context

You can use the following methods to enable IPv6 BFD for IS-IS:

- **Enabling IPv6 BFD for IS-IS Globally:** When most IS-IS interfaces on a node need to be enabled with IPv6 BFD for IS-IS, you are recommended to use this method.
- **Enabling IPv6 BFD for IS-IS on the Interface:** When only a few IS-IS interfaces on a node need to be enabled with IPv6 BFD for IS-IS, you are recommended to use this method.

### Procedure

- Enabling IPv6 BFD for IS-IS Globally

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
isis process-id
```

The IS-IS view is displayed.

3. Run:

```
ipv6 bfd all-interfaces enable
```

IPv6 BFD for IS-IS is enabled globally.

After IPv6 BFD for IS-IS is enabled globally, IS-IS establishes IPv6 BFD sessions on the interfaces whose IS-IS neighbor status is Up (the DIS is Up in the broadcast network) by using the default IPv6 BFD parameters.

4. (Optional) To use non-default IPv6 BFD parameters to establish IPv6 BFD sessions, run:

```
ipv6 bfd all-interfaces { min-rx-interval receive-interval | min-tx-interval transmit-interval | detect-multiplier multiplier-value | frr-binding } *
```

IPv6 BFD parameters are specified.

5. (Optional) If some IS-IS interfaces do not need to be enabled with IPv6 BFD for IS-IS, you need to block IPv6 BFD for IS-IS on these interfaces:

- Run the **interface** *interface-type interface-number* command to enter the IS-IS interface view.
- Run the **isis ipv6 bfd block** command to block IPv6 BFD for IS-IS on the interface.

- Enabling IPv6 BFD for IS-IS on the Interface

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
interface interface-type interface-number
```

The IS-IS interface view is displayed.

3. Run:

```
isis ipv6 bfd enable
```

IPv6 BFD for IS-IS is enabled on the interface.

After IPv6 BFD for IS-IS is enabled on the interface and the IS-IS neighbor status of the interface is Up (the DIS is Up in the broadcast network), IS-IS establishes an IPv6 BFD session on the interface by using the default IPv6 BFD parameters.

4. (Optional) Run:

```
isis ipv6 bfd { min-rx-interval receive-interval | min-tx-interval transmit-interval | detect-multiplier multiplier-value | frr-binding } *
```

IPv6 BFD parameters on the interface are specified.

----End

## 7.16.4 Checking the Configuration

After configuring dynamic IPv6 BFD for IS-IS, you can check information about the IPv6 BFD session and IPv6 BFD for IS-IS on an interface.

### Prerequisite

All the configurations of dynamic IPv6 BFD for IS-IS are complete.

## Procedure

- Run the **display isis** [*process-id* | **vpn-instance** *vpn-instance-name* ] **ipv6 bfd session** { **all** | **peer** *ipv6-address* | **interface** *interface-type interface-number* } command to check information about the IPv6 BFD session for IS-IS.
- Run the **display isis** [*process-id* ] **ipv6 bfd interface** command to check the configurations of IPv6 BFD for IS-IS on the interface.

----End

## Example

Run the **display isis ipv6 bfd session** command, and you can view the status of the IPv6 BFD session. For example:

```
<HUAWEI> display isis 10 ipv6 bfd session all
 IPv6 BFD session information for ISIS(1)

Peer System ID : 0000.0000.0003 Interface : GE2/0/0 Type : L2
IPv6 BFD State : up TX : 100 RX : 100 Multiplier : 3
LocDis : 8184 Local IPv6 Address : FE80::1
RemDis : 8192 Peer IPv6 Address : FE80::2
Diag : No diagnostic information

Total IPv6 BFD session(s) : 1
```

Run the **display isis** [*process-id* ] **ipv6 bfd interface** command, and you can view all the interfaces that are enabled with IPv6 BFD for IS-IS and view the IPv6 BFD parameters that are configured on the interfaces.

```
<HUAWEI> display isis 1 ipv6 bfd interface
 IPV6 BFD information of interface for ISIS(1)

Interface BFD6.State Min-Tx Min-Rx Mul
GigabitEthernet1/0/0 enable 1000 1000 10
Total interfaces: 1 Total IPv6 bfd enabled interfaces: 1
```

## 7.17 Improving Security of an IS-IS Network

On a network that requires high security, you can configure IS-IS authentication to improve the security of the IS-IS network.

### 7.17.1 Establishing the Configuration Task

Before improving the security of an IS-IS network, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

In a network that has a high requirement for security, you can configure IS-IS authentication to improve security of the IS-IS network. IS-IS authentication consists of area authentication, route domain authentication, and interface authentication.

#### Pre-configuration Tasks

Before configuring IS-IS authentication, complete the following tasks:

- Configuring IP addresses of interfaces to make neighboring nodes reachable
- [7.2 Configuring Basic IS-IS Functions](#)

## Data Preparation

To configure IS-IS authentication, you need the following data.

| No. | Data                                                        |
|-----|-------------------------------------------------------------|
| 1   | Authentication mode and password used in the authentication |

### 7.17.2 Configuring the Area or Domain Authentication

After the IS-IS area or domain authentication is configured, authentication information can be encapsulated into LSPs or SNPs to ensure the security of packet transmission.

#### Context

By default, sent IS-IS packets are not encapsulated with authentication information, and received packets are not authenticated.

If the area authentication is required, the area authentication password is encapsulated in Level-1 LSPs, CSNPs, and PSNPs in a specified mode. The area authentication modes and passwords of the routers in the same area must be consistent; otherwise, IS-IS packets cannot be flooded normally.

Similarly, in domain authentication, the password is also encapsulated in Level-2 LSPs in a specified mode. Configuration procedures and parameter configuration of the domain authentication are the same as those of the area authentication. The domain authentication modes and passwords of the routers in the same domain must be consistent; otherwise, IS-IS packets cannot be flooded normally.

Regardless of whether packets pass the area or domain authentication, the establishment of Level-1 or Level-2 neighbor relationship is not affected.

Do as follows on the router that runs IS-IS:

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis [process-id]
```

The IS-IS view is displayed.

**Step 3** Run the following commands as required:

- To configure **simple** or **md5** password, run:  

```
area-authentication-mode { simple password | md5 password-key } [ip | osi]

[snp-packet { authentication-avoid | send-only } | all-send-only]
```

The area authentication mode is configured.

 **NOTE**

The MD5 authentication password that starts and ends with @\$@\$ is invalid, because @\$@\$ is used to distinguish old and new passwords.

- To configure **keychain** password, run:  
`area-authentication-mode keychain keychain-name [ snp-packet { authentication-avoid | send-only } | all-send-only ]`

The area authentication mode is configured.

**Step 4** Run the following commands as required:

- To configure **simple** or **md5** password, run:  
`domain-authentication-mode { simple password | md5 password-key } [ ip | osi ] [ snp-packet { authentication-avoid | send-only } | all-send-only ]`

The routing domain authentication mode is configured.

 **NOTE**

The MD5 authentication password that starts and ends with @\$@\$ is invalid, because @\$@\$ is used to distinguish old and new passwords.

- To configure **keychain** password, run:  
`domain-authentication-mode keychain keychain-name [ snp-packet { authentication-avoid | send-only } | all-send-only ]`

The routing domain authentication mode is configured.

The authentication involves the following situations:

- Authentication information is encapsulated in the sent LSPs and SNPs. The received LSPs and SNPs should pass the authentication, and the ones that do not pass the authentication are discarded. In this case, **snp-packet** or **all-send-only** is inapplicable.
- Authentication information is encapsulated in the sent LSPs and received LSPs are checked; however, authentication information is not encapsulated in the sent SNPs and the received SNPs are not checked. In this case, **snp-packet authentication-avoid** needs to be configured.
- Authentication information is encapsulated in the sent LSPs and SNPs. The received LSPs are checked and the received SNPs are not checked. In this case, **snp-packet send-only** needs to be configured.
- Authentication information is encapsulated in the sent LSPs and SNPs and the received LSPs and SNPs are not checked. In this case, **all-send-only** needs to be configured.

When you configure the area or domain authentication, **ip** and **osi** are not affected by the actual network environment.

---End

## 7.17.3 Configuring the Interface Authentication

After IS-IS interface authentication is configured, encapsulation information can be encapsulated in the Hello packet to confirm the validity and correctness of neighbors.

### Context

The authentication set on the interface is mainly used in the Hello packet to confirm the validity and correctness of its neighbors.

Do as follows on the router that runs IS-IS:

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

### Step 3 Run the following commands as required:

- To configure **simple** or **md5** password, run:

```
isis authentication-mode { simple password | md5 password-key } [level-1 |
level-2] [ip | osi] [send-only]
```

The IS-IS authentication mode and password are configured on the interface.

#### NOTE

The MD5 authentication password that starts and ends with \$@\$@ is invalid, because \$@\$@ is used to distinguish old and new passwords.

- To configure **keychain** password, run:

```
isis authentication-mode keychain keychain-name [level-1 | level-2] [send-
only]
```

The IS-IS authentication mode and password are configured on the interface.

- If **send-only** is specified correctly, it indicates that the router only encapsulates the sent Hello packets with authentication information rather than check whether the received Hello packets pass authentication. The neighbor relationship can be set up when the authentication is not necessary or packets pass the authentication.
- If **send-only** is not configured, ensure that passwords of all interfaces with the same level in the same network are consistent.

When IS-IS interfaces are Level-1-2 interfaces and **level-1** or **level-2** is not specified in the command, authentication modes and passwords are configured for both Level-1 and Level-2 Hello packets.

When the interface authentication is configured, **ip** and **osi** are not affected by the actual network environment.

#### NOTE

Run the **isis enable** command to enable IS-IS on the interface. **level-1** and **level-2** can be set only on Ethernet interfaces.

----End

## 7.17.4 Checking the Configuration

By configuring various IS-IS authentication modes, you can improve the security of the IS-IS network.

## Prerequisite

The configurations of Improving Security of an IS-IS Network are complete.

## Procedure

**Step 1** Run **display isis peer** [ **verbose** ] [ *process-id* | **vpn-instance** *vpn-instance-name* ] command to check information about the IS-IS neighbor.

----End

## Example

On GE2/0/0, set the interface authentication mode to simple and password to 123. Neighbor relationship can be established when authentication information on the two routers are consistent. Run the **display isis 1 peer verbose** command. The display is as follows:

```
<HUAWEI> display isis peer 1 verbose
Peer information for ISIS(1)

System Id Interface Circuit Id State HoldTime Type PRI

0000.0000.0040 GE2/0/0 0000.0000.0040.04 Up 7s L1(L1L2) 64
Area Address(es) :10
Peer IP Address(es): 12.40.41.1
Uptime : 00:01:08
Adj Protocol : IPV4
Restart Capable : Yes
Suppressed Adj : NO
MT IDs supported : 0(UP)
0000.0000.0040 GE2/0/0 0000.0000.0040.04 Up 8s L2(L1L2) 64
Area Address(es) :10
Peer IP Address(es): 12.40.41.1
Uptime : 00:01:14
Adj Protocol : IPV4
Restart Capable : Yes
Suppressed Adj : NO
MT IDs supported : 0(UP)
Total Peer(s) : 2
```

## 7.18 Configuring IS-IS Multi-Topology (IPv4)

By configuring multi-topology on an IS-IS network, you can properly allocate network resources.

### 7.18.1 Establishing the Configuration Task

Before configuring IS-IS multi-topology (IPv4), familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

#### Applicable Environment

In traditional IP networks, there is only one unicast topology and one unicast forwarding table on each device. In this case, service traffic with the same destination IP address share the same PHB. This means that various end-to-end services (for example, voice services and data services) share the same physical links. As a result, some links may be heavily congested whereas some other links are relatively idle. Different types of services have different QoS requirements, which cannot be met in the traditional unicast topology.

IS-IS multi-topology enables the operation of multiple independent logical topologies in an IS-IS Autonomous System (AS), and sets up an independent multicast topology for multicast services. In this manner, the multicast topology is separated from the unicast topology.



Configuring IS-IS multi-topology will help customers construct networks flexibly and save customers' costs for network construction.

## Pre-configuration Tasks

Before configuring IS-IS multi-topology (IPv4), complete the following tasks:

- Configuring IP addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- Configuring IPv4 multi-topology globally
- [Configuring Basic IS-IS Functions](#)

## Data Preparation

To configure IS-IS multi-topology (IPv4), you need the following data.

| No. | Data                                                   |
|-----|--------------------------------------------------------|
| 1   | Cost style of each IS-IS process running on the router |
| 2   | ID of a topology instance                              |

### 7.18.2 Enabling IS-IS Multi-Topology (IPv4)

Based on service requirements and network planning, you can associate IS-IS processes with multiple different topology instances. In this manner, an IS-IS AS can be divided into multiple logical topologies.

#### Context

Each topology instance is a subset of a base topology instance. Each topology instance bears one or more types of services and maintains its own routing table and forwarding table.

Do as follows on the device that needs to be enabled with IS-IS multi-topology:

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis [process-id]
```

The IS-IS view is displayed.

**Step 3** Run:

```
cost-style { narrow | wide | wide-compatible }
```

The cost style for the packets received and sent by the router is **wide** or **wide-compatible**.

**Step 4** Run:

```
topology topology-name [topology-id { multicast | topology-id }]
```

The IS-IS process is associated with a specified topology instance and the IS-IS topology view is displayed.

---End

### 7.18.3 (Optional) Setting IS-IS Parameters in IPv4 Topology Instances

The setting of IS-IS parameters (including the link cost, bandwidth reference value, and protocol preference) in IPv4 topology instances can meet the service requirements of different topology instances.

#### Context

An IS-IS process can be associated with different topology instances, and the parameters of this IS-IS process vary with the topology instances.

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis [process-id]
```

The IS-IS view is displayed.

**Step 3** Run:

```
topology topology-name [topology-id topology-id]
```

The IS-IS topology view is displayed.

**Step 4** Run the following commands as required to set IS-IS parameters in IPv4 topology instances.

- **auto-cost enable**
- **bandwidth-reference** *value*
- **circuit-cost** *cost* [ **level-1** | **level-2** ]
- **circuit default-tag** *tag* [ **level-1** | **level-2** ]
- **default-route-advertise** [ **always** | **match default** | **route-policy** *route-policy-name* ]  
[ [ **cost** *cost* ] | [ **tag** *tag* ] | [ **level-1** | **level-1-2** | **level-2** ] ] \* [ **avoid-learning** ]
- **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [ *protocol* [ *process-id* ] ]
- **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **import**
- **frr**
- **import-route** *protocol* [ *process-id* ] [ **cost-type** { **external** | **internal** } ] [ **cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* ] [ **level-1** | **level-2** | **level-1-2** ] ] \*
- **import-route** { { **rip** | **isis** | **ospf** } [ *process-id* ] | **bgp** } **inherit-cost** [ **tag** *tag* | **route-policy** *route-policy-name* ] [ **level-1** | **level-2** | **level-1-2** ] ] \*

- **import-route isis level-1 into level-2** [ **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } ] [ **tag** *tag* ]
  - **import-route isis level-2 into level-1** [ **tag** *tag* | **filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } ] \*
  - **maximum load-balancing** *number*
  - **nexthop** *ip-address* **weight** *value*
  - **preference** *preference* **route-policy** *route-policy-name*
  - **prefix-priority** [ **level-1** | **level-2** ] { **critical** | **high** | **medium** } { **ip-prefix** *prefix-name* | **tag** *tag-value* }
  - **set-overload** [ **on-startup** [ *timeout1* | **start-from-nbr** *system-id* [ *timeout1* [ *timeout2* ] ] ] ] [ **allow** { **interlevel** | **external** } \* ]
  - **spf-priority** *priority-value*
  - **summary** *ip-address mask* [ **avoid-feedback** | **generate\_null0\_route** | **tag** *tag* | [ **level-1** | **level-1-2** | **level-2** ] ] \*
- End

## 7.18.4 Enabling IS-IS Multi-Topology on a Specified Interface

After enabling IS-IS multi-topology, you need to associate a specified interface with the IS-IS topology instance.

### Context

Do as follows on the device that needs to be enabled with IS-IS multi-topology:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
isis topology topology-name
```

The IS-IS topology instance is enabled on an interface.

----End

## 7.18.5 (Optional) Setting IS-IS Interface Parameters in IPv4 Topology Instances

After enabling IS-IS multi-topology on an interface, you can configure other features and parameters in the topology instance where the interface resides to meet different application requirements.

## Context

Do as follows to configure features and parameters in the topology instance where the interface resides, for example, change the cost of the interface:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run the following commands as required to set IS-IS interface parameters in IPv4 topology instances.

- **isis** [ **topology topology-name** ] **cost cost** [ **level-1** | **level-2** ]
- **undo isis lfa-backup** [ **topology topology-name** ] { **level-1** | **level-2** | **level-1-2** }
- **isis** [ **topology topology-name** ] **suppress-reachability** [ **level-1** | **level-1-2** | **level-2** ]
- **isis** [ **topology topology-name** ] **tag-value tag** [ **level-1** | **level-2** ]
- **isis suppress topology base**

----End

## 7.18.6 Checking the Configuration

After the configuration of IS-IS multi-topology (IPv4) is complete, you can view information about IS-IS multi-topology.

### Prerequisite

All configurations of IS-IS multi-topology (IPv4) are complete.

### Procedure

- Run the **display isis peer** [ **verbose** ] [ *process-id* | **vpn-instance vpn-instance-name** ] command to check information about IS-IS neighbors.
- Run the **display isis route** [ *process-id* | **vpn-instance vpn-instance-name** ] [ **ipv4** ] [ **topology topology-name** ] [ **verbose** | [ **level-1** | **level-2** ] | *ip-address* [ *mask* | *mask-length* ] ] \* command to check IS-IS routing information.
- Run the **display isis spf-tree** [ **systemid systemid** | **dname dname** ] [ [ **level-1** | **level-2** ] | **ipv6** | **verbose** ] \* [ *process-id* | **vpn-instance vpn-instance-name** ] [ **topology topology-name** ] command to check information about the SPF tree of IS-IS.

----End

### Example

Run the **display isis peer verbose** command, and you can view that the ID of the IS-IS topology instance with the neighbor status being Up is 10.

<HUAWEI> **display isis peer verbose**

```

Peer information for ISIS(1)

System Id Interface Circuit Id State HoldTime Type PRI

0000.0000.0003 GE1/0/2 0000.0000.0003.01 Up 7s L2 64

MT IDs supported : 0 (UP) 10 (UP)
Local MT IDs : 0 10
Area Address(es) : 10
Peer IP Address(es) : 10.1.2.2
Uptime : 00:03:46
Adj Protocol : IPV4
Restart Capable : YES
Suppressed Adj : NO

```

Total Peer(s): 2

Run the **display isis route topology Red** command, and you can view the routes of IS-IS topology instance **Red**.

<HUAWEI> **display isis route topology Red**

```

Route information for ISIS(1)

topology Red

ISIS(1) Level-2 Forwarding Table

IPV4 Destination IntCost ExtCost ExitInterface NextHop Flags

10.1.4.0/24 20 NULL GE1/0/2 10.1.2.2 A/-/-/-
10.1.2.0/24 10 NULL GE1/0/2 Direct D/-/L/-
22.22.22.22/32 20 NULL GE1/0/2 10.1.2.2 A/-/-/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
U-Up/Down Bit Set

```

Run the **display isis spf-tree topology Red** command, and you can view information about the SPF tree of IS-IS topology instance **Red**.

<HUAWEI> **display isis spf-tree topology Red**

```

Shortest Path Tree for ISIS(1)

topology Red

Flags: T-System is on SPF TREE R-System is directly reachable
O-System is Overload D-System or Link is to be deleted
C-Neighbor is child P-Neighbor is parent
G-Cost gets greater L-Cost gets lower
H-Nexthop is changed U-Protocol usage is changed
V-Link is involved N-Link is a new path
S-Link is IGP Shortcut *-Relative cost

ISIS(1) Level-2 Shortest Path Tree

SpfNode NodeFlags NeighbourNode LinkCost LinkFlags

>0000.0000.0001.00 T/-/-/- 0000.0000.0003.01 10 C/-/-/-/-/-/-
0000.0000.0002.01 -/-/-/- 0000.0000.0002.00 0 -/-/-/-/-/-/-

```

```

>0000.0000.0001.00 0 -/-/-/-/-/-/-
0000.0000.0002.02 -/-/-/- 0 -/-/-/-/-/-/-
0000.0000.0002.00 0 -/-/-/-/-/-/-
0000.0000.0004.00 0 -/-/-/-/-/-/-
0000.0000.0003.00 T/-/-/- 10 P/-/-/-/-/-/-
0000.0000.0003.01 T/R/-/- 10 C/-/-/-/-/-/-
0000.0000.0003.02 0 C/-/-/-/-/-/-
0000.0000.0003.01 T/R/-/- 0 C/-/-/-/-/-/-
>0000.0000.0001.00 0 P/-/-/-/-/-/-
0000.0000.0003.02 T/-/-/- 0 P/-/-/-/-/-/-
0000.0000.0004.00 0 C/-/-/-/-/-/-
0000.0000.0003.02 10 P/-/-/-/-/-/-

```

## 7.19 Configuring IS-IS Multi-Topology (IPv6)

By configuring multi-topology on an IS-IS network, you can properly allocate network resources.

### 7.19.1 Establishing the Configuration Task

Before configuring IS-IS multi-topology (IPv6), familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

#### Applicable Environment

In traditional IP networks, there is only one unicast topology and one unicast forwarding table on each device. In this case, service traffic with the same destination IP address share the same PHB. This means that various end-to-end services (for example, voice services and data services) share the same physical links. As a result, some links may be heavily congested whereas some other links are relatively idle. Different types of services have different QoS requirements, which cannot be met in the traditional unicast topology.

IS-IS multi-topology enables the operation of multiple independent logical topologies in an IS-IS Autonomous System (AS), and sets up an independent multicast topology for multicast services. In this manner, the multicast topology is separated from the unicast topology.

Configuring IS-IS multi-topology will help customers construct networks flexibly and save customers' costs for network construction.

#### Pre-configuration Tasks

Before configuring IS-IS multi-topology (IPv6), complete the following tasks:

- Configuring IPv6 addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- Configuring IPv6 multi-topology globally
- [Configuring IPv6 IS-IS Features](#)

#### Data Preparation

To configure IS-IS multi-topology (IPv6), you need the following data.

| No. | Data                                                   |
|-----|--------------------------------------------------------|
| 1   | Cost style of each IS-IS process running on the router |
| 2   | ID of a topology instance                              |

## 7.19.2 Enabling IS-IS Multi-Topology (IPv6)

Based on service requirements and network planning, you can associate IS-IS processes with multiple different topology instances. In this manner, an IS-IS AS can be divided into multiple logical topologies.

### Context

Each topology instance is a subset of a base topology instance. Each topology instance bears one or more types of services and maintains its own routing table and forwarding table.

Do as follows on the device that needs to be enabled with IS-IS multi-topology:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis [process-id]
```

The IS-IS view is displayed.

**Step 3** Run:

```
cost-style { narrow | wide | wide-compatible }
```

The cost style for the packets received and sent by the router is **wide** or **wide-compatible**.

**Step 4** Run:

```
ipv6 topology topology-name [topology-id { multicast | topology-id }]
```

The IS-IS process is associated with a specified topology instance and the IS-IS IPv6 topology view is displayed.

----End

## 7.19.3 (Optional) Setting IS-IS Parameters in IPv6 Topology Instances

The setting of IS-IS parameters (including the link cost, bandwidth reference value, and protocol preference) in IPv6 topology instances can meet the service requirements of different topology instances.

## Context

An IS-IS process can be associated with different topology instances, and the parameters of this IS-IS process vary with the topology instances.

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis [process-id]
```

The IS-IS view is displayed.

**Step 3** Run:

```
ipv6 topology topology-name [topology-id topology-id]
```

The IS-IS topology view is displayed.

**Step 4** Run the following commands as required to set IS-IS parameters in IPv6 topology instances.

- **auto-cost enable**
- **bandwidth-reference** *value*
- **circuit-cost** *cost* [ **level-1** | **level-2** ]
- **circuit default-tag** *tag* [ **level-1** | **level-2** ]
- **default-route-advertise** [ **always** | **match default** | **route-policy** *route-policy-name* ]  
[ [ **cost** *cost* ] | [ **tag** *tag* ] | [ **level-1** | **level-1-2** | **level-2** ] ] \* [ **avoid-learning** ]
- **filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **export** [ *protocol* [ *process-id* ] ]
- **filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **import**
- **import-route** *protocol* [ *process-id* ] [ **cost** *cost* ] [ **tag** *tag* ] [ **route-policy** *route-policy-name* ] [ **level-1** | **level-2** | **level-1-2** ]
- **import-route** { { **ripng** | **isis** | **ospfv3** } [ *process-id* ] | **bgp** } **inherit-cost** [ **tag** *tag* | **route-policy** *route-policy-name* ] [ **level-1** | **level-2** | **level-1-2** ] ] \*
- **import-route isis level-1 into level-2** [ **filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } ] [ **tag** *tag* ]
- **import-route isis level-2 into level-1** [ **tag** *tag* | **filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } ] \*
- **maximum load-balancing** *number*
- **preference** *preference* **route-policy** *route-policy-name*
- **set-overload** [ **on-startup** [ *timeout1* | **start-from-nbr** *system-id* [ *timeout1* [ *timeout2* ] ] ] ]  
[ **allow** { **interlevel** | **external** } \* ]
- **spf-priority** *priority-value*
- **summary** *ip-address mask* [ **avoid-feedback** | **generate\_null0\_route** | **tag** *tag* ] [ **level-1** | **level-1-2** | **level-2** ] ] \*

----End



## 7.19.4 Enabling IS-IS Multi-Topology on a Specified Interface

After enabling IS-IS multi-topology, you need to associate a specified interface with the IS-IS topology instance.

### Context

Do as follows on the device that needs to be enabled with IS-IS multi-topology:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
isis ipv6 topology topology-name
```

The IS-IS topology instance is enabled on an interface.

----End

## 7.19.5 (Optional) Setting IS-IS Interface Parameters in IPv6 Topology Instances

After enabling IS-IS multi-topology on an interface, you can configure other features and parameters in the topology instance where the interface resides to meet different application requirements.

### Context

Do as follows to configure features and parameters in the topology instance where the interface resides, for example, change the cost of the interface.

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run the following commands as required to set IS-IS interface parameters in IPv6 topology instances.

- **isis ipv6** [ **topology** *topology-name* ] **cost** *cost* [ **level-1** | **level-2** ]

- **isis** [ **ipv6** ] [ **topology topology-name** ] **suppress-reachability** [ **level-1** | **level-1-2** | **level-2** ]
  - **isis** [ **ipv6** ] [ **topology topology-name** ] **tag-value tag** [ **level-1** | **level-2** ]
  - **isis ipv6 suppress topology base**
- End

## 7.19.6 Checking the Configuration

After the configuration of IS-IS multi-topology (IPv6) is complete, you can view information about IS-IS multi-topology.

### Prerequisite

All configurations of IS-IS multi-topology (IPv6) are complete.

### Procedure

- Run the **display isis peer** [ **verbose** ] [ **process-id** | **vpn-instance vpn-instance-name** ] command to check information about IS-IS neighbors.
- Run the **display isis route** [ **process-id** | **vpn-instance vpn-instance-name** ] **ipv6** [ **topology topology-name** ] [ **verbose** | [ **level-1** | **level-2** ] | **ip-address** [ **mask** | **mask-length** ] ] \* command to check IS-IS routing information.
- Run the **display isis spf-tree** [ **systemid systemid** | **dname dname** ] [ [ **level-1** | **level-2** ] | **ipv6** | **verbose** ] \* [ **process-id** | **vpn-instance vpn-instance-name** ] [ **topology topology-name** ] command to check information about the SPF tree of IS-IS.

----End

### Example

Run the **display isis peer verbose** command, and you can view that the ID of the IS-IS topology instance with the neighbor status being Up is 10.

```
<HUAWEI> display isis peer verbose
```

```
Peer information for ISIS(1)

System Id Interface Circuit Id State HoldTime Type PRI

0000.0000.0003 GE1/0/2 0000.0000.0003.01 Up 7s L2 64

MT IDs supported : 0 (UP) 10 (UP)
Local MT IDs : 0 10
Area Address(es) : 10
Peer IPv6 Address(es): FE80::2E0:6CFF:FE57:8300
Uptime : 00:00:29
Adj Protocol : IPV6
Restart Capable : YES
Suppressed Adj : NO
```

```
Total Peer(s) : 2
```

Run the **display isis route ipv6 topology Red** command, and you can view the routes of IS-IS topology instance **Red**.

```
<HUAWEI> display isis route ipv6 topology Red
```

```

Route information for ISIS(1)

 ipv6 topology Red

ISIS(1) Level-2 Forwarding Table

IPV6 Dest. ExitInterface NextHop Cost Flags

30:1::/64 GE1/0/2 FE80::2E0:6CFF:FE57:8300 20 A/-/-
10:2::/64 GE1/0/2 Direct 10 D/L/-
10:4::/64 GE1/0/2 FE80::2E0:6CFF:FE57:8300 20 A/-/-

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set

```

Run the **display isis spf-tree ipv6 topology Red** command, and you can view information about the SPF tree of IS-IS topology instance **Red**.

```

<HUAWEI> display isis spf-tree ipv6 topology Red

Shortest Path Tree for ISIS(1)

 ipv6 topology Red

Flags: T-System is on SPF TREE R-System is directly reachable
 O-System is Overload D-System or Link is to be deleted
 C-Neighbor is child P-Neighbor is parent
 G-Cost gets greater L-Cost gets lower
 H-NextHop is changed U-Protocol usage is changed
 V-Link is involved N-Link is a new path
 S-Link is IGP Shortcut *-Relative cost

ISIS(1) Level-2 Shortest Path Tree

SpfNode NodeFlags NeighbourNode LinkCost LinkFlags

>0000.0000.0001.00 T/-/-/- 0000.0000.0003.01 10 C/-/-/-/-/-/-
0000.0000.0002.01 -/-/-/- 0000.0000.0002.00 0 -/-/-/-/-/-/-
0000.0000.0002.02 -/-/-/- >0000.0000.0001.00 0 -/-/-/-/-/-/-
0000.0000.0002.02 -/-/-/- 0000.0000.0002.00 0 -/-/-/-/-/-/-
0000.0000.0002.02 -/-/-/- 0000.0000.0004.00 0 -/-/-/-/-/-/-
0000.0000.0003.00 T/-/-/- 0000.0000.0003.02 10 C/-/-/-/-/-/-
0000.0000.0003.00 T/-/-/- 0000.0000.0003.01 10 P/-/-/-/-/-/-
0000.0000.0003.01 T/R/-/- 0000.0000.0003.00 0 C/-/-/-/-/-/-
0000.0000.0003.01 >0000.0000.0001.00 0 P/-/-/-/-/-/-
0000.0000.0003.02 T/-/-/- 0000.0000.0003.00 0 P/-/-/-/-/-/-
0000.0000.0003.02 T/-/-/- 0000.0000.0004.00 0 C/-/-/-/-/-/-
0000.0000.0004.00 T/-/-/- 0000.0000.0003.02 10 P/-/-/-/-/-/-

```

## 7.20 Maintaining IS-IS

Maintaining IS-IS involves resetting IS-IS and clearing IS-IS statistics.

### 7.20.1 Resetting IS-IS Data Structure

By restarting IS-IS, you can reset IS-IS. You can also reset IS-IS in GR mode.

## Context



### CAUTION

The IS-IS data structure cannot be restored after you reset it. All the previous structure information and the neighbor relationship are reset. So, confirm the action before you use the command.

---

To clear the IS-IS data structure, run the following **reset** command in the user view.

## Procedure

**Step 1** Run **reset isis all** [*process-id* | **vpn-instance** *vpn-instance-name* ] command to reset the IS-IS data structure.

By default, the IS-IS data structure is not reset.

----End

## 7.20.2 Resetting a Specific IS-IS Neighbor

By restarting IS-IS neighbors, you can reset the IS-IS neighbor relationship, and thus make the new configuration take effect.

## Context



### CAUTION

The specified IS-IS neighbor relationship is deleted after you reset a specified IS-IS neighbor by using the **reset isis peer** command. So, confirm the action before you use the command.

---

After the IS-IS routing policy or the protocol changes, you can reset a specific IS-IS neighbor to validate the new configuration.

To reset a specific IS-IS neighbor, run the following **reset** command in the user view.

## Procedure

**Step 1** Run **reset isis peer** *system-id* [*process-id* | [**vpn-instance** *vpn-instance-name* ]\* ] command to reset a specific IS-IS neighbor.

----End

## 7.21 Configuration Examples

This section provides several configuration examples of IS-IS together with the configuration flowchart. The configuration examples explain networking requirements, configuration notes, and configuration roadmap.

**NOTE**

This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.

## 7.21.1 Example for Configuring Basic IS-IS Functions

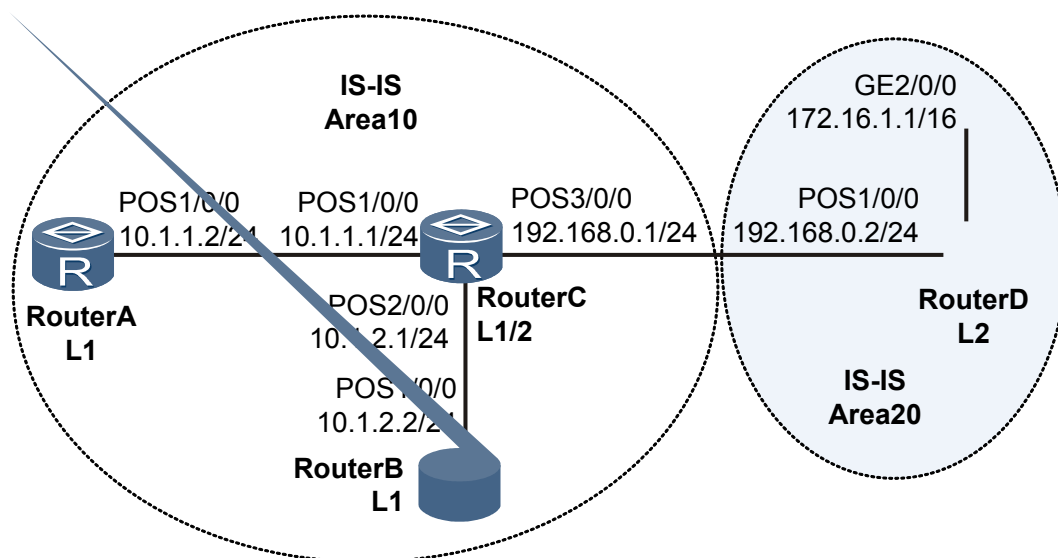
This part provides an example for interconnecting IPv4 networks through IS-IS.

### Networking Requirements

As shown in **Figure 7-7**:

- Router A, Router B, Router C, and Router D belong to the same AS. IS-IS is enabled on the routers to implement interconnection in the IP network.
- The area addresses of Router A, Router B, and Router C are all 10, and the area address of Router D is 20.
- Router A and Router B are Level-1 routers, Router C is a Level-1-2 router. Router D is a Level-2 router.

**Figure 7-7** Networking diagram for configuring basic IS-IS functions



### Configuration Roadmap

The configuration roadmap is as follows:

1. Enable IS-IS on each router, configure the levels of routers, and specify an NET.
2. Set RouterA and RouterC to authenticate Hello packets in specified mode and with the specified password.
3. Check the IS-IS database and the routing table of each router.

### Data Preparation

To complete the configuration, you need the following data:

- Area addresses of Router A, Router B, Router C and Router D
- Levels of Router A, Router B, Router C, and Router D

## Procedure

**Step 1** Configure an IP address for each interface.

The configuration details are not mentioned here.

**Step 2** Configure basic IS-IS functions.

# Configure Router A.

```
[RouterA] isis 1
[RouterA-isis-1] is-level level-1
[RouterA-isis-1] network-entity 10.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface Pos 1/0/0
[RouterA-Pos1/0/0] isis enable 1
[RouterA-Pos1/0/0] quit
```

# Configure Router B.

```
[RouterB] isis 1
[RouterB-isis-1] is-level level-1
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface Pos 1/0/0
[RouterB-Pos1/0/0] isis enable 1
[RouterB-Pos1/0/0] quit
```

# Configure Router C.

```
[RouterC] isis 1
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface Pos 1/0/0
[RouterC-Pos1/0/0] isis enable 1
[RouterC-Pos1/0/0] quit
[RouterC] interface Pos 2/0/0
[RouterC-Pos2/0/0] isis enable 1
[RouterC-Pos2/0/0] quit
[RouterC] interface Pos 3/0/0
[RouterC-Pos3/0/0] isis enable 1
[RouterC-Pos3/0/0] quit
```

# Configure Router D.

```
[RouterD] isis 1
[RouterD-isis-1] is-level level-2
[RouterD-isis-1] network-entity 20.0000.0000.0004.00
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 2/0/0
[RouterD-GigabitEthernet2/0/0] isis enable 1
[RouterD-GigabitEthernet2/0/0] quit
[RouterD] interface Pos 1/0/0
[RouterD-Pos1/0/0] isis enable 1
[RouterD-Pos1/0/0] quit
```

**Step 3** Configure the authentication mode and password for RouterA and RouterC to authenticate Hello packets.

# Configure RouterA.

```
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] isis authentication-mode md5 huawei
```

# Configure RouterC.

```
[RouterC] interface pos 1/0/0
[RouterC-Pos1/0/0] isis authentication-mode md5 huawei
```

#### Step 4 Verify the configuration.

# Display the IS-IS LSDB of each router.

```
[RouterA] display isis lsdb
Database information for ISIS(1)

Level-1 Link State Database
LSPID Seq Num Checksum Holdtime Length ATT/P/OL

0000.0000.0001.00-00* 0x00000006 0xbf7d 649 68 0/0/0
0000.0000.0002.00-00 0x00000003 0xef4d 545 68 0/0/0
0000.0000.0003.00-00 0x00000008 0x3340 582 111 1/0/0
Total LSP(s): 3
*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
ATT-Attached, P-Partition, OL-Overload
```

```
[RouterB] display isis lsdb
Database information for ISIS(1)

Level-1 Link State Database
LSPID Seq Num Checksum Holdtime Length ATT/P/OL

0000.0000.0001.00-00 0x00000006 0xbf7d 642 68 0/0/0
0000.0000.0002.00-00* 0x00000003 0xef4d 538 68 0/0/0
0000.0000.0003.00-00 0x00000008 0x3340 574 111 1/0/0
Total LSP(s): 3
*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
ATT-Attached, P-Partition, OL-Overload
```

```
[RouterC] display isis lsdb
Database information for ISIS(1)

Level-1 Link State Database
LSPID Seq Num Checksum Holdtime Length ATT/P/OL

0000.0000.0001.00-00 0x00000006 0xbf7d 638 68 0/0/0
0000.0000.0002.00-00 0x00000003 0xef4d 533 68 0/0/0
0000.0000.0003.00-00* 0x00000008 0x3340 569 111 1/0/0
Total LSP(s): 3
*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
ATT-Attached, P-Partition, OL-Overload
```

```
Level-2 Link State Database
LSPID Seq Num Checksum Holdtime Length ATT/P/OL

0000.0000.0003.00-00* 0x00000008 0x55bb 650 100 0/0/0
0000.0000.0004.00-00 0x00000005 0x6510 629 84 0/0/0
Total LSP(s): 2
*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
ATT-Attached, P-Partition, OL-Overload
```

```
[RouterD] display isis lsdb
Database information for ISIS(1)

Level-2 Link State Database
LSPID Seq Num Checksum Holdtime Length ATT/P/OL

0000.0000.0003.00-00 0x00000008 0x55bb 644 100 0/0/0
0000.0000.0004.00-00* 0x00000005 0x6510 624 84 0/0/0
Total LSP(s): 2
*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
ATT-Attached, P-Partition, OL-Overload
```

# Display the IS-IS routing information of each router. A default route must exist in the Level-1 routing table and the next hop is a Level-1-2 router. A Level-2 router must have all Level-1 and Level-2 routes.

```
[RouterA] display isis route
```

```

Route information for ISIS(1)

ISIS(1) Level-1 Forwarding Table

IPV4 Destination IntCost ExtCost ExitInterface NextHop Flags

10.1.1.0/24 10 NULL P1/0/0 Direct D/-/L/-
10.1.2.0/24 20 NULL P1/0/0 10.1.1.1 A/-/-/-
192.168.0.0/24 20 NULL P1/0/0 10.1.1.1 A/-/-/-
0.0.0.0/0 10 NULL P1/0/0 10.1.1.1 A/-/-/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set

[RouterC] display isis route
Route information for ISIS(1)

ISIS(1) Level-1 Forwarding Table

IPV4 Destination IntCost ExtCost ExitInterface NextHop Flags

10.1.1.0/24 10 NULL P1/0/0 Direct D/-/L/-
10.1.2.0/24 10 NULL P2/0/0 Direct D/-/L/-
192.168.0.0/24 10 NULL P3/0/0 Direct D/-/L/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set

ISIS(1) Level-2 Forwarding Table

IPV4 Destination IntCost ExtCost ExitInterface NextHop Flags

10.1.1.0/24 10 NULL P1/0/0 Direct D/-/L/-
10.1.2.0/24 10 NULL P2/0/0 Direct D/-/L/-
192.168.0.0/24 10 NULL P3/0/0 Direct D/-/L/-
172.16.0.0/16 20 NULL P3/0/0 192.168.0.2 A/-/-/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set

[RouterD] display isis route
Route information for ISIS(1)

ISIS(1) Level-2 Forwarding Table

IPV4 Destination IntCost ExtCost ExitInterface NextHop Flags

192.168.0.0/24 10 NULL P1/0/0 Direct D/-/L/-
10.1.1.0/24 20 NULL P1/0/0 192.168.0.1 A/-/-/-
10.1.2.0/24 20 NULL P1/0/0 192.168.0.1 A/-/-/-
172.16.0.0/16 10 NULL GE2/0/0 Direct D/-/L/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set

```

----End

## Configuration Files

- Configuration file of Router A

```

#
 sysname RouterA
#
 isis 1
 is-level level-1
 network-entity 10.0000.0000.0001.00
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
 isis authentication-mode md5 N`C55QK<`=/Q=^Q`MAF4<1!!
#
 return

```



## ● Configuration file of Router B

```
#
 sysname RouterB
#
 isis 1
 is-level level-1
 network-entity 10.0000.0000.0002.00
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.2.2 255.255.255.0
 isis enable 1
#
 return
```

## ● Configuration file of Router C

```
#
 sysname RouterC
#
 isis 1
 network-entity 10.0000.0000.0003.00
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
 isis authentication-mode md5 N`C55QK<`= /Q=^Q`MAF4<1!!
#
 interface Pos2/0/0
 link-protocol ppp
 ip address 10.1.2.1 255.255.255.0
 isis enable 1
#
 interface Pos3/0/0
 link-protocol ppp
 ip address 192.168.0.1 255.255.255.0
 isis enable 1
#
 return
```

## ● Configuration file of Router D

```
#
 sysname RouterD
#
 isis 1
 is-level level-2
 network-entity 20.0000.0000.0004.00
#
 interface GigabitEthernet2/0/0
 ip address 172.16.1.1 255.255.0.0
 isis enable 1
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 192.168.0.2 255.255.255.0
 isis enable 1
#
 return
```

## 7.21.2 Example for Configuring IS-IS in an NBMA Network

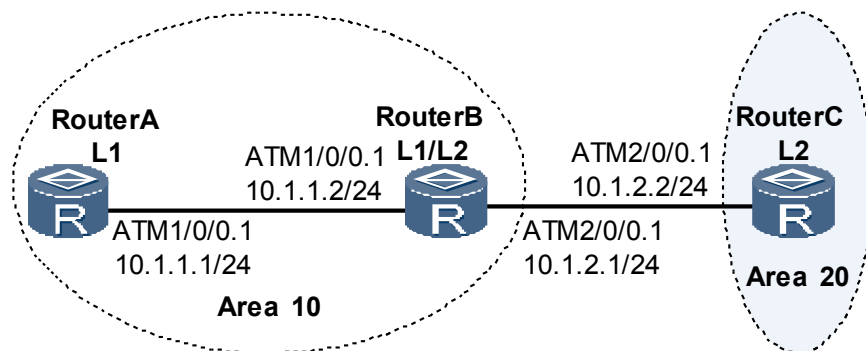
This part provides an example for interconnecting ATM networks through IS-IS.

### Networking Requirements

As shown in [Figure 7-8](#):

- Router A, Router B, and Router C are connected through ATM links. IS-IS runs on the three routers.
- Router A and Router B belong to area 10. Router C belongs to area 20.
- Router A is a Level-1 device, Router B is a Level-1-2 device, and Router C is a Level-2 device.

Figure 7-8 Diagram of configuring IS-IS in an NBMA network



## Configuration Roadmap

The configuration roadmap is as follows:

1. Set the type of the sub-interface to P2P when creating an ATM sub-interface, because IS-IS does not support the NBMA network.
2. Enable IS-IS on each router, configure the level, and specify an NET.

## Data Preparation

To complete the configuration, you need the following data:

- Area addresses of Router A, Router B, and Router C
- Levels of Router A, Router B, and Router C

## Procedure

### Step 1 Configure an ATM network.

# Configure Router A.

```
[RouterA] interface atm 1/0/0.1 p2p
[RouterA-Atm1/0/0.1] ip address 10.1.1.1 24
[RouterA-Atm1/0/0.1] pvc 2/2
[RouterA-atm-pvc-Atm1/0/0.1-2/2] map ip 10.1.1.2 broadcast
[RouterA-atm-pvc-Atm1/0/0.1-2/2] quit
[RouterA-Atm1/0/0.1] quit
```

# Configure Router B.

```
[RouterB] interface atm 1/0/0.1 p2p
[RouterB-Atm1/0/0.1] ip address 10.1.1.2 24
[RouterB-Atm1/0/0.1] pvc 2/2
[RouterB-atm-pvc-Atm1/0/0.1-2/2] map ip 10.1.1.1 broadcast
[RouterB-atm-pvc-Atm1/0/0.1-2/2] quit
```

```
[RouterB-Atm1/0/0.1] quit
[RouterB] interface atm 2/0/0.1 p2p
[RouterB-Atm2/0/0.1] ip address 10.1.2.1 24
[RouterB-Atm2/0/0.1] pvc 2/2
[RouterB-atm-pvc-Atm2/0/0.1-2/2] map ip 10.1.2.2 broadcast
[RouterB-atm-pvc-Atm2/0/0.1-2/2] quit
[RouterB-Atm2/0/0.1] quit
```

# Configure Router C.

```
[RouterC] interface atm 2/0/0.1 p2p
[RouterC-Atm2/0/0.1] ip address 10.1.2.2 24
[RouterC-Atm2/0/0.1] pvc 2/2
[RouterC-atm-pvc-Atm2/0/0.1-2/2] map ip 10.1.2.1 broadcast
[RouterC-atm-pvc-Atm2/0/0.1-2/2] quit
[RouterC-Atm2/0/0.1] quit
```

### Step 2 Configure basic IS-IS functions.

# Configure Router A.

```
[RouterA] isis 1
[RouterA-isis-1] is-level level-1
[RouterA-isis-1] network-entity 10.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface atm 1/0/0.1 p2p
[RouterA-Atm1/0/0.1] isis enable 1
[RouterA-Atm1/0/0.1] quit
```

# Configure Router B.

```
[RouterB] isis 1
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface atm 1/0/0.1 p2p
[RouterB-Atm1/0/0.1] isis enable 1
[RouterB-Atm1/0/0.1] quit
[RouterB] interface atm 2/0/0.1 p2p
[RouterB-Atm2/0/0.1] isis enable 1
[RouterB-Atm2/0/0.1] quit
```

# Configure Router C.

```
[RouterC] isis 1
[RouterC-isis-1] is-level level-2
[RouterC-isis-1] network-entity 20.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface atm 2/0/0.1 p2p
[RouterC-Atm2/0/0.1] isis enable 1
[RouterC-Atm2/0/0.1] quit
```

### Step 3 Verify the configuration.

# Display the IS-IS routing table of each router.

```
[RouterA] display isis route
 Route information for ISIS(1)

 ISIS(1) Level-1 Forwarding Table

 IPv4 Destination IntCost ExtCost ExitInterface NextHop Flags

 0.0.0.0/0 10 NULL Atm1/0/0.1 10.1.1.2 A/-/L/-
 10.1.1.0/24 10 NULL Atm1/0/0.1 Direct D/-/L/-
 10.1.2.0/24 20 NULL Atm1/0/0.1 10.1.1.2 A/-/L/-
 Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set

[RouterB] display isis route
 Route information for ISIS(1)

```

```

 ISIS(1) Level-1 Forwarding Table

 IPV4 Destination IntCost ExtCost ExitInterface NextHop Flags

 10.1.1.0/24 10 NULL Atm1/0/0.1 Direct D-/L/-
 10.1.2.0/24 10 NULL Atm2/0/0.1 Direct D-/L/-
 Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set
 ISIS(1) Level-2 Forwarding Table

 IPV4 Destination IntCost ExtCost ExitInterface NextHop Flags

 10.1.1.0/24 10 NULL Atm1/0/0.1 Direct D-/L/-
 10.1.2.0/24 10 NULL Atm2/0/0.1 Direct D-/L/-
 Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set

 [RouterC] display isis route
 Route information for ISIS(1)

 ISIS(1) Level-2 Forwarding Table

 IPV4 Destination IntCost ExtCost ExitInterface NextHop Flags

 10.1.1.0/24 20 NULL Atm2/0/0.1 10.1.2.1 A-/L/-
 10.1.2.0/24 10 NULL Atm2/0/0.1 Direct D-/L/-
 Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set

```

---End

## Configuration Files

- Configuration file of Router A

```

#
sysname RouterA
#
isis 1
 is-level level-1
 network-entity 10.0000.0000.0001.00
#
interface Atm1/0/0
#
interface Atm1/0/0.1 p2p
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
 pvc 2/2
 map ip 10.1.1.2 broadcast
#
return

```

- Configuration file of Router B

```

#
sysname RouterB
#
isis 1
 network-entity 10.0000.0000.0002.00
#
interface Atm1/0/0
#
interface Atm1/0/0.1 p2p
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
 pvc 2/2
 map ip 10.1.1.1 broadcast
#
interface Atm2/0/0
#
interface Atm2/0/0.1 p2p

```

```

ip address 10.1.2.1 255.255.255.0
isis enable 1
pvc 2/2
 map ip 10.1.2.2 broadcast
#
return

```

- Configuration file of Router C

```

#
sysname RouterC
#
isis 1
 is-level level-2
 network-entity 20.0000.0000.0003.00
#
interface Atm2/0/0
#
interface Atm2/0/0.1 p2p
 ip address 10.1.2.2 255.255.255.0
 isis enable 1
 pvc 2/2
 map ip 10.1.2.1 broadcast
#
return

```

## 7.21.3 Example for Configuring Route Aggregation

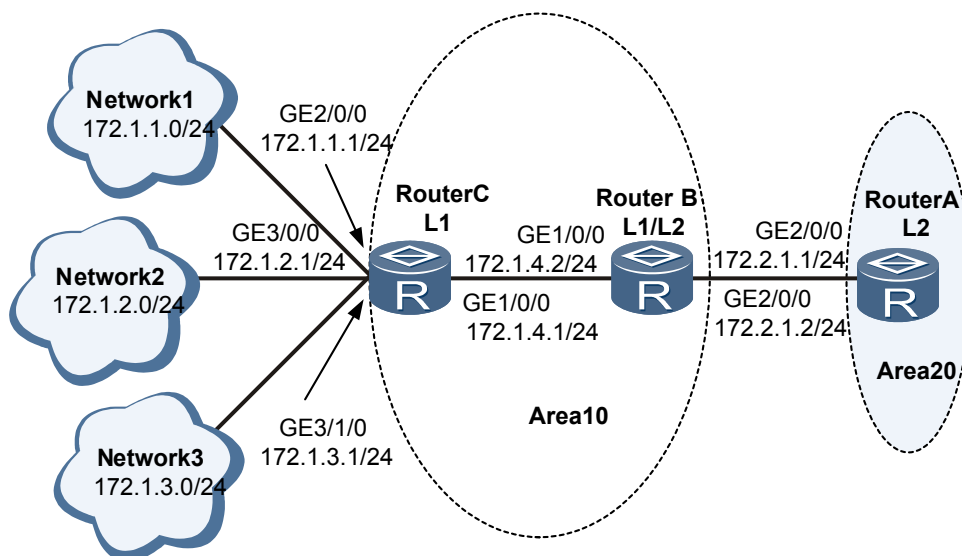
This part provides an example for implementing route aggregation through IS-IS.

### Networking Requirements

As shown in [Figure 7-9](#):

- Router A, Router B, and Router C run IS-IS to implement interconnection in the network.
- Router A belongs to area 20. Router B and Router C belong to area 10.
- Router A is a Level-2 router, Router B is a Level-1-2 router, and Router C is a Level-1 router.
- The IP addresses in area 10 can be aggregated to 172.1.0.0/16.

**Figure 7-9** Networking diagram of configuring IS-IS route aggregation



## Configuration Roadmap

The configuration roadmap is as follows:

1. Enable IS-IS on each router, configure the level, and specify an NET.
2. Check the IS-IS routing table of Router A.
3. Configure route aggregation on Router B.

## Data Preparation

To complete the configuration, you need the following data:

- Area addresses of Router A, Router B, and Router C
- Levels of Router A, Router B, and Router C

## Procedure

**Step 1** Configure an IP address for each interface.

The configuration details are not mentioned here.

**Step 2** Configure basic IS-IS functions.

# Configure Router A.

```
[RouterA] isis 1
[RouterA-isis-1] is-level level-2
[RouterA-isis-1] network-entity 20.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] isis enable 1
[RouterA-GigabitEthernet2/0/0] quit
```

# Configure Router B.

```
[RouterB] isis 1
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] isis enable 1
[RouterB-GigabitEthernet2/0/0] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] isis enable 1
[RouterB-GigabitEthernet1/0/0] quit
```

# Configure Router C.

```
[RouterC] isis 1
[RouterC-isis-1] is-level level-1
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] isis enable 1
[RouterC-GigabitEthernet1/0/0] quit
```

The configurations of GigabitEthernet 2/0/0, GigabitEthernet 3/0/0 and GigabitEthernet 3/1/0 are similar to that of GigabitEthernet 1/0/0, and are not mentioned here.

**Step 3** Check the IS-IS routing table of Router A.

```
[RouterA] display isis route
```

```

Route information for ISIS(1)

ISIS(1) Level-2 Forwarding Table

IPV4 Destination IntCost ExtCost ExitInterface NextHop Flags

172.1.1.0/24 30 NULL GE2/0/0 172.2.1.2 A/-/L/-
172.1.2.0/24 30 NULL GE2/0/0 172.2.1.2 A/-/L/-
172.1.3.0/24 30 NULL GE2/0/0 172.2.1.2 A/-/L/-
172.1.4.0/24 20 NULL GE2/0/0 172.2.1.2 A/-/L/-
172.2.1.0/24 10 NULL GE2/0/0 Direct D/-/L/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set

```

#### Step 4 Configure route aggregation on Router B.

# Converge routes 172.1.1.0/24, 172.1.2.0/24, 172.1.3.0/24 and 172.1.4.0/24 as route 172.1.0.0/16 on Router B.

```

[RouterB] isis 1
[RouterB-isis-1] summary 172.1.0.0 255.255.0.0 level-1-2
[RouterB-isis-1] quit

```

#### Step 5 Verify the configuration.

# Check the routing table of Router A, and you can find that routes 172.1.1.0/24, 172.1.2.0/24, 172.1.3.0/24 and 172.1.4.0/24 are aggregated as route 172.1.0.0/16.

```

[RouterA] display isis route
Route information for ISIS(1)

ISIS(1) Level-2 Forwarding Table

IPV4 Destination IntCost ExtCost ExitInterface NextHop Flags

172.1.0.0/16 20 NULL GE2/0/0 172.2.1.2 A/-/L/-
172.2.1.0/24 10 NULL GE2/0/0 Direct D/-/L/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
 U-Up/Down Bit Set

```

----End

## Configuration Files

- Configuration file of Router A

```

#
 sysname RouterA
#
 isis 1
 is-level level-2
 network-entity 20.0000.0000.0001.00
#
 interface GigabitEthernet2/0/0
 ip address 172.2.1.1 255.255.255.0
 isis enable 1
#
 return

```

- Configuration file of Router B

```

#
 sysname RouterB
#
 isis 1
 network-entity 10.0000.0000.0002.00
 summary 172.1.0.0 255.255.0.0 level-1-2
#
 interface GigabitEthernet2/0/0

```

```
ip address 172.2.1.2 255.255.255.0
isis enable 1
#
interface GigabitEthernet1/0/0
ip address 172.1.4.2 255.255.255.0
isis enable 1
#
return
```

- Configuration file of Router C

```
#
sysname RouterC
#
isis 1
is-level level-1
network-entity 10.0000.0000.0003.00
#
interface GigabitEthernet1/0/0
ip address 172.1.4.1 255.255.255.0
isis enable 1
#
interface GigabitEthernet2/0/0
ip address 172.1.1.1 255.255.255.0
isis enable 1
#
interface GigabitEthernet3/0/0
ip address 172.1.2.1 255.255.255.0
isis enable 1
#
interface GigabitEthernet3/1/0
ip address 172.1.3.1 255.255.255.0
isis enable 1
return
```

## 7.21.4 Example for Configuring the DIS Election of IS-IS

This part provides an example for specifying the DIS on a broadcast network.

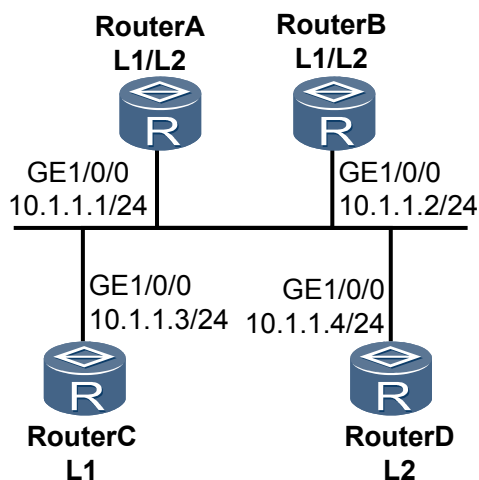
### Networking Requirements

As shown in [Figure 7-10](#):

- Router A, Router B, Router C, and Router D run IS-IS to implement interconnection in the network.
- The four routers belong to area 10, and the network type is broadcast (Ethernet).
- Router A and Router B are Level-1-2 routers, Router C is a Level-1 router, and Router D is a Level-2 router.
- The DIS priority of Router A is 100.
- You can change the DIS priority of the interface to configure Router A as a Level-1-2 DIS.



Figure 7-10 Configuring the DIS election of IS-IS



## Configuration Roadmap

The configuration roadmap is as follows:

1. Enable IS-IS on each router and specify the network entity to implement interconnection.
2. Check information about IS-IS interfaces on each router in the case of the default preference.
3. Configure the DIS priority of each router.

## Data Preparation

To complete the configuration, you need the following data:

- Area addresses of routerA, routerB, routerC and routerD
- Levels of routerA, routerB, routerC and routerD
- DIS priority of RouterA

## Procedure

**Step 1** Configure an IPv4 address for each interface.

The configuration details are not mentioned here.

**Step 2** Check the MAC address of the GE interface on each router.

# Check the MAC address of GigabitEthernet 1/0/0 on Router A.

```

[RouterA] display arp interface gigabitethernet 1/0/0
IP ADDRESS MAC ADDRESS EXPIRE (M) TYPE INTERFACE VPN-INSTANCE
 VLAN PVC

10.1.1.1 00e0-fc10-afec I GE1/0/0

Total:1 Dynamic:0 Static:0 Interface:1

```

# Check the MAC address of GigabitEthernet1/0/0 on Router B.

```
[RouterB] display arp interface gigabitethernet 1/0/0
IP ADDRESS MAC ADDRESS EXPIRE (M) TYPE INTERFACE VPN-INSTANCE
 VLAN PVC

10.1.1.2 00e0-fccd-acdf I GE1/0/0

Total:1 Dynamic:0 Static:0 Interface:1
```

# Check the MAC address of GigabitEthernet1/0/0 on Router C.

```
[RouterC] display arp interface gigabitethernet 1/0/0
IP ADDRESS MAC ADDRESS EXPIRE (M) TYPE INTERFACE VPN-INSTANCE
 VLAN PVC

10.1.1.3 00e0-f100-25fe I GE1/0/0

Total:1 Dynamic:0 Static:0 Interface:1
```

# Check the MAC address of GigabitEthernet1/0/0 on Router D.

```
[RouterD] display arp interface gigabitethernet 1/0/0
IP ADDRESS MAC ADDRESS EXPIRE (M) TYPE INTERFACE VPN-INSTANCE
 VLAN PVC

10.1.1.4 00e0-ff1d-305c I GE1/0/0

Total:1 Dynamic:0 Static:0 Interface:1
```

### Step 3 Enable IS-IS.

# Configure Router A.

```
[RouterA] isis 1
[RouterA-isis-1] network-entity 10.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] isis enable 1
[RouterA-GigabitEthernet1/0/0] quit
```

# Configure Router B.

```
[RouterB] isis 1
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] isis enable 1
[RouterB-GigabitEthernet1/0/0] quit
```

# Configure Router C.

```
[RouterC] isis 1
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] is-level level-1
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] isis enable 1
[RouterC-GigabitEthernet1/0/0] quit
```

# Configure Router D.

```
[RouterD] isis 1
[RouterD-isis-1] network-entity 10.0000.0000.0004.00
[RouterD-isis-1] is-level level-2
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] isis enable 1
[RouterD-GigabitEthernet1/0/0] quit
```

# Display the IS-IS neighbors of Router A.

```
[RouterA] display isis peer
Peer information for ISIS(1)

System Id Interface Circuit Id State HoldTime Type PRI
0000.0000.0002 GE1/0/0 0000.0000.0002.01 Up 9s L1 (L1L2) 64
0000.0000.0003 GE1/0/0 0000.0000.0002.01 Up 27s L1 64
0000.0000.0002 GE1/0/0 0000.0000.0004.01 Up 28s L2 (L1L2) 64
0000.0000.0004 GE1/0/0 0000.0000.0004.01 Up 7s L2 64

Total Peer(s) : 4
```

# Display the IS-IS interface of Router A.

```
[RouterA] display isis interface
Interface information for ISIS(1)

Interface Id IPV4.State IPV6.State MTU Type DIS
GE1/0/0 001 Up Down 1497 L1/L2 No/No
```

# Display the IS-IS interface on Router B.

```
[RouterB] display isis interface
Interface information for ISIS(1)

Interface Id IPV4.State IPV6.State MTU Type DIS
GE1/0/0 001 Up Down 1497 L1/L2 Yes/No
```

# Display the IS-IS interface of Router D.

```
[RouterD] display isis interface
Interface information for ISIS(1)

Interface Id IPV4.State IPV6.State MTU Type DIS
GE1/0/0 001 Up Down 1497 L1/L2 No/Yes
```

**NOTE**

When the default DIS priority is used, the MAC address of the interface on Router B is the largest one among those of Level-1 routers. Router B is thus the DIS of the Level-1 area. The MAC address of interface on Router D is the largest one among those of Level-2 routers. Router D is the DIS of the Level-2 area. The Level-1 and Level-2 pseudo nodes are 0000.0000.0002.01 and 0000.0000.0004.01 respectively.

**Step 4** Configure the DIS priority of Router A.

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] isis dis-priority 100
```

# Display the IS-IS neighbors of Router A.

```
[RouterA] display isis peer
Peer information for ISIS(1)

System Id Interface Circuit Id State HoldTime Type PRI
0000.0000.0002 GE1/0/0 0000.0000.0001.01 Up 21s L1 (L1L2) 64
0000.0000.0003 GE1/0/0 0000.0000.0001.01 Up 27s L1 64
0000.0000.0002 GE1/0/0 0000.0000.0001.01 Up 28s L2 (L1L2) 64
0000.0000.0004 GE1/0/0 0000.0000.0001.01 Up 30s L2 64

Total Peer(s) : 4
```

**Step 5** Verify the configuration.

# Display the IS-IS interface of Router A.

```
[RouterA] display isis interface
Interface information for ISIS(1)

Interface Id IPV4.State IPV6.State MTU Type DIS
GE1/0/0 001 Up Down 1497 L1/L2 Yes/Yes
```

 **NOTE**

After the DIS priority of the IS-IS interface changes, Router A becomes the DIS of the Level-1-2 area instantly and its pseudo node is 0000.0000.0001.01.

# Display the IS-IS neighbors and IS-IS interfaces of Router B.

```
[RouterB] display isis peer
Peer information for ISIS(1)

System Id Interface Circuit Id State HoldTime Type PRI
0000.0000.0001 GE1/0/0 0000.0000.0001.01 Up 7s L1 (L1L2) 100
0000.0000.0003 GE1/0/0 0000.0000.0001.01 Up 25s L1 64
0000.0000.0001 GE1/0/0 0000.0000.0001.01 Up 7s L2 (L1L2) 100
0000.0000.0004 GE1/0/0 0000.0000.0001.01 Up 25s L2 64
```

Total Peer(s): 4

```
[RouterB] display isis interface
Interface information for ISIS(1)

Interface Id IPV4.State IPV6.State MTU Type DIS
GE1/0/0 001 Up Down 1497 L1/L2 No/No
```

# Display the IS-IS neighbors and interfaces of Router D.

```
[RouterD] display isis peer
Peer information for ISIS(1)

System Id Interface Circuit Id State HoldTime Type PRI
0000.0000.0001 GE1/0/0 0000.0000.0001.01 Up 9s L2 100
0000.0000.0002 GE1/0/0 0000.0000.0001.01 Up 28s L2 64
```

Total Peer(s): 2

```
[RouterD] display isis interface
Interface information for ISIS(1)

Interface Id IPV4.State IPV6.State MTU Type DIS
GE1/0/0 001 Up Down 1497 L1/L2 No/No
```

----End

## Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
isis 1
network-entity 10.0000.0000.0001.00
#
interface GigabitEthernet1/0/0
ip address 10.1.1.1 255.255.255.0
isis enable 1
isis dis-priority 100
#
return
```

- Configuration file of Router B

```
#
sysname RouterB
#
isis 1
network-entity 10.0000.0000.0002.00
#
interface GigabitEthernet1/0/0
ip address 10.1.1.2 255.255.255.0
isis enable 1
#
```

- ```
return
```
- Configuration file of Router C

```
#
 sysname RouterC
#
 isis 1
  is-level level-1
  network-entity 10.0000.0000.0003.00
#
 interface GigabitEthernet1/0/0
  ip address 10.1.1.3 255.255.255.0
  isis enable 1
#
return
```
 - Configuration file of Router D

```
#
 sysname RouterD
#
 isis 1
  is-level level-2
  network-entity 10.0000.0000.0004.00
#
 interface GigabitEthernet1/0/0
  ip address 10.1.1.4 255.255.255.0
  isis enable 1
#
return
```

7.21.5 Example for Configuring IS-IS Load Balancing

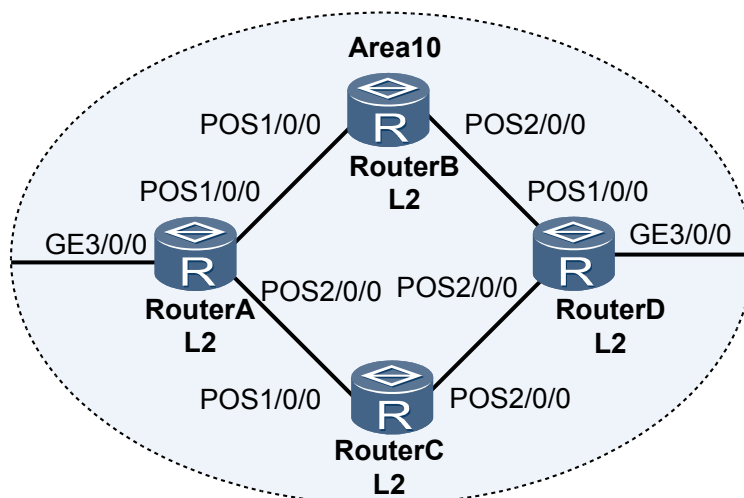
This part provides an example for implementing load balancing through IS-IS.

Networking Requirements

As shown in [Figure 7-11](#):

- Router A, Router B, Router C, and Router D run IS-IS to implement interconnection in the IP network.
- Router A, Router B, Router C, and Router D are Level-2 routers in area 10.
- Load balancing is required to transmit the traffic of Router A to Router D through Router B and Router C.

Figure 7-11 Networking diagram of configuring IS-IS load balancing



Device	Interface	IP Address	Device	Interface	IP Address
Router A	GE 3/0/0	172.16.1.1/24	Router C	POS 1/0/0	10.1.2.2/24
	POS 1/0/0	10.1.1.1/24		POS 2/0/0	192.168.1.1/24
	POS 2/0/0	10.1.2.1/24			
Router B	POS 1/0/0	10.1.1.2/24	Router D	GE 3/0/0	172.17.1.1/24
	POS 2/0/0	192.168.0.1/24		POS 1/0/0	192.168.0.2/24
				POS 2/0/0	192.168.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic IS-IS functions on each router to implement interconnection.
2. Cancel load balancing and check the routing table.
3. Configure load balancing on Router A and check the routing table of it.
4. (Optional) Configure the preference for equal-cost routes on Router A.

Data Preparation

To complete the configuration, you need the following data:

- Levels and the area addresses of the four routers.
- Number of load balancing paths on Router A is 1.
- Preference value of equal-cost routes on Router C is 1.

Procedure

Step 1 Assign an IP address for each router.

The configuration details are not mentioned here.

Step 2 Configure basic IS-IS functions.

For details about the configuration of basis IS-IS functions, see [7.21.1 Example for Configuring Basic IS-IS Functions](#).

Step 3 Cancel load balancing on Router A.

```
[RouterA] isis 1
[RouterA-isis-1] maximum load-balancing 1
[RouterA-isis-1] quit
```

Check the routing table of Router A.

```
[RouterA] display isis route
                Route information for ISIS(1)
                -----
                ISIS(1) Level-2 Forwarding Table
                -----
IPV4 Destination   IntCost   ExtCost  ExitInterface  NextHop      Flags
-----
192.168.1.0/24     20        NULL     P2/0/0         10.1.2.2     A/-/L/-
10.1.1.0/24        10        NULL     P1/0/0         Direct       D/-/L/-
172.16.1.0/24      10        NULL     GE3/0/0        Direct       D/-/L/-
172.17.1.0/24      30        NULL     P1/0/0         10.1.1.2     A/-/L/-
10.1.2.0/24        10        NULL     P2/0/0         Direct       D/-/L/-
192.168.0.0/24     20        NULL     P1/0/0         10.1.1.2     A/-/L/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
       U-Up/Down Bit Set
```

As shown in the routing table, when the maximum number of equal-cost routes for load balancing is set to 1, the next hop to network segment 172.17.1.0 is 10.1.1.2. This is because the system ID of Router B is small. IS-IS chooses the route with the next hop being 10.1.1.2 as the unique optimal route.

Step 4 Restore the default number of load balancing paths on Router A.

```
[RouterA] isis 1
[RouterA-isis-1] undo maximum load-balancing
[RouterA-isis-1] quit
```

Check the routing table of Router A.

```
[RouterA] display isis route
                Route information for ISIS(1)
                -----
                ISIS(1) Level-2 Forwarding Table
                -----
IPV4 Destination   IntCost   ExtCost  ExitInterface  NextHop      Flags
-----
192.168.1.0/24     20        NULL     P2/0/0         10.1.2.2     A/-/L/-
10.1.1.0/24        10        NULL     P1/0/0         Direct       D/-/L/-
172.16.1.0/24      10        NULL     GE3/0/0        Direct       D/-/L/-
172.17.1.0/24      30        NULL     P1/0/0         10.1.1.2     A/-/L/-
10.1.2.0/24        10        NULL     P2/0/0         10.1.2.2     D/-/L/-
192.168.0.0/24     20        NULL     P1/0/0         10.1.1.2     A/-/L/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
       U-Up/Down Bit Set
```

As shown in the routing table, the default value is used when load balancing is canceled. The two next hops of Router A, that is, 10.1.1.2 (that is, Router B) and 10.1.1.2 (that is, Router C), are valid routes. This is because the default value of the maximum equal-cost routes is 3.

 **NOTE**

For different products and different protocols, the maximum number of equal-cost routes is different. You can adjust the maximum number by purchasing licenses.

Step 5 (Optional) Configure the preference of equal-cost routes on Router A.

If you do not perform load balancing through Router B and Router C, configure the preference of the equal-cost routes and specify the next hop.

```
[RouterA] isis
[RouterA-isis-1] nexthop 10.1.2.2 weight 1
[RouterA-isis-1] quit
```

Step 6 Verify the configuration.

Check the routing table of Router A.

```
[RouterA] display isis route
                        Route information for ISIS(1)
                        -----
                        ISIS(1) Level-2 Forwarding Table
                        -----
IPv4 Destination      IntCost   ExtCost  ExitInterface  NextHop      Flags
-----
192.168.1.0/24        20        NULL    P2/0/0         10.1.2.2     A/-/L/-
10.1.1.0/24           10        NULL    P1/0/0         Direct       D/-/L/-
172.16.1.0/24         10        NULL    GE3/0/0        Direct       D/-/L/-
172.17.1.0/24         30        NULL    P1/0/0         10.1.2.2     A/-/L/-
10.1.2.0/24           10        NULL    P2/0/0         Direct       D/-/L/-
192.168.0.0/24        20        NULL    P1/0/0         10.1.1.2     A/-/L/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
       U-Up/Down Bit Set
```

As shown in the routing table, because the preference (metric is 1) of next hop 10.1.2.2 (that is, Router C) is higher than that of next hop 10.1.1.2 (that is, Router B), IS-IS chooses the route with the next hop being 10.1.2.2 as the optimal route.

----End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
 isis 1
 is-level level-2
 network-entity 10.0000.0000.0001.00
 nexthop 10.1.2.2 weight 1
#
 interface GigabitEthernet3/0/0
 ip address 172.16.1.1 255.255.255.0
 isis enable 1
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
#
 interface Pos2/0/0
 link-protocol ppp
 ip address 10.1.2.1 255.255.255.0
 isis enable 1
#
return
```


- Configuration file of Router B

```
#
 sysname RouterB
#
 isis 1
  is-level level-2
  network-entity 10.0000.0000.0002.00
#
 interface Pos1/0/0
  link-protocol ppp
  ip address 10.1.1.2 255.255.255.0
  isis enable 1
#
 interface Pos2/0/0
  link-protocol ppp
  ip address 192.168.0.1 255.255.255.0
  isis enable 1
#
 return
```

- Configuration file of Router C

```
#
 sysname RouterC
#
 isis 1
  is-level level-2
  network-entity 10.0000.0000.0003.00
#
 interface Pos1/0/0
  link-protocol ppp
  ip address 10.1.2.2 255.255.255.0
  isis enable 1
#
 interface Pos2/0/0
  link-protocol ppp
  ip address 192.168.1.1 255.255.255.0
  isis enable 1
#
 return
```

- Configuration file of Router D

```
#
 sysname RouterD
#
 isis 1
  is-level level-2
  network-entity 10.0000.0000.0004.00
#
 interface GigabitEthernet3/0/0
  ip address 172.17.1.1 255.255.255.0
  isis enable 1
#
 interface Pos1/0/0
  link-protocol ppp
  ip address 192.168.0.2 255.255.255.0
  isis enable 1
#
 interface Pos2/0/0
  link-protocol ppp
  ip address 192.168.1.2 255.255.255.0
  isis enable 1
#
 return
```

7.21.6 Example for Configuring IS-IS to Interact with BGP

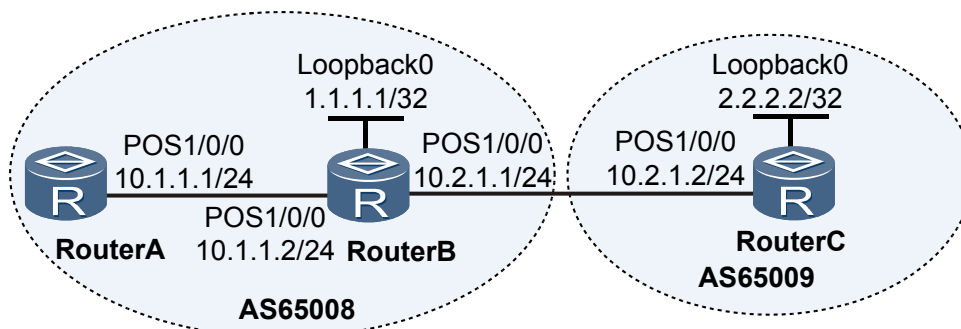
This part provides an example for configuring two ASs running IS-IS to import routes from each other.

Networking Requirements

As shown in [Figure 7-12](#):

- Router A and Router B belong to the same AS, and the IS-IS neighbor relationship is established between Router A and Router B; Router A is a non-BGP router in the AS.
- EBGP connections are established between Router B and Router C. IS-IS and BGP import routes of each other. When IS-IS imports BGP routes, a routing policy is configured to change the cost of the BGP routes.

Figure 7-12 Networking diagram of configuring IS-IS to interact with BGP



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable IS-IS on Router A and Router B and specify a network entity.
2. Configure EBGP connections on Router B and Router C.
3. Configure IS-IS to interact with BGP on Router B, and check route information.

Data Preparation

To complete the configuration, you need the following data:

- Area addresses of Router A and Router B
- Router ID and AS number of Router B
- Router ID and AS number of Router C

Procedure

Step 1 Configure an IP address for each interface. The configuration details are not mentioned here.

Step 2 Configure basic IS-IS functions.

Configure Router A.

```
[RouterC] isis 1
[RouterC-isis-1] network-entity 10.0000.0000.0001.00
[RouterC-isis-1] quit
[RouterC] interface pos 1/0/0
```

```
[RouterC-Pos1/0/0] isis enable 1
[RouterC-Pos1/0/0] quit
```

Configure Router B.

```
[RouterB] isis 1
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface pos 1/0/0
[RouterB-Pos1/0/0] isis enable 1
[RouterB-Pos1/0/0] quit
```

Step 3 Configure an EBGP connection.

Configure Router B.

```
[RouterB] bgp 65008
[RouterB-bgp] router-id 1.1.1.1
[RouterB-bgp] peer 10.2.1.2 as-number 65009
[RouterB-bgp] ipv4-family unicast
[RouterB-bgp-af-ipv4] network 10.2.1.0 255.255.255.0
```

Configure Router C.

```
[RouterC] bgp 65009
[RouterC-bgp] router-id 2.2.2.2
[RouterC-bgp] peer 10.2.1.1 as-number 65008
[RouterC-bgp] ipv4-family unicast
[RouterC-bgp-af-ipv4] network 10.2.1.0 255.255.255.0
```

Step 4 Configure IS-IS to import BGP routes.

Configure a static route on Router C.

```
[RouterC] ip route-static 200.1.1.1 32 NULL 0
```

On Router C, configure BGP to import the static route.

```
[RouterC] bgp 65009
[RouterC-bgp] import-route static
```

On Router B, configure IS-IS to import the BGP route.

```
[RouterB] isis 1
[RouterB-isis-1] import-route bgp
[RouterB-isis-1] quit
```

View the routing table of Router A, and you can find that IS-IS successfully imports the BGP route 200.1.1.1/32.

```
[RouterA] display ip routing-table
Route Flags: R - relied, D - download to fib
-----
Routing Tables: Public
          Destinations : 6          Routes : 6
Destination/Mask  Proto  Pre  Cost    Flags NextHop         Interface
10.1.1.0/24      Direct  0    0        D   10.1.1.1         Pos1/0/0
10.1.1.1/32      Direct  0    0        D   127.0.0.1        InLoopBack0
10.1.1.2/32      Direct  0    0        D   10.1.1.2         Pos1/0/0
127.0.0.0/8      Direct  0    0        D   127.0.0.1        InLoopBack0
127.0.0.1/32     Direct  0    0        D   127.0.0.1        InLoopBack0
200.1.1.1/32     ISIS-L2 15  74  D   10.1.1.2         Pos1/0/0
```

On Router B, configure the AS-Path filter, and apply the filter in the routing policy named RTC.

```
[RouterB] ip as-path-filter 1 permit 65009
[RouterB] route-policy RTC permit node 0
[RouterB-route-policy] if-match as-path-filter 1
```

```
[RouterB-route-policy] apply cost 20
[RouterB-route-policy] quit
```

On Router B, configure IS-IS to import the BGP route on Router C.

```
[RouterB] isis 1
[RouterB-isis-1] import-route bgp route-policy RTC
[RouterB-isis-1] quit
```

View the routing table of Router A, and you can find that the AS-Path filter is successfully applied and the cost of the imported route 200.1.1.1/32 changes from 74 to 94.

```
[RouterA] display ip routing-table
Route Flags: R - relied, D - download to fib
-----
Routing Tables: Public
  Destinations : 6          Routes : 6
Destination/Mask    Proto Pre  Cost    Flags NextHop         Interface
10.1.1.0/24         Direct 0     0       D 10.1.1.1       Pos1/0/0
10.1.1.1/32         Direct 0     0       D 127.0.0.1      Pos1/0/0
10.1.1.2/32         Direct 0     0       D 10.1.1.2       Pos1/0/0
127.0.0.0/8         Direct 0     0       D 127.0.0.1      InLoopBack0
127.0.0.1/32        Direct 0     0       D 127.0.0.1      InLoopBack0
200.1.1.1/32        ISIS-L2 15 94 D 10.1.1.2       Pos1/0/0
```

Step 5 Configure BGP to import an IS-IS route.

```
[RouterB] bgp 65008
[RouterB-bgp] import-route isis 1
[RouterB-bgp] quit
```

View the routing table of Router C, and you can find that BGP successfully imports the IS-IS route 10.1.1.0/24.

```
[RouterC] display ip routing-table
Route Flags: R - relied, D - download to fib
-----
Routing Tables: Public
  Destinations : 7          Routes : 7
Destination/Mask    Proto Pre  Cost    Flags NextHop         Interface
10.1.1.0/24         EBGP  255 0 D 10.2.1.1       Pos1/0/0
10.2.1.0/24         Direct 0     0       D 10.2.1.2       Pos1/0/0
10.2.1.1/32         Direct 0     0       D 10.2.1.1       Pos1/0/0
10.2.1.2/32         Direct 0     0       D 127.0.0.1      InLoopBack0
127.0.0.0/8         Direct 0     0       D 127.0.0.1      InLoopBack0
127.0.0.1/32        Direct 0     0       D 127.0.0.1      InLoopBack0
200.1.1.1/32        Static 60    0       D 0.0.0.0        NULL0
```

----End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
 isis 1
 network-entity 10.0000.0000.0001.00
#
 interface Pos1/0/0
  link-protocol ppp
  ip address 10.1.1.1 255.255.255.0
  isis enable 1
#
 return
```

- Configuration file of Router B

```

#
 sysname RouterB
#
 isis 1
 network-entity 10.0000.0000.0002.00
 import-route bgp route-policy RTC
#
 interface Pos1/0/0
  link-protocol ppp
  ip address 10.1.1.2 255.255.255.0
  isis enable 1
#
 interface Pos2/0/0
  link-protocol ppp
  ip address 10.2.1.1 255.255.255.0
#
 interface LoopBack0
  ip address 1.1.1.1 255.255.255.255
#
 bgp 65008
  router-id 1.1.1.1
  peer 10.2.1.2 as-number 65009
#
 ipv4-family unicast
  undo synchronization
  network 10.2.1.0 255.255.255.0
  import-route isis 1
  peer 10.2.1.2 enable
#
 route-policy RTC permit node 0
  if-match as-path-filter 1
  apply cost 20
#
 ip as-path-filter 1 permit 65009
#
 return
  
```

- Configuration file of Router C

```

#
 sysname RouterC
#
 interface Pos1/0/0
  link-protocol ppp
  ip address 10.2.1.2 255.255.255.0
#
 interface LoopBack0
  ip address 2.2.2.2 255.255.255.255
#
 bgp 65009
  router-id 2.2.2.2
  peer 10.2.1.1 as-number 65008
#
 ipv4-family unicast
  undo synchronization
  network 10.2.1.0 255.255.255.0
  import-route static
  peer 10.2.1.1 enable
#
 ip route-static 200.1.1.1 255.255.255.255 NULL0
#
 return
  
```

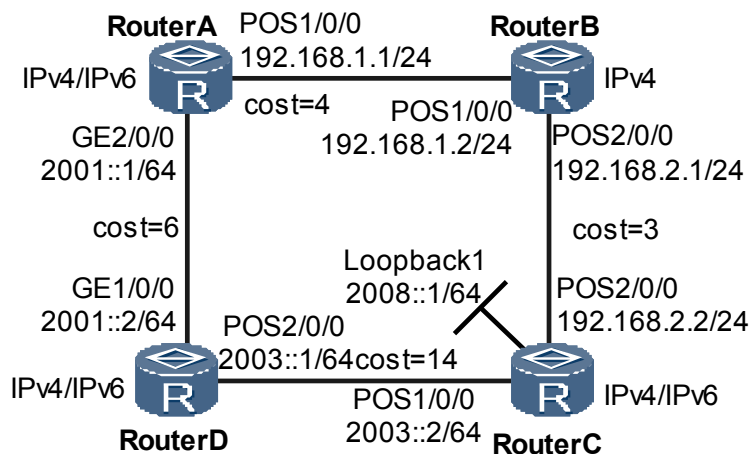
7.21.7 Example for Configuring IS-IS MT

This part provides an example for interconnecting IPv4 and IPv6 networks through IS-IS.

Networking Requirements

IP address and link cost of each interface on routers are shown in **Figure 7-13**. Router B supports only IPv4. It is required that Loopback1 of Router C is reachable. If the network does not support IS-IS MT, the shortest path computed by SPF passes by Router B and IPv6 packets cannot reach the destination. To forward IPv6 packets successfully, enable IS-IS MT and perform SPF calculation in the IPv6 topology.

Figure 7-13 Networking diagram of IS-IS MT



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the IPv4/IPv6 address of each interface.
2. Enable IPv6 on routers that supporting IPv4/IPv6 dual stack protocol.
3. Enable IS-IS globally and configure the name of the network entity.
4. Enable IPv6 of the IPv6 topology type on routers that support the IPv4/IPv6 dual stack protocol.
5. Enable IS-IS on each interface and configure the link cost according to networking requirements.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each router interface is needed. For example, in **Figure 7-13**, the area address is 86; the system ID of Router A is 0000.0000.0001; system IDs of other routers increase based on that of Router A; all the routers are Level-1 routers.
- The link cost of Router D → Router A, Router A → Router B, Router B → Router C and Router D → Router C is 6, 4, 3 and 14 respectively. The cost of Loopback1 on Router D defaults to be 0. The costs of other links default to be 10.

Procedure

Step 1 Configure an IP address of each interface.

Configure an IPv4/IPv6 address and mask of each interface as shown in [Figure 7-13](#).

The configuration details are not mentioned here.

Step 2 Enable IPv6 of the IPv4/ IPv6 dual stack router.

Enable IPv6 of Router A.

```
[RouterA] ipv6
```

Configurations of Router C and Router D are the same as Router A.

Step 3 Configure IS-IS to advertise routes.

Configure basic IS-IS functions on Router A, enable IS-IS and adopt the IPv6 topology type.

```
[RouterA] isis 1
[RouterA-isis-1] network-entity 86.0000.0000.0001.00
[RouterA-isis-1] is-level level-1
[RouterA-isis-1] ipv6 enable topology ipv6
[RouterA-isis-1] quit
```

Enable IS-IS on each interface and set the link cost from Router A to Router B to 4.

```
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] isis enable 1
[RouterA-Pos1/0/0] isis cost 4
[RouterA-Pos1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] isis ipv6 enable 1
[RouterA-GigabitEthernet2/0/0] quit
```

Configure basic IS-IS functions on Router B.

```
[RouterB] isis 1
[RouterB-isis-1] network-entity 86.0000.0000.0002.00
[RouterB-isis-1] is-level level-1
[RouterB-isis-1] quit
```

Enable IS-IS on each interface and set the link cost from Router B to Router C to 3.

```
[RouterB] interface pos 1/0/0
[RouterB-Pos1/0/0] isis enable 1
[RouterB-Pos1/0/0] quit
[RouterB] interface pos 2/0/0
[RouterB-Pos2/0/0] isis enable 1
[RouterB-Pos2/0/0] isis cost 3
[RouterB-Pos2/0/0] quit
```

Configure basic IS-IS functions on Router C, enable IS-IS and adopt the IPv6 topology type.

```
[RouterC] isis 1
[RouterC-isis-1] network-entity 86.0000.0000.0003.00
[RouterC-isis-1] is-level level-1
[RouterC-isis-1] ipv6 enable topology ipv6
[RouterC-isis-1] quit
```

Enable IS-IS on each interface.

```
[RouterC] interface pos 1/0/0
[RouterC-Pos1/0/0] isis ipv6 enable 1
[RouterC-Pos1/0/0] quit
[RouterC] interface pos 2/0/0
[RouterC-Pos2/0/0] isis enable 1
[RouterC-Pos2/0/0] quit
```

```
[RouterC] interface loopback 1
[RouterC-LoopBack1] isis ipv6 enable 1
```

Configure basic IS-IS functions on Router D, enable IS-IS and adopt the IPv6 topology type.

```
[RouterD] isis 1
[RouterD-isis-1] network-entity 86.0000.0000.0004.00
[RouterD-isis-1] is-level level-1
[RouterD-isis-1] ipv6 enable topology ipv6
[RouterD-isis-1] quit
```

Enable IS-IS on each interface; set the link cost from Router D to Router A to 6 and the link cost from Router D to Router C to 14.

```
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] isis ipv6 enable 1
[RouterD-GigabitEthernet1/0/0] isis cost 6
[RouterD-GigabitEthernet1/0/0] isis ipv6 cost 6
[RouterD-GigabitEthernet1/0/0] quit
[RouterD] interface pos 2/0/0
[RouterD-Pos2/0/0] isis ipv6 enable 1
[RouterD-Pos2/0/0] isis cost 14
[RouterD-Pos2/0/0] isis ipv6 cost 14
[RouterD-Pos2/0/0] quit
```

Step 4 Verify the configuration.

After the configuration, run **display isis route** command on each router, and you can find that each router learns related routes. Take the display of Router D as an example:

View routing information of Router D.

```
[RouterD] display isis route
                Route information for ISIS(1)
                -----
                ISIS(1) Level-1 Forwarding Table
                -----
IPV6 Dest.      ExitInterface  NextHop          Cost      Flags
-----
2008::/64      Pos2/0/0      FE80::D11:0:36D4:1  14        A/-/-
2003::/64      Pos2/0/0      Direct           14        D/L/-
2001::/64      GE1/0/0       Direct            6         D/L/-
                Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                U-Up/Down Bit Set
```

Because IPv6 routes are calculated only on the IPv6 topology, the outgoing interface to 2008::/64 on Router D is POS 2/0/0.

Run the **tracert** command on Router D.

```
[RouterD] tracert ipv6 2008::1
traceroute to 2008::1 30 hops max,60 bytes packet
 1 2008::1 62 ms 63 ms 31 ms
```

You can compare this with the routing information when IS-IS is enabled and IPv4/IPv6 integrated topology type is adopted.

```
[RouterD] isis 1
[RouterD-isis-1] ipv6 enable
```

The modification of Router A and Router C is the same as that of Router D.

After modifying the configuration, run **display isis route** command to view the routes again. Take the display of Router D as an example:

View routing information of Router D.

```
[RouterD] display isis route
```



```

Route information for ISIS(1)
-----
ISIS(1) Level-1 Forwarding Table
-----
IPV6 Dest.   ExitInterface  NextHop          Cost    Flags
-----
2008::/64    GE1/0/0        FE80::200:5EFF:FE01:100    13     A/-/-
2003::/64    Pos2/0/0       Direct           14     D/L/-
2001::/64    GE1/0/0        Direct           6      D/L/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
      U-Up/Down Bit Set

```

From the preceding information, you can see that the route to 2008::/64 can be calculated on Router D and the outgoing interface is GE 1/0/0. Outgoing interface GE 1/0/0 is selected because the cost of link from this outgoing interface to destination 2008::1/64 is smaller in integrated topology calculation.

```

[RouterD] tracert ipv6 2008::1
tracert to 2008::1 30 hops max,60 bytes packet
1 2001::1 31 ms !N 31 ms !N 32 ms !N

```

Run the **tracert** command, and you can find that IPv6 packets fail to reach the destination.

View routing information of Router A

```

[RouterA] display isis route
Route information for ISIS(1)
-----
ISIS(1) Level-1 Forwarding Table
-----
IPV4 Destination  IntCost  ExtCost  ExitInterface  NextHop          Flags
-----
192.168.2.0/24    7        NULL     Pos1/0/0       192.168.1.2     A/-/-/-
192.168.1.0/24    4        NULL     Pos1/0/0       Direct          D/-/L/-
IPV6 Dest.       ExitInterface  NextHop          Cost    Flags
-----
2003::/64        Pos1/0/0       FE80::2E0:A9FF:FE47:8302    24     A/-/-
2001::/64        GE2/0/0        Direct           10     D/L/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
      U-Up/Down Bit Set

```

From the preceding information, you can see that Router A does not have information the outgoing interface to 2008::/64. This is because the link between Router A and Router B does not support IPv6 and IPv6 packets sent by Router D are discarded here.

----End

Configuration Files

- Configuration file of Router A

```

#
sysname RouterA
#
ipv6
#
isis 1
is-level level-1
network-entity 86.0000.0000.0001.00
#
ipv6 enable topology ipv6
#
#
interface Pos1/0/0
link-protocol ppp
ip address 192.168.1.1 255.255.255.0
isis enable 1
isis cost 4

```

```
#
interface GigabitEthernet2/0/0
  ipv6 enable
  ipv6 address 2001::1/64
  isis ipv6 enable 1
#
return
```

● Configuration file of Router B

```
#
 sysname RouterB
#
isis 1
  is-level level-1
  network-entity 86.0000.0000.0002.00
#
interface Pos1/0/0
  link-protocol ppp
  ip address 192.168.1.2 255.255.255.0
  isis enable 1
#
interface Pos2/0/0
  link-protocol ppp
  ip address 192.168.2.1 255.255.255.0
  isis enable 1
  isis cost 3
#
return
```

● Configuration file of Router C

```
#
 sysname RouterC
#
 ipv6
#
isis 1
  is-level level-1
  network-entity 86.0000.0000.0003.00
#
  ipv6 enable topology ipv6
#
#
interface Pos1/0/0
  link-protocol ppp
  ipv6 enable
  ipv6 address 2003::2/64
  isis ipv6 enable 1
#
interface Pos2/0/0
  link-protocol ppp
  ip address 192.168.2.2 255.255.255.0
  isis enable 1
#
interface LoopBack1
  ipv6 enable
  ipv6 address 2008::1/64
  isis ipv6 enable 1
#
return
```

● Configuration file of Router D

```
#
 sysname RouterD
#
 ipv6
#
isis 1
  is-level level-1
  network-entity 86.0000.0000.0004.00
#
```

```

        ipv6 enable topology ipv6
    #
    #
    interface GigabitEthernet1/0/0
    ipv6 enable
    ipv6 address 2001::2/64
    isis ipv6 enable 1
    isis ipv6 cost 6
    isis cost 6
    #
    interface Pos2/0/0
    link-protocol ppp
    ipv6 enable
    ipv6 address 2003::1/64
    isis ipv6 enable 1
    isis ipv6 cost 14
    isis cost 14
    #
    return
    
```

7.21.8 Example for Configuring Local MT

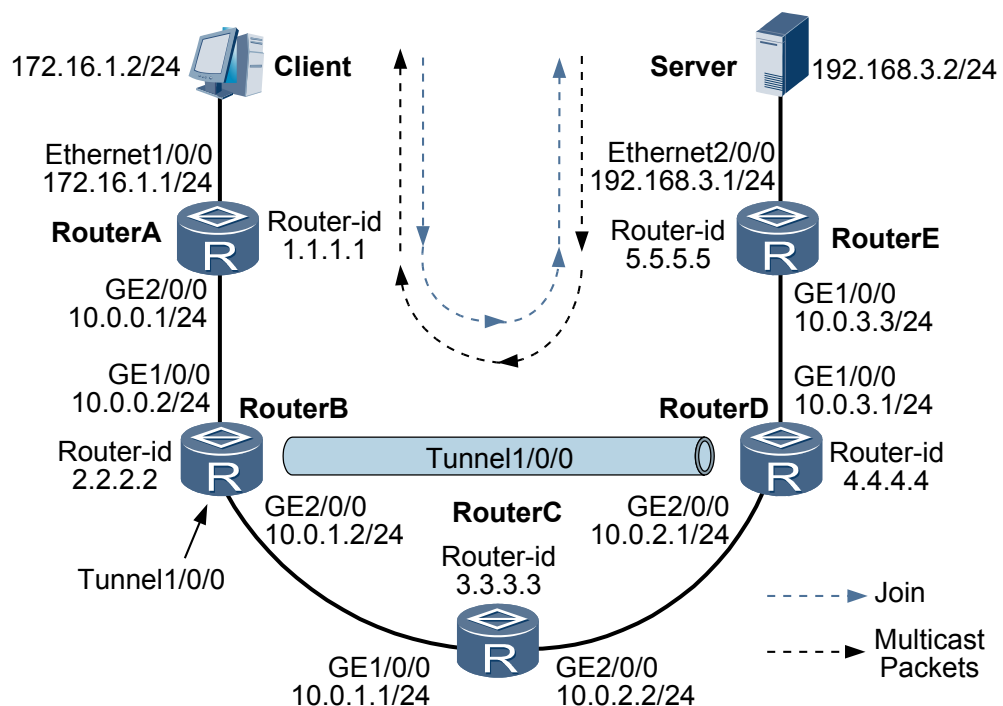
This part provides an example for configuring multicast packets to be forwarded through TE tunnels on IS-IS networks.

Networking Requirements

As shown in [Figure 7-14](#):

- Router A, Router B, Router C, Router D, and Router E run IS-IS, and they are Level-2 routers.
- A TE tunnel is established between Router B and Router D.
- IGP Shortcut is enabled on Router B.

Figure 7-14 Configuring local MT



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic IS-IS functions on each router.
2. Configure the Protocol Independent Multicast Sparse Mode (PIM-SM).
3. Configure an MPLS Resource Reservation Protocol (RSVP) TE tunnel and enable IGP Shortcut.
4. Enable local MT.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each router interface is shown in [Figure 7-14](#). The area address is 10, the originating system ID is 0000.0000.0001 and is incremental, and the routers are Level-2 routers.
- Tunnel interface is TE tunnel 1/0/0, the tunnel interface borrows the IP address of Loopback 0, the tunnel encapsulation protocol is MPLS TE, the destination address is 4.4.4.4, the tunnel ID is 100, and the tunnel signaling protocol is RSVP-TE.

Procedure

Step 1 Assign an IP address for each interface and enable IS-IS.

As shown in [Figure 7-14](#), assign an IP address and the mask for each interface and enable IS-IS. The configuration details are not mentioned here.

Step 2 Configure PIM-SM.

Enable multicast on all routers and enable PIM-SM on all interfaces except GigabitEthernet 1/0/0 on Router A. The configurations on Router B, Router C, Router D, and Router E are similar to those on Router A and are not mentioned here.

```
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] pim sm
[RouterA-GigabitEthernet2/0/0] quit
```

Enable IGMP on the interface through which Router A is connected to hosts.

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] igmp enable
[RouterA-GigabitEthernet1/0/0] igmp version 3
```

Configure a C-BSR and a C-RP. Set the service range of the RP on Router D and specify the locations of the C-BSR and the C-RP.

```
[RouterD] pim
[RouterD-pim] c-bsr gigabitethernet 1/0/0
[RouterD-pim] c-rp gigabitethernet 1/0/0
```

Run the **display multicast routing-table** command to view the multicast routing table of a router. The multicast routing table on Router C is as follows:

```
[RouterC] display multicast routing-table
Multicast routing table of VPN-Instance: public net
```

```
Total 1 entry
00001. (192.168.3.2, 224.31.31.31)
  Uptime: 15:03:04
  Upstream Interface: GigabitEthernet2/0/0
  List of 1 downstream interface
    1: GigabitEthernet1/0/0
```

Step 3 Configure an MPLS RSVP-TE tunnel.

Configure Router B.

```
[RouterB] mpls lsr-id 2.2.2.2
[RouterB] mpls
[RouterB-mpls] mpls te
[RouterB-mpls] mpls rsvp-te
[RouterB-mpls] mpls te cspf
[RouterB-mpls] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] mpls
[RouterB-GigabitEthernet2/0/0] mpls te
[RouterB-GigabitEthernet2/0/0] mpls rsvp-te
[RouterB-GigabitEthernet2/0/0] quit
[RouterB] isis 1
[RouterB-isis-1] cost-style wide
[RouterB-isis-1] traffic-eng level-2
[RouterB-isis-1] quit
```

Configure Router C.

```
[RouterC] mpls lsr-id 3.3.3.3
[RouterC] mpls
[RouterC-mpls] mpls te
[RouterC-mpls] mpls rsvp-te
[RouterC-mpls] mpls te cspf
[RouterC-mpls] quit
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] mpls
[RouterC-GigabitEthernet1/0/0] mpls te
[RouterC-GigabitEthernet1/0/0] mpls rsvp-te
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] mpls
[RouterC-GigabitEthernet2/0/0] mpls te
[RouterC-GigabitEthernet2/0/0] mpls rsvp-te
[RouterC-GigabitEthernet2/0/0] quit
[RouterC] isis 1
[RouterC-isis-1] cost-style wide
[RouterC-isis-1] traffic-eng level-2
[RouterC-isis-1] quit
```

Configure Router D.

```
[RouterD] mpls lsr-id 4.4.4.4
[RouterD] mpls
[RouterD-mpls] mpls te
[RouterD-mpls] mpls rsvp-te
[RouterD-mpls] mpls te cspf
[RouterD-mpls] quit
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] mpls
[RouterD-GigabitEthernet1/0/0] mpls te
[RouterD-GigabitEthernet1/0/0] mpls rsvp-te
[RouterD-GigabitEthernet1/0/0] quit
[RouterD] isis 1
[RouterD-isis-1] cost-style wide
[RouterD-isis-1] traffic-eng level-2
[RouterD-isis-1] quit
```

Configure an MPLS TE tunnel and enable IGP Shortcut.

Configure an MPLS TE tunnel on Router B and enable IGP Shortcut.

```
[RouterB] interface tunnel 1/0/0
[RouterB-Tunnel1/0/0] ip address unnumbered interface loopback 0
[RouterB-Tunnel1/0/0] tunnel-protocol mpls te
[RouterB-Tunnel1/0/0] destination 4.4.4.4
[RouterB-Tunnel1/0/0] mpls te tunnel-id 100
[RouterB-Tunnel1/0/0] mpls te commit
[RouterB-Tunnel1/0/0] mpls te igp shortcut isis
[RouterB-Tunnel1/0/0] mpls te igp metric relative -10
[RouterB-Tunnel1/0/0] isis enable 1
[RouterB-Tunnel1/0/0] mpls te commit
[RouterB-Tunnel1/0/0] quit
```

View the routing table on Router B. You can find that IGP Shortcut is enabled.

```
[RouterB] display isis route
          Route information for ISIS(1)
          -----
          ISIS(1) Level-2 Forwarding Table
          -----
          IPv4 Destination      IntCost      ExtCost      ExitInterface      NextHop      Flags
          -----
          3.3.3.3/32             10           NULL         GE2/0/0             10.0.1.1     A/-/-/-
          172.16.1.0/24          20           NULL         GE1/0/0             10.0.0.1     A/-/-/-
          2.2.2.2/32              0           NULL         Loop0                Direct       D/-/L/-
          192.168.3.0/24         25           NULL         Tun1/0/0             2.2.2.2     A/S/-/-
          5.5.5.5/32              15           NULL         Tun1/0/0             2.2.2.2     A/S/-/-
          10.0.0.0/24             10           NULL         GE1/0/0             Direct       D/-/L/-
          10.0.1.0/24             10           NULL         GE2/0/0             Direct       D/-/L/-
          4.4.4.4/32              5            NULL         Tun1/0/0             2.2.2.2     A/S/-/-
          10.0.2.0/24             15           NULL         Tun1/0/0             2.2.2.2     A/S/-/-
          10.0.3.0/24             15           NULL         Tun1/0/0             2.2.2.2     A/S/-/-
          Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                  U-Up/Down Bit Set
```

View the multicast routing table on Router C spanned by the TE tunnel.

```
[RouterC] display multicast routing-table
```

No multicast routing entry is displayed. This indicates that the multicast packet is discarded.

Step 4 Configure local MT.

Enable local MT on Router B.

```
[RouterB] isis
[RouterB-isis-1] local-mt enable
```

Step 5 Verify the configuration.

View the multicast routing table on Router C again. You can find that multicast routes are displayed.

```
[RouterC] display multicast routing-table
Multicast routing table of VPN-Instance: public net
Total 1 entry
00001. (192.168.3.2, 224.31.31.31)
    Uptime: 00:00:19
    Upstream Interface: GigabitEthernet2/0/0
    List of 1 downstream interface
        1: GigabitEthernet1/0/0
```

View the MIGP routing table on Router B.

```
[RouterB] display mign routing-table
Route Flags: R - relied, D - download to fib
-----
Routing Tables: MIGP
```

Destinations : 5				Routes : 5			
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface	
4.4.4.4/32	ISIS	15	20		10.0.1.1	GE2/0/0	
5.5.5.5/32	ISIS	15	30		10.0.1.1	GE2/0/0	
10.0.2.0/24	ISIS	15	20		10.0.1.1	GE2/0/0	
10.0.3.0/24	ISIS	15	30		10.0.1.1	GE2/0/0	
192.168.3.0/24	ISIS	15	40		10.0.1.1	GE2/0/0	

The physical outgoing interface of the next hop of the route with the previous outgoing interface being a TE tunnel interface is found in the MIGP routing table.

----End

Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
router id 1.1.1.1
#
multicast routing-enable
#
isis 1
is-level level-2
cost-style wide
network-entity 10.0000.0000.0001.00
#
interface GigabitEthernet2/0/0
ip address 10.0.0.1 255.255.255.0
isis enable 1
pim sm
#
interface GigabitEthernet1/0/0
ip address 172.16.1.1 255.255.255.0
isis enable 1
igmp enable
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
#
return
```

- Configuration file of Router B

```
#
sysname RouterB
#
router id 2.2.2.2
#
multicast routing-enable
#
mpls lsr-id 2.2.2.2
mpls
mpls te
mpls rsvp-te
mpls te cspf
#
isis 1
is-level level-2
cost-style wide
network-entity 10.0000.0000.0002.00
traffic-eng level-2
local-mt enable
#
interface GigabitEthernet1/0/0
ip address 10.0.0.2 255.255.255.0
isis enable 1
pim sm
```

```
#
interface GigabitEthernet2/0/0
 ip address 10.0.1.2 255.255.255.0
 isis enable 1
 pim sm
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
 pim sm
#
interface Tunnell1/0/0
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 4.4.4.4
 mpls te tunnel-id 100
 mpls te igp shortcut isis
 mpls te igp metric relative -10
 isis enable 1
 pim sm
#
pim
 C-BSR LoopBack0
 C-RP LoopBack0
#
return
```

● Configuration file of Router C

```
#
sysname RouterC
#
router id 3.3.3.3
#
multicast routing-enable
#
mpls lsr-id 3.3.3.3
mpls
 mpls te
 mpls rsvp-te
 mpls te cspf
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 10.0000.0000.0003.00
 traffic-eng level-2
#
interface GigabitEthernet1/0/0
 ip address 10.0.1.1 255.255.255.0
 isis enable 1
 pim sm
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 10.0.2.2 255.255.255.0
 isis enable 1
 pim sm
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
```


return

- Configuration file of Router D

```
#
sysname RouterD
#
router id 4.4.4.4
#
multicast routing-enable
#
mpls lsr-id 4.4.4.4
mpls
mpls te
mpls rsvp-te
mpls te cspf
#
isis 1
is-level level-2
cost-style wide
network-entity 10.0000.0000.0004.00
traffic-eng level-2
#
interface GigabitEthernet1/0/0
ip address 10.0.3.1 255.255.255.0
isis enable 1
pim sm
#
interface GigabitEthernet2/0/0
ip address 10.0.2.1 255.255.255.0
isis enable 1
pim sm
mpls
mpls te
mpls rsvp-te
#
interface LoopBack0
ip address 4.4.4.4 255.255.255.255
isis enable 1
pim sm
#
return
```

- Configuration file of Router E

```
#
sysname RouterE
#
router id 5.5.5.5
#
multicast routing-enable
#
isis 1
is-level level-2
cost-style wide
network-entity 10.0000.0000.0005.00
#
interface GigabitEthernet1/0/0
ip address 10.0.3.3 255.255.255.0
isis enable 1
pim sm
#
interface Ethernet2/0/0
ip address 192.168.3.1 255.255.255.0
isis enable 1
pim sm
#
interface LoopBack0
ip address 5.5.5.5 255.255.255.255
isis enable 1
pim sm
#
```

return

7.21.9 Example for Configuring Basic IS-IS IPv6 Functions

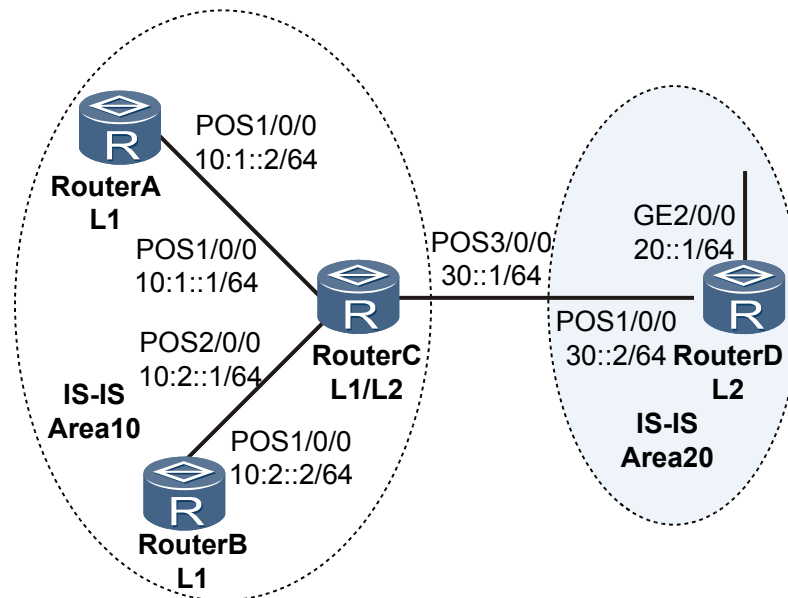
This part provides an example for interconnecting IPv6 networks through IS-IS.

Networking Requirements

As shown in [Figure 7-15](#):

- Router A, Router B, Router C, and Router D belong to the same AS. They are interconnected through IS-IS in the IPv6 network.
- Router A, Router B, and Router C belong to area 10. Router D belongs to area 20.
- Router A and Router B are Level-1 routers. Router C is a Level-1-2 router. Router D is a Level-2 router.

Figure 7-15 Networking diagram of basic IS-IS IPv6 feature



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the capability of IPv6 forwarding on each router.
2. Configure an IPv6 address for each interface.
3. Enable IS-IS on each router.
4. Configure the level.
5. Specify the network entity.

Data Preparation

To complete the configuration, you need the following data:

- IPv6 address of each interface on Router A, Router B, Router C, and Router D
- Area numbers of Router A, Router B, Router C, and Router D
- Levels of Router A, Router B, Router C, and Router D

Procedure

Step 1 Enable the capability of IPv6 forwarding, and configure IPv6 address for each interface. Take the display on Router A as an example. The configurations of Router B, Router C and Router D are similar to that of Router A. The detailed configurations are not mentioned here.

```
<HUAWEI> system-view
[HUAWEI] sysname RouterA
[RouterA] ipv6
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] ipv6 enable
[RouterA-Pos1/0/0] ipv6 address 10:1::2/64
```

Step 2 Configure IS-IS.

Configure Router A.

```
[RouterA] isis 1
[RouterA-isis-1] is-level level-1
[RouterA-isis-1] network-entity 10.0000.0000.0001.00
[RouterA-isis-1] ipv6 enable
[RouterA-isis-1] quit
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] isis ipv6 enable 1
[RouterA-Pos1/0/0] quit
```

Configure Router B.

```
[RouterB] isis 1
[RouterB-isis-1] is-level level-1
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] ipv6 enable
[RouterB-isis-1] quit
[RouterB] interface pos 1/0/0
[RouterB-Pos1/0/0] isis ipv6 enable 1
[RouterB-Pos1/0/0] quit
```

Configure Router C.

```
[RouterC] isis 1
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] ipv6 enable
[RouterC-isis-1] quit
[RouterC] interface pos 1/0/0
[RouterC-Pos1/0/0] isis ipv6 enable 1
[RouterC-Pos1/0/0] quit
[RouterC] interface pos 2/0/0
[RouterC-Pos2/0/0] isis ipv6 enable 1
[RouterC-Pos2/0/0] quit
[RouterC] interface pos 3/0/0
[RouterC-Pos3/0/0] isis ipv6 enable 1
[RouterC-Pos3/0/0] isis circuit-level level-2
[RouterC-Pos3/0/0] quit
```

Configure Router D.

```
[RouterD] isis 1
[RouterD-isis-1] is-level level-2
[RouterD-isis-1] network-entity 20.0000.0000.0004.00
[RouterD-isis-1] ipv6 enable
[RouterD-isis-1] quit
[RouterD] interface pos 1/0/0
[RouterD-Pos1/0/0] isis ipv6 enable 1
```

```
[RouterD-Pos1/0/0] quit
[RouterD] interface gigabitethernet 2/0/0
[RouterD-GigabitEthernet2/0/0] isis ipv6 enable 1
[RouterD-GigabitEthernet2/0/0] quit
```

Step 3 Verify the configuration.

Display the IS-IS routing table of Router A.

```
[RouterA] display isis route
                Route information for ISIS(1)
                -----
                ISIS(1) Level-1 Forwarding Table
                -----
IPV6 Dest.      ExitInterface  NextHop          Cost           Flags
-----
::/0           Pos1/0/0       FE80::A83E:0:3ED2:1  10             A/-/-
10:1::/64      Pos1/0/0       Direct           10             D/L/-
10:2::/64      Pos1/0/0       FE80::A83E:0:3ED2:1  20             A/-/-
                Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
```

Display the IS-IS neighbors of Router C.

```
[RouterC] display isis peer verbose
                Peer information for ISIS(1)
                -----
System Id      Interface      Circuit Id      State HoldTime Type  PRI
-----
0000.0000.0001 Pos1/0/0      00000000001    Up    24s    L1    --
MT IDs supported : 0 (UP)
Area Address(es) : 10
Peer IPv6 Address(es): FE80::996B:0:9419:1
Uptime          : 00:44:43
Adj Protocol    : IPV6
0000.0000.0002 Pos2/0/0      00000000001    Up    28s    L1    --
MT IDs supported : 0 (UP)
Area Address(es) : 10
Peer IPv6 Address(es): FE80::DC40:0:47A9:1
Uptime          : 00:46:13
Adj Protocol    : IPV6
0000.0000.0004 Pos3/0/0      00000000001    Up    24s    L2    --
MT IDs supported : 0 (UP)
Area Address(es) : 20
Peer IPv6 Address(es): FE80::F81D:0:1E24:2
Uptime          : 00:53:18
Adj Protocol    : IPV6
Total Peer(s): 3
```

Display the IS-IS LSDB of Router C.

```
[RouterC] display isis lsdb verbose
                Database information for ISIS(1)
                -----
                Level-1 Link State Database
LSPID          Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-----
0000.0000.0001.00-00 0x0000000c  0x4e06        1117          113    0/0/0
SOURCE        0000.0000.0001.00
NLPID         IPV6
AREA ADDR     10
INTF ADDR V6 10:1::2
Topology      Standard
NBR ID        0000.0000.0003.00 COST: 10
IPV6          10:1::/64    COST: 10
0000.0000.0002.00-00 0x00000009  0x738c        1022          83    0/0/0
SOURCE        0000.0000.0002.00
NLPID         IPV6
AREA ADDR     10
INTF ADDR V6 10:2::2
Topology      Standard
NBR ID        0000.0000.0003.00 COST: 10
```

```

    IPV6          10:2::/64                                COST: 10
0000.0000.0003.00-00* 0x00000020 0x6b10                771          140      1/0/0
SOURCE          0000.0000.0003.00
NLPID           IPV6
AREA ADDR       10
INTF ADDR V6    30::1
INTF ADDR V6    10:2::1
INTF ADDR V6    10:1::1
Topology        Standard
NBR ID          0000.0000.0002.00 COST: 10
NBR ID          0000.0000.0001.00 COST: 10
IPV6            10:2::/64                                COST: 10
IPV6            10:1::/64                                COST: 10

```

Level-2 Link State Database					
LSPID	Seq Num	Checksum	Holdtime	Length	ATT/P/OL
0000.0000.0003.00-00*	0x00000017	0x61b4	771	157	0/0/0

SOURCE	0000.0000.0003.00				
NLPID	IPV6				
AREA ADDR	10				
INTF ADDR V6	30::1				
INTF ADDR V6	10:2::1				
INTF ADDR V6	10:1::1				
Topology	Standard				
NBR ID	0000.0000.0004.00	COST: 10			
IPV6	30::/64		COST: 10		
IPV6	10:2::/64		COST: 10		
IPV6	10:1::/64		COST: 10		
0000.0000.0004.00-00	0x0000000b	0x6dfa	1024	124	0/0/0
SOURCE	0000.0000.0004.00				
NLPID	IPV6				
AREA ADDR	20				
INTF ADDR V6	30::2				
INTF ADDR V6	20::1				
Topology	Standard				
NBR ID	0000.0000.0003.00	COST: 10			
NBR ID	0000.0000.0005.00	COST: 10			
IPV6	30::/64		COST: 10		
IPV6	20::/64		COST: 10		

---End

Configuration Files

- Configuration file of Router A

```

#
 sysname RouterA
#
 ipv6
#
 isis 1
  is-level level-1
  network-entity 10.0000.0000.0001.00
#
 ipv6 enable topology standard
#
 interface Pos1/0/0
  link-protocol ppp
  ipv6 enable
  ipv6 address 10:1::2/64
  isis ipv6 enable 1
#
 return

```

- Configuration file of Router B

```

#
 sysname RouterB
#

```

```
        ipv6
        #
        isis 1
            is-level level-1
            network-entity 10.0000.0000.0002.00
        #
            ipv6 enable topology standard
        #
        interface Pos1/0/0
            link-protocol ppp
            ipv6 enable
            ipv6 address 10:2::2/64
            isis ipv6 enable 1
        #
        return
```

- Configuration file of Router C

```
#
sysname RouterC
#
ipv6
#
isis 1
    network-entity 10.0000.0000.0003.00
#
    ipv6 enable topology standard
#
interface Pos1/0/0
    link-protocol ppp
    ipv6 enable
    ipv6 address 10:1::1/64
    isis ipv6 enable 1
#
interface Pos2/0/0
    link-protocol ppp
    ipv6 enable
    ipv6 address 10:2::1/64
    isis ipv6 enable 1
#
interface Pos3/0/0
    link-protocol ppp
    ipv6 enable
    ipv6 address 30::1/64
    isis ipv6 enable 1
    isis circuit-level level-2
#
return
```

- Configuration file of Router D

```
#
sysname RouterD
#
ipv6
#
isis 1
    is-level level-2
    network-entity 20.0000.0000.0004.00
#
    ipv6 enable topology standard
#
interface GigabitEthernet2/0/0
    ipv6 enable
    ipv6 address 20::1/64
    isis ipv6 enable 1
#
interface Pos1/0/0
    link-protocol ppp
    ipv6 enable
    ipv6 address 30::2/64
    isis ipv6 enable 1
```

```
#
return
```

7.21.10 Example for Configuring IS-IS Auto FRR (IP protecting IP)

This part provides an example for fast switching services to the backup link in the case of IS-IS link failures through IS-IS Auto FRR (IP protecting IP).

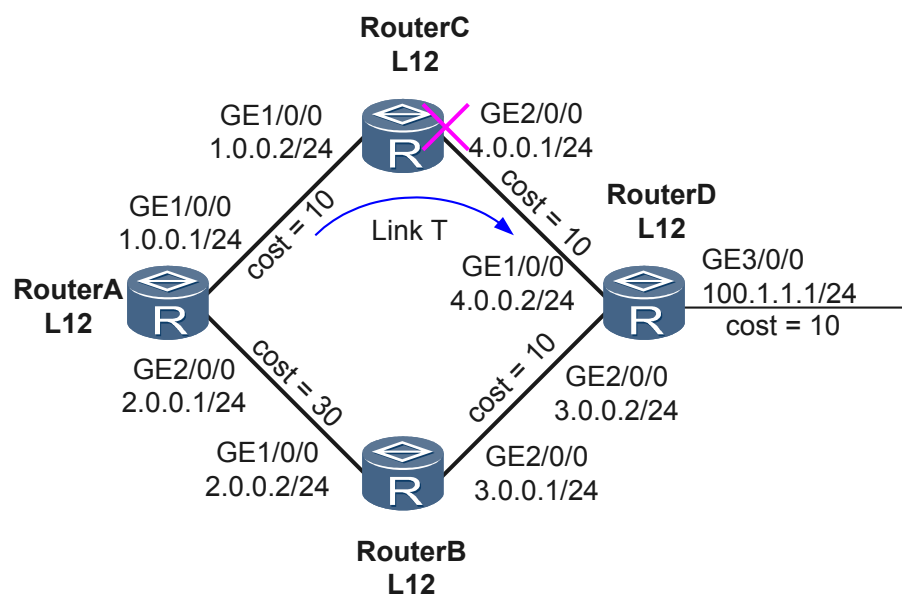
Networking Requirements

When a fault occurs on a network, IS-IS Auto FRR fast switches traffic to a backup link before the route convergence. This prevents traffic interruption.

In **Figure 7-16**:

- IS-IS runs between four routers.
- The four routers are all Level-1-2 routers.
- If Router C or Link T fails, it is required that the traffic forwarded by Router A is rapidly switched to the backup link.

Figure 7-16 Networking diagram of configuring IS-IS Auto FRR



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic IS-IS functions on each router.
2. Set a larger link cost (in compliance with the traffic protection inequality of IS-IS Auto FRR) on GE 2/0/0 of Router A, and ensure that Link T is preferentially selected.
3. Enable IS-IS Auto FRR on Router A that forwards the protected traffic.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses of interfaces on each router
- NET of each router
- Level of each router
- Costs of interfaces on each router

Procedure

Step 1 Configure IP addresses for interfaces. The details are omitted.

Step 2 Configure basic IS-IS functions.

Configure Router A.

```
[RouterA] isis 1
[RouterA-isis-1] is-level level-1-2
[RouterA-isis-1] network-entity 10.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] isis enable 1
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] isis enable 1
[RouterA-GigabitEthernet2/0/0] quit
```

Configure Router B.

```
[RouterB] isis 1
[RouterB-isis-1] is-level level-1-2
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] isis enable 1
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] isis enable 1
[RouterB-GigabitEthernet2/0/0] quit
```

Configure Router C.

```
[RouterC] isis 1
[RouterC-isis-1] is-level level-1-2
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] isis enable 1
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] isis enable 1
[RouterC-GigabitEthernet2/0/0] quit
```

Configure Router D.

```
[RouterD] isis 1
[RouterD-isis-1] is-level level-1-2
[RouterD-isis-1] network-entity 10.0000.0000.0004.00
[RouterD-isis-1] quit
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] isis enable 1
[RouterD-GigabitEthernet1/0/0] quit
[RouterD] interface gigabitethernet 2/0/0
[RouterD-GigabitEthernet2/0/0] isis enable 1
```



```
[RouterD-GigabitEthernet2/0/0] quit
```

Step 3 Set the cost of Gigabit Ethernet 2/0/0 on RouterA to 30, and then check routing information.

Configure the cost of GE 2/0/0 on Router A to 30.

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] isis cost 30
[RouterA-GigabitEthernet2/0/0] quit
```

Check information about the link from Router A to Router D. Link T has a lower cost, and thereby IS-IS optimally selects Link T to send traffic that is forwarded by Router A.

```
<RouterA> display isis route 100.1.1.1 verbose
```

```
Route information for ISIS(1)
-----

ISIS(1) Level-1 Forwarding Table
-----

IPV4 Dest  : 100.1.1.0/24      Int. Cost : 30          Ext. Cost : NULL
Admin Tag  : -                Src Count  : 1          Flags     : A/-/L/-
Priority    : Low
NextHop    :                  Interface   :                ExitIndex  :
                1.0.0.2                GE1/0/0                0x00000003

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
      U-Up/Down Bit Set
```

```
ISIS(1) Level-2 Forwarding Table
-----

IPV4 Dest  : 100.1.1.0/24      Int. Cost : 30          Ext. Cost : NULL
Admin Tag  : -                Src Count  : 3          Flags     : -/-/-/-
Priority    : Low

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
      U-Up/Down Bit Set
```

Run the **display fib 100.1.1.1 verbose** command on Router A to check the forwarding entry from Router A to Router D.

```
<RouterA> display fib 100.1.1.1 verbose
```

```
Route Entry Count: 1
Destination: 100.1.1.0      Mask      : 255.255.255.0
NextHop   : 1.0.0.2      OutIf    : GigabitEthernet1/0/0
LocalAddr   : 1.0.0.1      LocalMask : 0.0.0.0
Flags       : DGU         Age       : 26sec
ATIndex     : 0           Slot      : 0
LspFwdFlag  : 0           LspToken  : 0x0
InLabel     : NULL        OriginAs  : 0
BGPNextHop  : 0.0.0.0     PeerAs    : 0
QosInfo     : 0x0         OriginQos : 0x0
NextHopBak  : 0.0.0.0     OutIfBak  : [No Intf]
LspTokenBak : 0x0         InLabelBak : NULL
LspToken_ForInLabelBak : 0x0
EntryRefCount : 0
rt_ulVlanId : 0x0
LspType     : 0           Label_ForLspTokenBak : 0
MplsMtu     : 0           Gateway_ForLspTokenBak : 0
NextToken   : 0           IfIndex_ForLspTokenBak : 0
Label_NextToken : 0       Label      : 0
LspBfdState : 0
```

As shown in the command output, the traffic from Router A to Router D is only forwarded through Link T.

Step 4 Enable IS-IS Auto FRR on Router A, and then check the routing information.

Enable IS-IS Auto FRR on Router A.

```
<RouterA> isis
[RouterA-isis-1] frr
[RouterA-isis-1-frr] loop-free-alternate
```

Check information about the link from Router A to Router D. You can find that IS-IS creates a backup link because IS-IS Auto FRR is enabled.

```
<RouterA> display isis route 100.1.1.1 verbose
```

```
Route information for ISIS(1)
-----

ISIS(1) Level-1 Forwarding Table
-----

IPv4 Dest   : 100.1.1.0/24      Int. Cost : 30           Ext. Cost : NULL
Admin Tag   : -             Src Count  : 1           Flags     : A/-/L/-
Priority    : Low
NextHop     :              Interface   :              ExitIndex  :
  1.0.0.2   :              GE1/0/0     :              0x00000003
  (B) 2.0.0.2 :              GE2/0/0     :              0x00000004

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
      U-Up/Down Bit Set
```

```
ISIS(1) Level-2 Forwarding Table
-----

IPv4 Dest   : 100.1.1.0/24      Int. Cost : 30           Ext. Cost : NULL
Admin Tag   : -             Src Count  : 3           Flags     : -/-/-/-
Priority    : Low

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
      U-Up/Down Bit Set
```

Check the protection type for the traffic from Router A to Router D.

```
<RouterA> display isis spf-tree systemid 0000.0000.0004 verbose
```

```
Shortest Path Tree for ISIS(1)
-----

ISIS(1) Level-1 Shortest Path Tree
-----

0000.0000.0004.00
  Distance           : 20
  Distance-URT       : 20
  Flags              : SPT/V6_Islt
  IPv4 Nexthops-URT  : 1
    (1) 1.0.0.2      IF:GE1/0/0 NBR:0000.0000.0003.00
    (B) 2.0.0.2      IF:GE2/0/0 NBR:0000.0000.0002.00
                     TYPE:LOOP-FREE PROTECT:LINK-NODE
  IPv4 Nexthops-MIGP : 0
  IPv6 Nexthops      : 0
  Neighbors: 2 (Children:1 Parents:1 Others:0)
    (1) 0000.0000.0003.02
        Cost : 10
        Flags : Parent
    (2) 0000.0000.0004.03
```

```

Cost : 10
Flags : Child

ISIS(1) Level-2 Shortest Path Tree
-----
0000.0000.0004.00
  Distance : 20
  Distance-URT : 20
  Flags : SPT/V6_Islt
  IPv4 Nexthops-URT : 1
    (1) 1.0.0.2 IF:GE1/0/0 NBR:0000.0000.0003.00
    (B) 2.0.0.2 IF:GE2/0/0 NBR:0000.0000.0002.00
      TYPE:LOOP-FREE PROTECT:LINK-NODE
  IPv4 Nexthops-MIGP : 0
  IPv6 Nexthops : 0
  Neighbors: 2 (Children:1 Parents:1 Others:0)
    (1) 0000.0000.0003.02
      Cost : 10
      Flags : Parent
    (2) 0000.0000.0004.03
      Cost : 10
      Flags : Child
    
```

As shown in the preceding command output, link-node dual protection is enabled from Router A to Router D.

Run the **display fib 100.1.1.1 verbose** command on Router A to check the backup forwarding entry from Router A to Router D.

```

<RouterA> display fib 100.1.1.1 verbose
  Route Entry Count: 1
  Destination: 100.1.1.0      Mask : 255.255.255.0
  Nexthop : 1.0.0.2          OutIf : GigabitEthernet1/0/0
  LocalAddr : 1.0.0.1        LocalMask: 0.0.0.0
  Flags : DGU                Age : 6sec
  ATIndex : 0                Slot : 0
  LspFwdFlag : 0             LspToken : 0x0
  InLabel : NULL             OriginAs : 0
  BGPNextHop : 0.0.0.0       PeerAs : 0
  QosInfo : 0x0              OriginQos: 0x0
  NexthopBak : 2.0.0.2       OutIfBak : GigabitEthernet2/0/0
  LspTokenBak: 0x0           InLabelBak : NULL
  LspToken_ForInLabelBak : 0x0
  EntryRefCount : 0
  rt_ulVlanId : 0x0
  LspType : 0                Label_ForLspTokenBak : 0
  MplsMtu : 0                Gateway_ForLspTokenBak : 0
  NextToken : 0              IfIndex_ForLspTokenBak : 0
  Label_NextToken : 0        Label : 0
  LspBfdState : 0
    
```

As shown in the command output, the master link from Router A to Router D is Link T, the relevant backup link follows the route with GE 2/0/0 as the outbound interface and 2.0.0.2 as the next hop.

Step 5 Verify the configuration.

Run the **shutdown** command on GE 2/0/0 of Router C to make the link down.

```

[RouterC] interface gigabitethernet 2/0/0
[RouterC-GigabitEthernet2/0/0] shutdown
    
```

Run the **display fib 100.1.1.1 verbose** command immediately on Router A to check information about the route from Router A to Router D.

```
<RouterA> display fib 100.1.1.1 verbose
Route Entry Count: 1
Destination: 100.1.1.0          Mask      : 255.255.255.0
NextHop      : 2.0.0.2          OutIf     : GigabitEthernet2/0/0
LocalAddr    : 2.0.0.1          LocalMask : 0.0.0.0
Flags        : DGU              Age        : 124sec
ATIndex      : 0                Slot       : 0
LspFwdFlag   : 0                LspToken   : 0x0
InLabel      : NULL             OriginAs   : 0
BGPNextHop   : 0.0.0.0          PeerAs     : 0
QosInfo      : 0x0              OriginQos  : 0x0
NextHopBak   : 0.0.0.0          OutIfBak   : [No Intf]
LspTokenBak  : 0x0              InLabelBak : NULL
LspToken_ForInLabelBak : 0x0
EntryRefCount : 0
rt_ulVlanId  : 0x0
LspType      : 0                Label_ForLspTokenBak : 0
MplsMtu      : 0                Gateway_ForLspTokenBak : 0
NextToken    : 0                IfIndex_ForLspTokenBak : 0
Label_NextToken : 0              Label      : 0
LspBfdState  : 0
```

As shown in the command output, the traffic forwarded by the Router A is switched to the backup link, with GE 2/0/0 as the outbound interface and 2.0.0.2 as the next hop.

 **NOTE**

If a fault occurs on the network, IS-IS Auto FRR ensures the fast switchover of the traffic to the backup link before the network convergence, and consequently protects traffic.

----End

Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
isis 1
frr
loop-free-alternate level-1
loop-free-alternate level-2
network-entity 10.0000.0000.0001.00
#
interface gigabitethernet 1/0/0
ip address 1.0.0.1 255.255.255.0
isis enable 1
#
interface gigabitethernet 2/0/0
ip address 2.0.0.1 255.255.255.0
isis enable 1
isis cost 30
#
return
```

- Configuration file of Router B

```
#
sysname RouterB
#
isis 1
network-entity 10.0000.0000.0002.00
#
interface gigabitethernet 1/0/0
ip address 2.0.0.2 255.255.255.0
isis enable 1
#
interface gigabitethernet 2/0/0
```

```
    ip address 3.0.0.1 255.255.255.0
    isis enable 1
#
return
```

- Configuration file of Router C

```
#
sysname RouterC
#
isis 1
network-entity 10.0000.0000.0003.00
#
interface gigabitethernet 1/0/0
ip address 1.0.0.2 255.255.255.0
isis enable 1
#
interface gigabitethernet 2/0/0
shutdown
ip address 4.0.0.1 255.255.255.0
isis enable 1
#
return
```

- Configuration file of Router D

```
#
sysname RouterD
#
isis 1
network-entity 10.0000.0000.0004.00
#
interface gigabitethernet 1/0/0
ip address 4.0.0.2 255.255.255.0
isis enable 1
#
interface gigabitethernet 2/0/0
ip address 3.0.0.2 255.255.255.0
isis enable 1
#
interface gigabitethernet 3/0/0
ip address 100.1.1.1 255.255.255.0
isis enable 1
#
return
```

7.21.11 Example for Configuring IS-IS Auto FRR (TE protecting IP)

This part provides an example for fast switching services to the backup link in the case of IS-IS link failures through IS-IS Auto FRR (TE protecting IP).

Networking Requirements

Figure 7-17 Networking diagram of configuring IS-IS Auto FRR

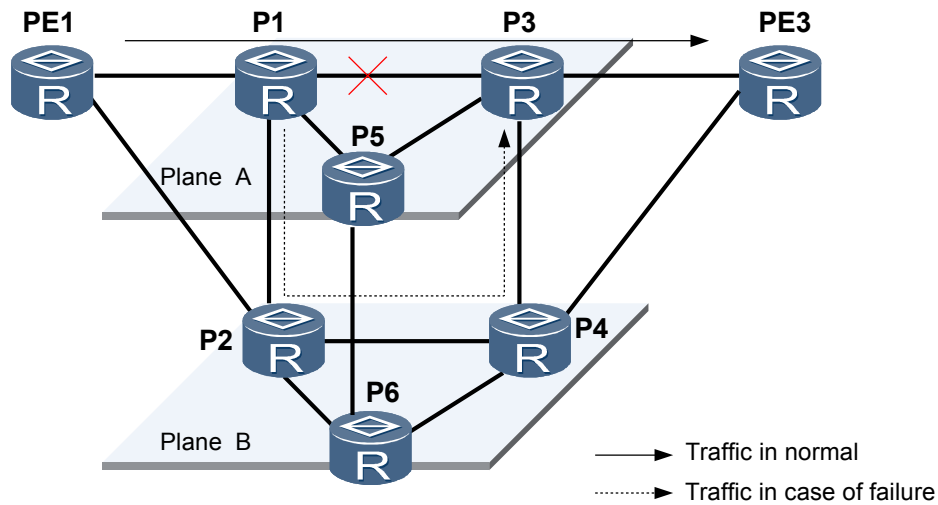


Figure 7-17 is the simplified networking diagram of MPLS VPN double planes, and PEs are dual-homed to the two planes. It is required that:

- IS-IS should be configured to implement IP connectivity between nodes.
- Traffic between P nodes at the core layer should be transmitted through the direct link when no link fault occurs.
- The MPLS TE tunnel should be configured as the backup path so that traffic between P nodes can be switched to the other plane when the link between P nodes fails.
- IS-IS Auto FRR should be configured so that service traffic between P nodes can be rapidly switched to the TE tunnel when the direct link fails.
- Traffic between P nodes should be transmitted only between the P nodes at the core layer to prevent traffic between P nodes from going back to PE nodes.

NOTE

In this configuration example, PE1 and PE3 are used for illustration, only three P nodes of each plane at the core layer are illustrated, and only the MPLS TE tunnel between P1 and P3 is illustrated. In practice, there are far more PE nodes, P nodes, and MPLS TE tunnels.

Configuration Roadmap

The configuration roadmap is as follows:

1. Assign IP addresses to interfaces on each node, configure the loopback addresses that are used as LSR IDs, and configure IS-IS to implement IP connectivity.
2. Configure an MPLS TE tunnel between P nodes as the backup path in Loop-Free Alternate (LFA) calculation.
3. Enable forwarding adjacency and configure LDP over TE.
4. Enable IS-IS Auto FRR so that traffic can be rapidly switched in the case of a link fault.

- Run the **undo isis lfa-backup** command on the interfaces that connect P nodes to PE nodes to disable these interfaces from becoming the backup interfaces in LFA calculation and prevent traffic between P nodes from going back to PE nodes.

Data Preparation

To complete the configuration, you need the following data.

Table 7-2 IP addresses of physical interfaces

Device Name	Interface and IP Address	Remote IP Address	Remote Device
P1	GE 1/0/0 10.1.1.1/30	GE 1/0/0 10.1.1.2/30	P2
P1	GE 2/0/0 10.1.2.1/30	GE 2/0/0 10.1.2.2/30	P3
P1	GE 3/0/0 10.1.3.1/30	GE 2/0/0 10.1.3.2/30	P5
P2	GE 2/0/0 10.1.4.1/30	GE 2/0/0 10.1.4.2/30	P4
P2	GE 3/0/0 10.1.5.1/30	GE 2/0/0 10.1.5.2/30	P6
P3	GE 1/0/0 10.1.6.1/30	GE 1/0/0 10.1.6.2/30	P4
P3	GE 3/0/0 10.1.7.1/30	GE 3/0/0 10.1.7.2/30	P5
P4	GE 3/0/0 10.1.8.1/30	GE 3/0/0 10.1.8.2/30	P6
P5	GE 1/0/0 10.1.9.1/30	GE 1/0/0 10.1.9.2/30	P6
PE1	GE 1/0/0 10.1.10.1/30	GE 3/1/0 10.1.10.2/30	P1
PE1	GE 2/0/0 10.1.11.1/30	GE 3/1/0 10.1.11.2/30	P2
PE3	GE 1/0/0 10.1.12.1/30	GE 3/1/0 10.1.12.2/30	P3
PE3	GE 2/0/0 10.1.13.1/30	GE 3/1/0 10.1.13.2/30	P4

Table 7-3 IP address of Loopback 0

Device Name	IP Address of Loopback 0
P1	1.1.1.1/32
P2	2.2.2.2/32
P3	3.3.3.3/32
P4	4.4.4.4/32
P5	5.5.5.5/32
P6	6.6.6.6/32
PE1	7.7.7.7/32
PE3	8.8.8.8/32

Table 7-4 IS-IS parameters

Parameter	Value
Router ID	IP address of Loopback 0
IS-IS process ID	64
Level	2
NET	In the format of Area-ID.System-ID.00 <ul style="list-style-type: none"> ● Area-ID: 86.0010 ● System-ID: is based on the expansion of the IP address of Loopback 0. For example, if the IP address of Loopback 0 is 1.1.1.1, the system ID becomes 0010.0100.1001.
IS-IS name	Same as the device name
Metric type	Wide
Metric value	Physical interface: 5 Tunnel interface: 6
Other parameters	Default values

Table 7-5 MPLS parameter

Parameter	Value
LSR ID	IP address of Loopback 0

Parameter	Value
Tunnel interface number	Number of the physical outbound interface of the tunnel
Tunnel interface description	to_destination node
Tunnel interface address	IP address of Loopback 0
Tunnel ID	100
Name of the explicit path	Tunnel description
Tunnel metric value	Smaller than the metric value of the primary path and greater than the metric values of other paths so that the tunnel can become the backup path and LDP over TE can be implemented
Tunnel bandwidth	200 Mbit/s
Name of the LDP peer	to_destination node
Other parameters	Default values

Procedure

Step 1 Configure IP addresses for interfaces.

Configure the IP address and mask for each interface according to [Table 7-2](#) and [Table 7-3](#). The configuration details are not mentioned here.

Step 2 Configure IS-IS.

Configure IS-IS on all the PE and P nodes, and configure P1 and PE1. The configurations of other nodes are similar to the configurations of P1 and PE1 and thus are not mentioned here.

Configure P1.

```
[P1] router id 1.1.1.1
[P1] isis 64
[P1-isis-64] network-entity 86.0010.0010.0100.1001.00
[P1-isis-64] is-level level-2
[P1-isis-64] cost-style wide
[P1-isis-64] is-name P1
[P1-isis-64] quit
[P1] interface loopback 0
[P1-LoopBack0] isis enable 64
[P1-LoopBack0] quit
[P1] interface gigabitethernet 1/0/0
[P1-GigabitEthernet1/0/0] isis enable 64
[P1-GigabitEthernet1/0/0] isis cost 5
[P1-GigabitEthernet1/0/0] quit
[P1] interface gigabitethernet 2/0/0
[P1-GigabitEthernet2/0/0] isis enable 64
[P1-GigabitEthernet2/0/0] isis cost 5
[P1-GigabitEthernet2/0/0] quit
[P1] interface gigabitethernet 3/0/0
[P1-GigabitEthernet3/0/0] isis enable 64
[P1-GigabitEthernet3/0/0] isis cost 5
[P1-GigabitEthernet3/0/0] quit
```

```
[P1] interface gigabitethernet 3/1/0
[P1-GigabitEthernet3/1/0] isis enable 64
[P1-GigabitEthernet3/1/0] isis cost 5
[P1-GigabitEthernet3/1/0] quit

# Configure PE1.

[PE1] router id 7.7.7.7
[PE1] isis 64
[PE1-isis-64] network-entity 86.0010.0070.0700.7007.00
[PE1-isis-64] is-level level-2
[PE1-isis-64] cost-style wide
[PE1-isis-64] is-name PE1
[PE1-isis-64] quit
[PE1] interface loopback 0
[PE1-LoopBack0] isis enable 64
[PE1-LoopBack0] quit
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] isis enable 64
[PE1-GigabitEthernet1/0/0] isis cost 5
[PE1-GigabitEthernet1/0/0] quit
[PE1] interface gigabitethernet 2/0/0
[PE1-GigabitEthernet2/0/0] isis enable 64
[PE1-GigabitEthernet2/0/0] isis cost 5
[PE1-GigabitEthernet2/0/0] quit
```

After the preceding configurations, run the **display ip routing-table** command on each node. The command output shows that the nodes have learned routes from each other. For example, when checking whether there are routes to the IP address of Loopback 0 on PE1, you can find the following information:

```
[PE1] display ip routing-table 1.1.1.1 32
Route Flags: R - relay, D - download to fib
-----
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto  Pre  Cost           Flags NextHop           Interface
-----
          1.1.1.1/32  ISIS   15   5              D   10.1.10.2             GigabitEthernet1/0/0
```

Step 3 Configure an MPLS TE tunnel.

Enable MPLS, MPLS TE, and RSVP-TE on the interfaces of P1, P2, P3, and P4, and enable CSPF on the ingress of the tunnel.

Configure P1 and P2. The configuration of P3 is similar to that of P1, and the configuration of P4 is similar to that of P2.

Configure P1.

```
[P1] mpls lsr-id 1.1.1.1
[P1] mpls
[P1-mpls] mpls te
[P1-mpls] mpls rsvp-te
[P1-mpls] mpls te cspf
[P1-mpls] quit
[P1] interface gigabitethernet 1/0/0
[P1-GigabitEthernet1/0/0] mpls
[P1-GigabitEthernet1/0/0] mpls te
[P1-GigabitEthernet1/0/0] mpls rsvp-te
[P1-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 200000
[P1-GigabitEthernet1/0/0] mpls te bandwidth bc0 200000
[P1-GigabitEthernet1/0/0] quit
```

Configure P2.

```
[P2] mpls lsr-id 2.2.2.2
[P2] mpls
```

```
[P2-mpls] mpls te
[P2-mpls] mpls rsvp-te
[P2-mpls] quit
[P2] interface gigabitethernet 1/0/0
[P2-GigabitEthernet1/0/0] mpls
[P2-GigabitEthernet1/0/0] mpls te
[P2-GigabitEthernet1/0/0] mpls rsvp-te
[P2-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 200000
[P2-GigabitEthernet1/0/0] mpls te bandwidth bc0 200000
[P2-GigabitEthernet1/0/0] quit
[P2] interface gigabitethernet 2/0/0
[P2-GigabitEthernet2/0/0] mpls
[P2-GigabitEthernet2/0/0] mpls te
[P2-GigabitEthernet2/0/0] mpls rsvp-te
[P2-GigabitEthernet2/0/0] mpls te bandwidth max-reservable-bandwidth 200000
[P2-GigabitEthernet2/0/0] mpls te bandwidth bc0 200000
[P2-GigabitEthernet2/0/0] quit
```

On P1, configure an explicit path for the TE tunnel. The configuration of P3 is similar to that of P1 and is not mentioned here.

```
[P1] explicit-path to_p3
[P1-explicit-path-to_p3] next hop 10.1.1.2
[P1-explicit-path-to_p3] next hop 10.1.4.2
[P1-explicit-path-to_p3] next hop 10.1.6.1
[P1-explicit-path-to_p3] next hop 3.3.3.3
[P1-explicit-path-to_p3] quit
```

Configure a tunnel interface on P1. The configuration of P3 is similar to that of P1 and is not mentioned here.

```
[P1] interface Tunnel1/0/0
[P1-Tunnel1/0/0] to_p3
[P1-Tunnel1/0/0] ip address unnumbered interface LoopBack0
[P1-Tunnel1/0/0] tunnel-protocol mpls te
[P1-Tunnel1/0/0] destination 3.3.3.3
[P1-Tunnel1/0/0] mpls te tunnel-id 100
[P1-Tunnel1/0/0] mpls te bandwidth ct0 200000
[P1-Tunnel1/0/0] mpls te path explicit-path to_p3
[P1-Tunnel1/0/0] mpls te commit
```

After the preceding configurations, run the **display interface tunnel 1/0/0** command on P1 and P3. The command output shows that the status of the tunnel interface is Up.

```
[P1] display interface tunnel 1/0/0
Tunnel1/0/0 current state : UP
Line protocol current state : UP
Last up time: 2009-09-29, 16:35:10
Description : to_p3
```

Step 4 Configure LDP over TE.

Enable MPLS LDP, and configure PE1, P1, P3, and P5. The configurations of other nodes are similar to the configurations of PE1, P1, P3, and P5 and thus are not mentioned here.

Configure PE1.

```
[PE1] mpls lsr-id 7.7.7.7
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] mpls
[PE1-GigabitEthernet1/0/0] mpls ldp
[PE1-GigabitEthernet1/0/0] quit
```

Configure P1.

```
[P1] mpls ldp
[P1] interface gigabitethernet 2/0/0
[P1-GigabitEthernet2/0/0] mpls ldp
[P1-GigabitEthernet2/0/0] quit
[P1] interface gigabitethernet 3/0/0
[P1-GigabitEthernet3/0/0] mpls ldp
[P1-GigabitEthernet3/0/0] quit
[P1] interface gigabitethernet 3/1/0
[P1-GigabitEthernet3/1/0] mpls ldp
[P1-GigabitEthernet3/1/0] quit
[P1] mpls ldp remote-peer to_P3
[P1-mpls-ldp-remote-to_P3] remote-ip 3.3.3.3
[P1-mpls-ldp-remote-to_P3] quit
```

Configure P3.

```
[P3] mpls ldp
[P3] interface gigabitethernet 2/0/0
[P3-GigabitEthernet2/0/0] mpls ldp
[P3-GigabitEthernet2/0/0] quit
[P3] interface gigabitethernet 3/0/0
[P3-GigabitEthernet3/0/0] mpls ldp
[P3-GigabitEthernet3/0/0] quit
[P3] interface gigabitethernet 3/1/0
[P3-GigabitEthernet3/1/0] mpls ldp
[P3-GigabitEthernet3/1/0] quit
[P3] mpls ldp remote-peer to_P1
[P3-mpls-ldp-remote-to_P1] remote-ip 1.1.1.1
[P3-mpls-ldp-remote-to_P1] quit
```

Configure P5.

```
[P5] mpls lsr-id 5.5.5.5
[P5] mpls
[P5-mpls] quit
[P5] mpls ldp
[P5-mpls-ldp] quit
[P5] interface gigabitethernet 2/0/0
[P5-GigabitEthernet2/0/0] mpls
[P5-GigabitEthernet2/0/0] mpls ldp
[P5-GigabitEthernet2/0/0] quit
[P5] interface gigabitethernet 3/0/0
[P5-GigabitEthernet3/0/0] mpls
[P5-GigabitEthernet3/0/0] mpls ldp
[P5-GigabitEthernet3/0/0] quit
```

On the tunnel interface, enable forwarding adjacency and the IS-IS process, and adjust the metric of the tunnel interface so that the tunnel interface can become the outbound interface of the second best IS-IS route. Take the configuration of P1 as an example. The configuration of P3 is similar to that of P1 and is not mentioned here.

```
[P1] interface tunnel 1/0/0
[P1-Tunnel1/0/0] mpls te igp advertise
[P1-Tunnel1/0/0] mpls te igp metric absolute 6
[P1-Tunnel1/0/0] mpls te commit
[P1-Tunnel1/0/0] isis enable 1
```

After the preceding configuration, run the **display mpls ldp lsp** command on PE1. The command output shows that an LDP LSP is established. Take the display on PE1 as an example.

```
[PE1] display mpls ldp lsp 8.8.8.8 32
```

LDP LSP Information

DestAddress/Mask	In/OutLabel	UpstreamPeer	NextHop	OutInterface
8.8.8.8/32	NULL/3	-	10.1.10.2	GE1/0/0
8.8.8.8/32	1024/3	1.1.1.1	10.1.10.2	GE1/0/0

```
TOTAL: 2 Normal LSP(s) Found.
TOTAL: 0 Liberal LSP(s) Found.
TOTAL: 0 Frr LSP(s) Found.
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
A '*' before a UpstreamPeer means the session is in GR state
A '*' before a NextHop means the LSP is FRR LSP
```

Step 5 Configure IS-IS Auto FRR.

Enable IS-IS Auto FRR on P1 and P3, and disable the interfaces that connect P nodes to PE nodes from becoming IS-IS LFA backup interfaces.

Configure P1.

```
[P1] isis 64
[P1-isis-64] frr
[P1-isis-64-frr] loop-free-alternate level-2
[P1-isis-64-frr] quit
[P1-isis-64] quit
[P1] interface gigabitethernet3/1/0
[P1-GigabitEthernet3/1/0] undo isis lfa-backup
[P1-GigabitEthernet3/1/0] quit
```

Configure P3.

```
[P3] isis 64
[P3-isis-64] frr
[P3-isis-64-frr] loop-free-alternate level-2
[P3-isis-64-frr] quit
[P3-isis-64] quit
[P3] interface gigabitethernet3/1/0
[P3-GigabitEthernet3/1/0] undo isis lfa-backup
[P3-GigabitEthernet3/1/0] quit
```

Step 6 Verify the configuration.

Run the **display fib 3.3.3.3 32 verbose** command on P1 to view the FIB entry to P3.

```
[P1] display fib 3.3.3.3 32 verbose
Route Entry Count: 1
Destination: 3.3.3.3           Mask      : 255.255.255.255
NextHop   : 10.1.2.2         OutIf    : GE2/0/0
LocalAddr   : 10.1.2.1         LocalMask : 0.0.0.0
Flags       : DGU              Age        : 124sec
ATIndex     : 0                Slot       : 0
LspFwdFlag  : 0                LspToken   : 0x0
InLabel     : NULL             OriginAs   : 0
BGPNextHop  : 0.0.0.0          PeerAs     : 0
QosInfo     : 0x0              OriginQos  : 0x0
NextHopBak : 10.1.1.2         OutIfBak : Tunnel1/0/0
LspTokenBak : 0x0              InLabelBak : NULL
LspToken_ForInLabelBak      : 0x0
EntryRefCount : 0
rt_ulVlanId  : 0x0
LspType      : 0                Label_ForLspTokenBak : 0
MplsMtu      : 0                Gateway_ForLspTokenBak : 0
NextToken    : 0                IfIndex_ForLspTokenBak : 0
Label_NextToken : 0              Label : 0
LspBfdState  : 0
```

Run the **shutdown** command on GE 2/0/0 of P1 or P3 to simulate a link fault. Take the configuration of P1 as an example.

```
[P1] interface gigabitethernet 2/0/0
[P1-GigabitEthernet2/0/0] shutdown
```

Run the **display fib 3.3.3.3 32 verbose** command on P1 to view the FIB entry to P3.

```
[P1] display fib 3.3.3.3 32 verbose
Route Entry Count: 1
Destination: 3.3.3.3          Mask      : 255.255.255.255
Nexthop   : 10.1.1.2        OutIf    : Tunnel1/0/0
LocalAddr   : 10.1.1.1        LocalMask : 0.0.0.0
Flags       : DGU              Age        : 124sec
ATIndex     : 0                Slot       : 0
LspFwdFlag  : 0                LspToken  : 0x0
InLabel     : NULL             OriginAs   : 0
BGPNextHop  : 0.0.0.0         PeerAs     : 0
QosInfo     : 0x0              OriginQos  : 0x0
NexthopBak  : 0.0.0.0         OutIfBak  : [No Intf]
LspTokenBak : 0x0              InLabelBak : NULL
LspToken_ForInLabelBak : 0x0
EntryRefCount : 0
rt_ulVlanId : 0x0
LspType     : 0                Label_ForLspTokenBak : 0
MplsMtu     : 0                Gateway_ForLspTokenBak : 0
NextToken   : 0                IfIndex_ForLspTokenBak : 0
Label_NextToken : 0            Label      : 0
LspBfdState : 0
```

The command output shows that traffic from P1 to P3 has been switched to the backup link with the outbound interface being Tunnel 1/0/0.

----End

Configuration Files

- Configuration file of P1

```
#
sysname P1
#
router id 1.1.1.1
#
mpls lsr-id 1.1.1.1
mpls
mpls te
mpls rsvp-te
mpls te cspf
#
explicit-path to_p3
next hop 10.1.1.2
next hop 10.1.4.2
next hop 10.1.6.1
next hop 3.3.3.3
#
mpls ldp
#
mpls ldp remote-peer to_p3
remote-ip 3.3.3.3
undo remote-ip pwe3
#
isis 64
frr
loop-free-alternate level-2
is-level level-2
cost-style wide
network-entity 86.0010.0010.0100.1001.00
is-name P1
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
isis enable 64
#
interface Tunnel1/0/0
description toP3
```

```
ip address unnumbered interface LoopBack0
tunnel-protocol mpls te
destination 3.3.3.3
mpls te tunnel-id 100
mpls te bandwidth ct0 200000
mpls te path explicit-path to_p3
mpls te igp advertise
mpls te igp metric absolute 6
mpls te commit
isis enable 64
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.1 255.255.255.252
isis enable 64
isis cost 5
mpls
mpls te
mpls rsvp-te
mpls te bandwidth max-reservable-bandwidth 200000
mpls te bandwidth bc0 200000
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.1.2.1 255.255.255.252
isis enable 64
isis cost 5
mpls
mpls ldp
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 10.1.3.1 255.255.255.252
isis enable 64
isis cost 5
mpls
mpls ldp
#
interface GigabitEthernet3/1/0
undo shutdown
ip address 10.1.10.2 255.255.255.252
isis enable 64
isis cost 5
undo isis lfa-backup
mpls
mpls ldp
#
return
```

● Configuration file of P2

```
#
sysname P2
#
router id 2.2.2.2
#
mpls lsr-id 2.2.2.2
mpls
mpls te
mpls rsvp-te
#
mpls ldp
#
isis 64
is-level level-2
cost-style wide
network-entity 86.0010.0020.0200.2002.00
is-name P2
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
```

```
isis enable 64
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.252
isis enable 64
isis cost 5
mpls
mpls te
mpls rsvp-te
mpls te bandwidth max-reservable-bandwidth 200000
mpls te bandwidth bc0 200000
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.1.4.1 255.255.255.252
isis enable 64
isis cost 5
mpls
mpls te
mpls te bandwidth max-reservable-bandwidth 200000
mpls te bandwidth bc0 200000
mpls ldp
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 10.1.5.1 255.255.255.252
isis enable 64
isis cost 5
mpls
mpls ldp
#
interface GigabitEthernet3/1/0
undo shutdown
ip address 10.1.11.2 255.255.255.252
isis enable 64
isis cost 5
mpls
mpls ldp
#
return
```

● Configuration file of P3

```
#
sysname P3
#
router id 3.3.3.3
#
mpls lsr-id 3.3.3.3
mpls
mpls te
mpls rsvp-te
mpls te cspf
#
explicit-path to_p3
next hop 10.1.6.2
next hop 10.1.4.1
next hop 10.1.1.1
next hop 1.1.1.1
#
mpls ldp
#
mpls ldp remote-peer to_p1
remote-ip 1.1.1.1
undo remote-ip pwe3
#
isis 64
frr
loop-free-alternate level-2
is-level level-2
```



```

cost-style wide
network-entity 86.0010.0030.0300.3003.00
is-name P3
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
 isis enable 64
#
interface Tunnell1/0/0
 description toP1
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te tunnel-id 100
 mpls te bandwidth ct0 200000
 mpls te path explicit-path to_p1
 mpls te igp advertise
 mpls te igp metric absolute 6
 mpls te commit
 isis enable 64
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.6.1 255.255.255.252
 isis enable 64
 isis cost 5
 mpls
 mpls te
 mpls rsvp-te
 mpls te bandwidth max-reservable-bandwidth 200000
 mpls te bandwidth bc0 200000
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.1.2.2 255.255.255.252
 isis enable 64
 isis cost 5
 mpls
 mpls ldp
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 10.1.7.1 255.255.255.252
 isis enable 64
 isis cost 5
 mpls
 mpls ldp
#
interface GigabitEthernet3/1/0
 undo shutdown
 ip address 10.1.12.2 255.255.255.252
 isis enable 64
 isis cost 5
 undo isis lfa-backup
 mpls
 mpls ldp
#
return
    
```

● Configuration file of P4

```

#
sysname P4
#
router id 4.4.4.4
#
mpls lsr-id 4.4.4.4
mpls
 mpls te
 mpls rsvp-te
#
    
```

```

mpls ldp
#
isis 64
 is-level level-2
 cost-style wide
 network-entity 86.0010.0040.0400.4004.00
 is-name P4
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
 isis enable 64
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.6.2 255.255.255.252
 isis enable 64
 isis cost 5
 mpls
 mpls te
 mpls rsvp-te
 mpls te bandwidth max-reservable-bandwidth 200000
 mpls te bandwidth bc0 200000
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.1.4.2 255.255.255.252
 isis enable 64
 isis cost 5
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 200000
 mpls te bandwidth bc0 200000
 mpls ldp
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 10.1.8.1 255.255.255.252
 isis enable 64
 isis cost 5
 mpls
 mpls ldp
#
interface GigabitEthernet3/1/0
 undo shutdown
 ip address 10.1.13.2 255.255.255.252
 isis enable 64
 isis cost 5
 mpls
 mpls ldp
#
return
    
```

- Configuration file of P5

```

#
 sysname P5
#
 router id 5.5.5.5
#
 mpls lsr-id 5.5.5.5
 mpls
#
 mpls ldp
#
 isis 64
 is-level level-2
 cost-style wide
 network-entity 86.0010.0050.0500.5005.00
 is-name P5
#
interface LoopBack0
    
```

```
        ip address 5.5.5.5 255.255.255.255
        isis enable 64
#
interface GigabitEthernet1/0/0
    undo shutdown
    ip address 10.1.9.1 255.255.255.252
    isis enable 64
    isis cost 5
    mpls
    mpls ldp
#
interface GigabitEthernet2/0/0
    undo shutdown
    ip address 10.1.3.2 255.255.255.252
    isis enable 64
    isis cost 5
    mpls
    mpls ldp
#
interface GigabitEthernet3/0/0
    undo shutdown
    ip address 10.1.7.2 255.255.255.252
    isis enable 64
    isis cost 5
    mpls
    mpls ldp
#
return
```

● Configuration file of P6

```
#
sysname P6
#
router id 6.6.6.6
#
mpls lsr-id 6.6.6.6
mpls
#
mpls ldp
#
isis 64
    is-level level-2
    cost-style wide
    network-entity 86.0010.0060.0600.6006.00
    is-name P6
#
interface LoopBack0
    ip address 6.6.6.6 255.255.255.255
    isis enable 64
#
interface GigabitEthernet1/0/0
    undo shutdown
    ip address 10.1.9.2 255.255.255.252
    isis enable 64
    isis cost 5
    mpls
    mpls ldp
#
interface GigabitEthernet2/0/0
    undo shutdown
    ip address 10.1.5.2 255.255.255.252
    isis enable 64
    isis cost 5
    mpls
    mpls ldp
#
interface GigabitEthernet3/0/0
    undo shutdown
    ip address 10.1.8.2 255.255.255.252
    isis enable 64
```

```
isis cost 5
mpls
mpls ldp
#
return
```

- Configuration file of PE1

```
#
sysname PE1
#
router id 7.7.7.7
#
mpls lsr-id 7.7.7.7
mpls
#
mpls ldp
#
isis 64
is-level level-2
cost-style wide
network-entity 86.0010.0070.0700.7007.00
is-name PE1
#
interface LoopBack0
ip address 7.7.7.7 255.255.255.255
isis enable 64
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.10.1 255.255.255.252
isis enable 64
isis cost 5
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.1.11.1 255.255.255.252
isis enable 64
isis cost 5
mpls
mpls ldp
#
return
```

- Configuration file of PE3

```
#
sysname PE3
#
router id 8.8.8.8
#
mpls lsr-id 8.8.8.8
mpls
#
mpls ldp
#
isis 64
is-level level-2
cost-style wide
network-entity 86.0010.0080.0800.8008.00
is-name PE3
#
interface LoopBack0
ip address 8.8.8.8 255.255.255.255
isis enable 64
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 10.1.12.1 255.255.255.252
isis enable 64
```

```

isis cost 5
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 10.1.13.1 255.255.255.252
isis enable 64
isis cost 5
mpls
mpls ldp
#
return
    
```

7.21.12 Example for Configuring IS-IS GR

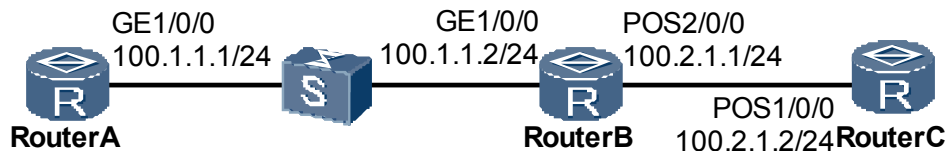
This part provides an example for implementing nonstop packet forwarding when master-slave switchover occurs on the device that runs IS-IS.

Networking Requirements

In the network shown in [Figure 7-18](#), Router A, Router B, and Router C belong to the same AS. Network interconnection is implemented through IS-IS and the GR mechanism is provided.

After IS-IS adjacencies are set up between Router A, Router B, and Router C, the three routers start to exchange routing information. When IS-IS on Router A restarts, Router A resends connection requests to neighbors to synchronize the LSDB.

Figure 7-18 Networking diagram for configuring IS-IS GR



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure GR in the IS-IS views of all the routers.
2. Set the same restart interval in the IS-IS views of all the routers.

Data Preparation

To complete the configuration, you need the following data:

- IS-IS process number
- Restart interval

Procedure

Step 1 Configure an IP address for each interface.

The configuration details are not mentioned here.

Step 2 Configure the basic IS-IS functions.

The configuration details are not mentioned here.

Step 3 Configure IS-IS GR.

Enable IS-IS GR on Router A and set the restart interval. The configurations of Router B and Router C are the same as the configuration of Router A. Take the configuration of Router A as an example.

```
[RouterA] isis 1
[RouterA-isis-1] graceful-restart
[RouterA-isis-1] graceful-restart interval 150
```

Step 4 Verify the configuration.

Run the **display fib** command on Router A to view the Forwarding Information Base (FIB) table.

```
<RouterA> display fib
FIB Table:
  Total number of Routes : 6
Destination/Mask  Nexthop      Flag TimeStamp      Interface      TunnelID
127.0.0.1/32     127.0.0.1    HU   t[21]              InLoop0        0x0
127.0.0.0/8      127.0.0.1    U    t[21]              InLoop0        0x0
100.1.1.1/32     127.0.0.1    HU   t[20678]           InLoop0        0x0
100.1.1.0/24     100.1.1.1    U    t[20678]           Pos1/0/0       0x0
100.1.1.2/32     100.1.1.2    HU   t[20678]           Pos1/0/0       0x0
100.2.1.0/24     100.1.1.2    DGU  t[79388]           Pos1/0/0       0x0
```

Restart the IS-IS process on Router A in GR mode.

```
<RouterA> reset isis all graceful-restart
```

 **NOTE**

A router restarts an IS-IS process in GR mode only when GR is enabled in the IS-IS process.

Run the **display fib** command on Router A, and view the FIB table to check whether GR works normally. If GR works normally, the FIB table does not change and the forwarding service is not affected when Router A restarts the IS-IS process in GR mode.

```
<RouterA> display fib
FIB Table:
  Total number of Routes : 6
Destination/Mask  Nexthop      Flag TimeStamp      Interface      TunnelID
127.0.0.1/32     127.0.0.1    HU   t[21]              InLoop0        0x0
127.0.0.0/8      127.0.0.1    U    t[21]              InLoop0        0x0
100.1.1.1/32     127.0.0.1    HU   t[20678]           InLoop0        0x0
100.1.1.0/24     100.1.1.1    U    t[20678]           Pos1/0/0       0x0
100.1.1.2/32     100.1.1.2    HU   t[20678]           Pos1/0/0       0x0
100.2.1.0/24     100.1.1.2    DGU  t[79388]           Pos1/0/0       0x0
```

As shown in the display, the FIB table on Router A does not change and the forwarding service is not affected.

Disable IS-IS GR on Router A.

```
[RouterA] isis 1
[RouterA-isis-1] undo graceful-restart
```

Restart the IS-IS process on Router A not in GR mode.

```
<RouterA> reset isis all
```

Run the **display fib** command on Router A immediately to view the FIB table.

```
<RouterA> display fib
FIB Table:
  Total number of Routes : 5
  Destination/Mask  Nexthop          Flag TimeStamp      Interface      TunnelID
  127.0.0.1/32     127.0.0.1        HU   t[21]              InLoop0        0x0
  127.0.0.0/8      127.0.0.1        U    t[21]              InLoop0        0x0
  100.1.1.1/32     127.0.0.1        HU   t[20678]           InLoop0        0x0
  100.1.1.0/24     100.1.1.1        U    t[20678]           Pos1/0/0       0x0
  100.1.1.2/32     100.1.1.2        HU   t[20678]           Pos1/0/0       0x0
```

As shown in the display, Router A does not restart the IS-IS process in GR mode; the FIB table changes; compared with the IS-IS process in GR mode, the route to network segment 100.2.1.0 does not exist; service forwarding is affected.

---End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
 isis 1
 graceful-restart
 graceful-restart interval 150
 is-level level-1
 network-entity 10.0000.0000.0001.00
#
 interface Pos1/0/0
 link-protocol ppp
 clock slave
 ip address 100.1.1.1 255.255.255.0
 isis enable 1
#
 return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
 isis 1
 graceful-restart
 graceful-restart interval 150
 is-level level-2
 network-entity 10.0000.0000.0002.00
#
 interface Pos1/0/0
 link-protocol ppp
 clock slave
 ip address 100.2.1.2 255.255.255.0
 isis enable 1
#
 return
```

- Configuration file of Router C

```
#
 sysname RouterC
#
 isis 1
 graceful-restart
 graceful-restart interval 150
 network-entity 10.0000.0000.0003.00
#
 interface Pos1/0/0
 link-protocol ppp
 clock master
 ip address 100.1.1.2 255.255.255.0
```

```

isis enable 1
#
interface Pos2/0/0
 link-protocol ppp
 clock master
 ip address 100.2.1.1 255.255.255.0
 isis enable 1
#
return
    
```

7.21.13 Example for Configuring Static BFD for IS-IS

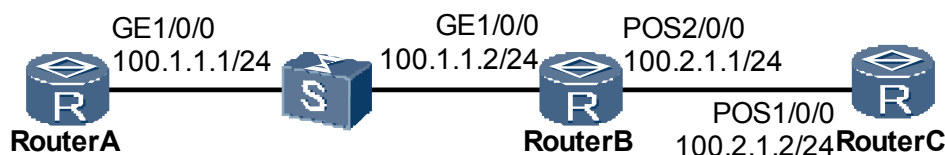
This part provides an example for configuring static BFD for IS-IS to fast detect faults and report them to IS-IS. In this manner, the fast switchover of service traffic is triggered.

Networking Requirements

As show in [Figure 7-19](#):

- A Layer 2 switch exists between Router A and Router B.
- Router A, Router B and Router C run IS-IS.
- BFD is configured to detect the IS-IS neighbor relationship between Router A and Router B. When the link between Router A and Router B is faulty, BFD can fast detect the default and report it to IS-IS.

Figure 7-19 Networking diagram of configuring static BFD for IS-IS



NOTE

BFD for IS-IS cannot be used to detect the multi-hops link between Router A and Router C, because the IS-IS neighbor relationship cannot be established between Router A and Router C.

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic IS-IS functions on each router.
2. Enable BFD on Router A and Router B.

Data Preparation

To complete the configuration, you need the following data:

- IS-IS process ID
- Area addresses of Router A, Router B, and Router C
- Levels of Router A, Router B, and Router C

- Name of the BFD session set up between Router A and Router B and the peer IP address to be detected
- Local and remote discriminators of the BFD session set up between Router A and Router B

Procedure

Step 1 Configure an IP address for each interface.

The configuration details are not mentioned here.

Step 2 Configuration basic IS-IS functions.

Configure Router A.

```
[RouterA] isis 1
[RouterA-isis-1] is-level level-2
[RouterA-isis-1] network-entity aa.1111.1111.1111.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] isis enable 1
[RouterA-GigabitEthernet1/0/0] quit
```

Configure Router B.

```
[RouterB] isis 1
[RouterB-isis-1] is-level level-2
[RouterB-isis-1] network-entity aa.2222.2222.2222.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] isis enable 1
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface Pos 2/0/0
[RouterB-Pos2/0/0] isis enable 1
[RouterB-Pos2/0/0] quit
```

Configure Router C.

```
[RouterC] isis 1
[RouterC-isis-1] is-level level-2
[RouterC-isis-1] network-entity aa.3333.3333.3333.00
[RouterC-isis-1] quit
[RouterC] interface pos 1/0/0
[RouterC-Pos1/0/0] isis enable 1
[RouterC-Pos1/0/0] quit
```

After the preceding configurations, you can view that the neighbor relationship is established between Router A and Router B.

```
[RouterA] display isis peer
Peer information for ISIS(1)
-----
System Id      Interface      Circuit Id      State      HoldTime  Type      PRI
2222.2222.2222 GE1/0/0        2222.2222.2222.00 Up         23s      L2
64
```

The IS-IS routing table of Router A has entries to Router B and Router C.

```
[RouterA] display isis route
Route information for ISIS(1)
-----
ISIS(1) Level-2 Forwarding Table
-----
IPV4 Destination  IntCost  ExtCost  ExitInterface  NextHop      Flags
-----
100.1.1.0/24      10       NULL     GE1/0/0        Direct       D-/L/-
```

```
100.2.1.0/24      20      NULL    GE1/0/0      100.1.1.2    A/-/L/-
Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
```

Step 3 Configure BFD.

Enable BFD on Router A and configure a BFD session.

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd atob bind peer-ip 100.1.1.2 interface gigabitethernet 1/0/0
[RouterA-bfd-session-atob] discriminator local 1
[RouterA-bfd-session-atob] discriminator remote 2
[RouterA-bfd-session-atob] commit
[RouterA-bfd-session-atob] quit
```

Enable BFD on Router B and configure a BFD session.

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bfd btoa bind peer-ip 100.1.1.1 interface gigabitethernet 1/0/0
[RouterB-bfd-session-btoa] discriminator local 2
[RouterB-bfd-session-btoa] discriminator remote 1
[RouterB-bfd-session-btoa] commit
[RouterB-bfd-session-btoa] quit
```

After the preceding configurations, you can view that the status of the BFD session is Up when the **display bfd session** command is used on Router A or Router B.

The display on Router A is as follows:

```
[RouterA] display bfd session all
-----
Local Remote PeerIpAddr      State   Type      InterfaceName
-----
1      2      100.1.1.2    Up     S_IP_IF   GE1/0/0
-----
Total UP/DOWN Session Number : 1/0
```

Step 4 Enable IS-IS fast sense.

Configure Router A.

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] isis bfd static
[RouterA-GigabitEthernet1/0/0] quit
```

Configure Router B.

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] isis bfd static
[RouterB-GigabitEthernet1/0/0] quit
```

Step 5 Verify the configuration.

Enable the terminal log information on Router A.

```
<RouterA> terminal logging
<RouterA> terminal monitor
```

Run the **shutdown** command on GigabitEthernet1/0/0 of Router B to simulate a link fault.

```
[RouterB-GigabitEthernet1/0/0] shutdown
```

On Router A, the following log information and debugging information are displayed. It indicates that IS-IS deletes the neighbor relationship with Router B according to the fault reported by BFD.

```
ISIS/4/PEER_DOWN_BFD/1880166931 UL/R "ISIS 1 neighbor
2222.2222.2222 is down on the interface GE1/0/0 because BFD node is Down.
```

```
ISIS/4/PEER_DOWN_BFDDOWN/1880166931 UL/R "ISIS 1 neighbor
2222.2222.2222 was Down on interface GE1/0/0
because the BFD node was down. The Hello packet was received at 11:32:10 last
time; the maximum interval for sending Hello packets was 9247;the local router sent
426 Hello
packets and received 61 packets;the type of the Hello packet was Lan Level-2."
```

Run the **display isis route** command or the **display isis peer** command on Router A, no information is displayed. This indicates that the IS-IS neighbor relationship between Router A and Router B is deleted.

---End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
bfd
#
isis 1
 is-level level-2
 network-entity aa.1111.1111.1111.00
#
interface GigabitEthernet1/0/0
 ip address 100.1.1.1 255.255.255.0
 isis enable 1
 isis bfd static
#
bfd atob bind peer-ip 100.1.1.2 interface GigabitEthernet1/0/0
 discriminator local 1
 discriminator remote 2
 commit
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
bfd
#
isis 1
 is-level level-2
 network-entity aa.2222.2222.2222.00
#
interface GigabitEthernet1/0/0
 ip address 100.1.1.2 255.255.255.0
 isis enable 1
 isis bfd static
#
interface Pos2/0/0
 ip address 100.2.1.1 255.255.255.0
 isis enable 1
#
bfd btoa bind peer-ip 100.1.1.1 interface GigabitEthernet1/0/0
 discriminator local 2
 discriminator remote 1
 commit
#
return
```

- Configuration file of Router C

```
#
 sysname RouterC
#
```

```
isis 1
 is-level level-2
 network-entity aa.3333.3333.3333.00
 #
 interface Pos1/0/0
  ip address 100.2.1.2 255.255.255.0
  isis enable 1
 #
 return
```

7.21.14 Example for Configuring Dynamic BFD for IS-IS

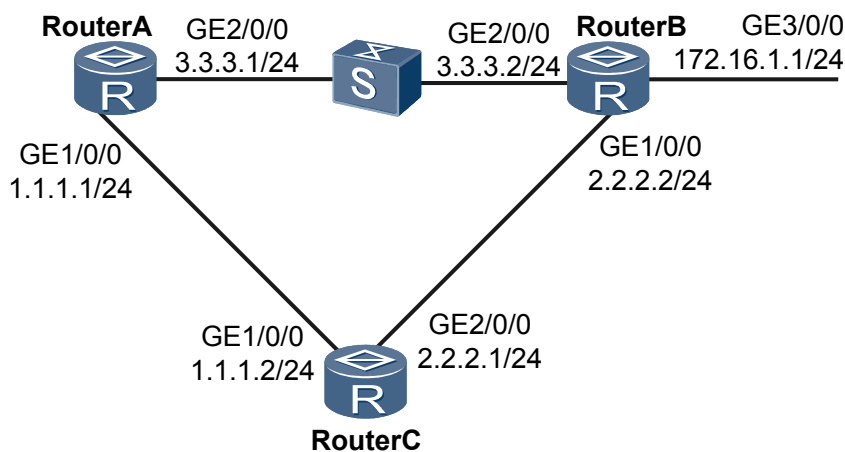
This part provides an example for configuring dynamic BFD for IS-IS to fast detect faults and report them to IS-IS. In this manner, the fast switchover of service traffic is triggered.

Networking Requirements

As shown in [Figure 7-20](#), it is required as follows:

- Run IS-IS on Router A, Router B, and Router C.
- Enable BFD of the IS-IS process on Router A, Router B, and Router C.
- Traffic is transmitted on the active link Router A → Router B. The link Router A → Router B → Router C acts as the standby link.
- Enable BFD of the interface on the link between Router A and Router B. When the link between Router A and Router B fails, BFD can quickly detect the fault and notify IS-IS of the fault; therefore, the traffic is transmitted on the standby link.

Figure 7-20 Networking diagram of configuring the dynamic BFD



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable IS-IS on each router and ensure the connectivity of the routers
2. Set the interface cost of IS-IS to control the route selection of the routers.
3. Enable global BFD.

4. Enable the BFD detection mechanism of the IS-IS process on Router A, Router B, and Router C.
5. Enable the BFD detection mechanism of the interfaces on Router A and Router B.

Data Preparation

To complete the configuration, you need the following data:

- Process ID of IS-IS
- Area numbers of Router A, Router B, and Router C
- Interface cost of Router A, Router B and Router C
- Interface number and type number of BFD enabled on Router A and Router B
- Minimum interval for sending the BFD packets, minimum interval for receiving the BFD packets, and local detection multiple on Router A and Router B

Procedure

Step 1 Assign an IP address to each interface.

The detailed configuration is not mentioned here.

Step 2 Configure the basic IS-IS functions.

Configure Router A.

```
[RouterA] isis
[RouterA-isis-1] is-level level-2
[RouterA-isis-1] network-entity 10.0000.0000.0001.00
[RouterA-isis-1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] isis enable 1
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] isis enable 1
[RouterA-GigabitEthernet2/0/0] quit
```

Configure Router B.

```
[RouterB] isis
[RouterB-isis-1] is-level level-2
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] isis enable 1
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet1/0/0] isis enable 1
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 3/0/0
[RouterB-GigabitEthernet3/0/0] isis enable 1
[RouterB-GigabitEthernet3/0/0] quit
```

Configure Router C.

```
[RouterC] isis
[RouterC-isis-1] is-level level-2
[RouterC-isis-1] network-entity 10.0000.0000.0003.00
[RouterC-isis-1] quit
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] isis enable 1
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface gigabitethernet 2/0/0
```

```
[RouterC-GigabitEthernet2/0/0] isis enable 1
[RouterC-GigabitEthernet2/0/0] quit
```

After the preceding configurations are complete, use the **display isis peer** command. You can view that the neighboring relationship is set up between Router A and Router B, and that between Router A and Router C. Take the configuration on Router A as an example:

```
[RouterA] display isis peer
Peer information for ISIS(1)
-----
System Id      Interface      Circuit Id      State HoldTime Type      PRI
0000.0000.0002 GE2/0/0        0000.0000.0002.01 Up    9s      L2        64
0000.0000.0003 GE1/0/0        0000.0000.0001.02 Up    21s     L2        64
Total Peer(s): 2
```

The routers have learnt routes of each other. Take the routing table of Router A as an example:

```
[RouterA] display ip routing-table
Route Flags: R - relied, D - download to fib
-----
Routing Tables: Public
Destinations : 8          Routes : 9
Destination/Mask Proto Pre Cost Flags NextHop Interface
1.1.1.0/24 Direct 0 0 D 1.1.1.1 GigabitEthernet1/0/0
1.1.1.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
2.2.2.0/24 ISIS-L2 15 20 D 1.1.1.2 GigabitEthernet1/0/0
3.3.3.0/24 Direct 0 0 D 3.3.3.1 GigabitEthernet2/0/0
3.3.3.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
172.16.1.0/24 ISIS-L2 15 20 D 3.3.3.2 GigabitEthernet2/0/0
```

As shown in the routing table, the next hop address of the route to 172.16.1.0/24 is 3.3.3.2 and traffic is transmitted on the active link from Router A to Router B.

Step 3 Set the interface cost.

Configure Router A.

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet1/0/0] isis cost 5
[RouterA-GigabitEthernet1/0/0] quit
```

Configure Router B.

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet1/0/0] isis cost 5
[RouterB-GigabitEthernet1/0/0] quit
```

Step 4 Configure BFD of the IS-IS process.

Enable BFD of the IS-IS process on Router A.

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] isis
[RouterA-isis-1] bfd all-interfaces enable
[RouterA-isis-1] quit
```

Enable BFD of the IS-IS process on Router B.

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] isis
[RouterB-isis-1] bfd all-interfaces enable
[RouterB-isis-1] quit
```

Enable BFD of the IS-IS process on Router C.

```
[RouterC] bfd
[RouterC-bfd] quit
[RouterC] isis
[RouterC-isis-1] bfd all-interfaces enable
[RouterC-isis-1] quit
```

After the preceding configurations are complete, run the **display isis bfd session all** command on Router A, Router B, or Router C. You can view that the status of BFD is Up.

Take the display of Router A as an example:

```
[RouterA] display isis bfd session all
          BFD session information for ISIS(1)
          -----
Peer System ID : 0000.0000.0002      Interface : GE2/0/0
TX : 100          BFD State : up      Peer IP Address : 3.3.3.2
RX : 100          LocDis : 8193       Local IP Address: 3.3.3.1
TX : 10           BFD State : up      Peer IP Address : 3.3.3.2
RX : 10           LocDis : 8192       Local IP Address: 3.3.3.1
Multiplier : 3    RemDis : 8192      Type : L2
Diag : No diagnostic information
Peer System ID : 0000.0000.0003      Interface : GE1/0/0
TX : 10           BFD State : up      Peer IP Address : 1.1.1.2
RX : 10           LocDis : 8193       Local IP Address: 1.1.1.1
Multiplier : 3    RemDis : 8192      Type : L2
Diag : No diagnostic information
```

From the preceding display, you can view that the status of the BFD session between Router A and Router B and that between Router A and Router C are Up.

Step 5 Configure BFD of the interfaces.

Configure BFD on GE 2/0/0 of Router A, set the minimum interval for sending the packets and the minimum interval for receiving the packets to 100 ms, and set the local detection time multiple to 4.

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] isis bfd enable
[RouterA-GigabitEthernet2/0/0] isis bfd min-tx-interval 100 min-rx-interval 100
detect-multiplier 4
[RouterA-GigabitEthernet2/0/0] quit
```

Configure BFD on GE 2/0/0 of Router B, set the minimum interval for sending the packets and the minimum interval for receiving the packets to 100 ms, and set the local detection time multiple to 4.

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] isis bfd enable
[RouterB-GigabitEthernet2/0/0] isis bfd min-tx-interval 100 min-rx-interval 100
detect-multiplier 4
[RouterB-GigabitEthernet2/0/0] quit
```

After the preceding configurations are complete, run the **display isis bfd session all** command on Router A or Router B. You can view that the parameters of the BFD have taken effect. Take the display of Router B as an example:

```
[RouterB] display isis bfd session all
          BFD session information for ISIS(1)
          -----
Peer System ID : 0000.0000.0001      Interface : GE2/0/0
TX : 100          BFD State : up      Peer IP Address : 3.3.3.1
RX : 100          LocDis : 8192       Local IP Address: 3.3.3.2
Multiplier : 4    RemDis : 8192      Type : L2
Diag : No diagnostic information
Peer System ID : 0000.0000.0003      Interface : GE1/0/0
```

```
TX : 100          BFD State : up          Peer IP Address : 2.2.2.1
RX : 100          LocDis : 8192          Local IP Address: 2.2.2.2
Multiplier : 3    RemDis : 8193          Type : L2
Diag : No diagnostic information
```

Step 6 Verify the configuration.

Run the **shutdown** command on GE 2/0/0 of Router B to simulate the active link failure.

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] shutdown
```

Step 7 # Display the routing table on Router A.

```
[RouterA] display ip routing-table
Route Flags: R - relied, D - download to fib
-----
Routing Tables: Public
  Destinations : 8          Routes : 8
Destination/Mask    Proto    Pre  Cost    Flags NextHop          Interface
1.1.1.0/24         Direct   0    0        D  1.1.1.1          GigabitEthernet1/0/0
1.1.1.1/32         Direct   0    0        D  127.0.0.1         InLoopBack0
2.2.2.0/24         ISIS-L2  15   20        D  1.1.1.2          GigabitEthernet1/0/0
3.3.3.0/24         Direct   0    0        D  3.3.3.1          GigabitEthernet1/0/0
3.3.3.1/32         Direct   0    0        D  127.0.0.1         InLoopBack0
127.0.0.0/8        Direct   0    0        D  127.0.0.1         InLoopBack0
127.0.0.1/32       Direct   0    0        D  127.0.0.1         InLoopBack0
172.16.1.0/24      ISIS-L2  15   20        D  1.1.1.2          GigabitEthernet1/0/0
```

As shown in the routing table, the standby link Router A → Router C → Router B takes effect after the active link fails. The next hop address of the route to 172.16.1.0/24 becomes 1.1.1.2.

Run the **display isis bfd session all** command on Router A. You can view the status of the BFD session is Up between Router A and Router C.

```
[RouterA] display isis bfd session all
          BFD session information for ISIS(1)
          -----
Peer System ID : 0000.0000.0003          Interface : GE1/0/0
TX : 100          BFD State : up          Peer IP Address : 1.1.1.2
RX : 100          LocDis : 8192          Local IP Address: 1.1.1.1
TX : 10           BFD State : up          Peer IP Address : 1.1.1.2
RX : 10           LocDis : 8193          Local IP Address: 1.1.1.1
Multiplier : 3    RemDis : 8192          Type : L2
Diag : No diagnostic information
```

---End

Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
 bfd
#
 isis 1
  is-level level-2
  bfd all-interfaces enable
  network-entity 10.0000.0000.0001.00
#
 interface GigabitEthernet1/0/0
  undo shutdown
  ip address 1.1.1.1 255.255.255.0
  isis enable 1
#
 interface GigabitEthernet2/0/0
  undo shutdown
```



```

        ip address 3.3.3.1 255.255.255.0
        isis enable 1
        isis cost 5
        isis bfd enable
        isis bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 4
    #
    return
    
```

- Configuration file of Router B

```

    #
    sysname RouterB
    #
    bfd
    #
    isis 1
        is-level level-2
        bfd all-interfaces enable
        network-entity 10.0000.0000.0002.00
    #
    interface GigabitEthernet1/0/0
    undo shutdown
    ip address 2.2.2.2 255.255.255.0
    isis enable 1
    #
    interface GigabitEthernet2/0/0
    undo shutdown
    ip address 3.3.3.2 255.255.255.0
    isis enable 1
    isis cost 5
    isis bfd enable
    isis bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 4
    #
    interface GigabitEthernet3/0/0
    undo shutdown
    ip address 172.16.1.1 255.255.255.0
    isis enable 1
    #
    return
    
```

- Configuration file of Router C

```

    #
    sysname RouterC
    #
    bfd
    #
    isis 1
        is-level level-2
        bfd all-interfaces enable
        network-entity 10.0000.0000.0003.00
    #
    interface GigabitEthernet1/0/0
    undo shutdown
    ip address 1.1.1.2 255.255.255.0
    isis enable 1
    #
    interface GigabitEthernet2/0/0
    undo shutdown
    ip address 2.2.2.1 255.255.255.0
    isis enable 1
    #
    return
    
```

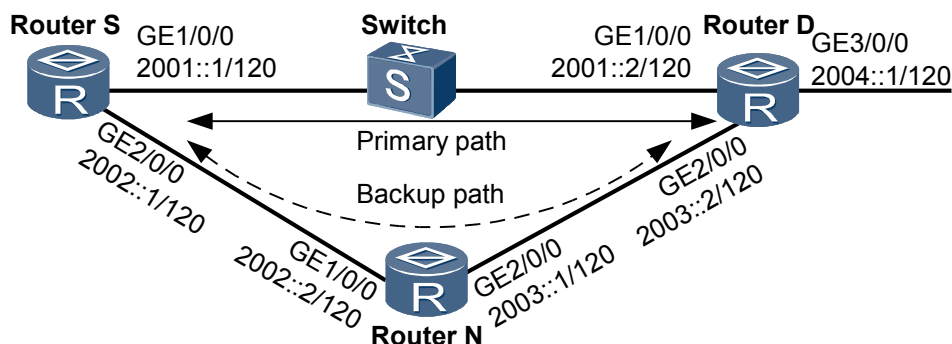
7.21.15 Example for Configuring Dynamic IPv6 BFD for IS-IS

This part provides an example for configuring dynamic BFD for fast failure detection to trigger fast switchover of service traffic on IS-IS IPv6 networks.

Networking Requirements

Figure 7-21 shows an IS-IS IPv6 network. The primary path of traffic between Router S and Router D is Router S-->Switch-->Router D, and the backup path is Router S-->Router N-->Router D.

Figure 7-21 Networking diagram of dynamic IPv6 BFD for IS-IS



It is required to configure IPv6 BFD for IS-IS so that traffic between Router S and Router D can be rapidly switched to the backup path when the primary path or Switch fails.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic IS-IS IPv6 functions on each router to ensure the IPv6 connectivity.
2. Adjust the IS-IS cost values of interfaces on each router so that the path Router S-->Switch-->Router D becomes the primary path, and the path Router S-->Router N-->Router D becomes the backup path.
3. Configure BFD globally on each router.
4. Enable IPv6 BFD for IS-IS in the IS-IS view of each router.

Data Preparation

To complete the configuration, you need the following data:

- IS-IS process ID
- IS-IS network entity title (NET)
- Level of each Router
- IS-IS cost value of each interface
- Interface to be enabled with IPv6 BFD for IS-IS
- Minimum interval for sending IPv6 BFD packets, minimum interval for receiving IPv6 BFD packets, and local BFD detection multiplier

Procedure

Step 1 Enable IPv6 forwarding capability and configure an IPv6 address for each interface.

The configurations of Router S are taken as an example. The configurations of other routers are as the same as those of Router S and thus are not mentioned here.

```
<HUAWEI> system-view
[HUAWEI] sysname RouterS
[RouterS] ipv6
[RouterS] interface gigabitethernet 1/0/0
[RouterS-GigabitEthernet1/0/0] ipv6 enable
[RouterS-GigabitEthernet1/0/0] ipv6 address 2001::1/120
```

Step 2 Configure basic IS-IS functions.

Configure Router S.

```
[RouterS] isis 10
[RouterS-isis-10] is-level level-2
[RouterS-isis-10] network-entity 10.0000.0000.0001.00
[RouterS-isis-10] ipv6 enable
[RouterS-isis-10] quit
[RouterS] interface gigabitethernet 1/0/0
[RouterS-GigabitEthernet1/0/0] isis ipv6 enable 10
[RouterS-GigabitEthernet1/0/0] quit
[RouterS] interface gigabitethernet 2/0/0
[RouterS-GigabitEthernet2/0/0] isis ipv6 enable 10
[RouterS-GigabitEthernet2/0/0] quit
```

Configure Router N.

```
[RouterN] isis 10
[RouterN-isis-10] is-level level-2
[RouterN-isis-10] network-entity 10.0000.0000.0002.00
[RouterN-isis-10] ipv6 enable
[RouterN-isis-10] quit
[RouterN] interface gigabitethernet 1/0/0
[RouterN-GigabitEthernet1/0/0] isis ipv6 enable 10
[RouterN-GigabitEthernet1/0/0] quit
[RouterN] interface gigabitethernet 2/0/0
[RouterN-GigabitEthernet2/0/0] isis ipv6 enable 10
[RouterN-GigabitEthernet2/0/0] quit
```

Configure Router D.

```
[RouterD] isis 10
[RouterD-isis-10] is-level level-2
[RouterD-isis-10] network-entity 10.0000.0000.0003.00
[RouterD-isis-10] ipv6 enable
[RouterD-isis-10] quit
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] isis ipv6 enable 10
[RouterD-GigabitEthernet1/0/0] quit
[RouterD] interface gigabitethernet 2/0/0
[RouterD-GigabitEthernet2/0/0] isis ipv6 enable 10
[RouterD-GigabitEthernet2/0/0] quit
```

After the preceding configurations, run the **display ipv6 routing-table** command. You can view that routers have learned IPv6 routes from each other.

Step 3 Set the IS-IS cost value of each interface.

Configure Router S.

```
[RouterS] interface gigabitethernet 1/0/0
[RouterS-GigabitEthernet1/0/0] isis ipv6 cost 1 level-2
[RouterS-GigabitEthernet1/0/0] quit
[RouterS] interface gigabitethernet 2/0/0
[RouterS-GigabitEthernet2/0/0] isis ipv6 cost 10 level-2
[RouterS-GigabitEthernet2/0/0] quit
```

Configure Router N.

```
[RouterN] interface gigabitethernet 1/0/0
[RouterN-GigabitEthernet1/0/0] isis ipv6 cost 10 level-2
[RouterN-GigabitEthernet1/0/0] quit
[RouterN] interface gigabitethernet 2/0/0
[RouterN-GigabitEthernet2/0/0] isis ipv6 cost 10 level-2
[RouterN-GigabitEthernet2/0/0] quit
```

Configure Router D.

```
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] isis ipv6 cost 1 level-2
[RouterD-GigabitEthernet1/0/0] quit
[RouterD] interface gigabitethernet 2/0/0
[RouterD-GigabitEthernet2/0/0] isis ipv6 cost 10 level-2
[RouterD-GigabitEthernet2/0/0] quit
```

Step 4 Configure IPv6 BFD for IS-IS.

On the Router S, Router N, and Router D, enable IPv6 BFD for IS-IS globally, set the minimum interval for sending BFD packets to 150 ms and the minimum interval for receiving BFD packets to 150 ms, and specify the local detection multiplier to 3.

Configure Router S.

```
[RouterS] bfd
[RouterS-bfd] quit
[RouterS] isis 10
[RouterS-isis-10] ipv6 bfd all-interfaces enable
[RouterS-isis-10] ipv6 bfd all-interfaces min-tx-interval 150 min-rx-interval 150
[RouterS-isis-10] quit
```

Configure Router N.

```
[RouterN] bfd
[RouterN-bfd] quit
[RouterN] isis 10
[RouterN-isis-10] ipv6 bfd all-interfaces enable
[RouterN-isis-10] ipv6 bfd all-interfaces min-tx-interval 150 min-rx-interval 150
[RouterN-isis-10] quit
```

Configure Router D.

```
[RouterD] bfd
[RouterD-bfd] quit
[RouterD] isis 10
[RouterD-isis-10] ipv6 bfd all-interfaces enable
[RouterD-isis-10] ipv6 bfd all-interfaces min-tx-interval 150 min-rx-interval 150
[RouterD-isis-10] quit
```

After the preceding configurations, run the **display isis ipv6 bfd session all** command on Router S or Router D, and you can view that IPv6 BFD detection parameters already take effect. Take the display on Router S as an example.

```
[RouterS] display isis 10 ipv6 bfd session all
                IPv6 BFD session information for ISIS(1)
                -----
Peer System ID : 0000.0000.0003          Interface : GE1/0/0  Type : L2
IPv6 BFD State : up TX : 150 RX : 150 Multiplier : 3
LocDis : 8184 Local IPv6 Address : FE80::E0:2F47:B107:1
RemDis : 8192 Peer IPv6 Address : FE80::E0:2F47:B103:1
Diag : No diagnostic information

Peer System ID : 0000.0000.0003          Interface : GE2/0/0  Type : L2
IPv6 BFD State : up TX : 150 RX : 150 Multiplier : 3
LocDis : 8184 Local IPv6 Address : FE80::C964:0:B8B6:1
RemDis : 8192 Peer IPv6 Address : FE80::C964:0:B203:1
Diag : No diagnostic information
```

Total IPv6 BFD session(s) : 2

Step 5 Verify the configuration.

Run the **display ipv6 routing-table 2004::1 120** command on Router S to check the IPv6 routing table. You can view that the next hop address is 2001:2 and the outbound interface is Gigabit Ethernet 1/0/0.

```
[RouterS] display ipv6 routing-table 2004::1 120
Routing Table : Public
Summary Count 1

Destination: 2004::                                PrefixLength : 120
NextHop: 2001:2                                     Preference   : 15
Interface   : GigabitEthernet1/0/0                 Protocol     : ISIS
State: Active Adv                                   Cost         : 20
Tunnel ID   : 0x0                                    Label        : NULL
Age         : 93sec
```

Run the **shutdown** command on Gigabit Ethernet 1/0/0 on Router D to simulate a primary path failure.

```
[RouterD] interface gigabitethernet 1/0/0
[RouterD-GigabitEthernet1/0/0] shutdown
```

Run the **display ipv6 routing-table 2004::1 120** command on Router S to view the IPv6 routing table.

```
[RouterS] display ipv6 routing-table 2004::1 120
Routing Table : Public
Summary Count 1

Destination: 2004::                                PrefixLength : 120
NextHop: 2002::2                                     Preference   : 15
Interface   : GigabitEthernet2/0/0                 Protocol     : ISIS
State: Active Adv                                   Cost         : 20
Tunnel ID   : 0x0                                    Label        : NULL
Age         : 93sec
```

As shown in the IPv6 routing table, after the primary path fails, the backup path takes effect; the next hop address of the route to 2004::/120 becomes 2002::2; the outbound interface becomes Gigabit Ethernet 2/0/0; the route cost may also change.

Run the **display isis ipv6 bfd session all** command on Router S, and you can view that there is only one BFD session in the Up state between Router S and Router N.

```
[RouterS] display isis 10 ipv6 bfd session all
                IPv6 BFD session information for ISIS(1)
                -----
Peer System ID : 0000.0000.0003          Interface : GE2/0/0  Type : L2
IPv6 BFD State : up TX : 150 RX : 150 Multiplier : 3
LocDis : 8184 Local IPv6 Address : FE80::C964:0:B8B6:1
RemDis : 8192 Peer IPv6 Address : FE80::C964:0:B203:1
Diag : No diagnostic information

Total IPv6 BFD session(s) : 1
```

----End

Configuration Files

- Configuration file of Router S

```
#
 sysname RouterS
#
```

```
    bfd
    #
    isis 10
    is-level level-2
    ipv6 bfd all-interfaces enable
    ipv6 bfd all-interfaces min-tx-interval 150 min-rx-interval 150
    network-entity 10.0000.0000.0001.00
    #
    ipv6 enable topology standard
    #
    #
    interface GigabitEthernet1/0/0
    undo shutdown
    ipv6 enable
    ipv6 address 2001::1/120
    isis ipv6 enable 10
    isis ipv6 cost 1
    #
    interface GigabitEthernet2/0/0
    undo shutdown
    ipv6 enable
    ipv6 address 2002::1/120
    isis ipv6 enable 10
    isis ipv6 cost 10
    #
    return
```

- Configuration file of Router N

```
    #
    sysname RouterN
    #
    bfd
    #
    isis 10
    is-level level-2
    ipv6 bfd all-interfaces enable
    ipv6 bfd all-interfaces min-tx-interval 150 min-rx-interval 150
    network-entity 10.0000.0000.0002.00
    #
    ipv6 enable topology standard
    #
    #
    interface GigabitEthernet1/0/0
    undo shutdown
    ipv6 enable
    ipv6 address 2002::2/120
    isis ipv6 enable 10
    isis ipv6 cost 10
    #
    interface GigabitEthernet2/0/0
    undo shutdown
    ipv6 enable
    ipv6 address 2003::1/120
    isis ipv6 enable 10
    isis ipv6 cost 10
    #
    return
```

- Configuration file of Router D

```
    #
    sysname RouterD
    #
    bfd
    #
    isis 10
    is-level level-2
    ipv6 bfd all-interfaces enable
    ipv6 bfd all-interfaces min-tx-interval 150 min-rx-interval 150
    network-entity 10.0000.0000.0003.00
    #
```

```
        ipv6 enable topology standard
#
#
interface GigabitEthernet1/0/0
undo shutdown
ipv6 enable
ipv6 address 2001::2/120
isis ipv6 enable 10
isis ipv6 cost 1
#
interface GigabitEthernet2/0/0
undo shutdown
ipv6 enable
ipv6 address 2003::2/120
isis ipv6 enable 10
isis ipv6 cost 10
#
return
```

- Configuration file of Switch
Configuration file of Switch is not mentioned here.

8 BGP Configuration

About This Chapter

BGP is used between ASs to transmit routing information on large-scale and complex networks.

8.1 Introduction of BGP

BGP is a dynamic routing protocol used between ASs.

8.2 Configuring Basic BGP Functions

Configuring basic BGP functions is the prerequisite to building a BGP network.

8.3 Configuring BGP Route Attributes

BGP has many route attributes. By configuring these attributes, you can change BGP routing policies.

8.4 Configuring BGP Filters

By using routing policies, BGP can flexibly send and receive routes.

8.5 Controlling the Advertisement of BGP Routing Information

BGP can perform routing policies on or filter only the routes to be advertised to a certain peer.

8.6 Controlling the Import of Routing Information

Importing routes of other routing protocols can enrich the BGP routing table. When importing IGP routes, BGP can filter the routes according to different routing protocols.

8.7 Configuring BGP Route Dampening

By configuring BGP route dampening, you can suppress unstable BGP routes.

8.8 Configuring Parameters of a BGP Peer Connection

By setting parameters of a BGP peer connection, you can adjust and optimize the BGP network performance.

8.9 Configuring BFD for BGP

By configuring BFD for BGP, you can provide a fast fault detection mechanism for BGP, and thus speed up network convergence.

8.10 Configuring BGP Auto FRR

As a protection measure against link faults, BGP Auto FRR is applicable to the network topology with primary and backup links. BGP Auto FRR is suitable for the services that are sensitive to packet delay and packet loss.

8.11 Configuring BGP Tracking

On a network where BFD is unsuitable to deploy, you can configure BGP tracking to implement the fast convergence of IBGP routes.

8.12 Configuring Prefix-based BGP ORF

Prefix-based BGP ORF enables a device to send its peer the prefix-based inbound policy that can be used by the peer to filter routes to be sent.

8.13 Configuring Path MTU Auto Discovery

By configuring path MTU auto discovery, you can discover the minimum MTU on the network path from the source to the destination.

8.14 Configuring the BGP Next Hop Delayed Response

By configuring the BGP next hop delayed response, you can reduce traffic loss during routes changes.

8.15 Configuring BGP Load Balancing

By configuring BGP load balancing, you can properly use network resources.

8.16 Configuring a BGP Peer Group

By configuring a BGP peer group, you can simplify the management of routing policies, and thus improve the efficiency of route advertisement.

8.17 Configuring a BGP Route Reflector

By configuring a BGP route reflector, you can solve the problem of establishing fully meshed connections between multiple IBGP peers.

8.18 Configuring a BGP Confederation

On a large-scale BGP network, configuring a BGP confederation can simplify the management of routing policies and improve the efficiency of route advertisement.

8.19 Configuring BGP Accounting

By configuring BGP accounting, you can collect the statistics of the incoming and outgoing BGP traffic of an AS.

8.20 Configuring BGP GR

By configuring BGP GR, you can avoid traffic interruption caused by protocol restart.

8.21 Configuring BGP Security

To improve BGP security, you can perform TCP connection authentication.

8.22 Maintaining BGP

Maintaining BGP involves resetting a BGP connection and clearing BGP statistics.

8.23 Configuration Examples

BGP configuration examples explain networking requirements, networking diagram, configuration notes, configuration roadmap, and configuration procedure.

8.1 Introduction of BGP

BGP is a dynamic routing protocol used between ASs.

8.1.1 BGP Overview

BGP is mainly used to control route transmission and select the optimal route.

The Border Gateway Protocol (BGP) is a dynamic routing protocol used between Autonomous Systems (ASs). BGP-1 (defined in RFC 1105), BGP-2 (defined in RFC 1163), and BGP-3 (defined in RFC 1267) are three earlier-released versions of BGP. The current BGP version is BGP-4 defined in RFC 4271.

As an exterior routing protocol on the Internet, BGP is widely used among Internet Service Providers (ISPs).

NOTE

Unless otherwise stated, BGP stated in this document refers to BGP-4.

Characteristics of BGP are as follows:

- Different from the Internal Gateway Protocol (IGP) such as the Open Shortest Path First (OSPF) and Routing Information Protocol (RIP), BGP is an Exterior Gateway Protocol (EGP), which controls route advertisement and selects the optimal route between ASs rather than discover or calculate routes.
- BGP uses the Transport Control Protocol (TCP) with the port number being 179 as the transport layer protocol. The reliability of BGP is thus enhanced.
- BGP supports Classless Inter-Domain Routing (CIDR).
- BGP transmits only the updated routes when routes are being updated. This reduces the bandwidth occupied by BGP for route distribution. Therefore, BGP is applicable to the Internet where a large number of routes are transmitted.
- BGP eliminates routing loops by adding AS path information to BGP routes.
- BGP provides rich routing policies to flexibly select and filter routes.
- BGP can be easily extended and adapt to the development of networks.

BGP runs on the router in either of the following modes:

- Internal BGP (IBGP)
- External BGP (EBGP)

When BGP runs within an AS, it is called IBGP. When BGP runs between ASs, it is called EBGP.

8.1.2 BGP Features Supported by the NE80E/40E

The system supports various BGP features, including load balancing, route summarization, route dampening, community, route reflector, confederation, MP-BGP, BFD for BGP, BGP GR, and BGP NSR.



Main Route Attributes

- Origin attribute
- AS_Path attribute
- Next_Hop attribute
- Multi-Exit-Discriminator (MED) attribute
- Local_Pref attribute
- Community attribute

Principles of Route Selection

On the NE80E/40E, when there are multiple active routes to the same destination, BGP selects routes according to the following principles:

1. Prefers the route with the highest PreVal.
PreVal is a Huawei-specific parameter. It is valid only on the device where it is configured.
2. Prefers the route with the highest Local_Pref.
A route without Local_Pref is considered to have had the value set by using the **default local-preference** command or to have a value of 100 by default.
3. Prefers a locally originated route. A locally originated route takes precedence over a route learned from a peer.
Locally originated routes include routes imported by using the **network** command or the **import-route** command, manually aggregated routes, and automatically summarized routes.
 - (1) A summarized route is preferred. A summarized route takes precedence over a non-summarized route.
 - (2) A route obtained by using the **aggregate** command is preferred over a route obtained by using the **summary automatic** command.
 - (3) A route imported by using the **network** command is preferred over a route imported by using the **import-route** command.
4. Prefers the route with the shortest AS_Path.
 - The AS_CONFED_SEQUENCE and AS_CONFED_SET are not included in the AS_Path length.
 - An AS_SET counts as 1, no matter how many ASs are in the set.
 - After the **bestroute as-path-ignore** command is run, the AS_Path attributes of routes are not compared in the route selection process.
5. Prefers the route with the highest Origin type. IGP is higher than EGP, and EGP is higher than Incomplete.
6. Prefers the route with the lowest Multi Exit Discriminator (MED).
 - The MEDs of only routes from the same AS but not a confederation sub-AS are compared. MEDs of two routes are compared only when the first AS number in the AS_SEQUENCE (excluding AS_CONFED_SEQUENCE) is the same for the two routes.
 - A route without any MED is assigned a MED of 0, unless the **bestroute med-none-as-maximum** command is run. If the **bestroute med-none-as-maximum** command is run, the route is assigned the highest MED of 4294967295.

- After **compare-different-as-med** command is run, the MEDs in routes sent from peers in different ASs are compared. Do not use this command unless it is confirmed that different ASs use the same IGP and route selection mode. Otherwise, a loop may occur.
 - If the **bestroute med-confederation** command is run, MEDs are compared for routes that consist only of AS_CONFED_SEQUENCE. The first AS number in the AS_CONFED_SEQUENCE must be the same for the routes.
 - After the **deterministic-med** command is run, routes are not selected in the sequence in which routes are received.
7. Prefers EBGp routes over IBGP routes.
- EBGP is higher than IBGP, IBGP is higher than LocalCross, and LocalCross is higher than RemoteCross.
- If the ERT of a VPNv4 route in the routing table of a VPN instance on a PE matches the IRT of another VPN instance on the PE, the VPNv4 route will be added to the routing table of the second VPN instance. This is called LocalCross. If the ERT of a VPNv4 route from a remote PE is learned by the local PE and matches the IRT of a VPN instance on the local PE, the VPNv4 route will be added to the routing table of that VPN instance. This is called RemoteCross.
8. Prefers the route with the lowest IGP metric to the BGP next hop.
-  **NOTE**
- Assume that load balancing is configured. If the preceding rules are the same and there are multiple external routes with the same AS_Path, load balancing will be performed based on the number of configured routes.
9. Prefers the route with the shortest Cluster_List.
10. Prefers the route advertised by the router with the smallest router ID.
-  **NOTE**
- If routes carry the Originator_ID, the originator ID is substituted for the router ID during route selection. The route with the smallest Originator_ID is preferred.
11. Prefers the route learned from the peer with the smallest address if the IP addresses of peers are compared in the route selection process.

Routing Selection Policies for Load Balancing

In BGP, the next-hop address of a generated route may not be the address of the peer that is directly connected to the local router. One common scenario is that the next hop is not changed when a route is advertised between IBGP peers. Therefore, before forwarding a packet, the router must find a directly reachable address, through which the packet can reach the next hop specified in the routing table. In this process, the route to the directly reachable address is called a dependent route. BGP routes depend on these dependent routes for packet forwarding. The process of finding a dependent route based on the next-hop address is called route iteration.

The NE80E/40E supports iteration-based BGP load balancing. If load balancing is configured for a dependent route (assume that there are three next-hop addresses), BGP generates the same number of next-hop addresses to forward packets. BGP load balancing based on iteration does not need to be configured by using commands. This feature is always enabled on the NE80E/40E.

BGP load balancing is different from IGP load balancing in the following implementation methods:

- In IGPs, if there are different routes to the same destination address, an IGP calculates metrics of these routes based on its own routing algorithm and performs load balancing among the routes with the same metric.
- BGP does not have a routing algorithm. Therefore, BGP cannot determine whether to perform load balancing among routes based on explicit metrics. BGP, however, contains many route attributes, which have different priorities in route selection policies. Therefore, BGP performs load balancing according to route selection policies. That is, load balancing is performed according to the configured maximum number of equal-cost routes only when all the routes have the same high preference.



NOTE

- By default, BGP performs load balancing only among the routes with the same AS_Path attribute. You can use the [bestroute as-path-ignore](#) command to configure BGP not to compare the AS_Path attribute of routes when performs load balancing.
- BGP load balancing is also applicable between ASs in a confederation.

Policies for BGP Route Advertisement

On the NE80E/40E, BGP advertises routes based on the following policies:

- When there are multiple active routes, the BGP speaker advertises only the optimal route to its peer.
- The BGP speaker advertises only the preferred routes to its peer.
- The BGP speaker advertises the routes learned from EBGP peers to all BGP peers (including EBGP peers and IBGP peers) except the peers that advertise these routes.
- The BGP speaker does not advertise the routes learned from IBGP peers to its IBGP peers.
- The BGP speaker advertises the routes learned from IBGP peers to its EBGP peers.
- The BGP speaker advertises all preferred BGP routes to the new peers when peer relationships are established.

Route Summarization

On a large-scale network, the BGP routing table is large. You can configure route summarization to reduce the size of the routing table.

Route summarization is the process of consolidating multiple routes into one single advertisement. After route summarization is configured, BGP advertises only the summarized route rather than all specific routes to its peers.

The NE80E/40E supports automatic summarization and manual summarization. Manual summarization can be used to control attributes of the summarized route and determine whether to advertise its specific routes.

Route Dampening

Route dampening is a method of solving the problem of route instability. Route instability is reflected by route flapping. That is, a route in the routing table disappears and appears repeatedly.

If route flapping occurs, a routing protocol sends an Update message to its peers. After receiving this Update message, the peers recalculate routes and modify their routing tables. Frequent route flapping consumes a lot of bandwidth and CPU resources, even affecting the normal operation of the network.

In most cases, BGP is applicable to complex networks where routes change frequently. To avoid the impact of frequent route flapping, BGP suppresses unstable routes by using route dampening.

Synchronization Between IBGP and IGP

Synchronization between IBGP and IGP is a method of preventing external routes from being imported by error.

If the synchronization function is configured, the IGP routing table is examined before an IBGP route is added to the routing table and advertised to EBGP peers. The IBGP route is added to the routing table and advertised to EBGP peers only when the IGP knows this IBGP route.

The synchronization function can be disabled in the following situations:

- The local AS is not a transit AS.
- Full-mesh IBGP connections are established between all routers in the local AS.

NOTE

In the NE80E/40E, the synchronization function is disabled by default.

Peer Group

A peer group is a group of peers with the same policies. After a peer is added to a peer group, it inherits the configurations of this peer group. When the configurations of the peer group are changed, the configurations of peers in the peer group are changed accordingly.

On a large-scale BGP network, there are a large number of peers and most of them have the same policies. To configure these peers, you have to repeatedly use some commands. In such a case, you can simplify configurations by using the peer group.

Adding many peers to a peer group also speeds up route advertisement.

Community

The community attribute is a route attribute. It is transmitted between BGP peers and is not restricted by the AS. A peer group allows a group of peers to share the same policies, whereas the community allows a group of BGP routers in multiple ASs to share the same policies.

Before a BGP router advertises the route with the community attribute to other peers, it can change the community attribute of this route.

Besides well-known communities, you can use a community filter to filter self-defined extended community attributes to control routing policies in a more flexible manner.

Route Reflector

To ensure the routing synchronization between IBGP peers, you need to establish full-mesh connections between the IBGP peers. If there are n routers in an AS, $n(n-1)/2$ IBGP connections need to be established. When there are a large number of IBGP peers, network resources and CPU resources are greatly consumed.

To solve this problem, route reflection is introduced. In an AS, one router functions as a route reflector (RR) and other routers serve as the clients of the RR. The clients establish IBGP connections with the RR. The RR transmits or reflects routes among clients, and the clients do not need to establish BGP connections.

A BGP router that is neither an RR nor a client is a non-client. Full-mesh connections must be established between non-clients and an RR, and between all non-clients.

Confederation

Confederation is another method of dealing with increasing IBGP connections in an AS. It divides an AS into several sub-ASs. IBGP connections are established between IBGP peers within each sub-AS, and EBGP connections are established between sub-ASs.

For BGP speakers outside a confederation, sub-ASs in the same confederation are invisible. External devices do not need to know the topology of each sub-AS. The confederation ID is the AS number that is used to identify the entire confederation.

The confederation has disadvantages. That is, if the router needs to be reconfigured in a confederation, the logical topology changes accordingly.

On a large-scale BGP network, the RR and confederation can be used together.

Introduction to MP-BGP

Traditional BGP-4 manages only IPv4 routing information and has limitations in inter-AS routing when used in the applications of other network layer protocols such as IPv6.

To support multiple network layer protocols, the Internet Engineering Task Force (IETF) extends BGP-4 to Multiprotocol Extensions for BGP-4 (MP-BGP). The current MP-BGP standard is RFC 2858 (Multiprotocol Extensions for BGP-4).

MP-BGP is forward compatible. That is, the routers that support MP-BGP can communicate with the routers that do not support MP-BGP.

Extended Attributes of MP-BGP

Among BGP-4 packets, an Update packet carries three IPv4-related attributes: Network Layer Reachability Information (NLRI), Next_Hop, and Aggregator. The Aggregator attribute contains the IP address of the BGP speaker that performs route summarization.

To support multiple types of network layer protocols, BGP-4 needs to carry network layer protocol information in the NLRI attribute and Next_Hop attribute. MP-BGP introduces two new route attributes:

- Multiprotocol Reachable NLRI (MP_REACH_NLRI): It is used to advertise reachable routes and next hops.
- Multiprotocol Unreachable NLRI (MP_UNREACH_NLRI): It is used to withdraw unreachable routes.

The two new attributes are optional non-transitive. Therefore, the BGP speakers that do not support the multiprotocol capability will ignore the two attributes, and do not advertise the information to peers.

Address Family

BGP uses address families to distinguish different network layer protocols. For the values of address families, see RFC 1700 (Assigned Numbers). The NE80E/40E supports multiple MP-BGP extensions, such as VPN extension and IPv6 extension, which are configured in their respective address family views.

 **NOTE**

This chapter does not describe the commands related to a specific application in the MP-BGP address family view.

For the configuration in the BGP IPv6 address family view, see the chapter "BGP4+ Configuration." For the application of MP-BGP in multicast, see the chapter "MBGP Configuration" in the *HUAWEI NetEngine80E/40E Router Configuration Guide - IP Multicast*.

For the configuration in the BGP VPNv4 address family view, BGP VPN instance address family view, and BGP L2VPN address family view, see the *HUAWEI NetEngine80E/40E Router Configuration Guide - VPN*.

BFD for BGP

The NE80E/40E supports Bidirectional Forwarding Detection (BFD) in IPv4 to provide fast link failure detection for BGP peer relationship.

BFD can rapidly detect faults on the links between BGP peers and report the faults to BGP, thus implementing fast convergence of BGP routes.

BGP GR

If BGP restarts, the peer relationship needs to be re-established and traffic forwarding is interrupted. After Graceful Restart (GR) is enabled, traffic interruption is avoided.

8.2 Configuring Basic BGP Functions

Configuring basic BGP functions is the prerequisite to building a BGP network.

8.2.1 Establishing the Configuration Task

Before configuring basic BGP functions, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

This section describes how to configure basic BGP functions.

Because BGP uses TCP connections, you need to specify the IP address of the peer when configuring BGP. The BGP peer may not be the neighboring router. The BGP peer relationship can also be established by using logical links. Loopback interface addresses are usually used to establish BGP connections to enhance the stability of these connections.

To configure BGP to advertise local routes and import default routes, see [Configuring BGP to Advertise Local Routes](#) and [Configuring BGP to Import Default Routes](#).

Most commands in the BGP extended address family view are the same as those in the BGP view. The commands run in the extended address family view, however, take effect only in related applications.

 **NOTE**

- In this section, BGP and MP-BGP are not distinguished from each other. For the applications of commands, see the views of the commands.
- Commands in the BGP-IPv4 unicast address family view can be run in the BGP view, facilitating the configuration. These commands are described in the BGP-IPv4 unicast address family view in configuration files.

Pre-configuration Tasks

Before configuring basic BGP functions, complete the following task:

- Configuring link layer protocol parameters and assigning IP addresses to interfaces to ensure that the link layer protocol of the interface is Up

Data Preparation

To configure basic BGP functions, you need the following data.

No.	Data
1	Local AS number and router ID
2	IPv4 address and AS number of a peer
3	Interface originating an Update message

8.2.2 Starting a BGP Process

Starting a BGP process is a prerequisite for configuring basic BGP functions. When starting a BGP process, you need to specify the number of the AS that a device belongs to.

Context

Do as follows on the router where a BGP connection needs to be established:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bgp as-number
```

A BGP process is enabled and the BGP view is displayed.

Step 3 (Optional) Run:

```
router-id ipv4-address
```

The router ID is set.

Configuring or changing the router ID of BGP causes the BGP peer relationship between routers to be reset.

 **TIP**

To enhance network reliability, configuring a loopback interface address as the router ID is recommended. If no router ID is set, BGP automatically selects the router ID in the system view as the router ID of BGP. For the rule for selecting a router ID in the system view, see the *HUAWEI NetEngine80E/40E Router Command Reference*.

----End

8.2.3 Configuring a BGP Peer

Devices can exchange BGP routing information only after BGP peers are configured and the BGP peer relationship is established.

Procedure

- Configuring an IBGP peer

Do as follows on the router where an IBGP connection needs to be established:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
peer ipv4-address as-number as-number
```

The IP address of the peer and the number of the AS where the peer resides are specified.

The number of the AS where the specified peer resides should be the same as the local AS number.

If the IP address of a specified peer is a loopback interface address or a sub-interface address, you need to complete the task of [Configuring the Local Interface for a BGP Connection](#) to ensure that the peer relationship is correctly established.

4. (Optional) Run:

```
peer { ipv4-address | group-name } description description-text
```

The description of a peer or a peer group is configured.

The descriptions are configured to simplify management.

- Configuring an EBGP peer

Do as follows on the router where an EBGP connection needs to be established:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
peer ipv4-address as-number as-number
```

The IP address of the peer and the number of the AS where the peer resides are specified.

The number of the AS where the specified peer resides should be different from the local AS number.

If the IP address of a specified peer is a loopback interface address or a sub-interface address, you need to complete the task of [Configuring the Local Interface for a BGP Connection](#) to ensure that the peer relationship is correctly established.

4. Run:

```
peer { ipv4-address | group-name } ebgp-max-hop [ hop-count ]
```

The maximum number of hops for an EBGP connection is set. By default, the maximum number of hops for an EBGP is 1.

Generally, there must be a directly connected physical link between EBGP peers. If there is no such a link, you need to run the `peer ebgp-max-hop` command to allow EBGP peers to establish TCP connections across multiple hops.

 **NOTE**

When establishing the EBGP peer relationship by using loopback interfaces, you need to run the `peer ebgp-max-hop` command in which *hop-count* is set to be greater than or equal to 2. Otherwise, the EBGP peer relationship cannot be established.

5. (Optional) Run:

```
peer { ipv4-address | group-name } description description-text
```

The description of a peer or a peer group is configured.

The descriptions are configured to simplify management.

---End

8.2.4 (Optional) Configuring the Local Interface for a BGP Connection

When establishing multiple peers between two devices through various links, you need to specify the local interface that is used for establishing a BGP session on the devices.

Context

When the interfaces whose IP addresses are used to establish peers are indirectly connected, do as follows on the routers:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bgp as-number
```

The BGP view is displayed.

Step 3 Run:

```
peer { ipv4-address | group-name } connect-interface interface-type interface-  
number [ ipv4-source-address ]
```

The local interface and source address, which are used by BGP to establish a TCP connection, are specified.

By default, BGP uses the physical interface that is directly connected to the peer as the local interface of a TCP connection.

To improve the stability and reliability of a BGP connection, you can configure a loopback interface as the local interface of the BGP connection. In this manner, when there are redundant links on the network, the BGP connection is not torn down due to the failure of a certain interface or a link.

 **NOTE**

When establishing multiple peers between two routers by using multiple links, run the **peer connect-interface** command to specify the interface through which a BGP connection is established.

----End

8.2.5 Checking the Configuration

After basic BGP functions are configured, you can check BGP peer information.

Prerequisite

The configurations of basic BGP functions are complete.

Procedure

- Run the **display tcp status** command to check TCP connection information.
- Run the **display bgp peer** [**verbose**] command to check BGP peer information.
- Run the **display bgp peer** *ipv4-address* { **log-info** | **verbose** } command to check BGP peer information.

----End

8.3 Configuring BGP Route Attributes

BGP has many route attributes. By configuring these attributes, you can change BGP routing policies.

8.3.1 Establishing the Configuration Task

Before configuring BGP route attributes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

BGP has many route attributes. You can set these attributes to change BGP routing policies.

- **BGP preference**
 Setting the BGP preference can affect route selection between BGP and another routing protocol.
- **PrefVal**
 After the PrefVals of BGP routes are set, the route with the greatest PrefVal is selected when there are multiple routes to the same destination in the BGP routing table.
- **Local_Pref**
 The Local_Pref attribute has the same function as the PrefVal attribute. The PrefVal attribute takes precedence over the Local_Pref attribute.
- **MED**
 After the MED attribute is set, EBGP peers select the route with the smallest MED for the incoming traffic of an AS.
- **Next_Hop**
 By setting the Next_Hop attribute, you can flexibly control BGP route selection.
- **Community**
 The community attribute is used to simplify the management of routing policies. The management scope of a community is much greater than that of a peer group. The community can control routing policies of multiple BGP routers.
- **AS_Path**
 The AS_Path attribute is used to prevent routing loops and control route selection.

Pre-configuration Tasks

Before configuring BGP route attributes, complete the following tasks:

- Assigning an IP address to each interface to make the neighboring nodes reachable on the network layer
- [8.2 Configuring Basic BGP Functions](#)

Data Preparation

To configure BGP route attributes, you need the following data.

No.	Data
1	AS number
2	BGP preference
3	Local_Pref
4	MED
5	Name of the routing policy to be applied if the community is used

8.3.2 Configuring the BGP Preference

Setting the BGP preference can affect route selection between BGP and another routing protocol.

Context

Do as follows on the BGP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bgp as-number
```

The BGP view is displayed.

Step 3 Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

Step 4 Run:

```
preference { external internal local | route-policy route-policy-name }
```

The BGP preference is set.

BGP has the following types of routes:

- Routes learned from EBGp peers
- Routes learned from IBGP peers
- Locally originated routes

Locally originated routes are the routes summarized by using commands, including the **summary automatic** command for automatic summarization and the **aggregate** command for manual summarization.

You can set different preferences for the three types of routes.

You can also use a routing policy to set preferences for the specified routes that meet the matching rules. You can set the default preference for the routes that do not meet the matching rules.

NOTE

Currently, the **peer route-policy** command cannot be used to apply routing policies on peers to set the BGP preference.

----End

8.3.3 Configuring the BGP Preferred Value for Routing Information

After preferred values are configured for routes, the route with the greatest preferred value is selected when multiple routes to the same destination exist in the BGP routing table.

Context

Do as follows on the BGP router:

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`bgp as-number`
The BGP view is displayed.
- Step 3** Run:
`peer { group-name | ipv4-address } preferred-value value`
The preferred value is set for a peer.
By default, the original preferred value of the route learned from a peer is 0.
----End

8.3.4 Configuring the Default Local_Pref Attribute

The Local_Pref attribute is used to select the optimal route for the outgoing traffic of an AS. When a BGP router learns multiple routes to the same destination but with different next hops from different IBGP peers, the route with the highest Local_Pref is selected.

Context

Do as follows on the BGP router:

Procedure

- Step 1** Run:
`system-view`
The system view is displayed.
- Step 2** Run:
`bgp as-number`
The BGP view is displayed.
- Step 3** Run:
`ipv4-family unicast`
The BGP IPv4 unicast address family view is displayed.
- Step 4** Run:
`default local-preference preference`
The default Local_Pref attribute is set for the local router.
----End

8.3.5 Configuring the MED Attribute

The MED attribute is similar to the metric used by an IGP. After MED attributes are set, EBGP peers select the route with the smallest MED value for the incoming traffic of an AS.

Procedure

- Setting the default MED of the local router

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

4. Run:

```
default med med
```

The default MED is set.

- Comparing the MEDs of routes from different ASs

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

4. Run:

```
compare-different-as-med
```

The MEDs of routes from different ASs are compared.

Generally, a BGP router compares only the MEDs of routes from different peers in the same AS. After this command is used, you can allow BGP to compare the MEDs of routes from different ASs.

- Configuring the deterministic-MED

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```


The BGP view is displayed.

3. Run:

```
deterministic-med
```

The deterministic-MED is enabled.

If this command is not configured, when an optimal route is to be selected from among routes that are received from different ASs and that carry the same prefix, the sequence in which routes are received is relevant to the result of route selection. After the command is configured, however, when an optimal route is to be selected from among routes that are received from different ASs and that carry the same prefix, routes are first grouped according to the leftmost AS in the AS_Path. Routes with the same leftmost AS are grouped together, and after comparison, an optimal route is selected for the group. The group optimal route is then compared with optimal routes from other groups to determine the final optimal route. This mode of route selection ensures that the sequence in which routes are received is irrelevant to the result of route selection.

- Configuring the processing method when the MED is not set

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

4. Run:

```
bestroute med-none-as-maximum
```

The MED is set to the maximum value if there is no MED in route attributes.

If this command is configured, BGP uses the maximum value of the MED if there is no MED in route attributes during route selection. If this command is not configured, the MED is 0.

- Comparing the MEDs of routes in a confederation

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

4. Run:
`bestroute med-confederation`

The MEDs of routes in a confederation are compared.

---End

8.3.6 Configuring the Next_Hop Attribute

By setting the Next_Hop attribute, you can flexibly control BGP route selection.

Procedure

- Changing the next-hop address when advertising a route to an IBGP peer

Do as follows on the IBGP router:

1. Run:
`system-view`

The system view is displayed.

2. Run:
`bgp as-number`

The BGP view is displayed.

3. Run:
`ipv4-family unicast`

The BGP IPv4 unicast address family view is displayed.

4. Run:
`peer { ipv4-address | group-name } next-hop-local`

The address of the router is set as the next-hop address when the router advertises routes.

On certain networks, to ensure that an IBGP peer finds the correct next hop, you can configure the router to change the next-hop address of a route to the address of the router when the router advertises the route to its IBGP peer. By default, the router does not change the next-hop address when advertising a route to its IBGP peer.

NOTE

If BGP load balancing is configured, the local router changes the next-hop address of a route to its own address when advertising the route to an IBGP peer group, regardless of whether the `peer next-hop-local` command is configured.

- Keeping the next-hop address unchanged when advertising a route learned from an IGP to an IBGP peer

Do as follows on the IBGP router that imports IGP routes:

1. Run:
`system-view`

The system view is displayed.

2. Run:
`bgp as-number`

The BGP view is displayed.

3. Run:
`ipv4-family unicast`

The BGP IPv4 unicast address family view is displayed.

4. Run:
`peer { ipv4-address | group-name } next-hop-invariable`

The router is configured to keep the next-hop address unchanged when advertising an imported IGP route to its peer.

By default, when the router advertises an imported IGP route to its peer, it changes the next-hop address to the address of the interface connecting it to the peer.

- Keeping the next-hop address unchanged when advertising a route to an EBGP peer

Do as follows on the PE router:

1. Run:
`system-view`
 The system view is displayed.

2. Run:
`bgp as-number`
 The BGP view is displayed.

3. Run:
`ipv4-family vpnv4 [unicast]`
 The BGP VPNv4 address family view is displayed.

4. Run:
`peer { group-name | ipv4-address } next-hop-invariable`
 The PE router is configured to keep the next-hop address unchanged when advertising a route to an EBGP peer.

By default, PEs in different ASs establish EBGP peer relationships, and change the next-hop address when advertising routes.

- Next-hop iteration based on the routing policy

Do as follows on the BGP router:

1. Run:
`system-view`
 The system view is displayed.

2. Run:
`bgp as-number`
 The BGP view is displayed.

3. Run:
`ipv4-family unicast`
 The BGP IPv4 unicast address family view is displayed.

4. Run:
`nexthop recursive-lookup route-policy route-policy-name`

Next-hop iteration based on the specified routing policy is configured.

By default, next-hop iteration based on the specified routing policy is not configured.

Next-hop iteration based on the routing policy can control the iterated route according to certain conditions. The route that fails to match the routing policy is ignored.

----End

8.3.7 Configuring BGP to Advertise the Community Attribute

The community attribute is used to simplify the management of routing policies. The management scope of a community is much greater than that of a peer group. The community attribute can control routing policies of multiple BGP routers.

Procedure

- Configuring BGP to advertise the community attribute to peers

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

4. Run the following command as required:

- Run:

```
peer { ipv4-address | group-name } advertise-community
```

BGP is configured to advertise the standard community attribute to a peer or peer group.

By default, the community attribute is not advertised to any peer or peer group.

- Run:

```
peer { ipv4-address | group-name } advertise-ext-community
```

BGP is configured to advertise the extended community attribute to a peer or peer group.

By default, the extended community attribute is not advertised to any peer or peer group.

- Applying routing policies to the advertised routes

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:
`bgp as-number`
The BGP view is displayed.
3. Run:
`ipv4-family unicast`
The BGP IPv4 unicast address family view is displayed.
4. Run:
`peer { ipv4-address | group-name } route-policy route-policy-name export`
The outbound routing policy is configured.

 **NOTE**

When configuring a BGP community, you need to use a routing policy to define the specific community attribute, and apply this routing policy when routes are advertised.

For the configuration of a routing policy, see [Routing Policy Configuration](#).

----End

8.3.8 Configuring the AS-Path Attribute

The AS_Path attribute is used to prevent routing loops and control route selection.

Procedure

- Allowing the Local AS Number to Be Repeated

Do as follows on the BGP router:

1. Run:
`system-view`
The system view is displayed.
2. Run:
`bgp as-number`
The BGP view is displayed.
3. Run:
`ipv4-family unicast`
The BGP IPv4 unicast address family view is displayed.
4. Run:
`peer { ipv4-address | group-name } allow-as-loop [number]`
The local AS number can be repeated.

Generally, BGP checks the AS_Path attribute of a route sent from the peer. If the AS_Path attribute of the route contains the local AS number, BGP ignores this route to prevent route loops.

In special cases, you can use this command to allow the AS_Path attribute of a route sent from a peer to contain the local AS number. You can also set the number of times that the local AS number is repeated.

- Configuring BGP not to consider the AS_Path attribute as a route selection rule

Do as follows on the BGP router:

1. Run:
`system-view`
The system view is displayed.
2. Run:
`bgp as-number`
The BGP view is displayed.
3. Run:
`ipv4-family unicast`
The BGP IPv4 unicast address family view is displayed.
4. Run:
`bestroute as-path-ignore`
The AS_Path attribute is not considered as a route selection rule.

- Setting a fake AS number

Do as follows on the BGP router:

1. Run:
`system-view`
The system view is displayed.
2. Run:
`bgp as-number`
The BGP view is displayed.
3. Run:
`peer { ipv4-address | group-name } fake-as fake-as-number`

A fake AS number is set.

The actual AS number is hidden after this command is run. EBGP peers in other ASs can learn only the fake AS number. That is, when peers in other ASs need to specify the number of the AS where the local peer resides, the specified AS number needs to be set as the fake AS number.

 NOTE

This command applies only to EBGP peers.

- Substituting the AS number in the AS_Path attribute

Do as follows on the BGP router:



CAUTION

If the `peer substitute-as` command is configured improperly, routing loops occur. Therefore, you need to configure this command with caution.

1. Run:
`system-view`
The system view is displayed.

2. Run:
`bgp as-number`

The BGP view is displayed.

3. Run:
`ipv4-family vpn-instance vpn-instance-name`

The BGP VPN instance IPv4 address family view is displayed.

4. Run:
`peer { ipv4-address | group-name } substitute-as`

The AS number in the AS_Path attribute is substituted.

After this command is run, if the AS_Path attribute of a route contains the AS number of the peer, you can substitute the local AS number for the AS number of the peer before advertising the route to the peer.

- Configuring the AS_Path attribute to carry only the public AS number

Do as follows on the BGP router:

1. Run:
`system-view`

The system view is displayed.

2. Run:
`bgp as-number`

The BGP view is displayed.

3. Run:
`ipv4-family unicast`

The BGP IPv4 unicast address family view is displayed.

4. Run:
`peer { ipv4-address | group-name } public-as-only`

The AS_Path attribute is configured to carry only the public AS number.

Generally, the AS number ranges from 1 to 4294967295. The public AS number ranges from 1 to 64511, and from 65536 (such as 1.0 in the format of x.y) to 4294967295 (such as 65535.65535 in the format of x.y), and the private AS number ranges from 64512 to 65534. The AS number 65535 is reserved for special use.

The public AS number can be used on the Internet, and are managed and assigned by the Internet Assigned Number Authority (IANA). The private AS number cannot be advertised to the Internet and is used only in a routing domain.

Generally, a route carries an AS number (either public or private) when being advertised to a peer. In certain cases, however, the private AS number does not need to be advertised. Then you can configure the AS_Path attribute to carry only the public AS number by using this command.

This command applies only to EBGp peers.

- Configuring the maximum number of AS numbers in the AS_Path attribute

Do as follows on the BGP router:

1. Run:
`system-view`
The system view is displayed.

2. Run:
`bgp as-number`
The BGP view is displayed.

3. Run:
`as-path-limit as-path-limit-num`
The maximum number of AS numbers in the AS_Path attribute is set.
By default, the maximum number of AS numbers in the AS_Path attribute is 255.

After the `as-path-limit` command is configured, the router checks whether the number of AS numbers in the AS_Path attribute of the incoming route exceeds the maximum value. If the number of AS numbers exceeds the maximum value, the router discards the route. Therefore, if the maximum number of AS numbers in the AS_Path attribute is set too small, routes are lost.

- Disabling BGP from checking the first AS number in the AS_Path attribute in the Update message sent by an EBGP peer

Do as follows on the BGP router:

1. Run:
`system-view`
The system view is displayed.

2. Run:
`bgp as-number`
The BGP view is displayed.

3. Run:
`undo check-first-as`
BGP is disabled from checking the first AS number in the AS_Path attribute in the Update message sent by an EBGP peer.

By default, BGP checks the first AS number in the AS_Path attribute in the Update message sent by an EBGP peer. If the first AS number is the number of the AS where the EBGP peer resides, the Update message is accepted. Otherwise, the Update message is rejected, and the EBGP connection is torn down.



If the `undo check-first-as` command is configured, there is a greater possibility of routing loops. Therefore, use the command with caution.

After modifying configurations, you need to run the `refresh bgp` command.

----End

8.3.9 Checking the Configuration

After BGP route attributes are configured, you can check information about route attributes.

Prerequisite

The configurations of BGP route attributes are complete.

Procedure

- Run the **display bgp paths** [*as-regular-expression*] command to check information about the AS_Path attribute.
- Run the **display bgp routing-table different-origin-as** command to check the routes that have the same destination but different source ASs.
- Run the **display bgp routing-table regular-expression** *as-regular-expression* command to check the routes matching the regular expression of the AS.
- Run the **display bgp routing-table** [*network*] [*mask* | *mask-length*] [**longer-prefixes**] command to check information about the BGP routing table.
- Run the **display bgp routing-table community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**] command to check routing information about the specified BGP community.
- Run the **display bgp routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* } command to check the routes matching the specified BGP community filter.

----End

8.4 Configuring BGP Filters

By using routing policies, BGP can flexibly send and receive routes.

8.4.1 Establishing the Configuration Task

Before configuring BGP filters, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

With the following powerful filters, BGP can flexibly send and receive routes.

- Access list
BGP has two private access lists, namely, the AS_Path filter and community filter. These lists can be used to display the BGP running status and used in routing policies.
The AS_Path filter is used to match the AS_Path attribute in a BGP route and filter the routes that do not meet the matching condition. You can define multiple rules (permit or deny) for the same AS_Path filter.
The community filter lists a series of community attributes. The community attribute lists are classified into two types, that is, standard community lists and extended community lists.

- **Route-policy**
 A route-policy is used to match certain routes or certain route attributes, and to change these attributes if certain matching conditions are met. The preceding lists can be used as the matching conditions.
 A route-policy consists of multiple nodes. Each node contains the following clauses:
 - **if-match** clause: defines matching rules, namely, matching conditions to be met before a route matches a route-policy. The matching objects are some route attributes.
 - **apply** clause: specifies actions, namely, configuration commands to be run after the matching conditions specified by **if-match** clauses are met. The **apply** clauses can be used to change some route attributes.
- **Controlling the received routes**
 BGP can filter the globally received routes or only the routes received from a certain peer or a peer group by using routing policies.
 A BGP router may be prone to service attacks. For example, a BGP router may receive a large number of routes from neighbors, and thus a lot of resources are consumed. In this case, the administrator must limit the consumed resources according to network planning and capacity of the router, regardless of whether malicious attacks or incorrect configurations result in too many BGP routes. BGP can control peers to limit the number of routes sent by peers.
- **Resetting BGP connections**
 After changing a BGP routing policy, you need to reset a BGP connection to make the new configuration take effect. This operation, however, temporarily interrupts the BGP connection.
 On the NE80E/40E, BGP supports the route-refresh capability. That is, after a routing policy is changed, the system can dynamically refresh the BGP routing table without interrupting BGP connections.
 If neighbors of the router support the route-refresh capability, you can run the **refresh bgp** command on the router to manually perform soft reset on their BGP connections. The routing table of the router is then refreshed.
 If neighbors of the router do not support the route-refresh capability, you can run the **peer keep-all-routes** command on the router to refresh the BGP routing table of the router.

Pre-configuration Tasks

Before configuring BGP filters, complete the following task:

- **Configuring Basic BGP Functions**

Data Preparation

To configure BGP filters, you need the following data.

No.	Data
1	Community attribute value
2	ACL number
3	Route-policy name, node sequence number, and matching condition

No.	Data
4	Names of inbound and outbound routing policies

8.4.2 Configuring Related Access Lists

By configuring ACLs, you can filter the unrequired routes as required.

Procedure

- Configuring an AS_Path filter

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ip as-path-filter { as-path-filter-number | as-path-filter-name }  
{ permit | deny } regular-expression
```

An AS_Path filter is configured.

If the **peer as-path-filter** command is used to apply a routing policy to BGP routes, the routes that do not meet the matching conditions are filtered based on the AS_Path filter.

The AS_Path filter defines the matching conditions by using the regular expression. The regular expression consists of the following parts:

- Metacharacter: defines matching conditions.
- General character: defines matching objects.

Table 8-1 Metacharacter description

Metacharacter	Description
\	Indicates an escape character.
.	Matches any single character except "\n", including spaces.
*	Indicates that the characters to its left are displayed 0 times or multiple consecutive times in the target object.
+	Indicates that the characters to its left are displayed once or multiple consecutive times in the target object.
	Matches either expression it separates.
^	Indicates that the characters to its right must be displayed at the beginning of the target object.
\$	Indicates that the characters to its left must be displayed at the end of the target object.

Metacharacter	Description
[xyz]	Matches any character in the square brackets.
[^xyz]	Matches a single character that is not contained in the square brackets (The "^" is to the left of the character).
[a-z]	Matches any character within the specified range.
[^a-z]	Matches any character that is not within the specified range.
{n}	The matching is displayed n times (n is a non-negative integer).
{n,}	The matching is displayed at least n times (n is a non-negative integer).
{n,m}	The matching is displayed n to m times. m and n are non-negative integers, and n is smaller than or equal to m. There is no space between n and m.

For example, ^10 indicates that only the AS_Path attribute with the first value being 10 is matched. ^ specifies the beginning of a string character.

You can define multiple matching rules (permit or deny) for the same filter. During the matching, the relationship between these rules is "OR". That is, if a route meets one matching rule, the route passes this AS_Path filter.

 **NOTE**

For details of the regular expression, see the chapter "Command Line Introduction" in the *HUAWEI NetEngine80E/40E Router Configuration Guide - Basic Configurations*.

- **Configuring the community filter**

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
ip community-filter
```

The community filter is configured.

- Run:

```
ip community-filter { basic comm-filter-name { permit | deny }
[ community-number | aa:nn ] * <1-9> | basic-comm-filter-num { permit
| deny } [ community-number | aa:nn ] * <1-16> } [ internet | no-export-
subconfed | no-advertise | no-export ] *
```

The standard community filter is configured.

- Run:

```
ip community-filter { advanced comm-filter-name | adv-comm-filter-num }
{ permit | deny } regular-expression
```

The advanced community filter is configured.

- Configuring the extended community filter

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. To configure the extended community filter, run the following command:

- Run:

```
ip extended-community-filter { basic-extended-community-filter-num | basic basic-extended-community-filter-name } { deny | permit } { rt { as-number:nn | ipv4-address:nn } } &<1-16>
```

The list of basic extended community filter is configured.

- Run:

```
ip extended-community-filter { adv-extended-community-filter-num | advanced adv-extended-community-filter-name } { deny | permit } regular-expression
```

The list of advanced extended community filter is configured.

You can define many entries for the same extended community filter. The relationship between these entries is "OR". That is, when the route matches one entry in the list, it means that the route passes the attribute list.

----End

8.4.3 Configuring Related Routing Policies

By configuring routing policies, you can filter routes or set route attributes.

Context



NOTE

This section describes only the routing policies related to BGP. For details of the route-policy, refer to [Routing Policy Configuration](#).

Procedure

- Creating a Routing Policy

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
route-policy route-policy-name { permit | deny } node node
```

A node of a route-policy is created, and the route-policy view is displayed.

- Configuring the **if-match** Clause

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
route-policy route-policy-name { permit | deny } node node
```

The route-policy view is displayed.

3. Run the following command as required:

- Run:

```
if-match as-path-filter { as-path-filter-number | as-path-filter-name } &<1-16>
```

The AS-Path attribute of the BGP route is matched.

- Run:

```
if-match community-filter { basic-comm-filter-num [ whole-match ] | adv-comm-filter-num }* &<1-16>  
if-match community-filter comm-filter-name [ whole-match ]
```

The community attribute of the BGP route is matched.

- Run:

```
if-match extcommunity-filter { { basic-extcomm-filter-num | adv-extcomm-filter-num } &<1-16> | basic-extcomm-filter-name | advanced-extcomm-filter-name }
```

The BGP extended community attribute is matched.

You can run the commands in Step 3 regardless of the sequence. There may be no **if-match** clause or multiple **if-match** clauses in a node.

 **NOTE**

- For the same node of a Route-Policy, the relationship between **if-match** clauses is AND. That is, only when the route meets all the matching rules, you can perform the actions defined by the **apply** clauses.
 - If the **if-match** clause is not specified, all the routes can pass the filtering of the node.
- Configuring the **apply** Clause

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
route-policy route-policy-name { permit | deny } node node
```

The route-policy view is displayed.

3. To configure the **apply** clause of the current node for the routing policy, run the following command:

- Run:

```
apply as-path as-number
```

The specified AS number is substituted or added to the AS-Path of BGP.

- Run:

```
apply comm-filter comm-filter-number delete
```

The specified BGP community attribute is deleted.

 **TIP**

The **apply comm-filter delete** command is used to delete the community attribute according to the specified value in the community filter. Each community filter defined by the **ip community-filter** command contains only one community attribute. If you want to delete several community attributes, use the **ip community-filter** command several times. If multiple community attributes are configured under the same filter number, these attributes cannot be deleted. For details of the example, refer to the *HUAWEI NetEngine80E/40E Router Command Reference*.

- Run:

```
apply community none
```

The community attribute of a BGP route is deleted.

- Run:

```
apply community { { community-number | aa:nn } &<1-32> | internet | no-advertise | no-export | no-export-subconfed }* [ additive ]
```

The community attribute of a BGP route is set.

- Run:

```
apply extcommunity { rt { as-number:nn | ipv4-address:nn } } &<1-16> [ additive ]
```

The BGP extended community attribute is set.

- Run:

```
apply local-preference preference
```

The local preference of a BGP route is set.

- Run:

```
apply origin { igp | egp as-number | incomplete }
```

The Origin attribute of a BGP route is set.

- Run:

```
apply preferred-value preferred-value
```

The PrefVal of a BGP route is set.

- Run:

```
apply dampening half-life-reach reuse suppress ceiling
```

Dampening parameters of EBGp routes are set.

You can run the commands in Step 3 regardless of the sequence.

---End

8.4.4 Configuring the Policy for Advertising BGP Routing Information

After the policy for advertising routes is configured, only the routes that match the policy can be added to the local BGP routing table and then advertised to BGP peers.

Procedure

- Configuring BGP to Filter the Globally Advertised Routes

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:
`bgp as-number`

The BGP view is displayed.

3. Run:
`ipv4-family unicast`

The BGP IPv4 unicast address family view is displayed.

4. Run:
`filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name } export [protocol [process-id]]`

The advertised routes are filtered.

After BGP filters the imported routes, only the routes that meet the matching rules are added to the local BGP routing table and advertised to BGP peers.

If *protocol* is specified, you can filter the routes of a specific routing protocol. If *protocol* is not specified, all the routes to be advertised are filtered, including the routes imported and the local routes advertised with the `network` command.

 **NOTE**

If the ACL is used in the `filter-policy` command and no VPN instance is specified in the ACL rules, BGP filters routes in all the address family views, including routes of the public network and the private network. If a VPN instance is specified, BGP filters data traffic from this VPN instance rather than the routes.

- Applying a Policy to the Routes Advertised by Specified BGP Peers

Do as follows on the BGP router:

1. Run:
`system-view`
 The system view is displayed.
2. Run:
`bgp as-number`
 The BGP view is displayed.
3. Run:
`ipv4-family unicast`
 The BGP IPv4 unicast family view is displayed.
4. Run:
`peer { ipv4-address | group-name } route-policy route-policy-name export`

The routing policy applied when routes are advertised is configured.

 **NOTE**

The routing policy applied in the `peer route-policy export` command does not support a certain interface as one of the matching rules. That is, the routing policy does not support the `if-match interface` command.

- Applying a Filter to the Routes Advertised by Specified BGP Peers

Do as follows on the BGP router:

1. Run:
`system-view`
The system view is displayed.
2. Run:
`bgp as-number`
The BGP view is displayed.
3. Run:
`ipv4-family unicast`
The BGP IPv4 unicast family view is displayed.
4. Run the following command as required:
 - Run:
`peer { ipv4-address | group-name } filter-policy { acl-number | acl-name acl-name } export`
BGP is configured to filter routes according to the ACL.
 - Run:
`peer { ipv4-address | group-name } as-path-filter { as-path-filter-number | as-path-filter-name } export`
BGP is configured to filter routes according to the AS-Path filter.
 - Run:
`peer { ipv4-address | group-name } ip-prefix ip-prefix-name export`
BGP is configured to filter routes according to the IP prefix list.
The members of a peer group and the peer group can use different outbound routing policies. That is, each peer group can select its policy when advertising routes.

----End

8.4.5 Configuring the Policy for Receiving BGP Routing Information

Only the routes that match the policy for receiving routes can be received by BGP and added to the routing table.

Procedure

- Configuring BGP to Filter All the Received Routes

Do as follows on the BGP router:

1. Run:
`system-view`
The system view is displayed.
2. Run:
`bgp as-number`
The BGP view is displayed.
3. Run:
`ipv4-family unicast`

The BGP IPv4 unicast address family view is displayed.

4. Run:

```
filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name } import
```

All the received routes are filtered.

The routes received by BGP are filtered. Only those routes that meet matching rules are received by BGP and added to the routing table.

- Applying a Routing Policy to the Routes Received by Specified Peers

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

4. Run:

```
peer { ipv4-address | group-name } route-policy route-policy-name import
```

A routing policy is applied to the received routes.

 **NOTE**

The routing policy applied in the **peer route-policy import** command does not support a certain interface as one of the matching rules. That is, the routing policy does not support the **if-match interface** command.

- Applying a Filter to the Routes Received by Specified Peers

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

4. Run the following command as required:

- Run:

```
peer { ipv4-address | group-name } filter-policy { acl-number | acl-name acl-name } import
```

BGP is configured to filter routes according to the ACL.

- Run:

```
peer { ipv4-address | group-name } as-path-filter { as-path-filter-  
number | as-path-filter-name } import
```

BGP is configured to filter routes according to the AS-Path filter.

- Run:

```
peer { ipv4-address | group-name } ip-prefix ip-prefix-name import
```

BGP is configured to filter routes according to the IP prefix list.

The members of a peer group and the peer group can use different outbound policies to filter routes. That is, each peer group can select its policy when receiving routes.

- Limiting the Number of Routes Received by a Peer

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
peer { group-name | ipv4-address } route-limit limit [ percentage ]  
[ alert-only | idle-forever | idle-timeout times ]
```

The number of routes received by a peer or peer group is set.

The command can be used to control the number of routes received from a peer. You can configure specific parameters as required to control BGP after the number of the routes received from a peer exceeds the threshold.

- **alert-only**: The peer relationship is not interrupted. The peer does not receive any routes that exceed the threshold, and an alarm is generated and recorded in the log.
- **idle-forever**: The peer relationship is interrupted. The router does not retry setting up a connection. An alarm is generated and recorded in the log. Run the **display bgp peer [verbose]** command, you can view that the status of the peer is Idle. If you want to restore the BGP connection, run the **reset bgp** command.
- **idle-timeout**: The peer relationship is interrupted. The router retries setting up a connection after the timer expires. An alarm is generated and recorded in the log. Run the **display bgp peer [verbose]** command. You can view that the status of the peer is Idle. If you want to restore the BGP connection before the timer expires, run the **reset bgp** command.
- If the three parameters are not set, the peer relationship is disconnected. The router retries setting up a connection after 30 seconds. An alarm is generated and recorded in the log.

----End

8.4.6 Configuring BGP Soft Resetting

When routing policies are changed, the system can refresh the BGP routing table dynamically without interrupting BGP connections.

Procedure

- Enabling the Route-Refresh Capability

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
peer { ipv4-address | group-name } capability-advertise { route-refresh |  
4-byte-as | conventional }
```

The Route-Refresh capability is enabled.

If the Route-Refresh capability is enabled on all BGP routers, the local router advertises Route-Refresh messages to its peer if the BGP routing policy changes. Upon receiving this message, the peer sends the message to the local router again. In this case, the BGP routing table is dynamically refreshed and the new policy is applied without interrupting BGP connections.

- Keeping All the Routing Updates of the Peers

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

4. Run:

```
peer { ipv4-address | group-name } keep-all-routes
```

All the routing updates of the peer are kept.

After this command is used, all routing updates of the specified peer are kept regardless of whether the filtering policy is used. When BGP connections are soft reset, this information can be used to generate BGP routes.

- Soft Resetting BGP Connections

Do as follows on the BGP router:

1. Run:

```
refresh bgp [ vpn-instance vpn-instance-name | vpnv4 ] { all | ipv4-  
address | group group-name | external | internal } { export | import }
```

BGP connections are soft reset.

Run the **refresh bgp** command in the user view.

----End

8.4.7 Checking the Configuration

After BGP filters are configured, you can check the routes that match the specified filter.

Prerequisite

The configurations of BGP filters are complete.

Procedure

- Run the **display bgp network** command to check the routes advertised by BGP.
- Run the **display bgp routing-table as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } command to check the routes matching the specified AS-path filter.
- Run the **display bgp routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* } command to check the routes matching the specified BGP community attribute filter.
- Run the **display bgp routing-table peer ipv4-address** { **advertised-routes** | **received-routes** } [**statistics**] command to check the routes advertised or received by BGP peers.

----End

8.5 Controlling the Advertisement of BGP Routing Information

BGP can perform routing policies on or filter only the routes to be advertised to a certain peer.

8.5.1 Establishing the Configuration Task

Before controlling the advertisement of BGP routes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

- BGP route aggregation
In medium or large BGP networks, route aggregation needs to be configured when the routes are advertised to the peers. This reduces the size of the routing table. BGP supports automatic aggregation and manual aggregation.
- Controlling the advertised routes
BGP can filter or perform routing policies on only the routes advertised by a certain peer or a peer group.

Pre-configuration Tasks

Before controlling BGP route advertisement, complete the following task:

- [8.2 Configuring Basic BGP Functions](#)

Data Preparation

To control the advertisement of BGP routing information, you need the following data.

No.	Data
1	Aggregation mode and route aggregated

8.5.2 Configuring BGP to Advertise Local Routes

The local routes to be advertised must be in the local IP routing table. You can use routing policies to control the routes to be advertised more flexibly.

Context

Do as follows on the BGP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bgp as-number
```

The BGP view is displayed.

Step 3 (Optional) Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

By default, the command is used in the IPv4 unicast address family view.

Step 4 Run:

```
network ipv4-address [ mask | mask-length ] [ route-policy route-policy-name ]
```

BGP is configured to advertise the exactly-matched local routes.

To be specific, the command can be used to advertise the routes only with the exactly-matched address prefix and mask. If the mask is not designated, the routes are exactly matched based on the natural network segment.

The local routes to be advertised should be in the local IP routing table. You can use routing policies to control the routes to be advertised more flexibly.

----End

8.5.3 Configuring BGP Route Aggregation

By configuring route aggregation, you can reduce the size of the routing table of a peer. BGP supports automatic aggregation and manual aggregation.

Procedure

- Configuring Automatic Aggregation

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv4-family unicast
```

The BGP IPv4 view is displayed.

4. Run:

```
summary automatic
```

Automatic aggregation of the subnet routes is configured.

The command is used to aggregate the routes imported by BGP. These routes can be direct routes, static routes, RIP routes, OSPF routes, or IS-IS routes. The command, however, is invalid for the routes imported with the **network** command.

- Configuring Manual Aggregation

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

4. Run:

```
aggregate ipv4-address { mask | mask-length } [ as-set | attribute-policy  
route-policy-name1 | detail-suppressed | origin-policy route-policy-name2  
| suppress-policy route-policy-name3 ] *
```

Manual route aggregation is configured.

Manual aggregation is valid for the entries in the local BGP routing table. For example, if 10.1.1.1/24 does not exist in the BGP routing table, BGP does not advertise the aggregated route after the **aggregate 10.1.1.1 16** command is used to aggregate routes.

You can apply multiple policies and configure the route attributes through manual aggregation.

----End

8.5.4 Configuring a Router to Advertise Default Routes to Its Peer

A router sends a default route with the local address being the next hop to the specified peer, regardless of whether there are default routes in the local routing table.

Context

Do as follows on the BGP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bgp as-number
```

The BGP view is displayed.

Step 3 Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

Step 4 Run:

```
peer { group-name | ipv4-address } default-route-advertise [ route-policy route-policy-name ] [ conditional-route-match-all { ipv4-address1 { mask1 | mask-length1 } } <1-4> | conditional-route-match-any { ipv4-address2 { mask2 | mask-length2 } } <1-4> ]
```

The default route is sent to its peer or peer group.

NOTE

After the **peer default-route-advertise** command is used, the router sends a default route with the local address as the next hop to the specified peer, regardless of whether there are default routes in the routing table.

----End

8.5.5 Checking the Configuration

After the advertisement of BGP routes is controlled, you can check the advertised routes that match the specified filter.

Prerequisite

The configurations of controlling the advertisement of BGP routing information are complete.

Procedure

- Run the **display bgp network** command to check the routes advertised by BGP.
- Run the **display bgp routing-table cidr** command to check the routes of CIDR.
- Run the **display bgp routing-table peer ipv4-address { advertised-routes | received-routes } [statistics]** command to check the routes advertised and received by BGP peers.

----End

8.6 Controlling the Import of Routing Information

Importing routes of other routing protocols can enrich the BGP routing table. When importing IGP routes, BGP can filter the routes according to different routing protocols.

8.6.1 Establishing the Configuration Task

Before controlling the import of routes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

BGP can send internal routes to its neighboring ASs, but it does not discover internal routes by itself. Instead, it imports IGP routes to the BGP routing table and advertises the BGP routing table to the peers. When importing IGP routes, BGP can filter routes according to the types of routing protocol.

Pre-configuration Tasks

Before controlling the import of routes, complete the following task:

- [Configuring Basic BGP Functions](#)

Data Preparation

None.

8.6.2 Configuring BGP to Import Default Routes

Only the default routes that exist in the local routing table can be imported.

Context

Do as follows on the BGP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bgp as-number
```

The BGP view is displayed.

Step 3 Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

Step 4 Run:

```
default-route imported
```

BGP is configured to import default routes.

----End

8.6.3 Configuring BGP to Import Routes

BGP can import the routes of other routing protocols. When the routes of dynamic routing protocols need to be imported, you need to specify the process ID of the protocol. Using routing policies can flexibly import required routes.

Context

Do as follows on the BGP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bgp as-number
```

The BGP view is displayed.

Step 3 Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

Step 4 Run:

```
import-route protocol [ process-id ] [ med med | route-policy route-policy-name ] *
```

BGP is configured to import routes discovered by other protocols.

 **NOTE**

When the type of an imported route is IS-IS, OSPF, or RIP, you must specify the process ID.

If the **default-route imported** command is not used, the default routes cannot be imported when you run the **import-route** command to import routes of other protocols.

----End

8.6.4 Checking the Configuration

After the import of routes is controlled, you can check the imported routes that match the specified filter.

Prerequisite

The configurations of controlling the import of routing information are complete.

Procedure

- Run the **display bgp routing-table as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } command to check the routes matching the specified AS-Path filter.
- Run the **display bgp routing-table cidr** command to check the routes of CIDR.
- Run the **display bgp routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* } command to check the routes matching the specified BGP community attribute filter.

----End

8.7 Configuring BGP Route Dampening

By configuring BGP route dampening, you can suppress unstable BGP routes.

8.7.1 Establishing the Configuration Task

Before configuring BGP route dampening, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

BGP dampening can suppress unstable routes. Thus, BGP does not add unstable routes to the routing table, and consequently no unstable route is advertised to other BGP peers.

Pre-configuration Tasks

Before configuring BGP route dampening, complete the following task:

- [Configuring Basic BGP Functions](#)

Data Preparation

To configure BGP route dampening, you need the following data.

No.	Data
1	Various parameters of dampening, including half-life of a reachable route, threshold for releasing the suppressed routes, threshold for suppressing routes, and upper threshold of the penalty

8.7.2 Configuring BGP Route Dampening

BGP route dampening can improve network stability. You can flexibly use routing policies for route dampening.

Context

Do as follows on the BGP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bgp as-number
```

The BGP view is displayed.

Step 3 Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast family view is displayed.

Step 4 Run:

```
dampening [ half-life-reach reuse suppress ceiling | route-policy route-policy-name ] *
```

Parameters are set for BGP route dampening.

When you configure BGP route dampening, the values of *reuse*, *suppress*, and *ceiling* should meet the relationship of *reuse*<*suppress*<*ceiling*.

The **dampening** command is applicable only to the EBGp routes.

----End

8.7.3 Checking the Configuration

After BGP route dampening is configured, you can check BGP suppressed routes, parameters of BGP route dampening, and flapped routes.

Prerequisite

The configurations of BGP route dampening are complete.

Procedure

- Run the **display bgp routing-table dampened** command to check BGP dampened routes.
- Run the **display bgp routing-table dampening parameter** command to check parameters of BGP route dampening.
- Run the **display bgp routing-table flap-info [regular-expression as-regular-expression | as-path-filter { as-path-filter-number | as-path-filter-name } | network-address [{ mask | mask-length } [longer-match]]]** command to check statistics of BGP flapped routes.

----End

8.8 Configuring Parameters of a BGP Peer Connection

By setting parameters of a BGP peer connection, you can adjust and optimize the BGP network performance.

8.8.1 Establishing the Configuration Task

Before configuring BGP connection parameters, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This will help you complete the configuration task quickly and efficiently.

Applicable Environment

After a BGP connection is established between peers, the peers periodically send Keepalive messages to each other. If the router does not receive any Keepalive message or any other types of messages from the peer within the specified holdtime, the BGP connection is considered closed.

After the router establishes a BGP connection with its peer, the two devices negotiate the holdtime. The smaller of the holdtime values of the two devices becomes the negotiated holdtime. If the negotiation result is 0, no Keepalive message is transmitted and the holdtime is not detected.

If the timer value changes, the BGP connection may be interrupted for a short time because the router and its peer must renegotiate the timer value.

A ConnectRetry timer is used to set the interval between BGP attempts to initiate TCP connections. After BGP initiates a TCP connection, the ConnectRetry timer is stopped if the TCP connection is established successfully. If the first attempt to establish a TCP connection fails, BGP tries again to establish the TCP connection after the ConnectRetry timer expires.

You can speed up or slow down the establishment of BGP peer relationships by changing the BGP ConnectRetry interval. For example, if the ConnectRetry interval is reduced, BGP will wait less time to retry establishing a TCP connection when an earlier attempt fails. This speeds up the establishment of the TCP connection. If a BGP peer flaps constantly, the ConnectRetry interval can be increased to suppress route flapping caused by BGP peer flapping. This speeds up route convergence.

Pre-configuration Tasks

Before configuring BGP connection parameters, complete the following task:

- [Configuring Basic BGP Functions](#)

Data Preparation

To configure BGP connection parameters, you need the following data.

No.	Data
1	Values of BGP timers
2	Interval for sending Update packets
3	BGP ConnectRetry interval

8.8.2 Configuring BGP Timers

Configuring timers properly can improve network performance. Changing the values of BGP timers will interrupt the peer relationship.

Context



CAUTION

If the values of the timers change after the **timer** command or the **peer timer** command is run, the BGP connection between routers is interrupted. So, confirm the action before you use the command.

Procedure

- Configuring the Global Timer

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
timer keepalive keepalive-time hold hold-time
```

The BGP timers are configured.

The proper maximum interval for sending Keepalive messages is one third of the hold time and is not less than one second. Thus, if the hold time is not set to 0, the lifetime should be at least 3 seconds.

By default, the lifetime is 60s and the hold time is 180s.

NOTE

Setting the hold interval of a BGP peer to be longer than 20s is recommended. If the hold interval of a BGP peer is shorter than 20s, the session may be closed.

Note the following when you set the values of *keepalive-time* and *hold-time*:

- The lifetime and hold time cannot be 0 at the same time. Otherwise, the BGP timer becomes invalid. That is, BGP does not detect faults on the link according to the timer.
- The hold time is much greater than that of the lifetime, such as, **timer keepalive 1 hold 65535**. If the hold time is too long, the faults on the link cannot be detected timely.

After peer relationships are set up, the actual lifetime and hold time are negotiated by both peers. The smaller hold time contained in Open messages of both peers is used

as the actual hold time. The smaller value between one third of the hold time and the configured lifetime is used as the actual lifetime.

- Configuring the Peer Timer

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
peer { ipv4-address | group-name } timer keepalive keepalive-time hold  
hold-time
```

The lifetime and the hold time are set for a peer or a peer group.

For the relationship between the lifetime and hold time, see [Configuring the Global Timer](#).

The peer timer takes precedence over the global timer.

----End

8.8.3 Configuring the Interval for Sending Update Packets

When a route changes, a router sends an Update packet to notify its peer. If a route changes frequently, to prevent the router from sending Update packets for every change, you can set the interval for sending Update packets for changes of this route.

Context

Do as follows on the BGP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bgp as-number
```

The BGP view is displayed.

Step 3 Run:

```
peer { ipv4-address | group-name } route-update-interval interval
```

The interval for sending Update messages is set.

----End

8.8.4 Setting the BGP ConnectRetry Interval

You can speed up or slow down the establishment of BGP peer relationships to adapt the network changes by changing the BGP ConnectRetry interval.

Context

When BGP initiates a TCP connection, the ConnectRetry timer is stopped if the TCP connection is established successfully. If the first attempt to establish a TCP connection fails, BGP tries again to establish the TCP connection after the ConnectRetry timer expires.

- Setting a short ConnectRetry interval reduces the period BGP waits between attempts to establish a TCP connection. This speeds up the establishment of the TCP connection.
- Setting a long ConnectRetry Interval suppresses route flapping caused by peer flapping. This speeds up route convergence.

Do as follows on the BGP router:

Procedure

- Set a ConnectRetry interval globally.

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
timer connect-retry connect-retry-time
```

A ConnectRetry interval is set globally.

By default, the ConnectRetry interval is 32s.

- Set a ConnectRetry interval on a peer or peer group.

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
peer { group-name | ipv4-address } timer connect-retry connect-retry-time
```

A ConnectRetry interval is set on a peer or peer group.

By default, the ConnectRetry interval is 32s.

The ConnectRetry interval configured on a peer or peer group takes precedence over a global ConnectRetry interval.

----End

8.8.5 Enabling Fast Reset of EBG P Connections

After quick resetting of EBG P connections is enabled, BGP rapidly detects the failure on an EBG P link and then resets the BGP connection on the interface immediately.

Context

Do as follows on the BGP router:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bgp as-number
```

The BGP view is displayed.

Step 3 Run:

```
ebgp-interface-sensitive
```

Fast reset is enabled for EBG P connections.

- After this function is enabled, BGP rapidly detects the failure on an EBG P link and then resets BGP connections on the interface immediately.
- After this function is disabled, the repeated establishment and deletion of the BGP session, which is caused by route flapping, is prevented. This saves the network bandwidth.

----End

8.8.6 Checking the Configuration

After parameters of a BGP peer connection are configured, you can check BGP peers and peer groups.

Prerequisite

The configurations of a BGP peer connection are complete.

Procedure

- Run the **display bgp peer** [*verbose*] command to check BGP peers.
- Run the **display bgp group** [*group-name*] command to check BGP peer groups.

----End

Example

Run the **display bgp peer verbose** command in the system view. You can view the configured Keepalive period, holdtime, ConnectRetry interval, and interval at which Update packets are sent.

```
<HUAWEI> display bgp peer verbose

BGP Peer is 10.1.1.1, remote AS 100
Type: IBGP link
BGP version 4, Remote router ID 1.1.1.1
Update-group ID: 0
BGP current state: Established, Up for 00h00m05s
BGP current event: RecvKeepalive
BGP last state: OpenConfirm
BGP Peer Up count: 2
Received total routes: 0
Received active routes total: 0
Advertised total routes: 0
Port: Local - 55219 Remote - 179
Configured: Connect-retry Time: 50 sec
Configured: Active Hold Time: 100 sec Keepalive Time:30 sec
Received : Active Hold Time: 180 sec
Negotiated: Active Hold Time: 100 sec Keepalive Time:30 sec
Peer optional capabilities:
Peer supports bgp multi-protocol extension
Peer supports bgp route refresh capability
Peer supports bgp 4-byte-as capability
Address family IPv4 Unicast: advertised and received
Received: Total 2 messages
    Update messages          0
    Open messages            1
    KeepAlive messages       1
    Notification messages    0
    Refresh messages         0
Sent: Total 2 messages
    Update messages          0
    Open messages            1
    KeepAlive messages       1
    Notification messages    0
    Refresh messages         0
Authentication type configured: None
Last keepalive received: 2010/11/17 15:51:57 UTC-08:00
Minimum route advertisement interval is 20 seconds
Optional capabilities:
Route refresh capability has been enabled
4-byte-as capability has been enabled
Peer Preferred Value: 0
Routing policy configured:
No routing policy is configured
```

8.9 Configuring BFD for BGP

By configuring BFD for BGP, you can provide a fast fault detection mechanism for BGP, and thus speed up network convergence.

8.9.1 Establishing the Configuration Task

Before configuring BFD for BGP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

BGP periodically sends Keepalive messages to the peer to detect faults on the neighbor. The detection, however, lasts more than one second. When the data transmission rate reaches the level of G bit/s, such a slow detection will cause a large amount of data to be lost. As a result, the requirement for high reliability of carrier-class networks cannot be met.

Therefore, BFD for BGP is introduced to fast detect faults on the links between BGP peers. This speeds up the network convergence.

NOTE

By default, a multi-hop BGP session is established between Huawei devices that set up an IBGP peer relationship. A BFD for IGP session and A BFD for IBGP session cannot be both set up between a Huawei device and a non-Huawei device that sets up a single-hop BGP session with its peer by default. In such a situation, setting up only A BFD for IGP session or A BFD for IBGP session between the Huawei and non-Huawei devices is recommended.

Pre-configuration Task

Before configuring BFD for BGP, complete the following tasks:

- Configuring link layer protocol parameters and assigning IP addresses to the interfaces to ensure that the status of the link layer protocol of the interface is Up
- [Configuring Basic BGP Functions](#)

Data Preparation

To configure BFD for BGP, you need the following data.

No.	Data
1	Type and number of the interface on which BFD is enabled
2	Related BFD detection parameters, including the minimum interval and the maximum interval for receiving BFD control packets, and the detection multiplier

8.9.2 Configuring BFD for BGP in the Public Network Instance

By configuring BFD for BGP, you can fast detect the BGP route status. A BFD session can be established only when two BFD peers are in the Established state.

Context

Do as follows on the two BGP routers where a BFD session needs to be set up:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

Global BFD is enabled on the local node.

Step 3 Run:

```
quit
```

Back to the system view.

Step 4 Run:

```
bgp as-number
```

The BGP view is displayed.

Step 5 (Optional) Run:

```
peer { group-name | ipv4-address } bfd { min-tx-interval min-tx-interval | min-rx-interval min-rx-interval | detect-multiplier multiplier } *
```

The parameters used to set up a BFD session are specified.

Step 6 Run:

```
peer { group-name | ipv4-address } bfd enable
```

BFD is configured for a peer or a peer group and the BFD session is set up.

If BFD is configured on a peer group, BFD sessions are set up between the peers that belong to the peer group and are not configured with the **peer bfd block** command.

 **NOTE**

- A BFD session is set up only when the BGP session is in the Established state.
- If BFD parameters of a peer are set, the BFD session is set up by using BFD parameters of the peer.

Step 7 (Optional) Run:

```
peer ipv4-address bfd block
```

The peer is prevented from inheriting BFD of its group.

If a peer joins a group enabled with BFD, the peer inherits BFD of the group and creates a BFD session. If you do not want the peer to inherit BFD of the group, you can prevent the peer from inheriting BFD of its group.

 **NOTE**

The **peer bfd block** command is mutually exclusive with the **peer bfd enable** command. After the **peer bfd block** command is used, the BFD session is automatically deleted.

----End

8.9.3 Configuring BFD for BGP in a Private Network

On a VPN network, configuring BFD for BGP can fast detect the status of VPN BGP routes. A BFD session can be established only when two BGP peers are in the Established state.

Context

Do as follows on the BGP routers at the both ends of the link that needs to set up a BFD session:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

Global BFD is enabled on the local node.

Step 3 Run:

```
quit
```

Back to the system view.

Step 4 Run:

```
bgp as-number
```

The BGP view is displayed.

Step 5 Run:

```
ipv4-family vpn-instance vpn-instance-name
```

The BGP-VPN instance view is displayed.

Step 6 (Optional) Run:

```
peer { group-name | ipv4-address } bfd { min-tx-interval min-tx-interval | min-rx-interval min-rx-interval | detect-multiplier multiplier } *
```

The parameters used to set up a BFD session are specified.

Step 7 Run:

```
peer { group-name | ipv4-address } bfd enable
```

BFD is configured for a peer or a peer group and the BFD session is set up.

If BFD is configured on a peer group, peers that belong to the group set up BFD sessions when the **peer bfd block** command is not used on the peers.

 **NOTE**

- A BFD session is set up only when the BGP session is in the Established state.
- If BFD parameters of a peer are set, the BFD session is set up by using BFD parameters of the peer.

Step 8 (Optional) Run:

```
peer ipv4-address bfd block
```

The peer is prevented from inheriting BFD of its group.

If a peer joins a group enabled with BFD, the peer inherits BFD of the group and creates a BFD session. If you do not want the peer to inherit BFD of the group, you can prevent the peer from inheriting BFD of its group.

 **NOTE**

The **peer bfd block** command is exclusive with the **peer bfd enable** command. After the **peer bfd block** command is used, the BFD session is automatically deleted.

----End

8.9.4 Checking the Configuration

After BFD for BGP is configured, you can check the BFD sessions established by BGP.

Prerequisite

The configurations of BFD for BGP are complete.

Procedure

- Run the **display bgp bfd session** { [**vpn4 vpn-instance** *vpn-instance-name*] **peer** *ipv4-address* | **all** } command to check the BFD sessions established by BGP.
- Run the **display bgp** [**vpn4 vpn-instance** *vpn-instance-name*] **peer** [[*ipv4-address*] **verbose**] command to check BGP peers.
- Run the **display bgp group** [*group-name*] command to check BGP peer groups.
- Run the **display bgp vpn4** { **all** | **vpn-instance** *vpn-instance-name* } **group** [*group-name*] command to check BGP peer groups.

----End

8.10 Configuring BGP Auto FRR

As a protection measure against link faults, BGP Auto FRR is applicable to the network topology with primary and backup links. BGP Auto FRR is suitable for the services that are sensitive to packet delay and packet loss.

8.10.1 Establishing the Configuration Task

Before configuring BGP Auto FRR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

BGP Auto FRR is applicable to IP services that are sensitive to packet loss and delay.

Pre-configuration Tasks

Before configuring BGP Auto FRR, complete the following tasks:

- Configuring static routes or enabling IGP to ensure that IP routes between routers are reachable
- Configuring BGP peers or MP-BGP peers

Data Preparation

To configure BGP Auto FRR, you need the following data.

No.	Data
1	(Optional) BGP-VPN instance view for configuring BGP Auto FRR

8.10.2 Enabling BGP Auto FRR

With BGP Auto FRR, switching between two BGP peers or two next hops can be implemented at the sub-second level.

Context

Do as follows on the router that requires BGP Auto FRR:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bgp as-number
```

The BGP view is displayed.

Step 3 Run:

```
auto-frr
```

BGP Auto FRR is enabled for unicast routes.

By default, BGP Auto FRR is not enabled for unicast routes.

Step 4 (Optional) Run:

```
ipv4-family vpn-instance vpn-instance-name
```

The BGP VPN instance view is displayed.

Step 5 (Optional) Run:

```
auto-frr
```

BGP Auto FRR is enabled for VPN instance routes.

---End

8.10.3 Checking the Configuration

After BGP Auto FRR is configured, you can check the backup forwarding information about routes.

Requirements

All BGP configurations are complete.

Checking the Configuration

Run the following commands to check the previous configurations.

- Run the **display ip routing-table** [**vpn-instance** *vpn-instance-name*] [*ip-address*] [*mask* | *mask-length*] [**longer-match**] **verbose** command to check backup forwarding information about routes in the routing table.

8.11 Configuring BGP Tracking

On a network where BFD is unsuitable to deploy, you can configure BGP tracking to implement the fast convergence of IBGP routes.

8.11.1 Establishing the Configuration Task

Before configuring BGP tracking, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

Since BFD is difficult to deploy and is of poor scalability, in a network where BFD is unsuitable to be deployed, you can configure BGP tracking as a substitution for BFD to implement the fast convergence of BGP routes.

BGP tracking is easy to deploy because it needs to be configured only on the local device, without the need of configuring it on the peer device. However, BGP route convergence in a network configured with BGP tracking is slower than that in a network enabled with BFD; therefore, BGP tracking cannot meet the requirement of voice services that demand high convergence speed.

Pre-configuration Tasks

Before configuring BGP tracking, complete the following tasks:

- Configuring parameters of the link layer protocol and IP addresses for interfaces to ensure that the link layer protocol on the interfaces is Up
- [Configuring basic BGP functions](#)

Data Preparation

To configure BGP tracking, you need the following data.

No.	Data
1	(Optional) Delay for tearing down a connection

8.11.2 Enabling BGP Tracking

Easy to deploy, BGP tracking can speed up network convergence and adjust the interval between a peer's being discovered unreachable and the connection's being torn down.

Context

Do as follows on the router enabled with BGP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bgp as-number
```

The BGP view is displayed.

Step 3 Run:

```
peer { group-name | ipv4-address } tracking [ delay delay-time ]
```

BGP tracking is enabled for the specified peer.

By default, BGP tracking is disabled.

A proper value of *delay-time* can ensure network stability when a peer is detected unreachable.

- If *delay-time* is set to 0, BGP immediately tears down the connection between the local device and its peer after the peer is detected unreachable.
- If IGP route flapping occurs and *delay-time* for an IBGP peer is set to 0, the peer relationship between the local device and the peer alternates between Up and Down. Therefore, *delay-time* for an IBGP peer should be set to a value greater than the actual IGP route convergence time.
- When BGP neighbors successfully perform the GR negotiation, the active/standby switchover occurs on the BGP neighbors, to prevent the failure of GR, *delay-time* should be set to a value greater than GR period. If *delay-time* is set to be smaller than the GR period, the connection between the local device and the BGP peer will be torn down, which leads to the failure of GR.

---End

8.11.3 Checking the Configuration

After BGP tracking is configured, you can check the configuration of BGP tracking by viewing detailed information about the BGP peer or peer group.

Prerequisite

All BGP tracking configurations are complete.

Checking the Configuration

Run the following commands to check the previous configuration.

- Run the **display bgp peer** [*ipv4-address*] [**verbose**] command to check information about the BGP peer.
- Run the **display bgp group** [*group-name*] command to check information about the BGP peer group.

8.12 Configuring Prefix-based BGP ORF

Prefix-based BGP ORF enables a device to send its peer the prefix-based inbound policy that can be used by the peer to filter routes to be sent.

8.12.1 Establishing the Configuration Task

Before configuring prefix-based BGP ORF, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

When a device wants to receive only required routes from its peer but the peer cannot maintain different outbound policies for each connected device, you can configure prefix-based ORF to meet the requirements of the two devices.

Pre-configuration Tasks

Before configuring prefix-based BGP ORF, complete the following tasks:

- [Configuring Basic BGP Functions](#)
- [Configuring an IPv4 Prefix List](#)

Data Preparation

To configure prefix-based BGP ORF, you need the following data.

No.	Data
1	Address of a peer or name of a peer group
2	Name of an IP prefix list

8.12.2 Enabling Prefix-based BGP ORF

Prefix-based BGP ORF supports on-demand route advertisement, which greatly reduces bandwidth consumption and effectively reduces the efforts of network cooperation and configuration.

Context

Do as follows on a BGP device:

Procedure

- Step 1** Run:
- ```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv4-family unicast
```

The IPv4 unicast address family view is displayed.

**Step 4** Run:

```
peer { group-name | ipv4-address } ip-prefix ip-prefix-name import
```

The prefix-based inbound policy is configured on a peer or a peer group.

**Step 5** Run:

```
peer { group-name | ipv4-address } capability-advertise orf [cisco-compatible] ip-prefix { both | receive | send }
```

The prefix-based ORF is configured on a BGP peer or a BGP peer group.

By default, prefix-based ORF is not enabled on a BGP peer or a BGP peer group.

----End

## 8.12.3 Checking the Configuration

After configuring prefix-based BGP ORF, you can view the result of prefix-based BGP ORF negotiation.

### Prerequisite

All prefix-based BGP ORF configurations are complete.

### Procedure

- Run the **display bgp peer** [ *ipv4-address* ] **verbose** command to check detailed information about BGP peers.
- Run the **display bgp peer** *ipv4-address* **orf ip-prefix** command to view the prefix-based ORF information received by a device from a specified peer.

----End

## 8.13 Configuring Path MTU Auto Discovery

By configuring path MTU auto discovery, you can discover the minimum MTU on the network path from the source to the destination.

### 8.13.1 Establishing the Configuration Task

Before configuring path MTU auto discovery, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

## Applicable Environment

When hosts need to communicate across multiple networks, the smallest MTU on the communication path is most important to both ends. This is because different networks along the communication path have different MTUs of the link layer. The minimum MTU on the communication path is called the path MTU.

During communication, path MTUs of host depend on the selected path and thus may change. In addition, the path MTUs of the inbound direction and outbound direction may be inconsistent. Path MTU auto discovery is the process of discovering the minimum MTU on the network path from the source to the destination. The discovered path MTU is used to ensure proper fragmentation during packet transmission.

## Pre-configuration Tasks

Before configuring path MTU auto discovery, complete the following task:

- [Configuring Basic BGP Functions](#)

## Data Preparation

None.

### 8.13.2 Enabling Path MTU Auto Discovery

By configuring path MTU auto discovery, you can discover the minimum MTU on the network path from the source to the destination.

## Context

Do as follows on the BGP router:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
peer { group-name | ipv4-address } path-mtu auto-discovery
```

Path MTU auto discovery is enabled.

----End

### 8.13.3 (Optional) Setting the IPv4 Path MTU Aging Time

The proper IPv4 path MTU (PMTU) aging time allows the system to update path MTUs, increasing the transmission efficiency.

## Context

After path MTU auto discovery is configured on the router runs BGP, the router transmits packets based on path MTUs.

The path MTUs of different routes may differ. The path MTU of hosts depends on the selected route and thus may change. If there are multiple routes between two communication hosts and the routes selected for packet transmission change frequently, the path MTU aging time needs to be configured. The system updates path MTUs based on the path MTU aging time, increasing the transmission efficiency.

Perform the following steps on a device that has been configured with path MTU auto discovery and needs to update path MTUs periodically:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
tcp timer pathmtu-age age-time
```

The aging time is set for an IPv4 path MTU.

By default, the IPv4 path MTU aging time is set to 0 seconds. That is, an IPv4 path MTU does not age.

----End

## 8.13.4 Checking the Configuration

After configuring path MTU auto discovery, you can check whether it is configured.

### Prerequisite

All configurations of path MTU auto discovery are complete.

### Procedure

- Run the **display bgp peer** [ *ipv4-address* ] **verbose** command to view detailed information about the BGP peer to check whether path MTU auto discovery is successfully configured.

----End

## 8.14 Configuring the BGP Next Hop Delayed Response

By configuring the BGP next hop delayed response, you can reduce traffic loss during routes changes.

### 8.14.1 Establishing the Configuration Task

Before configuring the BGP next hop delayed response, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

## Applicable Environment

When the route path on the upstream of a PE connected to an RR changes, if the PE detects that the iterated next hop becomes unreachable before the RR instructs the PE to switch the route, the PE withdraws the original optimal route advertised to its connected CE. After the RR re-advertises the switched route to the PE, the PE re-advertises an optimal route to the CE after route selection. During the route switchover, a huge volume of traffic will be dropped. In this case, if the PE delays responding to changes of route iteration information, that is, the PE updates routes only after the RR re-advertises an optimal route, less traffic is dropped during the route switchover.

## Pre-configuration Tasks

Before configuring the BGP next hop delayed response, complete the following task:

- [Configuring Basic BGP Functions](#)

## Data Preparation

To configure the BGP next hop delayed response, you need the following data.

| No. | Data                                           |
|-----|------------------------------------------------|
| 1   | Delay in responding to changes of the next hop |

## 8.14.2 Configuring the BGP Next Hop Delayed Response

By configuring the BGP next hop delayed response, you can reduce the dropped traffic during route changes and thus enhance the network stability.

### Context

Do as follows on the BGP router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
nexthop recursive-lookup delay [delay-time]
```

The delay in responding to changes of the next hop is set.

If *delay-time* is not specified, the delay in responding to changes of the next hop defaults to 5 seconds.

---End

### 8.14.3 Checking the Configuration

After the BGP next hop delayed response is configured, you can view the configured delay in responding to changes of the next hop.

#### Prerequisite

All configurations of the BGP next hop delayed response are complete.

#### Procedure

- Run the **display current-configuration | include nexthop recursive-lookup delay** command to check the delay in responding to changes of the next hop.

---End

#### Example

Run the **display current-configuration | include nexthop recursive-lookup delay** command. You can view the currently configured delay in responding to changes of the next hop. For example:

```
<HUAWEI> display current-configuration | include nexthop recursive-lookup delay
nexthop recursive-lookup delay 20
```

## 8.15 Configuring BGP Load Balancing

By configuring BGP load balancing, you can properly use network resources.

### 8.15.1 Establishing the Configuration Task

Before configuring BGP load balancing, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

Load balancing can be performed among equal-cost BGP routes whose first eight attributes described in "Principles of Route Selection" of [8.1.2 BGP Features Supported by the NE80E/40E](#) are the same and AS\_Path attributes are the same.

#### Pre-configuration Tasks

Before configuring BGP load balancing, complete the following task:

- [Configuring Basic BGP Functions](#)

#### Data Preparation

To configure BGP load balancing, you need the following data.

| No. | Data                                |
|-----|-------------------------------------|
| 1   | Number of routes for load balancing |

## 8.15.2 Setting the Number of Routes for BGP Load Balancing

Load balancing can be implemented among multiple equal-cost links between BGP peers.

### Procedure

- Configuring the Maximum Number of Routes for BGP Load Balancing

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

4. Run:

```
maximum load-balancing [ebgp | ibgp] number
```

The maximum number of routes for BGP load balancing is set.

By default, the number of routes for BGP load balancing is 1.

- Configuring the Maximum Number of EBGP and IBGP Routes for Load Balancing

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv4-family vpn-instance vpn-instance-name
```

The BGP-VPN instance view is displayed.

4. Run:

```
load-balancing as-path-ignore
```

A router is configured not to compare the AS-Path attributes of the routes among which load balancing is performed.



By default, a router compares the AS-Path attributes of the routes when load balancing is performed.

 **NOTE**

- The execution of the **load-balancing as-path-ignore** command will change the conditions of load balancing. Then, a router does not compare the AS-Path attributes of the routes when load balancing is performed. This command applies to the scenarios where EBGP and IBGP routes perform load balancing, and needs to be used with caution.
- The **load-balancing as-path-ignore** command and the **bestroute as-path-ignore** command are mutually exclusive.

5. Run:

```
maximum load-balancing eibgp number
```

The maximum number of EBGP and IBGP routes for load balancing is set.

By default, the maximum number of EBGP and IBGP routes for load balancing is not set.

---End

## 8.15.3 Checking the Configuration

After BGP load balancing is configured, you can check information about load balancing.

### Prerequisite

The configurations of BGP load balancing are complete.

### Procedure

- Run the **display bgp routing-table** [ *network* ] [ *mask* | *mask-length* ] [ **longer-prefixes** ] command to check information about the BGP routing table.
- Run the **display ip routing-table** [ **verbose** ] command to check information about the IP routing table.

---End

## 8.16 Configuring a BGP Peer Group

By configuring a BGP peer group, you can simplify the management of routing policies, and thus improve the efficiency of route advertisement.

### 8.16.1 Establishing the Configuration Task

Before configuring a BGP peer group, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

### Applicable Environment

A large number of peers exist in a large BGP network, which is inconvenient for configuration and maintenance. In this case, you can configure peer groups to simplify the management of peers and improve the efficiency in advertising routes. According to whether peers reside in the same AS, you can classify peer groups into IBGP peer groups and EBGP peer groups. For EBGP peer

groups, you can classify them into pure EBGP peer groups and mixed EBGP peer groups according to whether the peers are in the same external AS.

## Pre-configuration Tasks

Before configuring a BGP peer group, complete the following tasks:

- Configuring link layer protocol parameters and assigning IP addresses to the interfaces to ensure that the status of the link layer protocol of the interface is Up
- **Configuring Basic BGP Functions**

## Data Preparation

To configure a BGP peer group, you need the following data.

| No. | Data                                                         |
|-----|--------------------------------------------------------------|
| 1   | Type and name of the peer group, and peers in the peer group |

## 8.16.2 Creating an IBGP Peer Group

When BGP has multiple IBGP peers, you can create an IBGP peer group to simplify the management of routing policies. When creating an IBGP peer group, you do not need to specify the AS number.

### Context

Do as follows on the BGP router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
group group-name [internal]
```

An IBGP peer group is created.

**Step 4** Run:

```
peer ipv4-address group group-name
```

A peer is added to this peer group.

You need not to specify the number of the AS when creating an IBGP peer group.

----End

## 8.16.3 Creating a Pure EBGP Peer Group

When BGP has multiple EBGP peers that belong to one AS, you can create an EBGP peer group to simplify the management of routing policies. All the peers in a pure EBGP peer group must have the same AS number.

### Context

Do as follows on the BGP router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
group group-name external
```

An EBGP peer group is created.

**Step 4** Run:

```
peer group-name as-number as-number
```

The number of the AS where this peer group resides is set.

**Step 5** Run:

```
peer ipv4-address group group-name
```

A peer is added to the peer group.

 **NOTE**

You can add multiple peers to the peer group by repeating Step 5. The system automatically creates a peer in the BGP view, and sets its AS number to the local AS number.

If there are already peers in this peer group, you can neither change the AS number of this peer group nor delete the specified AS number with the **undo peer group-name as-number** command.

----End

## 8.16.4 Creating a Mixed EBGP Peer Group

When BGP has multiple EBGP peers that belong to different ASs, you can create a mixed EBGP peer group to simplify the management of routing policies. When creating a mixed EBGP peer group, you need to specify the AS number of each peer.

### Context

Do as follows on the BGP router:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
group group-name external
```

An EBGP peer group is created.

**Step 4** Run:

```
peer ipv4-address as-number as-number
```

All peers are created and their AS numbers are set.

**Step 5** Run:

```
peer ipv4-address group group-name
```

The peer is added to the peer group.

### NOTE

You can add multiple peers to the peer group by repeating Step 4 and Step 5.

In a mixed EBGP peer group, you need to specify the AS number of each peer.

----End

## 8.16.5 Checking the Configuration

After a BGP peer group is configured, you can check detailed information about the BGP peer and information about the BGP peer group.

### Prerequisite

The configurations of a BGP peer group are complete.

### Procedure

- Run the **display bgp peer** [ *ipv4-address* ] **verbose** command to check detailed information about the peer.
- Run the **display bgp group** [ *group-name* ] command to check information about the peer group.

----End

## 8.17 Configuring a BGP Route Reflector

By configuring a BGP route reflector, you can solve the problem of establishing fully meshed connections between multiple IBGP peers.

## 8.17.1 Establishing the Configuration Task

Before configuring a BGP route reflector, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

### Applicable Environment

To ensure the connectivity between IBGP peers inside an AS, you need to establish full-meshed IBGP peers. When there are many IBGP peers, establishing a full-meshed network is costly. You can use the RR or the confederation to solve the problem.

### Pre-configuration Tasks

Before configuring a BGP RR, complete the following tasks:

- Configuring link layer protocol parameters and assigning IP addresses to the interfaces to ensure that the link layer protocol of the interface is Up
- [Configuring Basic BGP Functions](#)

### Data Preparation

To configure a BGP RR, you need the following data.

| No. | Data                                             |
|-----|--------------------------------------------------|
| 1   | Role of each router (RR, client, and non-client) |

## 8.17.2 Configuring a Route Reflector and Specifying Clients

A route reflector and clients need to be configured in a specified address family.

### Context

Do as follows on the BGP router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

**Step 4** Run:

```
peer { ipv4-address | group-name } reflect-client
```

An RR is configured and its clients are specified.

The router where the command is run serves as the RR and the peer is specified as its client.

----End

## 8.17.3 (Optional) Disabling the Route Reflection Between Clients

If the clients of a route reflector are fully meshed, you can disable route reflection between clients to reduce the cost.

### Context

Do as follows on the BGP router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

**Step 4** Run:

```
undo reflect between-clients
```

Route reflection between clients is disabled.

If the clients of the RR are fully meshed, you can use the **undo reflect between-clients** command to disable route reflection between clients. This reduces the cost to a great degree.

By default, route reflection between clients is enabled.

This command is applicable to only the RR.

----End

## 8.17.4 (Optional) Configuring the Cluster ID for a Route Reflector

When there are multiple route reflectors in a cluster, you need to configure the same cluster ID for all the route reflectors in this cluster to avoid routing loops.

### Context

Do as follows on the BGP router:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

**Step 4** Run:

```
reflector cluster-id cluster-id
```

The cluster ID of an RR is set.

When there are multiple RRs in a cluster, you can configure all the RRs in this cluster with the same cluster ID with this command. This prevents routing loops.

----End

## 8.17.5 (Optional) Preventing BGP Routes from Being Added into the IP Routing Table

By preventing BGP routes from being added to the IP routing table, you can effectively reduce unnecessary interaction between BGP and the routing management module, and thus improve forwarding efficiency.

### Context

Do as follows on the BGP router:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv4-family unicast
```

The BGP IPv4 unicast address family view is displayed.

**Step 4** Run:

```
bgp-rib-only [route-policy route-policy-name]
```

Adding BGP routes to the IP routing table is forbidden.

By default, the preferred BGP routes are added to the IP routing table.

When the parameter **route-policy** *route-policy-name* is specified in the command, the routes that match the routing policy are not added to the IP routing table. Conversely, the routes that do not match the routing policy are added to the IP routing table, and the attributes of these routes are not modified.

 **NOTE**

The **bgp-rib-only** command and the **active-route-advertise** command are mutually exclusive.

----End

## 8.17.6 Checking the Configuration

After a BGP route reflector is configured, you can check BGP route information and peer group information.

### Prerequisite

The configurations of a BGP route reflector are complete.

### Procedure

- Run the **display bgp group** [ *group-name* ] command to check detailed information about the peer group.
- Run the **display bgp routing-table** [ *network* ] [ *mask* | *mask-length* ] [ **longer-prefixes** ] command to check information about the BGP routing table.

----End

## 8.18 Configuring a BGP Confederation

On a large-scale BGP network, configuring a BGP confederation can simplify the management of routing policies and improve the efficiency of route advertisement.

### 8.18.1 Establishing the Configuration Task

Before configuring a BGP confederation, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

### Applicable Environment

Confederation deals with increasing IBGP connections in an AS. The confederation divides an AS into multiple sub-ASs. In each sub-AS, IBGP peer relationships are set up or an RR is configured on one of the IBGP peers. EBGP connections are set up between sub-ASs.

### Pre-configuration Tasks

Before configuring a BGP confederation, complete the following tasks:

- Configuring link layer protocol parameters and assigning IP addresses to the interfaces to ensure that the status of the link layer protocol of the interface is Up



- **Configuring Basic BGP Functions**

## Data Preparation

To configure a BGP confederation, you need the following data.

| No. | Data             |
|-----|------------------|
| 1   | Confederation ID |
| 2   | Sub-AS number    |

## 8.18.2 Configuring a BGP Confederation

BGP confederations deal with increasing IBGP connections in an AS.

### Procedure

- **Configuring a BGP Confederation**

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
confederation id as-number
```

The confederation ID is set.

4. Run:

```
confederation peer-as as-number <1-32>
```

The number of the sub-AS where other EBGP peers connected to the local AS reside is set.

A confederation includes up to 32 sub-ASs. The parameter *as-number* used is valid for the confederation to which it belongs.

You must run the **confederation id** and **confederation peer-as** commands for all the EBGP peers in a confederation, and specify the same confederation ID for them.

#### **NOTE**

The old speaker with 2-byte AS numbers and the new speaker with 4-byte AS numbers cannot exist in the same confederation. Otherwise, routing loops may occur because AS4\_Path does not support confederations.

- **Configuring the Compatibility of the Confederation**

Do as follows on the BGP router:

1. Run:  
`system-view`  
The system view is displayed.
2. Run:  
`bgp as-number`  
The BGP view is displayed.
3. Run:  
`confederation nonstandard`  
The compatibility of the confederation is configured.  
  
Some routers in a confederation may not comply with the RFC standard. In this case, you can use this command to make the routers compatible with devices that do not comply with the RFC standard.

----End

### 8.18.3 Checking the Configuration

After a BGP confederation is configured, you can check BGP route information and detailed peer information.

#### Prerequisite

The configurations of a BGP confederation are complete.

#### Procedure

- Run the `display bgp peer [ ipv4-address ] verbose` command to check detailed information about the peer.
- Run the `display bgp routing-table [ network ] [ mask | mask-length ] [ longer-prefixes ]` command to check information about the BGP routing table.

----End

## 8.19 Configuring BGP Accounting

By configuring BGP accounting, you can collect the statistics of the incoming and outgoing BGP traffic of an AS.

### 8.19.1 Establishing the Configuration Task

Before configuring BGP accounting, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

BGP accounting sets traffic indexes through the matching BGP attributes to identify and classify routes, and then accounts services according to the traffic. BGP accounting is valid only when a router needs to search the forwarding table. For example, if BGP accounting is configured for the outgoing traffic on the originating interface, BGP accounting is invalid.

## Pre-configuration Tasks

Before configuring BGP accounting, complete the following tasks:

- [Configuring Basic BGP Functions](#)
- [Configure BGP to Advertise Local Routes](#)
- [\(Optional\) Configuring the Local Interface for a BGP Connection](#)
- [Configuring BGP Route Attributes](#)

## Data Preparation

To configure BGP accounting, you need the following data.

| No. | Data                                                                                                                                                           |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Defined types                                                                                                                                                  |
| 2   | ACL number, MAC address, interface type and number, DSCP value, IP preference, RTP protocol port number, IP protocol type, MPLS EXP value, and 802.1P priority |

## 8.19.2 Configuring the Routing Policy for Setting the Traffic Index

BGP accounting propagates traffic indexes through BGP community attributes to identify routes, and then accounts services.

### Context

Do as follows on the BGP router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
route-policy route-policy-name { permit | deny } node node
```

The node of the Route-Policy is created and the Route-Policy view is displayed.

**Step 3** Run the following command as required:

- Run:

```
if-match acl { acl-number | acl-name }
```

The ACL is configured to match routes.

- Run:

```
if-match as-path-filter { as-path-filter-number | as-path-filter-name } &<1-16>
```

The AS-Path filter is configured to match routes.

- Run:

```
if-match community-filter { basic-comm-filter-num [whole-match] | adv-comm-filter-num } * &<1-16>
```

The community attribute filter is configured to match routes.

- Run:

```
if-match cost cost
```

The cost of a route is set to match routes.

- Run:

```
if-match ip-prefix ip-prefix-name
```

The IP prefix list is configured to match routes.

**Step 4** Run:

```
apply traffic-index traffic-index
```

The traffic index is set.

----End

## 8.19.3 Applying the Routing Policy Configured with the Traffic Index

Routing policies configured with traffic indexes can be flexibly applied as required.

### Context

Do as follows on the BGP router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
peer ipv4-address as-number as-number
```

The BGP peer is created.

**Step 4** Run:

```
peer ipv4-address route-policy route-policy-name import
```

A policy is configured for receiving BGP routes.

----End

## 8.19.4 Applying the BGP Accounting to an Interface

At present, BGP accounting collects only the statistics of packets on the public network and must be configured on the inbound interface.

### Context

Do as follows on the BGP router:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
interface interface-type interface-number
```

The interface view is displayed.

**Step 3** Run:

```
ip bgp-accounting inbound [source]
```

BGP accounting is applied.

By default, BGP accounting matches the destination address. If **source** is configured, BGP accounting matches the source address.

At present, BGP accounting supports only the statistics of packets in the public network, and BGP accounting must be configured on the inbound interface at first.

----End

## 8.19.5 Checking the Configuration

After BGP accounting is configured, you can check BGP accounting information.

### Prerequisite

The configurations of BGP accounting are complete.

### Procedure

- Run the **display ip bgp-accounting inbound interface** [ *interface-type interface-number* ] command to check information about BGP accounting.

----End

## 8.20 Configuring BGP GR

By configuring BGP GR, you can avoid traffic interruption caused by protocol restart.

### 8.20.1 Establishing the Configuration Task

Before configuring BGP GR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

### Applicable Environment

To avoid the interruption of services due to the BGP restart, you need to enable BGP GR and set up BGP GR sessions between the GR restarter and its peers.

## Pre-configuration Tasks

Before configuring BGP GR, complete the following task:

- [Configuring Basic BGP Functions](#)

## Data Preparation

To configure BGP GR, you need the following data.

| No. | Data                                            |
|-----|-------------------------------------------------|
| 1   | AS number                                       |
| 2   | Maximum period for reestablishing a BGP session |
| 3   | Waiting time for the End-of-RIB messages        |

## 8.20.2 Enabling BGP GR

Enabling or disabling GR may delete and reestablish all sessions and instances.

### Context

Do as follows on the router that needs to be enabled with BGP GR:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
graceful-restart
```

BGP GR is enabled.

By default, BGP GR is disabled.

----End

## 8.20.3 Configuring Parameters of a BGP GR Session

You can adjust parameters of a BGP GR session as required. Generally, the default values are recommended. Modifying the value of the Restart timer leads to the reestablishment of the BGP peer relationship.

## Context

Do as follows on the router that needs to be enabled with BGP GR:

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
bgp as-number
```

The BGP view is displayed.

### Step 3 Run:

```
graceful-restart timer restart time
```

The maximum period for reestablishing a BGP session is set.

The restart period is the maximum period for performing GR on a router, that is, the maximum waiting period from the receiving speaker discovering that the peer restarts to the reestablishment of the BGP session. By default, the restart period is 150 seconds.

#### NOTE

Modifying the maximum period for reestablishing a BGP session leads to the reestablishment of the BGP peer relationship.

### Step 4 Run:

```
graceful-restart timer wait-for-rib time
```

The waiting time when the restarting speaker and receiving speaker wait for End-of-RIB messages is set.

By default, the waiting time for End-of-RIB messages is 600 seconds.

#### NOTE

You can adjust parameters of a BGP GR session as required. Generally, the default values are recommended.

----End

## 8.20.4 Checking the Configuration

After BGP GR is configured, you can check the BGP GR status.

## Prerequisite

The configurations of BGP GR are complete.

## Procedure

- Run the **display bgp peer verbose** command to check the status of BGP GR.

----End

## 8.21 Configuring BGP Security

To improve BGP security, you can perform TCP connection authentication.

### 8.21.1 Establishing the Configuration Task

Before improving BGP network security, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

- BGP authentication

BGP uses TCP as the transport layer protocol. To enhance BGP security, you can perform the Message Digest 5 (MD5) authentication when TCP connections are created. The MD5 authentication, however, does not authenticate BGP packets. Instead, it sets MD5 authentication passwords for TCP connections, and the authentication is then completed by TCP. If the authentication fails, TCP connections cannot be established.

- BGP GTSM

The Generalized TTL Security Mechanism (GTSM) is used to prevent attacks by using the TTL detection. If an attack simulates BGP packets and sends a large number of packets to a router, an interface through which the router receives the packets directly sends the packets to BGP of the control layer, without checking the validity of the packets. In this manner, routers on the control layer process the packets as valid packets. As a result, the system becomes busy, and CPU usage is high.

In this case, you can configure GTSM to solve the preceding problem. After GTSM is configured on a router, the router checks whether the TTL value in the IP header of a packet is in the pre-defined range after receiving the packet. If yes, the router forwards the packet; if not, the router discards the packet. This enhances the security of the system.

#### NOTE

- The NE80E/40E supports BGP GTSM.
- GTSM supports only unicast addresses; therefore, GTSM needs to be configured on all the routers configured with routing protocols.

#### Pre-configuration Tasks

Before configuring BGP security, complete the following task:

- [Configuring Basic BGP Functions](#)

#### Data Preparation

Before configure BGP security, you need the following data.

| No. | Data                                                      |
|-----|-----------------------------------------------------------|
| 1   | BGP peer address or name of the peer group of each router |
| 2   | MD5 authentication password                               |



| No. | Data                          |
|-----|-------------------------------|
| 3   | Key-Chain authentication name |

## 8.21.2 Configuring MD5 Authentication

In MD5 authentication of BGP, you only need to set MD5 authentication passwords for TCP connections, and the authentication is performed by TCP. If the authentication fails, TCP connections cannot be established.

### Context

Do as follows on the BGP router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
peer { ipv4-address | group-name } password { cipher cipher-password | simple simple-password }
```

The MD5 authentication password is configured.

 **NOTE**

When this command is used in the BGP view, the extensions on VPNv4 of MP-BGP are also valid because they use the same TCP connection.

Characters `^#^#` and `$$@` are used to identify passwords with variable lengths. Characters `^#^#` are the prefix and suffix of a new password, and characters `$$@` are the prefix and suffix of an old password. Neither of them can be both configured at the beginning and end of a plain text password.

----End

## 8.21.3 Configuring Keychain Authentication

You need to configure Keychain authentication on both BGP peers, and ensure that encryption algorithms and passwords configured for Keychain authentication on both peers are the same. Otherwise, TCP connections cannot be established between BGP peers, and BGP messages cannot be exchanged.

### Context

Do as follows on the BGP router:

## Procedure

### Step 1 Run:

```
system-view
```

The system view is displayed.

### Step 2 Run:

```
bgp as-number
```

The BGP view is displayed.

### Step 3 Run:

```
peer { ipv4-address | group-name } keychain keychain-name
```

The Keychain authentication is configured.

You must configure Keychain authentication on both BGP peers. Note that encryption algorithms and passwords configured for the Keychain authentication on both peers must be the same; otherwise, the TCP connection cannot be set up between BGP peers and BGP messages cannot be transmitted.

Before configuring the BGP Keychain authentication, configure a Keychain in accordance with the configured *keychain-name*. Otherwise, the TCP connection cannot be set up.

#### NOTE

- When this command is used in the BGP view, the extensions on VPNv4 of MP-BGP are also valid because they use the same TCP connection.
- The BGP MD5 authentication and BGP Keychain authentication are mutually exclusive.

----End

## 8.21.4 Configuring Basic BGP GTSM Functions

The GTSM mechanism protects a router by checking whether the TTL value in the IP header is in a pre-defined range.

## Procedure

- Configuring Basic BGP GTSM Functions

Do as follows on the two peers:

#### 1. Run:

```
system-view
```

The system view is displayed.

#### 2. Run:

```
bgp as-number
```

The BGP view is displayed.

#### 3. Run

```
peer { group-name | ipv4-address } valid-ttl-hops [hops]
```

Basic BGP GTSM functions are configured.

The range of TTL values of packets is [  $255-hops+1$ , 255 ]. By default, the value of *hops* is 255. That is, the valid TTL range is [ 1, 255 ]. For example, for the direct EBGP route, the value of *hops* is 1. That is, the valid TTL value is 255.

 **NOTE**

- The configuration in the BGP view is also valid for the VPNv4 extension of MP-BGP. This is because they use the same TCP connection.
- GSTM is exclusive with EBGP-MAX-HOP; therefore, you can enable only one of them on the same peer or the peer group.

After the BGP GTSM policy is configured, an interface board checks the TTL values of all BGP packets. According to the actual networking requirements, you can configure GTSM to discard or process the packets that do not match the GTSM policy. To configure the GTSM to discard packets by default, you can set an appropriate TTL value range. Then, packets whose TTL values are not within the specified range are discarded. In this manner, attacks by bogus BGP packets are avoided.

- Defining the Default GTSM Action

Do as follows on the router configured with GTSM:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
gtsm default-action { drop | pass }
```

The default action is configured for the packets that do not match the GTSM policy.

By default, the packets that do not match the GTSM policy can pass the filtering.

 **NOTE**

If only the default action is configured and the GTSM policy is not configured, GTSM does not take effect.

----End

## 8.21.5 Checking the Configuration

After BGP network security is configured, you can check authentication information of BGP peers.

### Prerequisite

The configurations of BGP security are complete.

### Procedure

- Run the **display gtsm statistics** { *slot-id* | **all** } command to check the statistics of GTSM.  
Run the **display gtsm statistics** command. You can view GTSM statistics on each board, including the total number of BGP packets, the total number of OSPF packets, the number of packets that match the GTSM policy, and the number of discarded packets.
- Run the **display bgp peer** [ *ipv4-address* ] **verbose** command to check information about BGP GTSM.
- Run the **display bgp group** [ *group-name* ] command to check GTSM of a BGP peer group.

----End

## 8.22 Maintaining BGP

Maintaining BGP involves resetting a BGP connection and clearing BGP statistics.

### 8.22.1 Resetting BGP Connections

You can also reset BGP in GR mode. Resetting a BGP connection will interrupt the peer relationship.

#### Context



#### CAUTION

The BGP peer relationship is interrupted after you reset BGP connections with the **reset bgp** command. So, confirm the action before you use the command.

---

When the BGP routing policy on the router that does not support Route-refresh changes, you need to reset BGP connections to validate the configuration. To reset BGP connections, run the following **reset** commands in the user view.

#### Procedure

- To validate the new configurations, run the **reset bgp all** command in the user view to reset all BGP connections.
- To validate the new configurations, run the **reset bgp as-number** command in the user view to reset the BGP connection between the specified AS.
- To validate the new configurations, run the **reset bgp ipv4-address** command in the user view to reset the BGP connection between a specified peer.
- To validate the new configurations, run the **reset bgp external** command in the user view to reset all the EBGP connections.
- To validate the new configurations, run the **reset bgp group group-name** command in the user view to reset the BGP connection with the specified peer-groups.
- To validate the new configurations, run the **reset bgp internal** command in the user view to reset all IBGP connections.

----End

### 8.22.2 Clearing BGP Information

This section describes how to clear the statistics of BGP accounting, flapped routes, and suppressed routes.

## Context



### CAUTION

BGP statistics cannot be restored after you clear it. So, confirm the action before you use the command.

---

## Procedure

- Run the **reset bgp flap-info** [ **regexp** *as-path-regexp* | **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *ipv4-address* [ *mask* | *mask-length* ] ] command in the user view to clear the statistics of flapped routes.
- Run the **reset bgp dampening** [ *ipv4-address* [ *mask* | *mask-length* ] ] command in the user view to clear the dampened routes and advertise the suppressed routes.
- Run the **reset bgp** *ipv4-address* **flap-info** command in the user view to clear the statistics of route flapping.
- Run the **reset ip bgp-accounting inbound interface** [ *interface-type* *interface-number* ] command in the user view to clear the statistics of BGP accounting.

----End

## 8.23 Configuration Examples

BGP configuration examples explain networking requirements, networking diagram, configuration notes, configuration roadmap, and configuration procedure.



### NOTE

This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.

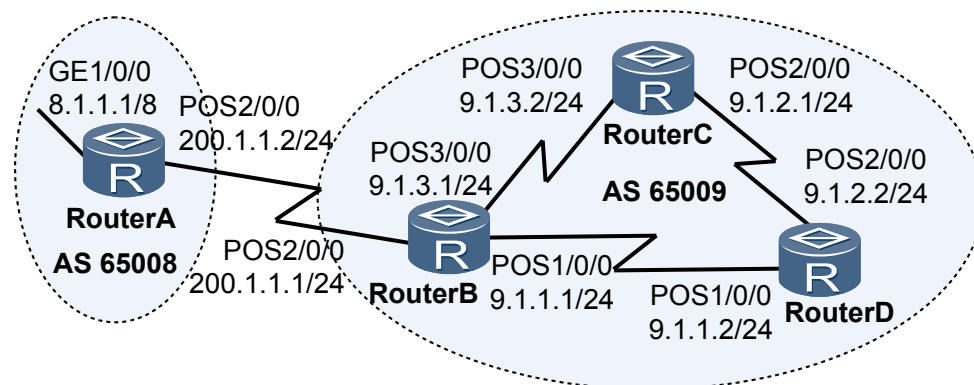
### 8.23.1 Example for Configuring Basic BGP Functions

Before building BGP networks, you need to configure basic BGP functions.

#### Networking Requirements

As shown in **Figure 8-1**, all routers run BGP. An EBGP connection is established between Router A and Router B. Router B, Router C, and Router D are full-meshed IBGP peers.

Figure 8-1 Networking diagram of configuring basic BGP functions



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IBGP connections between Router B, Router C, and Router D.
2. Configure an EBGP connection between Router A and Router B.
3. Advertise routes with the **network** command on Router A and check the routing tables of Router A, Router B, and Router C.
4. Configure BGP on Router B to import direct routes, and check the routing tables of Router A and Router C.

## Data Preparation

To complete the configuration, you need the following data:

- Route ID 1.1.1.1 of Router A and its AS number 65008
- Router IDs of Router B, Router C, and Router D are 2.2.2.2, 3.3.3.3, 4.4.4.4, respectively, and the number of the AS where they reside is 65009

## Procedure

**Step 1** Assign an IP address to each interface.

The configuration details are not mentioned here.

**Step 2** Configure IBGP connections.

# Configure Router B.

```
[RouterB] bgp 65009
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 9.1.1.2 as-number 65009
[RouterB-bgp] peer 9.1.3.2 as-number 65009
```

# Configure Router C.

```
[RouterC] bgp 65009
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 9.1.3.1 as-number 65009
[RouterC-bgp] peer 9.1.2.2 as-number 65009
```

# Configure Router D.

```
[RouterD] bgp 65009
[RouterD-bgp] router-id 4.4.4.4
[RouterD-bgp] peer 9.1.1.1 as-number 65009
[RouterD-bgp] peer 9.1.2.1 as-number 65009
```

### Step 3 Configure EBGP.

# Configure Router A.

```
[RouterA] bgp 65008
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 200.1.1.1 as-number 65009
```

# Configure Router B.

```
[RouterB-bgp] peer 200.1.1.2 as-number 65008
```

# Check the status of BGP connections.

```
[RouterB] display bgp peer
BGP local router ID : 2.2.2.2
Local AS number : 65009
Total number of peers : 3 Peers in established state : 3
Peer V AS MsgRcvd MsgSent OutQ Up/Down State PrefRcv
9.1.1.2 4 65009 49 62 0 00:44:58 Established 0
9.1.3.2 4 65009 56 56 0 00:40:54 Established 0
200.1.1.2 4 65008 49 65 0 00:44:03 Established 1
```

You can view that Router B has established BGP connections with other routers.

### Step 4 Configure Router A to advertise 8.0.0.0/8.

# Configure Router A to advertise routes.

```
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] network 8.0.0.0 255.0.0.0
```

# Check the routing table of Router A.

```
[RouterA] display bgp routing-table

BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 1
 Network NextHop MED LocPrf PrefVal Path/Ogn
*> 8.0.0.0 0.0.0.0 0 0 i
```

# Check the routing table of Router B.

```
[RouterB] display bgp routing-table

BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 1
 Network NextHop MED LocPrf PrefVal Path/Ogn
*> 8.0.0.0 200.1.1.2 0 0 65008i
```

# Check the routing table of Router C.

```
[RouterC] display bgp routing-table

BGP Local router ID is 3.3.3.3
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 1
 Network NextHop MED LocPrf PrefVal Path/Ogn

 i 8.0.0.0 200.1.1.2 0 100 0 65008i
```

 **NOTE**

You can view that Router C has learned the route to 8.0.0.0 in AS 65008, but the next hop 200.1.1.2 is unreachable. Therefore, this route becomes invalid.

**Step 5** Configure BGP to import direct routes.

# Configure Router B.

```
[RouterB-bgp] ipv4-family unicast
[RouterB-bgp-af-ipv4] import-route direct
```

# Check the BGP routing table of Router A.

```
[RouterA] display bgp routing-table

BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 7
 Network NextHop MED LocPrf PrefVal Path/Ogn

*> 8.0.0.0 0.0.0.0 0 0 0 i
*> 9.1.1.0/24 200.1.1.1 0 0 0 65009?
*> 9.1.1.2/32 200.1.1.1 0 0 0 65009?
*> 9.1.3.0/24 200.1.1.1 0 0 0 65009?
*> 9.1.3.2/32 200.1.1.1 0 0 0 65009?
*> 200.1.1.0 200.1.1.1 0 0 0 65009?
*> 200.1.1.2/32 200.1.1.1 0 0 0 65009?
```

# Check the BGP routing table of Router C.

```
[RouterC] display bgp routing-table

BGP Local router ID is 3.3.3.3
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 7
 Network NextHop MED LocPrf PrefVal Path/Ogn

*>i 8.0.0.0 200.1.1.2 0 100 0 65008i
*>i 9.1.1.0/24 9.1.3.1 0 100 0 ?
*>i 9.1.1.2/32 9.1.3.1 0 100 0 ?
*>i 9.1.3.0/24 9.1.3.1 0 100 0 ?
*>i 9.1.3.2/32 9.1.3.1 0 100 0 ?
*>i 200.1.1.0 9.1.3.1 0 100 0 ?
*>i 200.1.1.2/32 9.1.3.1 0 100 0 ?
```

You can view that the route to 8.0.0.0 becomes valid, and the next hop is the address of Router A.



# Use the **ping** command to verify the configuration.

```
[RouterC] ping 8.1.1.1
PING 8.1.1.1: 56 data bytes, press CTRL_C to break
 Reply from 8.1.1.1: bytes=56 Sequence=1 ttl=254 time=31 ms
 Reply from 8.1.1.1: bytes=56 Sequence=2 ttl=254 time=47 ms
 Reply from 8.1.1.1: bytes=56 Sequence=3 ttl=254 time=31 ms
 Reply from 8.1.1.1: bytes=56 Sequence=4 ttl=254 time=16 ms
 Reply from 8.1.1.1: bytes=56 Sequence=5 ttl=254 time=31 ms
--- 8.1.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 16/31/47 ms
```

----End

## Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
 interface GigabitEthernet1/0/0
 ip address 8.1.1.1 255.0.0.0
#
 interface Pos2/0/0
 link-protocol ppp
 ip address 200.1.1.2 255.255.255.0
#
 bgp 65008
 router-id 1.1.1.1
 peer 200.1.1.1 as-number 65009
#
 ipv4-family unicast
 undo synchronization
 network 8.0.0.0
 peer 200.1.1.1 enable
#
 return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 9.1.1.1 255.255.255.0
#
 interface Pos2/0/0
 link-protocol ppp
 ip address 200.1.1.1 255.255.255.0
#
 interface Pos3/0/0
 link-protocol ppp
 ip address 9.1.3.1 255.255.255.0
#
 bgp 65009
 router-id 2.2.2.2
 peer 9.1.1.2 as-number 65009
 peer 9.1.3.2 as-number 65009
 peer 200.1.1.2 as-number 65008
#
 ipv4-family unicast
 undo synchronization
 import-route direct
 peer 9.1.1.2 enable
 peer 9.1.3.2 enable
```

```
 peer 200.1.1.2 enable
#
return
```

- Configuration file of Router C

```
#
sysname RouterC
#
interface Pos2/0/0
link-protocol ppp
ip address 9.1.2.1 255.255.255.0
#
interface Pos3/0/0
link-protocol ppp
ip address 9.1.3.2 255.255.255.0
#
bgp 65009
router-id 3.3.3.3
peer 9.1.2.2 as-number 65009
peer 9.1.3.1 as-number 65009
#
ipv4-family unicast
undo synchronization
peer 9.1.2.2 enable
peer 9.1.3.1 enable
#
return
```

- Configuration file of Router D

```
#
sysname RouterD
#
interface Pos1/0/0
link-protocol ppp
ip address 9.1.1.2 255.255.255.0
#
interface Pos2/0/0
link-protocol ppp
ip address 9.1.2.2 255.255.255.0
#
bgp 65009
router-id 4.4.4.4
peer 9.1.1.1 as-number 65009
peer 9.1.2.1 as-number 65009
#
ipv4-family unicast
undo synchronization
peer 9.1.1.1 enable
peer 9.1.2.1 enable
#
return
```

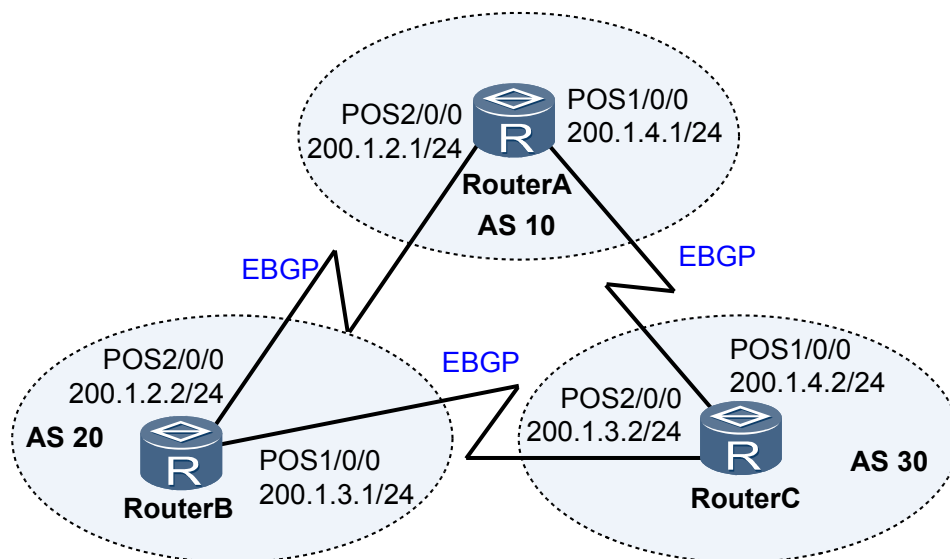
## 8.23.2 Example for Configuring AS-Path Filter

By configuring the AS\_Path filter according to the actual networking, you can improve network performance.

### Networking Requirements

As shown in [Figure 8-2](#), EBGP connections are set up between Router A, Router B, and Router C. Configure the AS-Path filter on Router B. AS 20 thus does not advertise routes of AS 30 to AS 10, or advertise routes of AS 10 to AS 30.

**Figure 8-2** Networking diagram of configuring the AS-Path filter



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure EBGP connections between Router A and Router B, Router B and Router C, and Router C and Router A, and import direct routes.
2. Configure the AS-Path on Router B, and apply the filtering rule.

## Data Preparation

To complete the configuration, you need the following data:

- The router ID of Router A is 1.1.1.1, and the number of its AS is 10.
- The router ID of Router B is 2.2.2.2, and the number of its AS is 20.
- The router ID of Router C is 3.3.3.3, and the number of its AS is 30.

## Procedure

**Step 1** Assign an IP address to each interface.

The configuration details are not mentioned here.

**Step 2** Configure IBGP connections.

# Configure Router A.

```
[RouterA] bgp 10
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 200.1.4.2 as-number 30
[RouterA-bgp] peer 200.1.2.2 as-number 20
[RouterA-bgp] import-route direct
```

# Configure Router B.

```
[RouterB] bgp 20
```

```
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 200.1.2.1 as-number 10
[RouterB-bgp] peer 200.1.3.2 as-number 30
[RouterB-bgp] import-route direct
[RouterB-bgp] quit
```

# Configure Router C.

```
[RouterC] bgp 30
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 200.1.3.1 as-number 20
[RouterC-bgp] peer 200.1.4.1 as-number 10
[RouterC-bgp] import-route direct
[RouterC-bgp] quit
```

# Check the routing table advertised by Router B to peer 200.1.3.2. Take the routing table advertised by Router B to Router C as an example. You can find that Router B advertises the routes destined to the network segment between Router A and Router C.

<RouterB> **display bgp routing-table peer 200.1.3.2 advertised-routes**

```
BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 9
```

|    | Network             | NextHop          | MED | LocPrf | PrefVal | Path/Ogn |
|----|---------------------|------------------|-----|--------|---------|----------|
| *> | 200.1.2.0           | 0.0.0.0          | 0   |        | 0       | ?        |
| *> | 200.1.2.1/32        | 0.0.0.0          | 0   |        | 0       | ?        |
| *> | 200.1.2.2/32        | 200.1.2.1        | 0   |        | 0       | 10?      |
| *> | 200.1.3.0           | 0.0.0.0          | 0   |        | 0       | ?        |
| *> | 200.1.3.1/32        | 200.1.3.2        | 0   |        | 0       | 30?      |
| *> | 200.1.3.2/32        | 0.0.0.0          | 0   |        | 0       | ?        |
| *> | <b>200.1.4.0</b>    | <b>200.1.2.1</b> | 0   |        | 0       | 10?      |
| *> | 200.1.4.1/32        | 200.1.3.2        | 0   |        | 0       | 30?      |
| *> | <b>200.1.4.2/32</b> | <b>200.1.2.1</b> | 0   |        | 0       | 10?      |

Check the routing table of Router C. You can find that Router C learns the route advertised by Router B.

<RouterC> **display bgp routing-table**

```
BGP Local router ID is 3.3.3.3
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 18
```

|    | Network      | NextHop          | MED | LocPrf | PrefVal  | Path/Ogn      |
|----|--------------|------------------|-----|--------|----------|---------------|
| *> | 200.1.2.0    | 200.1.4.1        | 0   |        | 0        | 10?           |
| *  |              | 200.1.3.1        | 0   |        | 0        | 20?           |
| *> | 200.1.2.1/32 | 200.1.3.1        | 0   |        | 0        | 20?           |
| *  |              | 200.1.4.1        |     |        | 0        | 10 20?        |
| *> | 200.1.2.2/32 | 200.1.4.1        | 0   |        | 0        | 10?           |
| *  |              | 200.1.3.1        |     |        | 0        | 20 10?        |
| *> | 200.1.3.0    | 0.0.0.0          | 0   |        | 0        | ?             |
| *  |              | 200.1.3.1        | 0   |        | 0        | 20?           |
| *  |              | 200.1.4.1        |     |        | 0        | 10 20?        |
| *> | 200.1.3.1/32 | 0.0.0.0          | 0   |        | 0        | ?             |
| *> | 200.1.3.2/32 | 200.1.3.1        | 0   |        | 0        | 20?           |
| *  |              | 200.1.4.1        |     |        | 0        | 10 20?        |
| *> | 200.1.4.0    | 0.0.0.0          | 0   |        | 0        | ?             |
| *  |              | 200.1.4.1        | 0   |        | 0        | 10?           |
| *  |              | <b>200.1.3.1</b> |     |        | <b>0</b> | <b>20 10?</b> |
| *> | 200.1.4.1/32 | 0.0.0.0          | 0   |        | 0        | ?             |

```
*> 200.1.4.2/32 200.1.4.1 0 0 10?
* 200.1.3.1 0 0 20 10?
```

**Step 3** Configure the AS-Path filter on Router B and apply the filter on the outbound interface of Router B.

# Create AS-Path filter 1, denying the passing of routes carrying AS 30. The regular expression "\_30\_" indicates any AS list that contains AS 30 and "." matches any character.

```
[RouterB] ip as-path-filter 1 deny _30_
[RouterB] ip as-path-filter 1 permit .*
```

# Create AS-Path filter 2, denying the passing of routes carrying AS 10.

```
[RouterB] ip as-path-filter 2 deny _10_
[RouterB] ip as-path-filter 2 permit .*
```

# Apply the AS-Path filter on two outbound interfaces of Router B.

```
[RouterB] bgp 20
[RouterB-bgp] peer 200.1.2.1 as-path-filter 1 export
[RouterB-bgp] peer 200.1.3.2 as-path-filter 2 export
[RouterB-bgp] quit
```

**Step 4** Check the routing table advertised by Router B, and you can find that the advertised routes to the network segment between Router A and Router C do not exist. Take the route advertised by Router B to Router C as an example.

```
<RouterB> display bgp routing-table peer 200.1.3.2 advertised-routes
```

```
BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 4
 Network NextHop MED LocPrf PrefVal Path/Ogn
*> 200.1.2.0 0.0.0.0 0 0 0 ?
*> 200.1.2.1/32 0.0.0.0 0 0 0 ?
*> 200.1.3.0 0.0.0.0 0 0 0 ?
*> 200.1.3.2/32 0.0.0.0 0 0 0 ?
```

Similarly, the BGP routing table of Router C does not have the two routes.

```
<RouterC> display bgp routing-table
```

```
BGP Local router ID is 3.3.3.3
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 15
 Network NextHop MED LocPrf PrefVal Path/Ogn
*> 200.1.2.0 200.1.4.1 0 0 0 10?
* 200.1.3.1 0 0 0 20?
*> 200.1.2.1/32 200.1.3.1 0 0 0 20?
* 200.1.4.1 0 0 0 10 20?
*> 200.1.2.2/32 200.1.4.1 0 0 0 10?
*> 200.1.3.0 0.0.0.0 0 0 0 ?
* 200.1.3.1 0 0 0 20?
* 200.1.4.1 0 0 0 10 20?
*> 200.1.3.1/32 0.0.0.0 0 0 0 ?
*> 200.1.3.2/32 200.1.3.1 0 0 0 20?
* 200.1.4.1 0 0 0 10 20?
*> 200.1.4.0 0.0.0.0 0 0 0 ?
* 200.1.4.1 0 0 0 10?
*> 200.1.4.1/32 0.0.0.0 0 0 0 ?
*> 200.1.4.2/32 200.1.4.1 0 0 0 10?
```

Check the routing table advertised by Router B, and you can find that advertised routes directly connected to Router A and Router C do not exist. Take the route advertised by Router B to Router A as an example.

```
<RouterB> display bgp routing-table peer 200.1.2.1 advertised-routes

BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 4
 Network NextHop MED LocPrf PrefVal Path/Ogn
* > 200.1.2.0 0.0.0.0 0 0 0 ?
* > 200.1.2.1/32 0.0.0.0 0 0 0 ?
* > 200.1.3.0 0.0.0.0 0 0 0 ?
* > 200.1.3.2/32 0.0.0.0 0 0 0 ?
```

Similarly, the BGP routing table of Router A does not have the two routes.

```
<RouterA> display bgp routing-table

BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 14
 Network NextHop MED LocPrf PrefVal Path/Ogn
* > 200.1.2.0 0.0.0.0 0 0 0 ?
* 200.1.2.2 0 0 0 20?
* > 200.1.2.1/32 200.1.2.2 0 0 0 20?
* 200.1.4.2 0 0 0 30 20?
* > 200.1.2.2/32 0.0.0.0 0 0 0 ?
* > 200.1.3.0 200.1.2.2 0 0 0 20?
* 200.1.4.2 0 0 0 30?
* > 200.1.3.1/32 200.1.4.2 0 0 0 30?
* > 200.1.3.2/32 200.1.2.2 0 0 0 20?
* 200.1.4.2 0 0 0 30 20?
* > 200.1.4.0 0.0.0.0 0 0 0 ?
* 200.1.4.2 0 0 0 30?
* > 200.1.4.1/32 200.1.4.2 0 0 0 30?
* > 200.1.4.2/32 0.0.0.0 0 0 0 ?
```

----End

## Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
interface Pos1/0/0
link-protocol ppp
ip address 200.1.4.1 255.255.255.0
#
interface Pos2/0/0
link-protocol ppp
ip address 200.1.2.1 255.255.255.0
#
bgp 10
router-id 1.1.1.1
peer 200.1.2.2 as-number 20
peer 200.1.4.2 as-number 30
#
ipv4-family unicast
```

```

 undo synchronization
 import-route direct
 peer 200.1.2.2 enable
 peer 200.1.4.2 enable
 #
 return

```

- Configuration file of Router B

```

#
sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 ip address 200.1.3.1 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 200.1.2.2 255.255.255.0
#
bgp 20
 router-id 2.2.2.2
 peer 200.1.2.1 as-number 10
 peer 200.1.3.2 as-number 30
#
 ipv4-family unicast
 undo synchronization
 import-route direct
 peer 200.1.2.1 enable
 peer 200.1.2.1 as-path-filter 1 export
 peer 200.1.3.2 enable
 peer 200.1.3.2 as-path-filter 2 export
#
 ip as-path-filter 1 deny _30_
 ip as-path-filter 1 permit .*
 ip as-path-filter 2 deny _10_
 ip as-path-filter 2 permit .*
#
Return

```

- Configuration file of Router C

```

#
sysname RouterC
#
interface Pos1/0/0
 link-protocol ppp
 ip address 200.1.4.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 200.1.3.2 255.255.255.0
#
bgp 30
 router-id 3.3.3.3
 peer 200.1.3.1 as-number 20
 peer 200.1.4.1 as-number 10
#
 ipv4-family unicast
 undo synchronization
 import-route direct
 peer 200.1.3.1 enable
 peer 200.1.4.1 enable
#
return

```

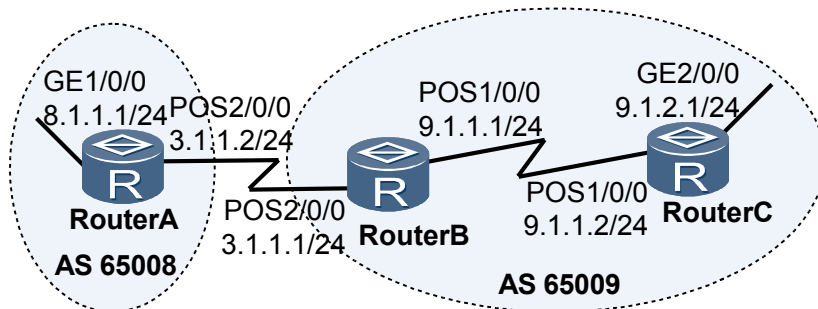
### 8.23.3 Example for Configuring BGP to Interact with IGP

By configuring BGP to interact with IGP, you can enrich the routing table.

## Networking Requirements

As shown in [Figure 8-3](#), OSPF is used inside AS 65009 as an IGP. EBGP is used between Router A and Router B. Router C is a non-BGP router inside the AS.

**Figure 8-3** Networking diagram of configuring BGP to interact with an IGP



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure OSPF on Router B and Router C to implement the interconnection.
2. Configure the EBGP connection on Router A and Router B.
3. Enable BGP and OSPF to import routes from each other on Router B, and check the routes.
4. Configure BGP route aggregation on Router B and simplify the BGP routing table.

## Data Preparation

To complete the configuration, you need the following data:

- The Router ID of Router A is 1.1.1.1, and the number of its AS where it resides is 65008
- The Router ID of Router B is 2.2.2.2, and the number of its AS where it resides is 65009
- The Router ID of Router C is 3.3.3.3, and the number of its AS where it resides is 65009

## Procedure

**Step 1** Assign an IP address to each interface.

The configuration details are not mentioned here.

**Step 2** Configure OSPF.

# Configure Router B.

```
[RouterB] ospf 1
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

# Configure Router C.

```
[RouterC] ospf 1
[RouterC-ospf-1] area 0
```



```
[RouterC-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 9.1.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

### Step 3 Configure the EBGP connections.

# Configure Router A.

```
[RouterA] bgp 65008
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 3.1.1.1 as-number 65009
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] network 8.1.1.0 255.255.255.0
```

# Configure Router B.

```
[RouterB] bgp 65009
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 3.1.1.2 as-number 65008
```

### Step 4 Configure BGP to interact with an IGP.

# On Router B, configure BGP to import OSPF routes.

```
[RouterB-bgp] ipv4-family unicast
[RouterB-bgp-af-ipv4] import-route ospf 1
[RouterB-bgp-af-ipv4] quit
[RouterB-bgp] quit
```

# Check the routing table of Router A.

```
[RouterA] display bgp routing-table
BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete
Total Number of Routes: 3
 Network NextHop MED LocPrf PrefVal Path/Ogn
*> 8.1.1.0/24 0.0.0.0 0 0 0 i
*> 9.1.1.0/24 3.1.1.1 0 0 0 65009?
*> 9.1.2.0/24 3.1.1.1 2 0 0 65009?
```

# Configure OSPF on Router B to import BGP routes.

```
[RouterB] ospf
[RouterB-ospf-1] import-route bgp
[RouterB-ospf-1] quit
```

# Check the routing table of Router C.

```
[RouterC] display ip routing-table
Route Flags: R - relay, D - download to fib

Routing Tables: Public
 Destinations : 7 Routes : 7

Destination/Mask Proto Pre Cost Flags NextHop Interface

 8.1.1.0/24 O_ASE 150 1 D 9.1.1.1 Pos1/0/0
 9.1.1.0/24 Direct 0 0 D 9.1.1.2 Pos1/0/0
 9.1.1.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0
 9.1.2.0/24 Direct 0 0 D 9.1.1.2.1
GigabitEthernet2/0/0
 9.1.2.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
 127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
 127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
```

### Step 5 Configure automatic route aggregation.

# Configure Router B.

```
[RouterB] bgp 65009
[RouterB-bgp] ipv4-family unicast
[RouterB-bgp-af-ipv4] summary automatic
```

# Check the BGP routing table of Router A.

```
[RouterA] display bgp routing-table
BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete
Total Number of Routes: 2
 Network NextHop MED LocPrf PrefVal Path/Ogn
*> 8.1.1.0/24 0.0.0.0 0
*> 9.0.0.0 3.1.1.1 0 65009?
```

# Perform the ping operation to verify the configuration.

```
[RouterA] ping -a 8.1.1.1 9.1.2.1
PING 9.1.2.1: 56 data bytes, press CTRL_C to break
 Reply from 9.1.2.1: bytes=56 Sequence=1 ttl=254 time=15 ms
 Reply from 9.1.2.1: bytes=56 Sequence=2 ttl=254 time=31 ms
 Reply from 9.1.2.1: bytes=56 Sequence=3 ttl=254 time=47 ms
 Reply from 9.1.2.1: bytes=56 Sequence=4 ttl=254 time=46 ms
 Reply from 9.1.2.1: bytes=56 Sequence=5 ttl=254 time=47 ms
--- 9.1.2.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 15/37/47 ms
[RouterA]
```

----End

## Configuration Files

- Configuration file of Router A

```
sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 8.1.1.1 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 3.1.1.2 255.255.255.0
#
bgp 65008
 router-id 1.1.1.1
 peer 3.1.1.1 as-number 65009
#
 ipv4-family unicast
 undo synchronization
 network 8.1.1.0 255.255.255.0
 peer 3.1.1.1 enable
#
return
#
```

- Configuration file of Router B

```
#
sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 ip address 9.1.1.1 255.255.255.0
```

```
#
interface Pos2/0/0
 link-protocol ppp
 ip address 3.1.1.1 255.255.255.0
#
bgp 65009
 router-id 2.2.2.2
 peer 3.1.1.2 as-number 65008
#
ipv4-family unicast
 undo synchronization
 summary automatic
 import-route ospf 1
 peer 3.1.1.2 enable
#
ospf 1
 import-route bgp
 area 0.0.0.0
 network 9.1.1.0 0.0.0.255
#
return
```

- Configuration file of Router C

```
#
sysname RouterC
#
interface GigabitEthernet2/0/0
 ip address 9.1.2.1 255.255.255.0
#
interface Pos1/0/0
 link-protocol ppp
 ip address 9.1.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 9.1.1.0 0.0.0.255
 network 9.1.2.0 0.0.0.255
#
return
```

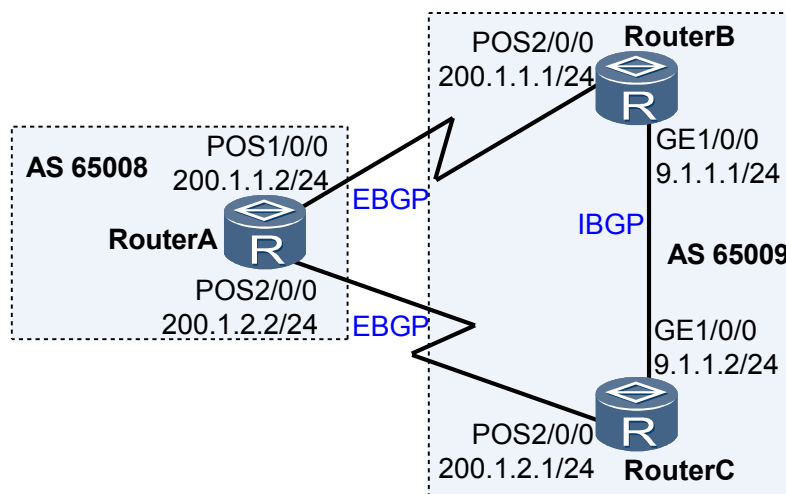
## 8.23.4 Example for Configuring BGP Load Balancing and the MED Attribute

By properly configuring load balancing, you can fully utilize network resources and thus reduce network congestion.

### Networking Requirements

As shown in [Figure 8-4](#), all routers are configured with BGP. Router A resides in AS65008. Router B and Router C reside in AS65009. EBGP runs between Router A and Router B, and between Router A and Router C. IBGP runs between Router B and Router C.

Figure 8-4 Networking diagram of BGP route selection



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure EBGP connections between Router A and Router B, and between Router A and Router C.
2. Configure IBGP connections between Router B and Router C.
3. Configure load balancing and set the MED on Router A, and check the routes.

## Data Preparation

To complete the configuration, you need the following data:

- The Router ID of Router A is 1.1.1.1, and the number of its AS where it resides is 65008. The number of routes for load balancing is 2
- The Router ID of Router B is 2.2.2.2, and the number of its AS where it resides is 65009. The default MED of Router B is 100
- The Router ID of Router C is 3.3.3.3, and the number of its AS where it resides is 65009

## Procedure

**Step 1** Assign an IP address to each interface.

The configuration details are not mentioned here.

**Step 2** Configure the BGP connection.

# Configure Router A.

```
[RouterA] bgp 65008
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 200.1.1.1 as-number 65009
[RouterA-bgp] peer 200.1.2.1 as-number 65009
[RouterA-bgp] quit
```

# Configure Router B.

```
[RouterB] bgp 65009
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 200.1.1.2 as-number 65008
[RouterB-bgp] peer 9.1.1.2 as-number 65009
[RouterB-bgp] ipv4-family unicast
[RouterB-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
[RouterB-bgp-af-ipv4] quit
[RouterB-bgp] quit
```

#### # Configure Router C.

```
[RouterC] bgp 65009
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 200.1.2.2 as-number 65008
[RouterC-bgp] peer 9.1.1.1 as-number 65009
[RouterC-bgp] ipv4-family unicast
[RouterC-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
[RouterC-bgp-af-ipv4] quit
[RouterC-bgp] quit
```

#### # Display the routing table of Router A.

```
[RouterA] display bgp routing-table 9.1.1.0 24

BGP local router ID : 1.1.1.1
Local AS number : 65008
Paths: 2 available, 1 best, 1 select
BGP routing table entry information of 9.1.1.0/24:
From: 200.1.1.1 (2.2.2.2)
Route Duration: 00h00m01s
Direct Out-interface: Pos1/0/0
Original nexthop: 200.1.1.1
Qos information : 0x0
AS-path 65009, origin igp, MED 0, pref-val 0, valid, external, best, select,
active, pre 255
Advertised to such 2 peers:
 200.1.1.1
 200.1.2.1
BGP routing table entry information of 9.1.1.0/24:
From: 200.1.2.1 (3.3.3.3)
Route Duration: 00h25m32s
Direct Out-interface: Pos2/0/0
Original nexthop: 200.1.2.1
Qos information : 0x0
AS-path 65009, origin igp, MED 0, pref-val 0, valid, external, pre 255, not
selected for router ID
Not advertised to any peer yet
```

You can view that there are two valid routes to the destination 9.1.1.0/24. The route whose next hop is 200.1.1.1 is the optimal route. This is because the router ID of Router B is smaller.

### Step 3 Configure load balancing.

#### # Configure Router A.

```
[RouterA] bgp 65008
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] maximum load-balancing 2
[RouterA-bgp-af-ipv4] quit
[RouterA-bgp] quit
```

#### # Check the routing table of Router A.

```
[RouterA] display bgp routing-table 9.1.1.0 24

BGP local router ID : 1.1.1.1
Local AS number : 65008
Paths: 2 available, 1 best, 2 select
BGP routing table entry information of 9.1.1.0/24:
```

```

 From: 200.1.1.1 (2.2.2.2)
 Route Duration: 00h13m55s
 Direct Out-interface: Pos1/0/0
 Original nexthop: 200.1.1.1
 Qos information : 0x0
 AS-path 65009, origin igp, MED 0, pref-val 0, valid, external, best, select,
 active, pre 255
 Advertised to such 2 peers:
 200.1.1.1
 200.1.2.1
 BGP routing table entry information of 9.1.1.0/24:
 From: 200.1.2.1 (3.3.3.3)
 Route Duration: 00h13m37s
 Direct Out-interface: Pos2/0/0
 Original nexthop: 200.1.2.1
 Qos information : 0x0
 AS-path 65009, origin igp, MED 0, pref-val 0, valid, external, select, active, pre
 255, not selected for router ID
 Not advertised to any peer yet

```

You can view that BGP route 9.1.1.0/24 has two next hops: 200.1.1.1 and 200.1.2.1. They are optimal routes.

#### Step 4 Set the MEDs.

# Set the MED sent by Router B to Router A through the policy.

```

[RouterB] route-policy 10 permit node 10
[RouterB-route-policy] apply cost 100
[RouterB-route-policy] quit
[RouterB] bgp 65009
[RouterB-bgp] peer 200.1.1.2 route-policy 10 export

```

# Check the routing table of Router A.

```

[RouterA] display bgp routing-table 9.1.1.0 24

BGP local router ID : 1.1.1.1
Local AS number : 65008
Paths: 2 available, 1 best, 1 select
BGP routing table entry information of 9.1.1.0/24:
From: 200.1.2.1 (3.3.3.3)
Route Duration: 00h18m05s
Direct Out-interface: Pos2/0/0
Original nexthop: 200.1.2.1
Qos information : 0x0
AS-path 65009, origin igp, MED 0, pref-val 0, valid, external, best, select,
active, pre 255, not selected for router ID
Advertised to such 2 peers:
 200.1.1.1
 200.1.2.1
BGP routing table entry information of 9.1.1.0/24:
From: 200.1.1.1 (2.2.2.2)
Route Duration: 00h00m13s
Direct Out-interface: Pos1/0/0
Original nexthop: 200.1.1.1
Qos information : 0x0
AS-path 65009, origin igp, MED 100, pref-val 0, valid, external, pre 255, not
selected for MED
Not advertised to any peer yet

```

You can view that the MED of the route with the next hop 200.1.1.1 (Router B) is 100, and the MED of the route with the next hop 200.1.2.1 is 0. Therefore, the route with the smaller MED is preferred.

----End

## Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 ip address 200.1.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 200.1.2.2 255.255.255.0
#
bgp 65008
 router-id 1.1.1.1
 peer 200.1.1.1 as-number 65009
 peer 200.1.2.1 as-number 65009
#
 ipv4-family unicast
 undo synchronization
 maximum load-balancing 2
 peer 200.1.1.1 enable
 peer 200.1.2.1 enable
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 9.1.1.1 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 200.1.1.1 255.255.255.0
#
bgp 65009
 router-id 2.2.2.2
 peer 9.1.1.2 as-number 65009
 peer 200.1.1.2 as-number 65008
#
 ipv4-family unicast
 undo synchronization
 network 9.1.1.0 255.255.255.0
 peer 9.1.1.2 enable
 peer 200.1.1.2 enable
#
 route-policy 10 permit node 10
 apply cost 100
#
return
```

- Configuration file of Router C

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 9.1.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 200.1.2.1 255.255.255.0
#
bgp 65009
 router-id 3.3.3.3
 peer 9.1.1.1 as-number 65009
 peer 200.1.2.2 as-number 65008
```

```
#
ipv4-family unicast
undo synchronization
network 9.1.1.0 255.255.255.0
peer 9.1.1.1 enable
peer 200.1.2.2 enable
#
return
```

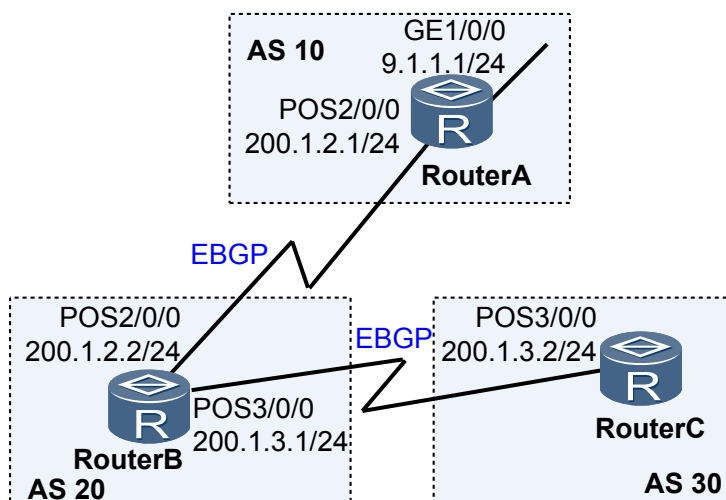
## 8.23.5 Example for Configuring the BGP Community Attribute

By setting the community attribute, you can flexibly control BGP route selection.

### Networking Requirements

As shown in [Figure 8-5](#), Router B creates EBGP connections with Router A and Router C. You can configure the No\_Export community attribute on Router A. Thus, the routes advertised from AS 10 to AS 20 are not advertised to other ASs.

**Figure 8-5** Networking diagram of configuring the BGP community



### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the EBGP connections between Router A and Router B, and between Router B and Router C.
2. Configure the routing policy on Router A, and advertise No\_Export community attribute.

### Data Preparation

To complete the configuration, you need the following data:

- The router ID of Router A is 1.1.1.1 and its AS number is 10.
- The router ID of Router B is 2.2.2.2 and its AS number is 20.
- The router ID of Router C is 3.3.3.3 and its AS number is 30.



## Procedure

### Step 1 Assign an IP address to each interface.

The configuration details are not mentioned here.

### Step 2 Configure EBGP.

# Configure Router A.

```
[RouterA] bgp 10
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 200.1.2.2 as-number 20
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
[RouterA-bgp-af-ipv4] quit
```

# Configure Router B.

```
[RouterB] bgp 20
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 200.1.2.1 as-number 10
[RouterB-bgp] peer 200.1.3.2 as-number 30
[RouterB-bgp] quit
```

# Configure Router C.

```
[RouterC] bgp 30
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 200.1.3.1 as-number 20
[RouterC-bgp] quit
```

# Check the routing table of Router B.

```
[RouterB] display bgp routing-table 9.1.1.0
BGP local router ID : 2.2.2.2
Local AS number : 20
Paths: 1 available, 1 best, 1 select
BGP routing table entry information of 9.1.1.0/24:
From: 200.1.2.1 (1.1.1.1)
Route Duration: 00h00m15s
Direct Out-interface: Pos2/0/0
Original nexthop: 200.1.2.1
Qos information : 0x0
AS-path 10, origin igp, MED 0, pref-val 0, valid, external, best, select, active,
pre 255
Advertised to such 2 peers:
 200.1.2.1
 200.1.3.2
```

You can view that Router B advertises the received routes to Router C in AS 30.

# Check the routing table of Router C.

```
[RouterC] display bgp routing-table
BGP Local router ID is 3.3.3.3
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete
Total Number of Routes: 1
 Network NextHop MED LocPrf PrefVal Path/Ogn
* > 9.1.1.0/24 200.1.3.1 0 0 20 10i
```

You can find that Router C has learned a route to the destination 9.1.1.0/24 from Router B.

### Step 3 Configure BGP community attributes.

# Configure the routing policy on Router A to enable Router B not to advertise the routes advertised by Router A to any other AS.

```
[RouterA] route-policy comm_policy permit node 10
[RouterA-route-policy] apply community no-export
[RouterA-route-policy] quit
```

# Apply routing policies.

```
[RouterA] bgp 10
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] peer 200.1.2.2 route-policy comm_policy export
[RouterA-bgp-af-ipv4] peer 200.1.2.2 advertise-community
```

# Check the routing table of Router B.

```
[RouterB] display bgp routing-table 9.1.1.0

BGP local router ID : 2.2.2.2
Local AS number : 20
Paths: 1 available, 1 best, 1 select
BGP routing table entry information of 9.1.1.0/24:
From: 200.1.2.1 (1.1.1.1)
Route Duration: 00h00m05s
Direct Out-interface: Pos1/0/0
Original nexthop: 200.1.2.1
Qos information : 0x0
Community:no-export
AS-path 10, origin igp, MED 0, pref-val 0, valid, external, best, select, pre 255
Not advertised to any peer yet
```

You can view the configured community attribute in the BGP routing table of Router B. At this time, there are no routes to the destination 9.1.1.0/24 in the BGP routing table of Router C.

----End

## Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
ip address 9.1.1.1 255.255.255.0
#
interface Pos2/0/0
link-protocol ppp
ip address 200.1.2.1 255.255.255.0
#
bgp 10
router-id 1.1.1.1
peer 200.1.2.2 as-number 20
#
ipv4-family unicast
undo synchronization
network 9.1.1.0 255.255.255.0
peer 200.1.2.2 enable
peer 200.1.2.2 route-policy comm_policy export
peer 200.1.2.2 advertise-community
#
route-policy comm_policy permit node 10
apply community no-export
#
return
```

- Configuration file of Router B

```
#
sysname RouterB
#
interface Pos2/0/0
```

```
link-protocol ppp
ip address 200.1.2.2 255.255.255.0
#
interface Pos3/0/0
link-protocol ppp
ip address 200.1.3.1 255.255.255.0
#
bgp 20
router-id 2.2.2.2
peer 200.1.2.1 as-number 10
peer 200.1.3.2 as-number 30
#
ipv4-family unicast
undo synchronization
peer 200.1.2.1 enable
peer 200.1.3.2 enable
#
return
```

- Configuration file of Router C

```
#
sysname RouterC
#
interface Pos3/0/0
link-protocol ppp
ip address 200.1.3.2 255.255.255.0
#
bgp 30
router-id 3.3.3.3
peer 200.1.3.1 as-number 20
#
ipv4-family unicast
undo synchronization
peer 200.1.3.1 enable
#
return
```

## 8.23.6 Example for Configuring a BGP Route Reflector

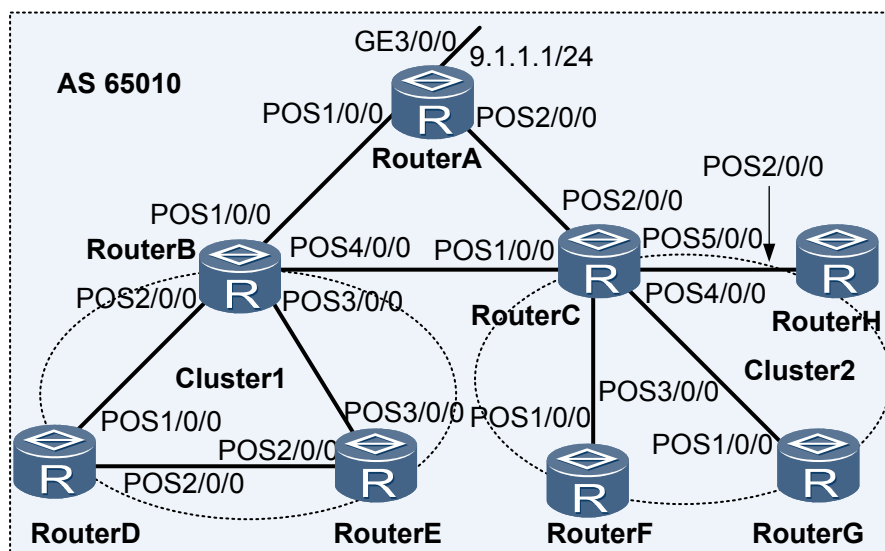
A BGP route reflector avoids fully meshed connections between IBGP peers and thus simplifies the network.

### Networking Requirements

As shown in [Figure 8-6](#), Router A is a non-client. Router B is an RR of Cluster 1. Router D and Router E are two clients of Cluster 1. Because the IBGP connection is created between Router D and Router E, they do not need an RR. Router C is the RR of Cluster 2. Router F, Router G, and Router H are the clients of Cluster 2.

It is required that peer groups be used to facilitate configuration and management.

**Figure 8-6** Networking diagram of configuring a BGP RR



| Device   | Interface | IP address  | Device   | Interface | IP address  |
|----------|-----------|-------------|----------|-----------|-------------|
| Router A | GE 3/0/0  | 9.1.1.1/24  | Router C | POS 4/0/0 | 10.1.8.1/24 |
|          | POS 1/0/0 | 10.1.1.2/24 |          | POS 5/0/0 | 10.1.9.1/24 |
|          | POS 2/0/0 | 10.1.3.2/24 | Router D | POS 1/0/0 | 10.1.4.2/24 |
| Router B | POS 1/0/0 | 10.1.1.1/24 | Router E | POS 2/0/0 | 10.1.6.1/24 |
|          | POS 2/0/0 | 10.1.4.1/24 | Router E | POS 2/0/0 | 10.1.6.2/24 |
|          | POS 3/0/0 | 10.1.5.1/24 | Router F | POS 3/0/0 | 10.1.5.2/24 |
|          | POS 4/0/0 | 10.1.2.1/24 | Router F | POS 1/0/0 | 10.1.7.2/24 |
| Router C | POS 1/0/0 | 10.1.2.2/24 | Router G | POS 1/0/0 | 10.1.8.2/24 |
|          | POS 2/0/0 | 10.1.3.1/24 | Router H | POS 2/0/0 | 10.1.9.2/24 |
|          | POS 3/0/0 | 10.1.7.1/24 |          |           |             |

## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the IBGP connection between the client and RR, and the non-client and RR.
2. Configure the RR on Router B and Router C, specify the clients, and check the routes.

## Data Preparation

To complete the configuration, you need the following data:

- The number of AS is 65010.
- The router IDs of Router A, Router B, Router C, Router D, Router E, Router F, Router G, and Router H are 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4, 5.5.5.5, 6.6.6.6, 7.7.7.7 and 8.8.8.8 respectively.

- The cluster IDs of the clusters that Router B and Router C belong to are 1 and 2, respectively.

## Procedure

**Step 1** Assign an IP address to each interface.

The configuration details are not mentioned here.

**Step 2** Configure the IBGP connections between the clients and the RR and between the non-clients and the RR.

The configuration details are not mentioned here.

**Step 3** Configure the RR.

# Configure Router B.

```
[RouterB] bgp 65010
[RouterB-bgp] group in_rr internal
[RouterB-bgp] peer 10.1.4.2 group in_rr
[RouterB-bgp] peer 10.1.5.2 group in_rr
[RouterB-bgp] ipv4-family unicast
[RouterB-bgp-af-ipv4] peer in_rr reflect-client
[RouterB-bgp-af-ipv4] undo reflect between-clients
[RouterB-bgp-af-ipv4] reflector cluster-id 1
[RouterB-bgp-af-ipv4] quit
```

# Configure Router C.

```
[RouterC] bgp 65010
[RouterC-bgp] group in_rr internal
[RouterC-bgp] peer 10.1.7.2 group in_rr
[RouterC-bgp] peer 10.1.8.2 group in_rr
[RouterC-bgp] peer 10.1.9.2 group in_rr
[RouterC-bgp] ipv4-family unicast
[RouterC-bgp-af-ipv4] peer in_rr reflect-client
[RouterC-bgp-af-ipv4] reflector cluster-id 2
[RouterC-bgp-af-ipv4] quit
```

# Display the routing table of Router D.

```
[RouterD] display bgp routing-table 9.1.1.0
BGP local router ID : 4.4.4.4
Local AS number : 65010
Paths: 1 available, 0 best, 0 select
BGP routing table entry information of 9.1.1.0/24:
From: 10.1.4.1 (2.2.2.2)
Route Duration: 00h00m14s
Relay IP Nexthop: 0.0.0.0
Relay IP Out-Interface:
Original nexthop: 10.1.1.2
Qos information : 0x0
AS-path Nil, origin igp, MED 0, localpref 100, pref-val 0, internal, pre 255
Originator: 1.1.1.1
Cluster list: 0.0.0.1
Not advertised to any peer yet
```

You can view that Router D has learned the route advertised by Router A from Router B. For details, see the Originator and Cluster\_ID attributes of the route.

----End

## Configuration Files

- Configuration file of Router A

#

```

 sysname RouterA
 #
 interface GigabitEthernet3/0/0
 ip address 9.1.1.1 255.255.255.0
 #
 interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.0
 #
 interface Pos2/0/0
 link-protocol ppp
 ip address 10.1.3.2 255.255.255.0
 #
 bgp 65010
 router-id 1.1.1.1
 peer 10.1.1.1 as-number 65010
 peer 10.1.3.1 as-number 65010
 #
 ipv4-family unicast
 undo synchronization
 network 9.1.1.0 255.255.255.0
 peer 10.1.1.1 enable
 peer 10.1.3.1 enable
 #
 return

```

● Configuration file of Router B

```

 #
 sysname RouterB
 #
 interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.0
 #
 interface Pos2/0/0
 link-protocol ppp
 ip address 10.1.4.1 255.255.255.0
 #
 interface Pos3/0/0
 link-protocol ppp
 ip address 10.1.5.1 255.255.255.0
 #
 interface Pos4/0/0
 link-protocol ppp
 ip address 10.1.2.1 255.255.255.0
 #
 bgp 65010
 router-id 2.2.2.2
 peer 10.1.1.2 as-number 65010
 peer 10.1.2.2 as-number 65010
 group in_rr internal
 peer 10.1.4.2 as-number 65010
 peer 10.1.4.2 group in_rr
 peer 10.1.5.2 as-number 65010
 peer 10.1.5.2 group in_rr
 #
 ipv4-family unicast
 undo synchronization
 undo reflect between-clients
 reflector cluster-id 1
 peer 10.1.1.2 enable
 peer 10.1.2.2 enable
 peer in_rr enable
 peer in_rr reflect-client
 peer 10.1.4.2 enable
 peer 10.1.4.2 group in_rr
 peer 10.1.5.2 enable
 peer 10.1.5.2 group in_rr
 #

```

```
return
```

- Configuration file of Router C

```
#
sysname RouterC
#
interface Pos1/0/0
link-protocol ppp
ip address 10.1.2.2 255.255.255.0
#
interface Pos2/0/0
link-protocol ppp
ip address 10.1.3.1 255.255.255.0
#
interface Pos3/0/0
link-protocol ppp
ip address 10.1.7.1 255.255.255.0
#
interface Pos4/0/0
link-protocol ppp
ip address 10.1.8.1 255.255.255.0
#
interface Pos5/0/0
link-protocol ppp
ip address 10.1.9.1 255.255.255.0
#
bgp 65010
router-id 3.3.3.3
peer 10.1.2.1 as-number 65010
peer 10.1.3.2 as-number 65010
group in_rr internal
peer 10.1.7.2 as-number 65010
peer 10.1.7.2 group in_rr
peer 10.1.8.2 as-number 65010
peer 10.1.8.2 group in_rr
peer 10.1.9.2 as-number 65010
peer 10.1.9.2 group in_rr
#
ipv4-family unicast
undo synchronization
reflector cluster-id 2
peer 10.1.2.1 enable
peer 10.1.3.2 enable
peer in_rr enable
peer in_rr reflect-client
peer 10.1.7.2 enable
peer 10.1.7.2 group in_rr
peer 10.1.8.2 enable
peer 10.1.8.2 group in_rr
peer 10.1.9.2 enable
peer 10.1.9.2 group in_rr
#
return
```

- Configuration file of Router D

```
#
sysname RouterD
#
interface Pos1/0/0
link-protocol ppp
ip address 10.1.4.2 255.255.255.0
#
interface Pos2/0/0
link-protocol ppp
ip address 10.1.6.1 255.255.255.0
#
bgp 65010
router-id 4.4.4.4
peer 10.1.4.1 as-number 65010
peer 10.1.6.2 as-number 65010
```

```
#
ipv4-family unicast
 undo synchronization
 peer 10.1.4.1 enable
 peer 10.1.6.2 enable
#
return
```

 **NOTE**

The configuration file of other routers is similar to that of Router D and is omitted here.

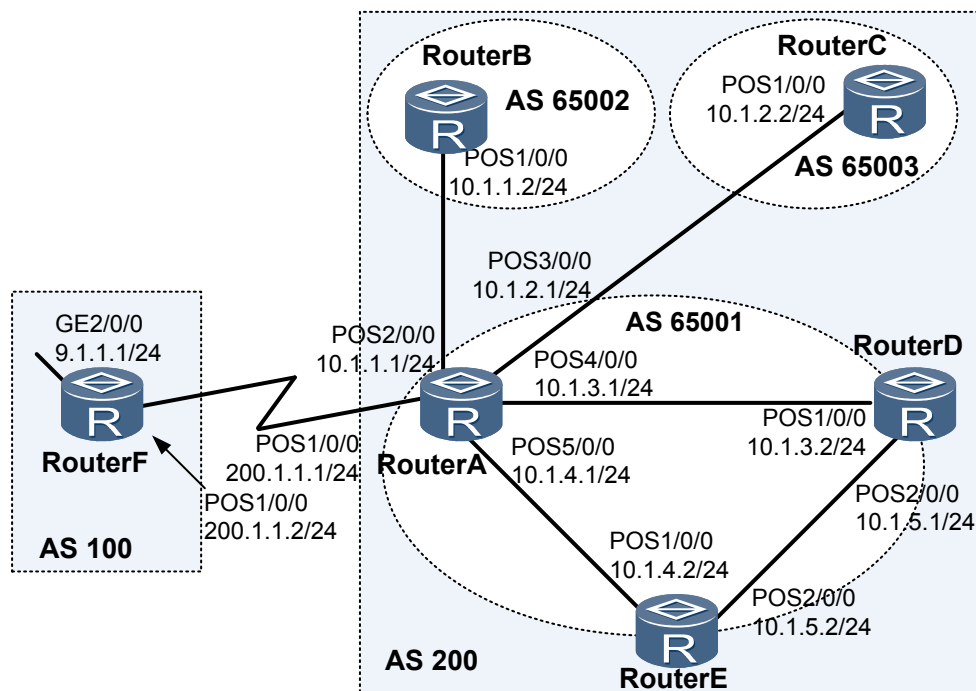
## 8.23.7 Example for Configuring a BGP Confederation

A BGP confederation can reduce increasing IBGP connections on a network.

### Networking Requirements

As shown in [Figure 8-7](#), there are several BGP routers in AS 200. AS 200 is divided into AS 65001, AS 65002 and AS 65003 to reduce IBGP connections, IBGP full meshes are established between the three routers in AS 65001.

**Figure 8-7** Networking diagram of configuring the confederation



### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the BGP confederation on each router.
2. Configure the IBGP connection in AS 65001.
3. Configure the EBGP connection between AS 100 and AS 200, and check the routes.



## Data Preparation

To complete the configuration, you need the following data:

- The router IDs of Router A, Router B, Router C, Router D, Router E, and Router F are 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4, 5.5.5.5, and 6.6.6.6.
- The AS number is 100. The three sub-ASs of AS 200 are AS 65001, AS 65002, and AS 65003.

## Procedure

**Step 1** Assign an IP address to each interface.

The configuration details are not mentioned here.

**Step 2** Configure the BGP confederation.

# Configure Router A.

```
[RouterA] bgp 65001
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] confederation id 200
[RouterA-bgp] confederation peer-as 65002 65003
[RouterA-bgp] peer 10.1.1.2 as-number 65002
[RouterA-bgp] peer 10.1.2.2 as-number 65003
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] peer 10.1.1.2 next-hop-local
[RouterA-bgp-af-ipv4] peer 10.1.2.2 next-hop-local
[RouterA-bgp-af-ipv4] quit
```

# Configure Router B.

```
[RouterB] bgp 65002
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] confederation id 200
[RouterB-bgp] confederation peer-as 65001
[RouterB-bgp] peer 10.1.1.1 as-number 65001
[RouterB-bgp] quit
```

# Configure Router C.

```
[RouterC] bgp 65003
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] confederation id 200
[RouterC-bgp] confederation peer-as 65001
[RouterC-bgp] peer 10.1.2.1 as-number 65001
[RouterC-bgp] quit
```

**Step 3** Configure IBGP connections inside AS 65001.

# Configure Router A.

```
[RouterA] bgp 65001
[RouterA-bgp] peer 10.1.3.2 as-number 65001
[RouterA-bgp] peer 10.1.4.2 as-number 65001
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] peer 10.1.3.2 next-hop-local
[RouterA-bgp-af-ipv4] peer 10.1.4.2 next-hop-local
[RouterA-bgp-af-ipv4] quit
```

# Configure Router D.

```
[RouterD] bgp 65001
[RouterD-bgp] router-id 4.4.4.4
[RouterD-bgp] confederation id 200
[RouterD-bgp] peer 10.1.3.1 as-number 65001
```

```
[RouterD-bgp] peer 10.1.5.2 as-number 65001
[RouterD-bgp] quit
```

# Configure Router E.

```
[RouterE] bgp 65001
[RouterE-bgp] router-id 5.5.5.5
[RouterE-bgp] confederation id 200
[RouterE-bgp] peer 10.1.4.1 as-number 65001
[RouterE-bgp] peer 10.1.5.1 as-number 65001
[RouterE-bgp] quit
```

#### Step 4 Configure the EBGP connection between AS 100 and AS 200.

# Configure Router A.

```
[RouterA] bgp 65001
[RouterA-bgp] peer 200.1.1.2 as-number 100
[RouterA-bgp] quit
```

# Configure Router F.

```
[RouterF] bgp 100
[RouterF-bgp] router-id 6.6.6.6
[RouterF-bgp] peer 200.1.1.1 as-number 200
[RouterF-bgp] ipv4-family unicast
[RouterF-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
[RouterF-bgp-af-ipv4] quit
```

#### Step 5 Verify the configuration.

# Check the routing table of Router B.

```
[RouterB] display bgp routing-table
BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete
Total Number of Routes: 1
 Network NextHop MED LocPrf PrefVal Path/Ogn
*>i 9.1.1.0/24 10.1.1.1 0 100 0 (65001) 100i
[RouterB] display bgp routing-table 9.1.1.0
BGP local router ID : 2.2.2.2
Local AS number : 65002
Paths: 1 available, 1 best, 1 select
BGP routing table entry information of 9.1.1.0/24:
From: 10.1.1.1 (1.1.1.1)
Route Duration: 00h12m29s
Relay IP Nexthop: 0.0.0.0
Relay IP Out-Interface: Pos1/0/0
Original nexthop: 10.1.1.1
Qos information : 0x0
AS-path (65001) 100, origin igp, MED 0, localpref 100, pref-val 0, valid, external-
confed, best, select, active, pre 255
Not advertised to any peer yet
```

# Check the BGP routing table of Router D.

```
[RouterD] display bgp routing-table
BGP Local router ID is 4.4.4.4
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete
Total Number of Routes: 1
 Network NextHop MED LocPrf PrefVal Path/Ogn
*>i 9.1.1.0/24 10.1.3.1 0 100 0 100i
[RouterD] display bgp routing-table 9.1.1.0
BGP local router ID : 4.4.4.4
Local AS number : 65001
Paths: 1 available, 1 best, 1 select
```

```
BGP routing table entry information of 9.1.1.0/24:
From: 10.1.3.1 (1.1.1.1)
Route Duration: 00h23m57s
Relay IP Nexthop: 0.0.0.0
Relay IP Out-Interface: Pos1/0/0
Original nexthop: 10.1.3.1
Qos information : 0x0
AS-path 100, origin igp, MED 0, localpref 100, pref-val 0, valid, internal-
confed, best, select, active, pre 255
Not advertised to any peer yet
```

----End

## Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 ip address 200.1.1.1 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.0
#
interface Pos3/0/0
 link-protocol ppp
 ip address 10.1.2.1 255.255.255.0
#
interface Pos4/0/0
 link-protocol ppp
 ip address 10.1.3.1 255.255.255.0
#
interface Pos3/2/0
 link-protocol ppp
 ip address 10.1.4.1 255.255.255.0
#
bgp 65001
 router-id 1.1.1.1
 confederation id 200
 confederation peer-as 65002 65003
 peer 200.1.1.2 as-number 100
 peer 10.1.1.2 as-number 65002
 peer 10.1.2.2 as-number 65003
 peer 10.1.3.2 as-number 65001
 peer 10.1.4.2 as-number 65001
#
ipv4-family unicast
 undo synchronization
 peer 200.1.1.2 enable
 peer 10.1.1.2 enable
 peer 10.1.1.2 next-hop-local
 peer 10.1.2.2 enable
 peer 10.1.2.2 next-hop-local
 peer 10.1.3.2 enable
 peer 10.1.3.2 next-hop-local
 peer 10.1.4.2 enable
 peer 10.1.4.2 next-hop-local
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
interface Pos1/0/0
```

```

 link-protocol ppp
 ip address 10.1.1.2 255.255.255.0
 #
 bgp 65002
 router-id 2.2.2.2
 confederation id 200
 confederation peer-as 65001
 peer 10.1.1.1 as-number 65001
 #
 ipv4-family unicast
 undo synchronization
 peer 10.1.1.1 enable
 #
 return

```

 **NOTE**

The configuration file of Router C is similar to that of Router B, and is not mentioned here.

● Configuration file of Router D

```

 #
 sysname RouterD
 #
 interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.3.2 255.255.255.0
 #
 interface Pos2/0/0
 link-protocol ppp
 ip address 10.1.5.1 255.255.255.0
 #
 bgp 65001
 router-id 4.4.4.4
 confederation id 200
 peer 10.1.3.1 as-number 65001
 peer 10.1.5.2 as-number 65001
 #
 ipv4-family unicast
 undo synchronization
 peer 10.1.3.1 enable
 peer 10.1.5.2 enable
 #
 return

```

 **NOTE**

The configuration file of Router E is similar to that of Router D, and is not mentioned here.

● Configuration file of Router F

```

 #
 sysname RouterF
 #
 interface GigabitEthernet2/0/0
 ip address 9.1.1.1 255.255.255.0
 #
 interface Pos1/0/0
 link-protocol ppp
 ip address 200.1.1.2 255.255.255.0
 #
 bgp 100
 router-id 6.6.6.6
 peer 200.1.1.1 as-number 200
 #
 ipv4-family unicast
 undo synchronization
 network 9.1.1.0 255.255.255.0
 peer 200.1.1.1 enable
 #
 Return

```

## 8.23.8 Example for Configuring a BGP Routing Policy

By configuring BGP routing policies, you can flexibly control the traffic on a complex network.

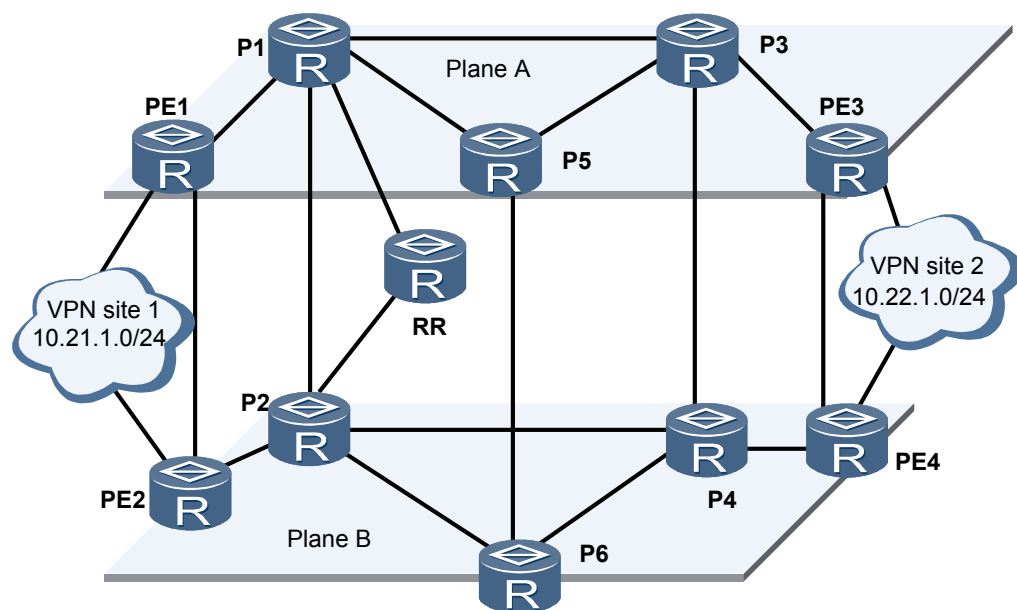
### Networking Requirements

**Figure 8-8** shows the simplified MPLS network that carries multiple types of L3VPN services, such as multimedia, signaling, and accounting. In **Figure 8-8**, two sites, each of which has two PEs accessing the core layer, are taken as an example. The core layer is divided into two planes. All the P nodes on the same plane are full-meshed P nodes. Nodes on different planes are connected to provide backup paths across plane. MP-BGP is used to advertise inner labels and VPNv4 routes between the PEs. All PEs set up MP-IBGP peer relationships with the RR.

#### NOTE

**Figure 8-8** is a simplified networking diagram, in which two sites are taken as an example and each plane takes three P nodes and one RR as an example. In the actual network, there are 14 sites with 28 PEs and each plane has four P nodes and two RR nodes, and each RR needs to set up MP-IBGP connections with 28 PEs.

**Figure 8-8** Networking diagram



In **Figure 8-8**, each PE sends BGP Update messages to the RR, other PEs receive BGP Update messages from different planes. Therefore, routing policies need to be deployed to ensure that one VPN flow is transmitted only through one plane.

### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure different RDs for two PEs in the same site to ensure that each PE can receive two routes from different BGP next hops in the remote site. When two PEs in a site advertise the routes to the same destination, configuring different RDs for the two PEs can ensure

that BGP peers consider the advertised routes as two different routes. This is because BGP-VPNv4 uses the VPNv4 addresses that consist of IPv4 addresses and RDs.

2. Assign different communities for BGP routes from PE in plane A and BGP routes from PE in plane B.
3. Set different local preferences for routes based on the community attributes of the routes. In this manner, the PEs in plane A choose the routes advertised by remote PEs in plane A, and the PEs in plane B always choose the routes advertised by the remote PEs in plane B.

## Data Preparation

To complete the configuration, you need the following data.

**Table 8-2** IP addresses of physical interfaces

| Local Device | Local Interface and Its IP Address | Remote Interface and Its IP Address | Remote Device |
|--------------|------------------------------------|-------------------------------------|---------------|
| P1           | GE 1/0/0<br>10.1.1.1/30            | GE 1/0/0<br>10.1.1.2/30             | P3            |
| P1           | GE 2/0/0<br>10.1.2.1/30            | GE 1/0/0<br>10.1.2.2/30             | P5            |
| P1           | GE 3/0/0<br>10.1.3.1/30            | GE 1/0/0<br>10.1.3.2/30             | RR            |
| P1           | GE 3/1/0<br>10.1.4.1/30            | GE 1/0/0<br>10.1.4.2/30             | P2            |
| P1           | GE 3/2/0<br>10.1.5.1/30            | GE 1/0/0<br>10.1.5.2/30             | PE1           |
| P2           | GE 3/1/0<br>10.1.6.1/30            | GE 1/0/0<br>10.1.6.2/30             | P6            |
| P2           | GE 3/0/0<br>10.1.7.1/30            | GE 1/0/0<br>10.1.7.2/30             | P4            |
| P2           | GE 2/0/0<br>10.1.8.1/30            | GE 2/0/0<br>10.1.8.2/30             | RR            |
| P2           | GE 3/2/0<br>10.1.9.1/30            | GE 1/0/0<br>10.1.9.2/30             | PE2           |
| P3           | GE 2/0/0<br>10.1.10.1/30           | GE 2/0/0<br>10.1.10.2/30            | P5            |
| P3           | GE 3/0/0<br>10.1.11.1/30           | GE 2/0/0<br>10.1.11.2/30            | P4            |
| P3           | GE 3/1/0<br>10.1.12.1/30           | GE 1/0/0<br>10.1.12.2/30            | PE3           |

| Local Device | Local Interface and Its IP Address | Remote Interface and Its IP Address | Remote Device |
|--------------|------------------------------------|-------------------------------------|---------------|
| P4           | GE 3/0/0<br>10.1.13.1/30           | GE 3/0/0<br>10.1.13.2/30            | P6            |
| P4           | GE 3/1/0<br>10.1.14.1/30           | GE 1/0/0<br>10.1.14.2/30            | PE4           |
| P5           | GE 3/0/0<br>10.1.15.1/30           | GE 2/0/0<br>10.1.15.2/30            | P6            |
| PE1          | GE 2/0/0<br>10.1.16.1/30           | GE 2/0/0<br>10.1.16.2/30            | PE2           |
| PE3          | GE 2/0/0<br>10.1.17.1/30           | GE 2/0/0<br>10.1.17.2/30            | PE4           |

**Table 8-3** IP addresses of loopback interfaces

| Local Device | IP Address of the local Loopback 0 Interface | Remote Device | IP Address of the Remote Loopback 0 Interface |
|--------------|----------------------------------------------|---------------|-----------------------------------------------|
| P1           | 10.1.1.9/32                                  | P2            | 10.2.2.9/32                                   |
| P3           | 10.3.3.9/32                                  | P4            | 10.4.4.9/32                                   |
| P5           | 10.5.5.9/32                                  | P6            | 10.6.6.9/32                                   |
| PE1          | 10.7.7.9/32                                  | PE2           | 10.8.8.9/32                                   |
| PE3          | 10.9.9.9/32                                  | PE4           | 10.10.10.9/32                                 |
| RR           | 10.11.11.9/32                                |               |                                               |

**Table 8-4** BGP parameter Value

| BGP Parameter           | Value                                       |
|-------------------------|---------------------------------------------|
| AS number               | 65000                                       |
| Router ID               | Same as the address of Loopback 0 interface |
| BGP community attribute | Plane A: 65000:100<br>Plane B: 65000:200    |

| BGP Parameter         | Value                                                                                                                                                                                                                                                                           |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BGP local preference  | Plane A: The local preference of community attribute 65000:100 is set to 200.<br>Plane B: The local preference of community attribute 65000:200 is set to 200.<br><b>NOTE</b><br>By default, the BGP local preference is 100. The greater the value, the higher the preference. |
| Routing policy name   | Route import policy: local_pre<br>Route export policy: comm                                                                                                                                                                                                                     |
| Community filter name | 1                                                                                                                                                                                                                                                                               |
| BGP peer group name   | Client                                                                                                                                                                                                                                                                          |

## Procedure

**Step 1** Configure names for devices and IP addresses for interfaces.

For detailed configurations, see the configuration files of this example.

**Step 2** Configure an IGP.

In this example, IS-IS is used as an IGP. For detailed configurations, see the configuration files of this example.

After the configuration, run the **display ip routing-table** command. You can view that PEs, Ps and PEs, and Ps have learned the addresses of Loopback 0 interfaces from each other.

**Step 3** Establish MP-IBGP connections between the PEs and RR.

# Take the configuration of PE1 as an example. Configurations of other PEs are the same as that of PE1, and are not mentioned here.

```
[PE1] bgp 65000
[PE1-bgp] peer 10.11.11.9 as-number 65000
[PE1-bgp] peer 10.11.11.9 connect-interface LoopBack0
[PE1-bgp] ipv4-family unicast
[PE1-bgp-af-ipv4] undo peer 10.11.11.9 enable
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 10.11.11.9 enable
```

# Configure the RR.

```
[RR] bgp 65000
[RR-bgp] group client internal
[RR-bgp] peer client connect-interface LoopBack0
[RR-bgp] ipv4-family unicast
[RR-bgp-af-ipv4] undo peer client enable
[RR-bgp-af-ipv4] quit
[RR-bgp] ipv4-family vpnv4
[RR-bgp-af-vpnv4] undo policy vpn-target
[RR-bgp-af-vpnv4] peer client enable
[RR-bgp-af-vpnv4] peer 10.7.7.9 group client
[RR-bgp-af-vpnv4] peer 10.8.8.9 group client
[RR-bgp-af-vpnv4] peer 10.9.9.9 group client
[RR-bgp-af-vpnv4] peer 10.10.10.9 group client
[RR-bgp-af-vpnv4] peer client reflect-client
```



 **NOTE**

You need to run the **undo policy vpn-target** command in the BGP-VPNv4 address family view of the RR to ensure that VPN-target-based filtering is not performed on VPNv4 routes. By default, an RR performs VPN-target-based filtering on the received VPNv4 routes. The matching routes are added to the VPN routing table, and the other routes are discarded. In this example, VPN instances are not configured on the RR. As a result, if VPN-target-based filtering is enabled, all the received VPNv4 routes will be discarded.

After the configuration, run the **display bgp vpnv4 all peer** command on the RR. You can view that the RR sets up MP-IBGP peers with all PEs.

```
<RR> display bgp vpnv4 all peer
BGP local router ID : 10.11.11.9
Local AS number : 65000
Total number of peers : 4 Peers in established state : 4
Peer V AS MsgRcvd MsgSent OutQ Up/Down State
PrefRcv
10.7.7.9 4 65000 79 82 0 00:01:31 Established
0
10.8.8.9 4 65000 42 66 0 00:01:16 Established
0
10.9.9.9 4 65000 21 34 0 00:00:50 Established
0
10.10.10.9 4 65000 2 4 0 00:00:21 Established
0
```

**Step 4** Configure a routing policy. **NOTE**

Take the configurations of PE1, PE2, and the RR as an example. The configurations of PE3 and PE4 are the same as the configurations of PE1 and PE2 respectively, and are not mentioned here.

# Configure a routing policy on PE1 so that the BGP VPNv4 route advertised by PE1 can carry community attribute 65000:100.

```
[PE1] route-policy comm permit node 10
[PE1] apply community 65000:100
```

# Configure the routing policy on PE2 so that the BGP VPNv4 route advertised by PE2 can carry community attribute 65000:200.

```
[PE2] route-policy com permit node 10
[PE2] apply community 65000:200
```

# On PE1, apply the routing policy to the BGP VPNv4 route advertised by PE1 to the RR so that the route can carry the community attribute.

```
[PE1] bgp 65000
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 10.11.11.9 route-policy comm export
[PE1-bgp-af-vpnv4] peer 10.11.11.9 advertise-community
```

# On PE2, apply the routing policy to the advertised BGP VPNv4 route advertised by PE2 to the RR so that the route can carry the community attribute.

```
[PE2] bgp 65000
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer 10.11.11.9 route-policy comm export
[PE2-bgp-af-vpnv4] peer 10.11.11.9 advertise-community
```

# Configure the RR to advertise the community attribute to the PEs.

```
[RR] bgp 65000
[RR-bgp] ipv4-family vpnv4
[RR-bgp-af-vpnv4] peer client advertise-community
```

# Configure the community attribute filter on PE1.

```
[PE1] ip community-filter 1 permit 65000:100

Configure the community attribute filter on PE2.

[PE2] ip community-filter 1 permit 65000:200

On PE1, configure a routing policy and set the local preference of the route with community
attribute 65000:100 to 200.

[PE1] route-policy local_pre permit node 10
[PE1-route-policy] if-match community-filter 1
[PE1-route-policy] apply local-preference 200
[PE1-route-policy] quit

On PE2, configure a routing policy and set the local preference of the route with community
attribute 65000:200 to 200.

[PE2] route-policy local_pre permit node 10
[PE2-route-policy] if-match community-filter 1
[PE2-route-policy] apply local-preference 200
[PE2-route-policy] quit

On PE1, apply the routing policy to the imported BGP VPNv4 route so that the PE1 chooses
the route advertised by the remote PEs in plane A.

[PE1] bgp 65000
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 10.11.11.9 route-policy local_pre import

On PE2, apply the routing policy to the imported BGP VPNv4 route so that the PE2 chooses
the route advertised by the remote PEs in plane B.

[PE2] bgp 65000
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer 10.11.11.9 route-policy local_pre import
```

 **NOTE**

After this configuration, you also need to configure MPLS, establish tunnels, configure MPLS L3VPN, and configure PEs to access CEs. For detailed configurations, see the configuration files in this example.

**Step 5** Verify the configuration.

Run the **display bgp vpnv4 all routing-table community** command on a PE. You can view information about the VPNv4 routes with community attributes. Take the display on PE1 and PE2 as an example.

```
[PE1] display bgp vpnv4 all routing-table community

BGP Local router ID is 10.7.7.9
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes from all PE: 2
Route Distinguisher: 65000:10001012

 Network NextHop MED LocPrf PrefVal Community
* > 10.22.1.0/24 10.9.9.9 0 200 65000:100
* 10.10.10.9 10.10.10.9 0 100 65000:200

VPN-Instance NGN_Media, router ID 10.7.7.9:

Total Number of Routes: 2
```

|     | Network      | NextHop    | MED | LocPrf | PrefVal | Community |
|-----|--------------|------------|-----|--------|---------|-----------|
| *>i | 10.22.1.0/24 | 10.9.9.9   | 0   | 200    | 0       | 65000:100 |
| *   |              | 10.10.10.9 | 0   | 100    | 0       | 65000:200 |

[PE2] **display bgp vpnv4 all routing-table community**

BGP Local router ID is 10.8.8.9  
 Status codes: \* - valid, > - best, d - damped,  
 h - history, i - internal, s - suppressed, S - Stale  
 Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes from all PE: 2  
 Route Distinguisher: 65000:10001011

|    | Network      | NextHop    | MED | LocPrf | PrefVal | Community |
|----|--------------|------------|-----|--------|---------|-----------|
| *> | 10.22.1.0/24 | 10.10.10.9 | 0   | 200    |         | 65000:200 |
| *  |              | 10.9.9.9   | 0   | 100    |         | 65000:100 |

VPN-Instance NGN\_Media, router ID 10.7.7.9:

Total Number of Routes: 2  
 Total routes of vpn-instance NGN\_Media: 2

|     | Network      | NextHop    | MED | LocPrf | PrefVal | Community |
|-----|--------------|------------|-----|--------|---------|-----------|
| *>i | 10.22.1.0/24 | 10.10.10.9 | 0   | 200    | 0       | 65000:200 |
| *   |              | 10.9.9.9   | 0   | 100    | 0       | 65000:100 |

Run the **display ip routing-table vpn-instance vpna 10.22.1.0 24** command on PE1, and you can find that the next hop of route 10.22.1.0/24 is PE3. That is, PE1 chooses the route advertised by PE3.

[PE1] **display ip routing-table vpn-instance NGN\_Media 10.22.1.0 24**

Route Flags: R - relay, D - download to fib

```

Routing Tables: NGN_Media
Destination/Mask Proto Pre Cost Flags NextHop Interface
10.22.1.0/24 IBGP 255 0 RD 10.9.9.9 GigabitEthernet1/0/0
```

----End

## Configuration Files

- Configuration file of P1

```
#
sysname P1
#
mpls lsr-id 10.1.1.9
mpls
#
mpls ldp
#
isis 64
network-entity 49.0091.0100.0100.1009.00
#
interface GigabitEthernet1/0/0
description toP3GE1/0/0
undo shutdown
ip address 10.1.1.1 255.255.255.252
isis enable 64
mpls
mpls ldp
#
```

```

interface GigabitEthernet2/0/0
 description toP5GE1/0/0
 undo shutdown
 ip address 10.1.2.1 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface GigabitEthernet3/0/0
 description toRRGE1/0/0
 undo shutdown
 ip address 10.1.3.1 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface GigabitEthernet3/1/0
 description toP2GE1/0/0
 undo shutdown
 ip address 10.1.4.1 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface GigabitEthernet3/2/0
 description toP2GE1/0/0
 undo shutdown
 ip address 10.1.5.1 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 10.1.1.9 255.255.255.255
 isis enable 64
#
return

```

● Configuration file of P2

```

#
sysname P2
#
mpls lsr-id 10.2.2.9
mpls
#
mpls ldp
#
isis 64
network-entity 49.0091.0100.0200.2009.00
#
interface GigabitEthernet1/0/0
 description toP1GE3/1/0
 undo shutdown
 ip address 10.1.4.2 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 description toRRGE2/0/0
 undo shutdown
 ip address 10.1.8.1 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface GigabitEthernet3/0/0
 description toP4GE1/0/0
 undo shutdown
 ip address 10.1.7.1 255.255.255.252

```

```
isis enable 64
mpls
mpls ldp
#
interface GigabitEthernet3/1/0
description toP6GE1/0/0
undo shutdown
ip address 10.1.6.1 255.255.255.252
isis enable 64
mpls
mpls ldp
#
interface GigabitEthernet3/2/0
description toPE2GE1/0/0
undo shutdown
ip address 10.1.9.1 255.255.255.252
isis enable 64
mpls
mpls ldp
#
interface LoopBack0
ip address 10.2.2.9 255.255.255.255
isis enable 64
#
return
```

● Configuration file of P3

```
#
sysname P3
#
mpls lsr-id 10.3.3.9
mpls
#
mpls ldp
#
isis 64
network-entity 49.0091.0100.0300.3009.00
#
interface GigabitEthernet1/0/0
description toP1GE1/0/0
undo shutdown
ip address 10.1.1.2 255.255.255.252
isis enable 64
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
description toP5GE2/0/0
undo shutdown
ip address 10.1.10.1 255.255.255.252
isis enable 64
mpls
mpls ldp
#
interface GigabitEthernet3/0/0
description toP4GE2/0/0
undo shutdown
ip address 10.1.11.1 255.255.255.252
isis enable 64
mpls
mpls ldp
#
interface GigabitEthernet3/1/0
description toPE3GE1/0/0
undo shutdown
ip address 10.1.12.1 255.255.255.252
isis enable 64
mpls
mpls ldp
#
```

```
interface LoopBack0
 ip address 10.3.3.9 255.255.255.255
 isis enable 64
#
return
```

● Configuration file of P4

```
#
 sysname P4
#
 mpls lsr-id 10.4.4.9
 mpls
#
 mpls ldp
#
 isis 64
 network-entity 49.0091.0100.0400.4009.00
#
interface GigabitEthernet1/0/0
 description toP2GE3/0/0
 undo shutdown
 ip address 10.1.7.2 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 description toP3GE3/0/0
 undo shutdown
 ip address 10.1.11.2 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface GigabitEthernet3/0/0
 description toP6GE3/0/0
 undo shutdown
 ip address 10.1.13.1 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface GigabitEthernet3/1/0
 description toPE4GE1/0/0
 undo shutdown
 ip address 10.1.14.1 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 10.4.4.9 255.255.255.255
 isis enable 64
#
return
```

● Configuration file of P5

```
#
 sysname P5
#
 mpls lsr-id 10.5.5.9
 mpls
#
 mpls ldp
#
 isis 64
 network-entity 49.0091.0100.0500.5009.00
#
interface GigabitEthernet1/0/0
 description toP1GE2/0/0
```

```
undo shutdown
ip address 10.1.2.2 255.255.255.252
isis enable 64
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
description toP3GE2/0/0
undo shutdown
ip address 10.1.10.2 255.255.255.252
isis enable 64
mpls
mpls ldp
#
interface GigabitEthernet3/0/0
description toP6GE2/0/0
undo shutdown
ip address 10.1.15.1 255.255.255.252
isis enable 64
mpls
mpls ldp
#
interface LoopBack0
ip address 10.5.5.9 255.255.255.255
isis enable 64
#
return
```

● Configuration file of P6

```
#
sysname P6
#
mpls lsr-id 10.6.6.9
mpls
#
mpls ldp
#
isis 64
network-entity 49.0091.0100.0600.6009.00
#
interface GigabitEthernet1/0/0
description toP2GE3/1/0
undo shutdown
ip address 10.1.6.2 255.255.255.252
isis enable 64
mpls
mpls ldp
#
interface GigabitEthernet2/0/0
description toP5GE3/0/0
undo shutdown
ip address 10.1.15.2 255.255.255.252
isis enable 64
mpls
mpls ldp
#
interface GigabitEthernet3/0/0
description toP4GE3/0/0
undo shutdown
ip address 10.1.13.2 255.255.255.252
isis enable 64
mpls
mpls ldp
#
interface LoopBack0
ip address 10.6.6.9 255.255.255.255
isis enable 64
#
return
```

● Configuration file of PE1

```
#
 sysname PE1
#
ip vpn-instance NGN_Media
 route-distinguisher 65000:10001012
 apply-label per-instance
 vpn-target 65000:100 export-extcommunity
 vpn-target 65000:100 65000:200 65000:300 import-extcommunity
ip vpn-instance NGN_Other
 route-distinguisher 65000:30001012
 apply-label per-instance
 vpn-target 65000:300 export-extcommunity
 vpn-target 65000:100 65000:200 65000:300 import-extcommunity
ip vpn-instance NGN_Signaling
 route-distinguisher 65000:20001012
 apply-label per-instance
 vpn-target 65000:200 export-extcommunity
 vpn-target 65000:100 65000:200 65000:300 import-extcommunity
#
 mpls lsr-id 10.7.7.9
 mpls
#
 mpls ldp
#
 isis 64
 network-entity 49.0091.0100.0700.7009.00
#
interface GigabitEthernet1/0/0
 description toP1GE3/2/0
 undo shutdown
 ip address 10.1.5.2 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 description toPE2GE2/0/0
 undo shutdown
 ip address 10.1.16.1 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface GigabitEthernet3/0/0
#
interface GigabitEthernet3/0/0.10
 vlan-type dot1q 10
 ip binding vpn-instance NGN_Media
 ip address 10.21.1.73 255.255.255.252
#
interface GigabitEthernet3/0/0.11
 vlan-type dot1q 11
 ip binding vpn-instance NGN_Signaling
 ip address 10.21.1.77 255.255.255.252
#
interface GigabitEthernet3/0/0.12
 vlan-type dot1q 12
 ip binding vpn-instance NGN_Other
 ip address 10.21.1.81 255.255.255.252
#
interface LoopBack0
 ip address 10.7.7.9 255.255.255.255
 isis enable 64
#
 bgp 65000
 peer 10.11.11.9 as-number 65000
 peer 10.11.11.9 connect-interface LoopBack0
#
```



```

 ipv4-family unicast
 undo synchronization
 undo peer 10.11.11.9 enable
 #
 ipv4-family vpnv4
 policy vpn-target
 peer 10.11.11.9 enable
 peer 10.11.11.9 route-policy local_pre import
 peer 10.11.11.9 route-policy comm export
 peer 10.11.11.9 advertise-community
 #
 ipv4-family vpn-instance NGN_Media
 aggregate 10.21.1.0 255.255.255.0 detail-suppressed
 import-route direct
 #
 ipv4-family vpn-instance NGN_Other
 aggregate 10.21.1.0 255.255.255.0 detail-suppressed
 import-route direct
 #
 ipv4-family vpn-instance NGN_Signaling
 aggregate 10.21.1.0 255.255.255.0 detail-suppressed
 import-route direct
 #
 route-policy comm permit node 10
 apply community 65000:100
 #
 route-policy local_pre permit node 10
 if-match community-filter 1
 apply local-preference 200
 #
 ip community-filter 1 permit 65000:100
 #
 return

```

● Configuration file of PE2

```

#
sysname PE2
#
ip vpn-instance NGN_Media
 route-distinguisher 65000:10001011
 apply-label per-instance
 vpn-target 65000:100 export-extcommunity
 vpn-target 65000:100 65000:200 65000:300 import-extcommunity
ip vpn-instance NGN_Other
 route-distinguisher 65000:30001011
 apply-label per-instance
 vpn-target 65000:300 export-extcommunity
 vpn-target 65000:100 65000:200 65000:300 import-extcommunity
ip vpn-instance NGN_Signaling
 route-distinguisher 65000:20001011
 apply-label per-instance
 vpn-target 65000:200 export-extcommunity
 vpn-target 65000:100 65000:200 65000:300 import-extcommunity
#
mpls lsr-id 10.8.8.9
mpls
#
mpls ldp
#
isis 64
 network-entity 49.0091.0100.0800.8009.00
#
interface GigabitEthernet1/0/0
 description toP2GE3/2/0
 undo shutdown
 ip address 10.1.9.2 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#

```

```

interface GigabitEthernet2/0/0
description toPE1GE2/0/0
undo shutdown
ip address 10.1.16.2 255.255.255.252
isis enable 64
mpls
mpls ldp
#
interface GigabitEthernet3/0/0
#
interface GigabitEthernet3/0/0.10
vlan-type dot1q 10
ip binding vpn-instance NGN_Media
ip address 10.21.1.13 255.255.255.252
#
interface GigabitEthernet3/0/0.11
vlan-type dot1q 11
ip binding vpn-instance NGN_Signaling
ip address 10.21.1.17 255.255.255.252
#
interface GigabitEthernet3/0/0.12
vlan-type dot1q 12
ip binding vpn-instance NGN_Other
ip address 10.21.1.21 255.255.255.252
#
interface LoopBack0
ip address 10.8.8.9 255.255.255.255
isis enable 64
#
bgp 65000
peer 10.11.11.9 as-number 65000
peer 10.11.11.9 connect-interface LoopBack0
#
ipv4-family unicast
undo synchronization
undo peer 10.11.11.9 enable
#
ipv4-family vpnv4
policy vpn-target
peer 10.11.11.9 enable
peer 10.11.11.9 route-policy local_pre import
peer 10.11.11.9 route-policy comm export
peer 10.11.11.9 advertise-community
#
ipv4-family vpn-instance NGN_Media
aggregate 10.21.1.0 255.255.255.0 detail-suppressed
import-route direct
#
ipv4-family vpn-instance NGN_Other
aggregate 10.21.1.0 255.255.255.0 detail-suppressed
import-route direct
#
ipv4-family vpn-instance NGN_Signaling
aggregate 10.21.1.0 255.255.255.0 detail-suppressed
import-route direct
#
route-policy comm permit node 10
apply community 65000:200
#
route-policy local_pre permit node 10
if-match community-filter 1
apply local-preference 200
#
ip community-filter 1 permit 65000:200
#
return

```

- Configuration file of PE3

```

#
sysname PE3

```

```

#
ip vpn-instance NGN_Media
 route-distinguisher 65000:10000811
 apply-label per-instance
 vpn-target 65000:100 export-extcommunity
 vpn-target 65000:100 65000:200 65000:300 import-extcommunity
ip vpn-instance NGN_Other
 route-distinguisher 65000:30000811
 apply-label per-instance
 vpn-target 65000:300 export-extcommunity
 vpn-target 65000:100 65000:200 65000:300 import-extcommunity
ip vpn-instance NGN_Signaling
 route-distinguisher 65000:20000811
 apply-label per-instance
 vpn-target 65000:200 export-extcommunity
 vpn-target 65000:100 65000:200 65000:300 import-extcommunity
#
mpls lsr-id 10.9.9.9
mpls
#
mpls ldp
#
isis 64
 network-entity 49.0091.0100.0900.9009.00
#
interface GigabitEthernet1/0/0
 description toP3GE3/1/0
 undo shutdown
 ip address 10.1.12.2 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 description toPE4GE2/0/0
 undo shutdown
 ip address 10.1.17.1 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface GigabitEthernet3/0/0
#
interface GigabitEthernet3/0/0.10
 vlan-type dot1q 10
 ip binding vpn-instance NGN_Media
 ip address 10.22.1.73 255.255.255.252
#
interface GigabitEthernet3/0/0.11
 vlan-type dot1q 11
 ip binding vpn-instance NGN_Signaling
 ip address 10.22.1.77 255.255.255.252
#
interface GigabitEthernet3/0/0.12
 vlan-type dot1q 12
 ip binding vpn-instance NGN_Other
 ip address 10.22.1.81 255.255.255.252
#
interface LoopBack0
 ip address 10.9.9.9 255.255.255.255
 isis enable 64
#
bgp 65000
 peer 10.11.11.9 as-number 65000
 peer 10.11.11.9 connect-interface LoopBack0
#
ipv4-family unicast
 undo synchronization
 undo peer 10.11.11.9 enable

```

```

#
ipv4-family vpnv4
 policy vpn-target
 peer 10.11.11.9 enable
 peer 10.11.11.9 route-policy local_pre import
 peer 10.11.11.9 route-policy comm export
 peer 10.11.11.9 advertise-community
#
ipv4-family vpn-instance NGN_Media
 aggregate 10.22.1.0 255.255.255.0 detail-suppressed
 import-route direct
#
ipv4-family vpn-instance NGN_Other
 aggregate 10.22.1.0 255.255.255.0 detail-suppressed
 import-route direct
#
ipv4-family vpn-instance NGN_Signaling
 aggregate 10.22.1.0 255.255.255.0 detail-suppressed
 import-route direct
#
route-policy comm permit node 10
 apply community 65000:100
#
route-policy local_pre permit node 10
 if-match community-filter 1
 apply local-preference 200
#
route-policy local_pre permit node 20
#
 ip community-filter 1 permit 65000:100
#
return

```

● Configuration file of PE4

```

#
 sysname PE4
#
ip vpn-instance NGN_Media
 route-distinguisher 65000:10000712
 apply-label per-instance
 vpn-target 65000:100 export-extcommunity
 vpn-target 65000:100 65000:200 65000:300 import-extcommunity
ip vpn-instance NGN_Other
 route-distinguisher 65000:30000712
 apply-label per-instance
 vpn-target 65000:300 export-extcommunity
 vpn-target 65000:100 65000:200 65000:300 import-extcommunity
ip vpn-instance NGN_Signaling
 route-distinguisher 65000:20000712
 apply-label per-instance
 vpn-target 65000:200 export-extcommunity
 vpn-target 65000:100 65000:200 65000:300 import-extcommunity
#
 mpls lsr-id 10.10.10.9
 mpls
#
 mpls ldp
#
 isis 64
 network-entity 49.0091.0100.1001.0009.00
#
interface GigabitEthernet1/0/0
 description toP4GE3/1/0
 undo shutdown
 ip address 10.1.14.2 255.255.255.252
 isis enable 64
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0

```

```

description toPE3GE2/0/0
undo shutdown
ip address 10.1.17.2 255.255.255.252
isis enable 64
mpls
mpls ldp
#
interface GigabitEthernet3/0/0
#
interface GigabitEthernet3/0/0.10
vlan-type dot1q 10
ip binding vpn-instance NGN_Media
ip address 10.22.1.13 255.255.255.252
#
interface GigabitEthernet3/0/0.11
vlan-type dot1q 11
ip binding vpn-instance NGN_Signaling
ip address 10.22.1.17 255.255.255.252
#
interface GigabitEthernet3/0/0.12
vlan-type dot1q 12
ip binding vpn-instance NGN_Other
ip address 10.22.1.21 255.255.255.252
#
interface LoopBack0
ip address 10.10.10.9 255.255.255.255
isis enable 64
#
bgp 65000
peer 10.11.11.9 as-number 65000
peer 10.11.11.9 connect-interface LoopBack0
#
ipv4-family unicast
undo synchronization
undo peer 10.11.11.9 enable
#
ipv4-family vpnv4
policy vpn-target
peer 10.11.11.9 enable
peer 10.11.11.9 route-policy local_pre import
peer 10.11.11.9 route-policy comm export
peer 10.11.11.9 advertise-community
#
ipv4-family vpn-instance NGN_Media
aggregate 10.22.1.0 255.255.255.0 detail-suppressed
import-route direct
#
ipv4-family vpn-instance NGN_Other
aggregate 10.22.1.0 255.255.255.0 detail-suppressed
import-route direct
#
ipv4-family vpn-instance NGN_Signaling
aggregate 10.22.1.0 255.255.255.0 detail-suppressed
import-route direct
#
route-policy comm permit node 10
apply community 65000:200
#
route-policy local_pre permit node 10
if-match community-filter 1
apply local-preference 200
#
ip community-filter 1 permit 65000:200
#
return

```

- Configuration file of the RR
 

```

#
sysname RR
#

```

```
isis 64
 network-entity 49.0091.0100.1101.1009.00
#
interface GigabitEthernet1/0/0
 description toP1GE3/0/0
 undo shutdown
 ip address 10.1.3.2 255.255.255.252
 isis enable 64
#
interface GigabitEthernet2/0/0
 description toP2GE2/0/0
 undo shutdown
 ip address 10.1.8.2 255.255.255.252
 isis enable 64
#
interface LoopBack0
 ip address 10.11.11.9 255.255.255.255
 isis enable 64
#
bgp 65000
 group client internal
 peer client connect-interface LoopBack0
 peer 10.7.7.9 as-number 65000
 peer 10.8.8.9 as-number 65000
 peer 10.9.9.9 as-number 65000
 peer 10.10.10.9 as-number 65000
#
ipv4-family unicast
 undo synchronization
 undo peer client enable
 undo peer 10.7.7.9 enable
 undo peer 10.8.8.9 enable
 undo peer 10.9.9.9 enable
 undo peer 10.10.10.9 enable
#
ipv4-family vpnv4
 undo policy vpn-target
 peer client enable
 peer client reflect-client
 peer client advertise-community
 peer 10.7.7.9 enable
 peer 10.7.7.9 group client
 peer 10.8.8.9 enable
 peer 10.8.8.9 group client
 peer 10.9.9.9 enable
 peer 10.9.9.9 group client
 peer 10.10.10.9 enable
 peer 10.10.10.9 group client
#
return
```

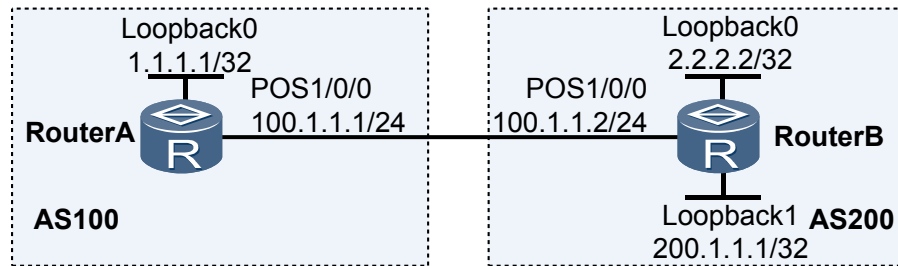
## 8.23.9 Example for Configuring the BGP Accounting

By configuring BGP accounting, you can collect the statistics of the incoming and outgoing BGP traffic of an AS.

### Networking Requirements

As shown in [Figure 8-9](#), Router A and Router B are BGP neighbors. Router B is the transmitter of BGP routes, and Router A is the receiver. BGP routes sent by Router B to Router A are configured with the community attribute. It is required that Router A collect traffic statistics only for the routes carrying certain community attributes.

**Figure 8-9** Configure the BGP accounting



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure OSPF on Router A and Router B to for interconnection.
2. Configure the BGP routes sent from Router B to Router A with the community attributes.
3. Configure the EBGP connection on Router A and Router B.
4. Set the traffic index on Router A by using the routing policy.
5. Configure the interface of Router A with BGP accounting to collect traffic statistics.

## Data Preparation

To complete the configuration, you need the following data:

- Numbers of the ASs where Router A and Router B reside: 100 and 200
- Community number and routing policy name of Router A, routing policy name and IP prefix list name of Router B

## Procedure

**Step 1** Assign an IP address to each interface.

The configuration details are not mentioned here.

**Step 2** Configure OSPF on Router A and Router B to implement the interconnection.

# Configure Router A.

```
[RouterA] router id 1.1.1.1
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

# Configure Router B.

```
[RouterB] router id 2.2.2.2
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
```

```
[RouterB-ospf-1] quit
```

**Step 3** Configure the routing policy of the community attributes on Router A.

# Configure the community filter.

```
[RouterA] ip community-filter 10 permit 10:10
```

# Configure the routing policy.

```
[RouterA] route-policy aa permit node 10
[RouterA-route-policy] if-match community-filter 10
[RouterA-route-policy] apply traffic-index 1
[RouterA-route-policy] quit
[RouterA] route-policy aa permit node 20
[RouterA-route-policy] quit
```

**Step 4** Configure the routing policy of the community attributes on Router B.

# Configure an IP prefix list.

```
[RouterB] ip ip-prefix bb permit 200.1.1.1 32
```

# Configure the routing policy.

```
[RouterB] route-policy aa permit node 10
[RouterB-route-policy] if-match ip-prefix bb
[RouterB-route-policy] apply community 10:10
[RouterB-route-policy] quit
[RouterB] route-policy aa permit node 20
[RouterB-route-policy] quit
```

**Step 5** Configure the EBGP neighbor.

# Configure Router A.

```
[RouterA] bgp 100
[RouterA-bgp] peer 2.2.2.2 as-number 200
[RouterA-bgp] peer 2.2.2.2 connect-interface loopback 0
[RouterA-bgp] peer 2.2.2.2 ebgp-max-hop 2
[RouterA-bgp] peer 2.2.2.2 route-policy aa import
[RouterA-bgp] quit
```

# Configure Router B.

```
[RouterB] bgp 200
[RouterB-bgp] peer 1.1.1.1 as-number 100
[RouterB-bgp] peer 1.1.1.1 connect-interface Loopback 0
[RouterB-bgp] peer 1.1.1.1 ebgp-max-hop 2
[RouterB-bgp] peer 1.1.1.1 advertise-community
[RouterB-bgp] peer 1.1.1.1 route-policy aa export
[RouterB-bgp] import-route direct
[RouterB-bgp] quit
```

**Step 6** Apply BGP accounting on the interface.

```
[RouterA] interface pos 1/0/0
[RouterA-Pos1/0/0] ip bgp-accounting inbound source
[RouterA-Pos1/0/0] quit
```

**Step 7** Verify the configuration.

# Check the FIB table of Router A.

```
[RouterA] display fib 200.1.1.1 32 verbose
Route Entry Count: 1
Destination: 200.1.1.1 Mask : 255.255.255.255
Nexthop : 100.1.1.2 OutIf : Pos1/0/0
LocalAddr : 100.1.1.1 LocalMask : 0.0.0.0
Flags : DGHU Age : 113sec
```



```

ATIndex : 51 Slot : 0
LspFwdFlag : 0 LspToken : 0x0
InLabel : NULL OriginAs : 200
BGPNextHop : 2.2.2.2 PeerAs : 200
QosInfo : 0x10010000 OriginQos : 0x10010000
NextHopBak : 0.0.0.0 OutIfBak : [No Intf]
LspTokenBak : 0x0 InLabelBak : NULL
LspToken_ForInLabelBak : 0x0
EntryRefCount : 0
rt_ulVlanId : 0x0
LspType : 0 Label_ForLspTokenBak : 0
MplsMtu : 0 Gateway_ForLspTokenBak : 0
NextToken : 0 IfIndex_ForLspTokenBak : 0
Label_NextToken : 0 Label : 0
LspBfdState : 0

```

# Send Ping packets from Router A to Router B. Check the statistics of Echo Reply packets that reach Router A.

```

[RouterA] ping 200.1.1.1
PING 200.1.1.1: 56 data bytes, press CTRL_C to break
 Reply from 200.1.1.1: bytes=56 Sequence=1 ttl=255 time=31 ms
 Reply from 200.1.1.1: bytes=56 Sequence=2 ttl=255 time=31 ms
 Reply from 200.1.1.1: bytes=56 Sequence=3 ttl=255 time=31 ms
 Reply from 200.1.1.1: bytes=56 Sequence=4 ttl=255 time=31 ms
 Reply from 200.1.1.1: bytes=56 Sequence=5 ttl=255 time=31 ms
--- 200.1.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/31/31 ms

```

```

[RouterA] display ip bgp-accounting inbound interface pos 1/0/0
statistics for interface Pos1/0/0

```

```

BGP based Policy accounting on inbound is enabled

```

| Index | Bytes | Packets |
|-------|-------|---------|
| 1     | 420   | 5       |
| 2     | 0     | 0       |
| 3     | 0     | 0       |
| 4     | 0     | 0       |
| 5     | 0     | 0       |
| 6     | 0     | 0       |
| 7     | 0     | 0       |
| 8     | 0     | 0       |
| 9     | 0     | 0       |
| 10    | 0     | 0       |
| 11    | 0     | 0       |
| 12    | 0     | 0       |
| 13    | 0     | 0       |
| 14    | 0     | 0       |
| 15    | 0     | 0       |
| 16    | 0     | 0       |
| 17    | 0     | 0       |
| 18    | 0     | 0       |
| 19    | 0     | 0       |
| 20    | 0     | 0       |
| 21    | 0     | 0       |
| 22    | 0     | 0       |
| 23    | 0     | 0       |
| 24    | 0     | 0       |
| 25    | 0     | 0       |
| 26    | 0     | 0       |
| 27    | 0     | 0       |
| 28    | 0     | 0       |
| 29    | 0     | 0       |
| 30    | 0     | 0       |
| 31    | 0     | 0       |
| 32    | 0     | 0       |
| 33    | 0     | 0       |
| 34    | 0     | 0       |
| 35    | 0     | 0       |

```

36 0 0
37 0 0
38 0 0
39 0 0
40 0 0
41 0 0
42 0 0
43 0 0
44 0 0
45 0 0
46 0 0
47 0 0
48 0 0
49 0 0
50 0 0
51 0 0
52 0 0
53 0 0
54 0 0
55 0 0
56 0 0
57 0 0
58 0 0
59 0 0
60 0 0
61 0 0
62 0 0
63 0 0
64 0 0

```

---End

## Configuration Files

- Configuration file of Router A

```

#
 sysname RouterA
#
 router id 1.1.1.1
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 100.1.1.1 255.255.0.0
 ip bgp-accounting inbound source
#
 interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
 bgp 100
 peer 2.2.2.2 as-number 200
 peer 2.2.2.2 ebgp-max-hop 2
 peer 2.2.2.2 connect-interface LoopBack0
#
 ipv4-family unicast
 undo synchronization
 peer 2.2.2.2 enable
 peer 2.2.2.2 route-policy aa import
#
 ospf 1
 area 0.0.0.0
 network 1.1.1.1 0.0.0.0
 network 100.1.1.0 0.0.0.255
#
 route-policy aa permit node 10
 if-match community 10
 apply traffic-index 1
#
 route-policy aa permit node 20

```

```
#
 ip community-filter 10 permit 10:10
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
 router id 2.2.2.2
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 100.1.1.2 255.255.0.0
#
 interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
 interface LoopBack1
 ip address 200.1.1.1 255.255.255.255
#
 bgp 200
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 ebgp-max-hop 2
 peer 1.1.1.1 connect-interface LoopBack0
#
 ipv4-family unicast
 undo synchronization
 import-route direct
 peer 1.1.1.1 enable
 peer 1.1.1.1 route-policy aa export
 peer 1.1.1.1 advertise-community
#
 ospf 1
 area 0.0.0.0
 network 2.2.2.2 0.0.0.0
 network 100.1.1.0 0.0.0.255
#
 route-policy aa permit node 10
 if-match ip-prefix bb
 apply community 10:10
#
 route-policy aa permit node 20
#
 ip ip-prefix bb index 10 permit 200.1.1.1 32
#
return
```

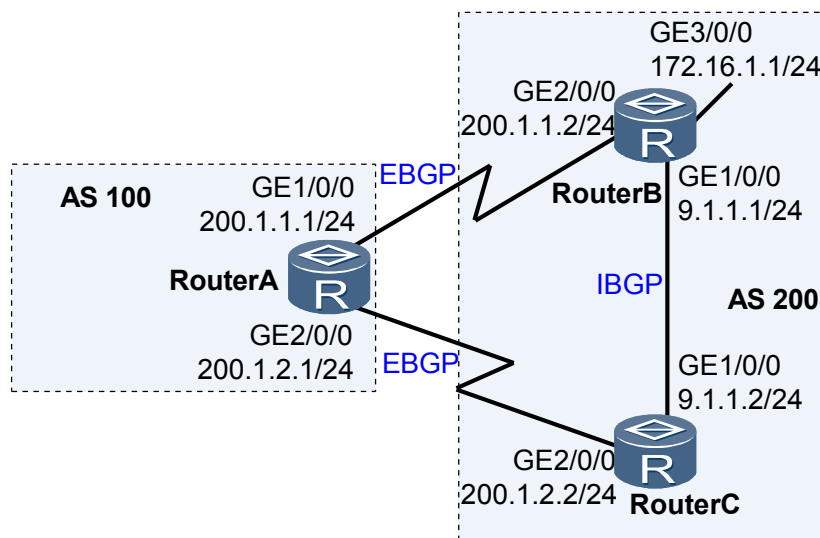
## 8.23.10 Example for Configuring BFD for BGP

After BFD for BGP is configured, BFD can fast detect the fault on the link between BGP peers and notify it to BGP so that service traffic can be transmitted through the backup link.

### Networking Requirements

- As shown in [Figure 8-10](#), Router A belongs to AS 100, and Router B and Router C belong to AS 200. EBGP connections are established between Router A and Router B, and between Router A and Router C.
- Traffic is transmitted on the active link Router A → Router B. The link Router A → Router C → Router B acts as the standby link.
- BFD is used to detect the BGP neighboring relationship between Router A and Router B. When the link between Router A and Router B fails, BFD can rapidly detect the failure and notify BGP of the failure. Traffic is transmitted on the standby link.

**Figure 8-10** Networking diagram of configuring BFD for BGP



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic BGP functions on each router.
2. Configure MED attributes to control the routing selection of the routers.
3. Enable BFD on Router A and Router B.

## Data Preparation

To complete the configuration, you need the following data:

- Router IDs and AS numbers of Router A, Router B and Router C
- Peer IP address detected by BFD
- Minimum interval for sending BFD control packets, minimum interval for receiving BFD control packets, and local detection multiplier

## Procedure

**Step 1** Assign an IP address to each interface.

The detailed configuration is not mentioned here.

**Step 2** Configure the basic BGP functions. Establish an EBGP connection between Router A and Router B, that between Router A and Router C. Establish an IBGP connection between Router B and Router C.

# Configure Router A.

```
[RouterA] bgp 100
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 200.1.1.2 as-number 200
[RouterA-bgp] peer 200.1.2.2 as-number 200
[RouterA-bgp] quit
```

# Configure Router B.

```
[RouterB] bgp 200
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 200.1.1.1 as-number 100
[RouterB-bgp] peer 9.1.1.2 as-number 200
[RouterB-bgp] network 172.16.1.0 255.255.255.0
[RouterB-bgp] quit
```

# Configure Router C.

```
[RouterC] bgp 200
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 200.1.2.1 as-number 100
[RouterC-bgp] peer 9.1.1.1 as-number 200
[RouterC-bgp] quit
```

# Check the established BGP neighbors on Router A.

```
[RouterA] display bgp peer
BGP local router ID : 1.1.1.1
Local AS number : 100
Total number of peers : 2 Peers in established state : 2
Peer V AS MsgRcvd MsgSent OutQ Up/Down State PrefRcv
200.1.1.2 4 200 2 5 0 00:01:25 Established 0
200.1.2.2 4 200 2 4 0 00:00:55 Established 0
```

**Step 3** Configure MED attributes.

Set the value of MED sent by Router B and Router C to Router A by using the policy.

# Configure Router B.

```
[RouterB] route-policy 10 permit node 10
[RouterB-route-policy] apply cost 100
[RouterB-route-policy] quit
[RouterB] bgp 200
[RouterB-bgp] peer 200.1.1.1 route-policy 10 export
```

# Configure Router C.

```
[RouterC] route-policy 10 permit node 10
[RouterC-route-policy] apply cost 150
[RouterC-route-policy] quit
[RouterC] bgp 200
[RouterC-bgp] peer 200.1.2.1 route-policy 10 export
```

# Check all BGP routing information.

```
<RouterA> display bgp routing-table
BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete
Total Number of Routes: 2
 Network NextHop MED LocPrf PrefVal Path/Ogn
*> 172.16.1.0/24 200.1.1.2 100 0 200i
* 200.1.2.2 150 0 200i
```

As shown in the BGP routing table, the next hop address of the route to 172.16.1.0/24 is 200.1.1.2 and traffic is transmitted on the active link Router A → Router B.

**Step 4** Configure BFD, the interval for sending the packets, the interval for receiving the packets, and the local detection multiplier.

# Enable BFD on Router A, set the minimum interval for sending the packets and the minimum interval for receiving the packets to 100 ms, and set the local detection multiplier to 4.

```
[RouterA] bfd
```

```
[RouterA-bfd] quit
[RouterA] bgp 100
[RouterA-bgp] peer 200.1.1.2 bfd enable
[RouterA-bgp] peer 200.1.1.2 bfd min-tx-interval 100 min-rx-interval 100 detect-
multiplier 4
```

# Enable BFD on Router B, set the minimum interval for sending the packets and the minimum interval for receiving the packets to 100 ms, and set the local detection multiplier to 4.

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bgp 200
[RouterB-bgp] peer 200.1.1.1 bfd enable
[RouterB-bgp] peer 200.1.1.1 bfd min-tx-interval 100 min-rx-interval 100 detect-
multiplier 4
```

# Display all BFD sessions set up by BGP on Router A.

```
<RouterA> display bgp bfd session all
Local_Address Peer_Address LD/RD Interface
200.1.1.1 200.1.1.2 8201/8201 GigabitEthernet2/0/0
Tx-interval(ms) Rx-interval(ms) Multiplier Session-State
100 100 4 Up
Wtr-interval(m)
0
```

### Step 5 Verify the Configuration.

# Run the **shutdown** command on GE 2/0/0 of Router B to simulate the active link failure.

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] shutdown
```

### Step 6 # Display the routing table on Router A.

```
<RouterA> display bgp routing-table
BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete
Total Number of Routes: 1
Network NextHop MED LocPrf PrefVal Path/Ogn
*> 172.16.1.0/24 200.1.2.2 150 0 200i
```

As shown in the BGP routing table, the standby link Router A → Router C → Router B takes effect after the active link fails. The next hop address of the route to 172.16.1.0/24 becomes 200.1.2.2.

----End

## Configuration Files

- Configuration file of Router A

```
#
sysname RouterA
#
bfd
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 200.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 200.1.2.1 255.255.255.0
#
bgp 100
router-id 1.1.1.1
```

```

peer 200.1.1.2 as-number 200
peer 200.1.1.2 bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier
4
peer 200.1.1.2 bfd enable
peer 200.1.2.2 as-number 200
#
ipv4-family unicast
undo synchronization
peer 200.1.1.2 enable
peer 200.1.2.2 enable
#
return

```

- Configuration file of Router B

```

#
sysname RouterB
#
bfd
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 9.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 200.1.1.2 255.255.255.0
#
interface GigabitEthernet3/0/0
undo shutdown
ip address 172.16.1.1 255.255.255.0
#
bgp 200
router-id 2.2.2.2
peer 9.1.1.2 as-number 200
peer 200.1.1.1 as-number 100
peer 200.1.1.1 bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier
4
peer 200.1.1.1 bfd enable
#
ipv4-family unicast
undo synchronization
network 172.16.1.0 255.255.255.0
peer 9.1.1.2 enable
peer 200.1.1.1 enable
peer 200.1.1.1 route-policy 10 export
#
route-policy 10 permit node 10
apply cost 100
#
return

```

- #

```

#
sysname RouterC
#
bfd
#
interface GigabitEthernet1/0/0
undo shutdown
ip address 9.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
undo shutdown
ip address 200.1.2.2 255.255.255.0
#
bgp 200
router-id 3.3.3.3
peer 9.1.1.1 as-number 200
peer 200.1.2.1 as-number 100
#
ipv4-family unicast

```

```

undo synchronization
peer 9.1.1.1 enable
peer 200.1.2.1 enable
peer 200.1.2.1 route-policy 10 export
#
route-policy 10 permit node 10
 apply cost 150
#
return

```

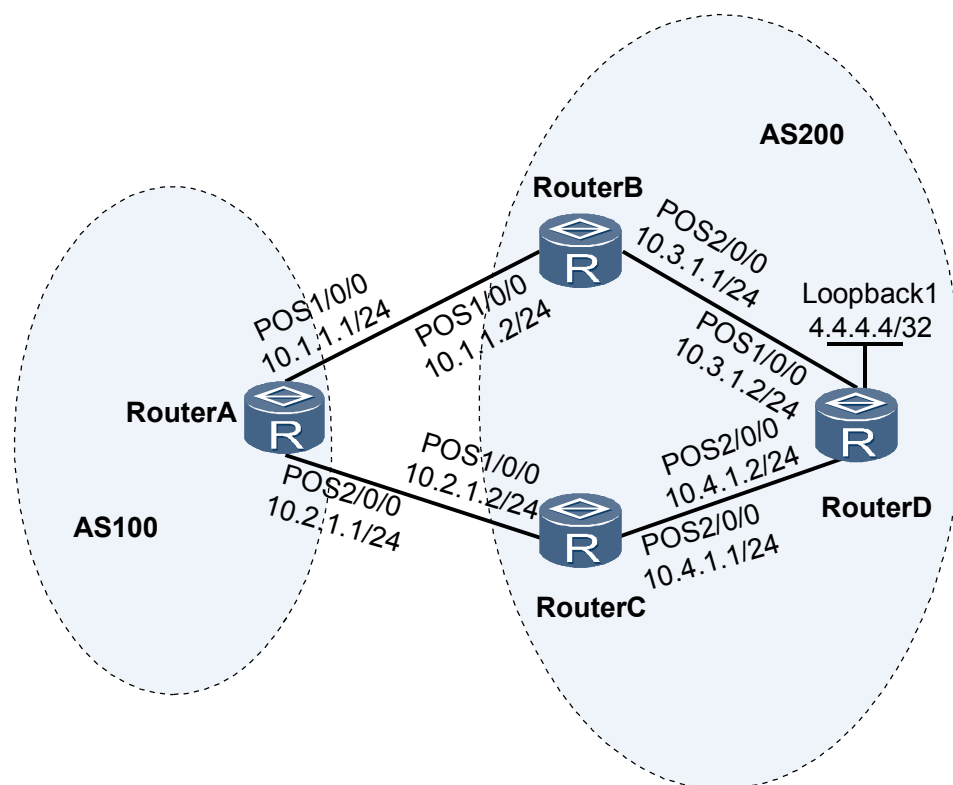
## 8.23.11 Example for Configuring BGP Auto FRR

After BGP Auto FRR is configured, forwarding information is backed up for routes, and thus network reliability is improved.

### Networking Requirements

As shown in [Figure 8-11](#), Router A belongs to AS 100; Router B, Router C, and Router D belong to AS 200. BGP Auto FRR needs to be configured so that the route from Router A to Router D can have backup forwarding information.

**Figure 8-11** Networking diagram of configuring BGP Auto FRR



### Configuration Roadmap

The configuration roadmap is as follows:



1. Configure EBGP connections between Router A and Router B and between Router A and Router C. Configure IBGP connections between Router D and Router B, and between Router D and Router C.
2. Configure routing policies on Router B and Router C to change the MED values of routes to Router D to facilitate route selection.
3. Configure BGP Auto FRR on Router A.

## Data Preparation

To complete the configuration, you need the following data:

- Router IDs and AS numbers of Router A, Router B, Router C, and Router D
- Names of routing policies and MED values of routes on Router B and Router C

## Procedure

**Step 1** Configure IP addresses for interfaces. The configuration details are not mentioned here.

**Step 2** Configure EBGP connections between Router A and Router B, and between Router A and Router C. Configure IBGP connections between Router B and Router D, and between Router C and Router D.

# Configure EBGP connections on Router A.

```
<RouterA> system-view
[RouterA] bgp 100
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 10.1.1.2 as-number 200
[RouterA-bgp] peer 10.2.1.2 as-number 200
```

### NOTE

The configurations of Router B and Router C are the same as that of Router A, and the detailed configurations are not mentioned here.

# Configure IBGP connections on Router D.

```
<RouterD> system-view
[RouterD] bgp 200
[RouterD-bgp] router-id 4.4.4.4
[RouterD-bgp] peer 10.3.1.1 as-number 200
[RouterD-bgp] peer 10.4.1.1 as-number 200
```

### NOTE

The configurations on Router B and Router C are similar, and the detailed configurations are not mentioned here.

**Step 3** Configuring routing policies on Router B and Router C so that the MED values of routes to Router D are different

# Configure a routing policy on Router B.

```
<RouterB> system-view
[RouterB] route-policy rtb permit node 10
[RouterB-route-policy] apply cost 80
[RouterB-route-policy] quit
[RouterB] bgp 200
[RouterB-bgp] ipv4-family unicast
[RouterB-bgp-af-ipv4] peer 10.1.1.1 route-policy rtb export
```

# Configure a routing policy on Router C.

```
<RouterC> system-view
```

```
[RouterC] route-policy rtc permit node 10
[RouterC-route-policy] apply cost 120
[RouterC-route-policy] quit
[RouterC] bgp 200
[RouterC-bgp] ipv4-family unicast
[RouterC-bgp-af-ipv4] peer 10.2.1.1 route-policy rtc export
```

# Advertise a route to 4.4.4.4/32 on Router D.

```
[RouterD] bgp 200
[RouterD-bgp] ipv4-family unicast
[RouterD-bgp] network 4.4.4.4 32
```

# Run the **display ip routing-table verbose** command on Router A to check detailed information about the learned route to 4.4.4.4/32.

```
<RouterA> display ip routing-table 4.4.4.4 32 verbose
Route Flags: R - relay, D - download to fib

Routing Table : Public
Summary Count : 1

Destination: 4.4.4.4/32
 Protocol: EBGp Process ID: 0
 Preference: 255 Cost: 80
 NextHop: 10.1.1.2 Neighbour: 10.1.1.2
 State: Active Adv Age: 00h00m12s
 Tag: 0 Priority: low
 Label: NULL QoSInfo: 0x0
 IndirectID: 0x4
 RelayNextHop: 0.0.0.0 Interface: Pos1/0/0
 TunnelID: 0x0 Flags: D
```

Because the MED value of the route learnt from Router B is smaller, on Router A, the route to 4.4.4.4/32 selects the path RouterA→RouterB→RouterD. Because FRR is not configured, no backup information is available.

#### Step 4 Enabling BGP Auto FRR on Router A, and checking the routing information

# Enable BGP Auto FRR on Router A.

```
<RouterA> system-view
[RouterA] bgp 100
[RouterA-bgp] ipv4-family unicast
[RouterA-bgp-af-ipv4] auto-frr
```

# After the configuration, run the **display ip routing-table verbose** command on Router A to check the routing information.

```
<RouterA> display ip routing-table 4.4.4.4 32 verbose
Route Flags: R - relay, D - download to fib

Routing Table : Public
Summary Count : 1

Destination: 4.4.4.4/32
 Protocol: EBGp Process ID: 0
 Preference: 255 Cost: 80
 NextHop: 10.1.1.2 Neighbour: 10.1.1.2
 State: Active Adv Age: 00h52m45s
 Tag: 0 Priority: low
 Label: NULL QoSInfo: 0x0
 IndirectID: 0x4
 RelayNextHop: 0.0.0.0 Interface: Pos1/0/0
 TunnelID: 0x0 Flags: D
 BkNextHop: 10.2.1.2 BkInterface: Pos2/0/0
 BkLabel: NULL SecTunnelID: 0x0
 BkPETunnelID: 0x0 BkPESecTunnelID: 0x0
 BkIndirectID: 0x2
```

The preceding information shows that Router A has a backup next hop and a backup outbound interface to 4.4.4.4/32.

---End

## Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
interface Pos1/0/0
 ip address 10.1.1.1 255.255.255.0
#
interface Pos2/0/0
 ip address 10.2.1.1 255.255.255.0
#
bgp 100
 router-id 1.1.1.1
 peer 10.1.1.2 as-number 200
 peer 10.2.1.2 as-number 200
#
 ipv4-family unicast
 auto-frr
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
interface Pos1/0/0
 ip address 10.1.1.2 255.255.255.0
#
interface Pos2/0/0
 ip address 10.3.1.1 255.255.255.0
#
bgp 200
 router-id 2.2.2.2
 peer 10.1.1.1 as-number 100
 peer 10.3.1.2 as-number 200
#
 ipv4-family unicast
 peer 10.1.1.1 route-policy rtb export
#
 route-policy rtb permit node 10
 apply cost 80
#
return
```

- Configuration file of Router C

```
#
 sysname RouterC
#
interface Pos1/0/0
 ip address 10.2.1.2 255.255.255.0
#
interface Pos2/0/0
 ip address 10.4.1.1 255.255.255.0
#
bgp 200
 router-id 3.3.3.3
 peer 10.2.1.1 as-number 100
 peer 10.4.1.2 as-number 200
#
 ipv4-family unicast
```

```

 peer 10.2.1.1 route-policy rtc export
 #
 route-policy rtc permit node 10
 apply cost 120
 #
 return

```

- Configuration file of Router D

```

 #
 sysname RouterD
 #
 interface Pos1/0/0
 ip address 10.3.1.2 255.255.255.0
 #
 interface Pos2/0/0
 ip address 10.4.1.2 255.255.255.0
 #
 interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 #
 bgp 200
 router-id 4.4.4.4
 peer 10.3.1.1 as-number 200
 peer 10.4.1.1 as-number 200
 #
 ipv4-family unicast
 network 4.4.4.4 255.255.255.255
 #
 return

```

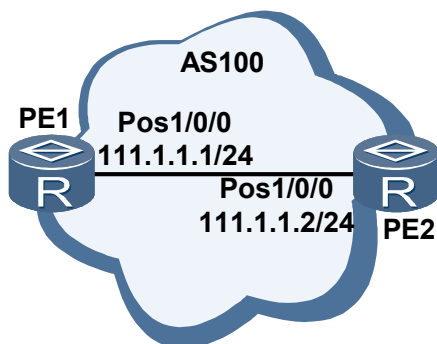
## 8.23.12 Example for Configuring Prefix-based BGP ORF

After prefix-based BGP ORF is configured, on-demand route advertisement can be implemented.

### Networking Requirements

As shown in [Figure 8-12](#), PE1 and PE2 are in AS 100; PE1 requires PE2 to send only the routes matching the inbound policy of PE1.

**Figure 8-12** Networking diagram of configuring prefix-based BGP ORF



### Configuration Roadmap

The configuration roadmap is as follows:

1. Establish an IPv4 unicast peer relationship between PE1 and PE2.
2. Apply prefix-based inbound policy to PE1 and configure PE1 to import routes from PE2. Then, check the sent routes and received routes.
3. Check the sent and received routes after configuring prefix-based BGP ORF.

## Data Preparation

To complete the configuration, you need the following data:

- Router ID and AS number of PE1 (in this example, the router ID of PE1 is 1.1.1.1, and the AS number of PE1 is 100)
- Router ID and AS number of PE2 (in this example, the router ID of PE2 is 2.2.2.2, and the AS number of PE2 is 100)

## Procedure

**Step 1** Establish an IPv4 unicast peer relationship between PE1 and PE2.

# Configure PE1.

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] interface pos 1/0/0
[PE1-Pos1/0/0] ip address 111.1.1.1 255.255.255.0
[PE1-Pos1/0/0] quit
[PE1] bgp 100
[PE1-bgp] peer 111.1.1.2 as-number 100
```

# Configure PE2.

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] interface pos 1/0/0
[PE2-Pos1/0/0] ip address 111.1.1.2 255.255.255.0
[PE2-Pos1/0/0] quit
[PE2] bgp 100
[PE2-bgp] peer 111.1.1.1 as-number 100
```

**Step 2** Apply the prefix-based inbound policy on PE1.

# Configure PE1.

```
[PE1] ip ip-prefix 1 index 10 permit 4.4.4.0 24 less-equal 32
[PE1] bgp 100
[PE1-bgp] peer 111.1.1.2 ip-prefix 1 import
```

# Configure PE2.

```
[PE2] ip route-static 3.3.3.3 255.255.255.255 NULL0
[PE2] ip route-static 4.4.4.4 255.255.255.255 NULL0
[PE2] ip route-static 5.5.5.5 255.255.255.255 NULL0
[PE2] bgp 100
[PE2-bgp] import-route static
```

# Check the routes sent by PE2 to PE1.

```
[PE2] display bgp routing peer 111.1.1.1 advertised-routes
```

```
BGP Local router ID is 111.1.1.2
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete
```

| Network | NextHop | MED | LocPrf | PrefVal | Path/Ogn |
|---------|---------|-----|--------|---------|----------|
|---------|---------|-----|--------|---------|----------|

```
Total Number of Routes: 3
*> 3.3.3.3/32 0.0.0.0 0 0 ?
*> 4.4.4.4/32 0.0.0.0 0 0 ?
*> 5.5.5.5/32 0.0.0.0 0 0 ?
```

# Check the routes received by PE1 from PE2.

```
[PE1] display bgp routing-table peer 111.1.1.2 received-routes

BGP Local router ID is 111.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 1
 Network NextHop MED LocPrf PrefVal Path/Ogn
*>i 4.4.4.4/32 111.1.1.2 0 100 0 ?
```

When prefix-based BGP ORF is not enabled, PE2 sends routes 3.3.3.3, 4.4.4.4, and 5.5.5.5 to PE1. Because the prefix-based inbound policy is applied on PE1, PE1 receives only route 4.4.4.4.

### Step 3 Enable prefix-based BGP ORF.

# Enable prefix-based BGP ORF on PE1.

```
[PE1] bgp 100
[PE1-bgp] peer 111.1.1.2 capability-advertise orf ip-prefix both
```

# Enable prefix-based BGP ORF on PE2.

```
[PE2] bgp 100
[PE2-bgp] peer 111.1.1.1 capability-advertise orf ip-prefix both
```

### Step 4 Verify the configuration.

# Check the negotiation of prefix-based BGP ORF.

```
<PE1> display bgp peer 111.1.1.2 verbose

BGP Peer is 111.1.1.2, remote AS 100
Type: IBGP link
BGP version 4, Remote router ID 111.1.1.2
Update-group ID: 2
BGP current state: Established, Up for 00h01m22s
BGP current event: KATimerExpired
BGP last state: OpenConfirm
BGP Peer Up count: 8
Received total routes: 1
Received active routes total: 1
Advertised total routes: 0
Port: Local - 54845 Remote - 179
Configured: Active Hold Time: 180 sec Keepalive Time:60 sec
Received : Active Hold Time: 180 sec
Negotiated: Active Hold Time: 180 sec Keepalive Time:60 sec
Peer optional capabilities:
Peer supports bgp multi-protocol extension
Peer supports bgp route refresh capability
Peer supports bgp outbound route filter capability
Support Address-Prefix: IPv4-UNC address-family, rfc-compatible, both
Peer supports bgp 4-byte-as capability
Address family IPv4 Unicast: advertised and received
Received: Total 5 messages
 Update messages 1
 Open messages 1
 KeepAlive messages 2
 Notification messages 0
 Refresh messages 1
```

```

Sent: Total 4 messages
 Update messages 0
 Open messages 1
 KeepAlive messages 2
 Notification messages 0
 Refresh messages 1
Authentication type configured: None
Last keepalive received: 2010/03/30 13:37:25 UTC-08:00
Minimum route advertisement interval is 15 seconds
Optional capabilities:
Route refresh capability has been enabled
Outbound route filter capability has been enabled
Enable Address-Prefix: IPv4-UNC address-family, rfc-compatible, both
4-byte-as capability has been enabled
Peer Preferred Value: 0
Routing policy configured:
No import update filter list
No export update filter list
Import prefix list is: 1
No export prefix list
No import route policy
No export route policy
No import distribute policy
No export distribute policy

```

# Check the routes sent by PE2 to PE1.

```
<PE2> display bgp routing peer 111.1.1.1 advertised-routes
```

```

BGP Local router ID is 111.1.1.2
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 1
 Network NextHop MED LocPrf PrefVal Path/Ogn
* > 4.4.4.4/32 0.0.0.0 0 0 0 ?

```

# Check the routes received by PE1 from PE2.

```
<PE1> display bgp routing-table peer 111.1.1.2 received-routes
```

```

BGP Local router ID is 111.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 1
 Network NextHop MED LocPrf PrefVal Path/Ogn
* > i 4.4.4.4/32 111.1.1.2 0 100 0 ?

```

After being enabled with prefix-based BGP ORF, PE2 sends only route 4.4.4.4 matching the inbound policy of PE1.

----End

## Configuration Files

- Configuration file of PE1

```

#
sysname PE1
#
interface Pos1/0/0
link-protocol ppp
ip address 111.1.1.1 255.255.255.0
#

```

```

 bgp 100
 peer 111.1.1.2 as-number 100
 #
 ipv4-family unicast
 undo synchronization
 peer 111.1.1.2 enable
 peer 111.1.1.2 ip-prefix 1 import
 peer 111.1.1.2 capability-advertise orf ip-prefix both
 #
 ip ip-prefix 1 index 10 permit 4.4.4.0 24 greater-equal 32 less-equal 32
 #
 return

```

- Configuration file of PE2

```

 #
 sysname PE2
 #
 interface Pos1/0/0
 link-protocol ppp
 ip address 111.1.1.2 255.255.255.0
 #
 bgp 100
 peer 111.1.1.1 as-number 100
 #
 ipv4-family unicast
 undo synchronization
 import-route static
 peer 111.1.1.1 enable
 peer 111.1.1.1 capability-advertise orf ip-prefix both
 #
 ip route-static 3.3.3.3 255.255.255.255 NULL0
 ip route-static 4.4.4.4 255.255.255.255 NULL0
 ip route-static 5.5.5.5 255.255.255.255 NULL0
 #
 return

```

### 8.23.13 Example for Configuring BGP GTSM

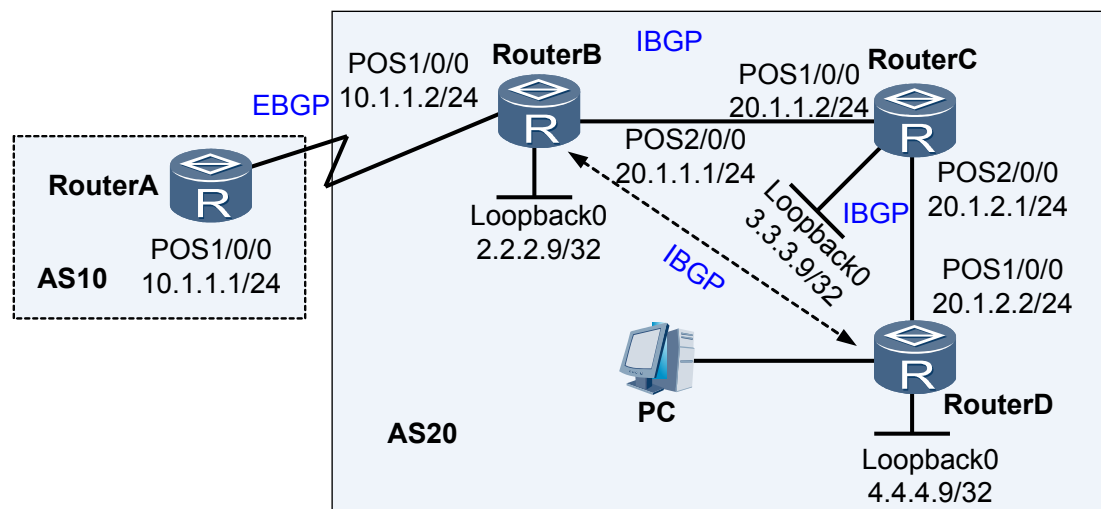
On a BGP network, BGP GTSM is configured to protect routers against CPU-utilization attacks.

#### Networking Requirements

As shown in [Figure 8-13](#), Router A belongs to AS 10, and Router B, Router C, and Router D belong to AS 20. BGP is run in the network and BGP GTSM is configured to protect Router B against CPU-utilization attacks.



Figure 8-13 Networking diagram of configuring BGP GTSM



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure OSPF on Router B, Router C, and Router D to implement interworking in AS 20.
2. Set up an EBGP connection between Router A and Router B, and set up IBGP connections between Router B, Router C, and Router D through loopback interfaces.
3. Configure GTSM on Router A, Router B, Router C, and Router D.

## Data Preparation

To complete the configuration, you need the following data:

- Route IDs of Router A, Router B, Router C, Router D and number of the AS where they reside
- TTL values between Router A and Router B, between Router B and Router C, between Router C and Router D, and between Router B and Router D.

## Procedure

**Step 1** Assign an IP address to each interface.

The configuration details are not mentioned here.

**Step 2** Configure OSPF.

The configuration details are not mentioned here.

**Step 3** Configure an IBGP connection.

# Configure Router B.

```
[RouterB] bgp 20
[RouterB-bgp] router-id 2.2.2.9
[RouterB-bgp] peer 3.3.3.9 as-number 20
```

```
[RouterB-bgp] peer 3.3.3.9 connect-interface LoopBack0
[RouterB-bgp] peer 3.3.3.9 next-hop-local
[RouterB-bgp] peer 4.4.4.9 as-number 20
[RouterB-bgp] peer 4.4.4.9 connect-interface LoopBack0
[RouterB-bgp] peer 4.4.4.9 next-hop-local
```

# Configure Router C.

```
[RouterC] bgp 20
[RouterC-bgp] router-id 3.3.3.9
[RouterC-bgp] peer 2.2.2.9 as-number 20
[RouterC-bgp] peer 2.2.2.9 connect-interface LoopBack0
[RouterC-bgp] peer 4.4.4.9 as-number 20
[RouterC-bgp] peer 4.4.4.9 connect-interface LoopBack0
```

# Configure Router D.

```
[RouterD] bgp 20
[RouterD-bgp] router-id 4.4.4.9
[RouterD-bgp] peer 2.2.2.9 as-number 20
[RouterD-bgp] peer 2.2.2.9 connect-interface LoopBack0
[RouterD-bgp] peer 3.3.3.9 as-number 20
[RouterD-bgp] peer 3.3.3.9 connect-interface LoopBack0
```

#### Step 4 Configure an EBGP connection.

# Configure Router A.

```
[RouterA] bgp 10
[RouterA-bgp] router-id 1.1.1.9
[RouterA-bgp] peer 10.1.1.2 as-number 20
```

# Configure Router B.

```
[RouterB-bgp] peer 10.1.1.1 as-number 10
```

# Display the connection status of the BGP peers.

```
<RouterB> display bgp peer
BGP local router ID : 2.2.2.9
Local AS number : 20
Total number of peers : 3 Peers in established state : 3
```

| Peer     | V | AS | MsgRcvd | MsgSent | OutQ | Up/Down  | State       | PrefRcv |
|----------|---|----|---------|---------|------|----------|-------------|---------|
| 3.3.3.9  | 4 | 20 | 8       | 7       | 0    | 00:05:06 | Established | 0       |
| 4.4.4.9  | 4 | 20 | 8       | 10      | 0    | 00:05:33 | Established | 0       |
| 10.1.1.1 | 4 | 10 | 7       | 7       | 0    | 00:04:09 | Established | 0       |

You can view that Router B has set up BGP connections with other routers.

#### Step 5 Configure GTSM on Router A and Router B. Router A and Router B are directly connected, so the range of the TTL value between the two routers is [255, 255]. The value of **valid-ttl-hops** is 1.

# Configure GTSM on Router A.

```
[RouterA-bgp] peer 10.1.1.2 valid-ttl-hops 1
```

# Configure GTSM of the EBGP connection on Router B.

```
[RouterB-bgp] peer 10.1.1.1 valid-ttl-hops 1
```

# Check the GTSM configuration.

```
<RouterB> display bgp peer 10.1.1.1 verbose
BGP Peer is 10.1.1.1, remote AS 10
Type: EBGP link
BGP version 4, Remote router ID 1.1.1.9
```

```

Update-group ID : 2
BGP current state: Established, Up for 00h49m35s
BGP current event: RecvKeepalive
BGP last state: OpenConfirm
BGP Peer Up count: 1
Received total routes: 0
Received active routes total: 0
Advertised total routes: 0
Port: Local - 179 Remote - 52876
Configured: Active Hold Time: 180 sec Keepalive Time:60 sec
Received : Active Hold Time: 180 sec
Negotiated: Active Hold Time: 180 sec Keepalive Time:60 sec
Peer optional capabilities:
Peer supports bgp multi-protocol extension
Peer supports bgp route refresh capability
Peer supports bgp 4-byte-as capability
Address family IPv4 Unicast: advertised and received
Received: Total 59 messages
 Update messages 0
 Open messages 2
 KeepAlive messages 57
 Notification messages 0
 Refresh messages 0
Sent: Total 79 messages
 Update messages 5
 Open messages 2
 KeepAlive messages 71
 Notification messages 1
 Refresh messages 0
Authentication type configured: None,
Last keepalive received: 2009-09-20 13:54:58
Minimum route advertisement interval is 30 seconds
Optional capabilities:
Route refresh capability has been enabled
4-byte-as capability has been enabled
GTSM has been enabled, valid-ttl-hops: 1
Peer Preferred Value: 0
Routing policy configured:
No routing policy is configured

```

You can view that GTSM is enabled, the valid hop count is 1, and the BGP connection is in the Established state.

**Step 6** Configure GTSM on Router B and Router C. Router B and Router C are directly connected, so the range of the TTL value between the two routers is [255, 255]. The value of **valid-ttl-hops** is 1.

# Configure GTSM on Router B.

```
[RouterB-bgp] peer 3.3.3.9 valid-ttl-hops 1
```

# Configure GTSM of the IBGP connection on Router C.

```
[RouterC-bgp] peer 2.2.2.9 valid-ttl-hops 1
```

# View the GTSM configuration.

```

<RouterB> display bgp peer 3.3.3.9 verbose
BGP Peer is 3.3.3.9, remote AS 20
Type: IBGP link
BGP version 4, Remote router ID 3.3.3.9

Update-group ID : 0
BGP current state: Established, Up for 00h54m36s
BGP current event: KATimerExpired
BGP last state: OpenConfirm
BGP Peer Up count: 1
Received total routes: 0

```

```

Received active routes total: 0
Advertised total routes: 0
Port: Local - 54998 Remote - 179
Configured: Active Hold Time: 180 sec Keepalive Time:60 sec
Received : Active Hold Time: 180 sec
Negotiated: Active Hold Time: 180 sec Keepalive Time:60 sec
Peer optional capabilities:
Peer supports bgp multi-protocol extension
Peer supports bgp route refresh capability
Peer supports bgp 4-byte-as capability
Address family IPv4 Unicast: advertised and received
Received: Total 63 messages
 Update messages 0
 Open messages 1
 KeepAlive messages 62
 Notification messages 0
 Refresh messages 0
Sent: Total 69 messages
 Update messages 10
 Open messages 1
 KeepAlive messages 58
 Notification messages 0
 Refresh messages 0
Authentication type configured: None,
Last keepalive received: 2009-09-20 13:57:43
Minimum route advertisement interval is 15 seconds
Optional capabilities:
Route refresh capability has been enabled
4-byte-as capability has been enabled
Nexthop self has been configured
Connect-interface has been configured
GTSM has been enabled, valid-ttl-hops: 1
Peer Preferred Value: 0
Routing policy configured:
No routing policy is configured

```

You can view that GTSM is enabled, the valid hop count is 1, and the BGP connection is in the Established state.

**Step 7** Configure GTSM on Router C and Router D. Router C and Router D are directly connected, so the range of the TTL value between the two routers is [255, 255]. The value of **valid-ttl-hops** is 1.

# Configure GTSM of the IBGP connection on Router C.

```
[RouterC-bgp] peer 4.4.4.9 valid-ttl-hops 1
```

# Configure GTSM of the IBGP connection on Router D.

```
[RouterD-bgp] peer 3.3.3.9 valid-ttl-hops 1
```

# Check the GTSM configuration.

```

<RouterC> display bgp peer 4.4.4.9 verbose
BGP Peer is 4.4.4.9, remote AS 20
 Type: IBGP link
 BGP version 4, Remote router ID 4.4.4.9

 Update-group ID : 1
 BGP current state: Established, Up for 00h56m06s
 BGP current event: KATimerExpired
 BGP last state: OpenConfirm
 BGP Peer Up count: 1
 Received total routes: 0
 Received active routes total: 0
 Advertised total routes: 0
 Port: Local - 179 Remote - 53758
 Configured: Active Hold Time: 180 sec Keepalive Time:60 sec
 Received : Active Hold Time: 180 sec

```

```

 Negotiated: Active Hold Time: 180 sec Keepalive Time:60 sec
 Peer optional capabilities:
 Peer supports bgp multi-protocol extension
 Peer supports bgp route refresh capability
 Peer supports bgp 4-byte-as capability
 Address family IPv4 Unicast: advertised and received
 Received: Total 63 messages
 Update messages 0
 Open messages 1
 KeepAlive messages 62
 Notification messages 0
 Refresh messages 0
 Sent: Total 63 messages
 Update messages 0
 Open messages 2
 KeepAlive messages 61
 Notification messages 0
 Refresh messages 0
 Authentication type configured: None,
 Last keepalive received: 2009-09-20 14:00:06
 Minimum route advertisement interval is 15 seconds
 Optional capabilities:
 Route refresh capability has been enabled
 4-byte-as capability has been enabled
 Connect-interface has been configured
 GTSM has been enabled, valid-ttl-hops: 1
 Peer Preferred Value: 0
 Routing policy configured:
 No routing policy is configured

```

You can view that GTSM is enabled, the valid hop count is 1, and the BGP connection is in the Established state.

**Step 8** Configure GTSM on Router B and Router D. Router B and Router D are connected by Router C, so the range of the TTL value between the two routers is [254, 255]. The value of **valid-ttl-hops** is 2.

# Configure GTSM of the IBGP connection on Router B.

```
[RouterB-bgp] peer 4.4.4.9 valid-ttl-hops 2
```

# Configure GTSM on Router D.

```
[RouterD-bgp] peer 2.2.2.9 valid-ttl-hops 2
```

# Check the GTSM configuration.

```

<RouterB> display bgp peer 4.4.4.9 verbose
BGP Peer is 4.4.4.9, remote AS 20
 Type: IBGP link
 BGP version 4, Remote router ID 4.4.4.9

 Update-group ID : 0
 BGP current state: Established, Up for 00h57m48s
 BGP current event: RecvKeepalive
 BGP last state: OpenConfirm
 BGP Peer Up count: 1
 Received total routes: 0
 Received active routes total: 0
 Advertised total routes: 0
 Port: Local - 53714 Remote - 179
 Configured: Active Hold Time: 180 sec Keepalive Time:60 sec
 Received : Active Hold Time: 180 sec
 Negotiated: Active Hold Time: 180 sec Keepalive Time:60 sec
 Peer optional capabilities:
 Peer supports bgp multi-protocol extension
 Peer supports bgp route refresh capability
 Peer supports bgp 4-byte-as capability
 Address family IPv4 Unicast: advertised and received

```

```

Received: Total 72 messages
 Update messages 0
 Open messages 1
 KeepAlive messages 71
 Notification messages 0
 Refresh messages 0
Sent: Total 82 messages
 Update messages 10
 Open messages 1
 KeepAlive messages 71
 Notification messages 0
 Refresh messages 0
Authentication type configured: None,
Last keepalive received: 2009-09-20 14:01:27
Minimum route advertisement interval is 15 seconds
Optional capabilities:
Route refresh capability has been enabled
4-byte-as capability has been enabled
Nexthop self has been configured
Connect-interface has been configured
GTSM has been enabled, valid-ttl-hops: 2
Peer Preferred Value: 0
Routing policy configured:
No routing policy is configured

```

You can view that GTSM is configured, the valid hop count is 2, and the BGP connection is in the Established state.

 **NOTE**

- In this example, if the value of **valid-ttl-hops** of either Router B or Router D is smaller than 2, the IBGP connection cannot be set up.
- GTSM must be configured on the two ends of the BGP connection.

**Step 9** Verify the configuration.

# Run the **display gtsm statistics all** command on Router B to check the GTSM statistics of Router B. By default, Router B does not discard any packet when all packets match the GTSM policy.

```

<RouterB> display gtsm statistics all
GTSM Statistics Table

SlotId Protocol Total Counters Drop Counters Pass Counters

0 BGP 17 0 17
0 BGPv6 0 0 0
0 OSPF 0 0 0
0 LDP 0 0 0
1 BGP 0 0 0
1 BGPv6 0 0 0
1 OSPF 0 0 0
1 LDP 0 0 0
2 BGP 0 0 0
2 BGPv6 0 0 0
2 OSPF 0 0 0
2 LDP 0 0 0
3 BGP 0 0 0
3 BGPv6 0 0 0
3 OSPF 0 0 0
3 LDP 0 0 0
4 BGP 32 0 32
4 BGPv6 0 0 0
4 OSPF 0 0 0
4 LDP 0 0 0
5 BGP 0 0 0
5 BGPv6 0 0 0
5 OSPF 0 0 0

```

|   |       |   |   |   |
|---|-------|---|---|---|
| 5 | LDP   | 0 | 0 | 0 |
| 7 | BGP   | 0 | 0 | 0 |
| 7 | BGPv6 | 0 | 0 | 0 |
| 7 | OSPF  | 0 | 0 | 0 |
| 7 | LDP   | 0 | 0 | 0 |

-----

If the host simulates the BGP packets of Router A to attack Router B, the packets are discarded because their TTL value is not 255 when reaching Router B. In the GTSM statistics of Router B, the number of dropped packets increases accordingly.

----End

## Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.0
#
 bgp 10
 router-id 1.1.1.9
 peer 10.1.1.2 as-number 20
 peer 10.1.1.2 valid-ttl-hops 1
#
 ipv4-family unicast
 undo synchronization
 peer 10.1.1.2 enable
#
 return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.0
#
 interface Pos2/0/0
 link-protocol ppp
 ip address 20.1.1.1 255.255.255.0
#
 interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
 bgp 20
 router-id 2.2.2.9
 peer 3.3.3.9 as-number 20
 peer 3.3.3.9 valid-ttl-hops 1
 peer 3.3.3.9 connect-interface LoopBack0
 peer 4.4.4.9 as-number 20
 peer 4.4.4.9 valid-ttl-hops 2
 peer 4.4.4.9 connect-interface LoopBack0
 peer 10.1.1.1 as-number 10
 peer 10.1.1.1 valid-ttl-hops 1
#
 ipv4-family unicast
 undo synchronization
 import-route ospf 1
 peer 3.3.3.9 enable
 peer 3.3.3.9 next-hop-local
 peer 4.4.4.9 enable
 peer 4.4.4.9 next-hop-local
```

```

 peer 10.1.1.1 enable
 #
 ospf 1
 area 0.0.0.0
 network 20.1.1.0 0.0.0.255
 network 2.2.2.9 0.0.0.0
 #
 return

```

● Configuration file of Router C

```

 #
 sysname RouterC
 #
 interface Pos1/0/0
 link-protocol ppp
 ip address 20.1.1.2 255.255.255.0
 #
 interface Pos2/0/0
 link-protocol ppp
 ip address 20.1.2.1 255.255.255.0
 #
 interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
 #
 bgp 20
 router-id 3.3.3.9
 peer 2.2.2.9 as-number 20
 peer 2.2.2.9 valid-ttl-hops 1
 peer 2.2.2.9 connect-interface LoopBack0
 peer 4.4.4.9 as-number 20
 peer 4.4.4.9 valid-ttl-hops 1
 peer 4.4.4.9 connect-interface LoopBack0
 #
 ipv4-family unicast
 undo synchronization
 peer 2.2.2.9 enable
 peer 4.4.4.9 enable
 #
 ospf 1
 area 0.0.0.0
 network 20.1.2.0 0.0.0.255
 network 20.1.1.0 0.0.0.255
 network 3.3.3.9 0.0.0.0
 #
 return

```

● Configuration file of Router D

```

 #
 sysname RouterD
 #
 interface Pos1/0/0
 link-protocol ppp
 ip address 20.1.2.2 255.255.255.0
 #
 interface LoopBack0
 ip address 4.4.4.9 255.255.255.255
 #
 bgp 20
 router-id 4.4.4.9
 peer 2.2.2.9 as-number 20
 peer 2.2.2.9 valid-ttl-hops 2
 peer 2.2.2.9 connect-interface LoopBack0
 peer 3.3.3.9 as-number 20
 peer 3.3.3.9 valid-ttl-hops 1
 peer 3.3.3.9 connect-interface LoopBack0
 #
 ipv4-family unicast
 undo synchronization
 peer 2.2.2.9 enable
 peer 3.3.3.9 enable

```



```

ospf 1
 area 0.0.0.0
 network 20.1.2.0 0.0.0.255
 network 4.4.4.9 0.0.0.0

return
```

# 9 BGP4+ Configuration

---

## About This Chapter

BGP4+, which is applicable to the large-scale IPv6 network with a complicated structure, is used between ASs to transmit routing information.

### [9.1 Introduction of BGP4+](#)

BGP4+ is a dynamic routing protocol used between ASs.

### [9.2 Configuring Basic BGP4+ Functions](#)

Before building BGP4+ networks, you need to configure basic BGP4+ functions.

### [9.3 Configuring BGP4+ Route Attributes](#)

BGP4+ has many route attributes. By configuring these attributes, you can change BGP4+ routing policies.

### [9.4 Controlling the Advertising and Receiving of BGP4+ Routing Information](#)

BGP4+ can perform routing policies on or filter only the routes to be advertised to a certain peer.

### [9.5 Configuring Parameters of a Connection Between BGP4+ Peers](#)

By setting parameters of a connection between BGP4+ peers, you can adjust and optimize the BGP4+ network performance.

### [9.6 Configuring BFD for BGP4+](#)

By configuring BFD for BGP4+, you can provide a fast fault detection mechanism for BGP4+, and thus speed up network convergence.

### [9.7 Configuring BGP4+ Tracking](#)

On a network where BFD is unsuitable to deploy, you can configure BGP4+ tracking to implement the fast convergence of IBGP routes.

### [9.8 Configuring BGP4+ Route Dampening](#)

By configuring BGP4+ route dampening, you can suppress unstable BGP4+ routes.

### [9.9 Configuring BGP4+ Load Balancing](#)

By configuring BGP4+ load balancing, you can properly use network resources.

### [9.10 Configuring a BGP4+ Peer Group](#)

By configuring a BGP4+ peer group, you can simplify the management of routing policies, and thus improve the efficiency of route advertisement.

### 9.11 Configuring a BGP4+ Route Reflector

By configuring a BGP4+ route reflector, you can solve the problem of establishing fully meshed connections between multiple IBGP peers.

### 9.12 Configuring a BGP4+ Confederation

On a large-scale BGP4+ network, configuring a BGP4+ confederation can simplify the management of routing policies and improve the efficiency of route advertisement.

### 9.13 Configuring BGP4+ 6PE

By configuring BGP4+ 6PE, you can connect separated IPv6 networks through the MPLS tunneling technology.

### 9.14 Configuring BGP4+ 6PE FRR

After you configure 6PE FRR on a router, the router can select a backup next hop for received 6PE routes. When the next hop of the primary route between PEs becomes unreachable, traffic will be quickly switched to the backup next hop.

### 9.15 Configuring BGP4+ Security

To improve BGP4+ security, you can perform TCP connection authentication.

### 9.16 Maintaining BGP4+

Maintaining BGP4+ involves resetting a BGP4+ connection and clearing BGP4+ statistics.

### 9.17 Configuration Examples

BGP4+ configuration examples explain networking requirements, networking diagram, configuration notes, configuration roadmap, and configuration procedure.

## 9.1 Introduction of BGP4+

BGP4+ is a dynamic routing protocol used between ASs.

### 9.1.1 BGP4+ Overview

BGP4+ is mainly used to control route transmission and select optimal routes.

BGP4+ is a dynamic routing protocol used between Autonomous Systems (ASs), and it is an extension of BGP.

The traditional BGP4 can manage only the IPv4 routing information. For other network layer protocols such as IPv6, the traditional BGP4 has a limited capability to transmit routing information.

The IETF introduces BGP4+ as a supplement to BGP4 to support multiple network layer protocols. The RFC for BGP4+ is RFC 2858 (Multiprotocol Extensions for BGP4).

To support IPv6, BGP4 needs to reflect the IPv6 protocol information to the Network Layer Reachable Information (NLRI) attribute and the Next\_Hop attribute.

BGP4+ introduces two NLRI attributes:

- Multiprotocol Reachable NLRI (MP\_REACH\_NLRI): advertises the reachable routes and the next hop information.
- Multiprotocol Unreachable NLRI (MP\_UNREACH\_NLRI): withdraws the unreachable routes.

The Next\_Hop attribute of BGP4+ is in the format of an IPv6 address. It can be an IPv6 global unicast address or the link-local address of the next hop.

BGP4+ can be applied to an IPv6 network by using the BGP attribute of multiple protocol extension. The message and routing mechanisms of BGP remain unaltered.

### 9.1.2 BGP4+ Features Supported by the NE80E/40E

The system supports various BGP4+ features, including load balancing, route aggregation, route dampening, community, route reflector, confederation, BGP4+ accounting, 6PE, BFD for BGP4+, BGP4+ GR, and BGP4+ NSR.

#### 6PE

After the 6PE function is enabled, the separated IPv6 networks can be connected through the Multi-Protocol Label Switch (MPLS) tunnel technology. The tunnel in 6PE mode implements the dual protocol stack of IPv4/IPv6 on PEs of the Internet Service Provider (ISP). It identifies IPv6 routes by using the label assigned by the Multiprotocol Border Gateway Protocol (MP-BGP), and implements IPv6 interworking through LSPs between PEs.

#### Other Attributes

Most of BGP4+ features supported by the NE80E/40E are similar to those of BGP supported by the NE80E/40E. For details, refer to the chapter "BGP Configuration".

BGP4+ does not support summary automatic and MP-BGP.

## 9.2 Configuring Basic BGP4+ Functions

Before building BGP4+ networks, you need to configure basic BGP4+ functions.

### 9.2.1 Establishing the Configuration Task

Before configuring basic BGP4+ functions, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

BGP4+ is configured in an IPv6 network.

#### Pre-configuration Tasks

Before configuring basic BGP4+ functions, complete the following tasks:

- Enabling IPv6
- Configuring link layer protocol parameters and IPv6 addresses for interfaces to make link layers of the interfaces Up

#### Data Preparation

To configure BGP4+, you need the following data.

| No. | Data                                                |
|-----|-----------------------------------------------------|
| 1   | Local AS number and Router ID                       |
| 2   | IPv6 address and AS number of the peer              |
| 3   | (Optional) Interfaces that set up the BGP4+ session |

### 9.2.2 Starting a BGP Process

Starting a BGP4+ process is a prerequisite for configuring basic BGP4+ functions. When starting a BGP4+ process, you need to specify the number of the AS that the device belongs to.

#### Context

Do as follows on the router on which the BGP4+ connection needs to be set up:

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

BGP is enabled (the local AS number is specified) and the BGP view is displayed.

**Step 3** (Optional) Run:

```
router-id ipv4-address
```

The router ID is set.

Setting or changing the router ID of BGP resets the BGP peer relationship between routers.

 **TIP**

- To enhance the network reliability, you can manually configure the address of a loopback interface as the router ID. If the router ID is not set, BGP uses the router ID in the system view. To select the router ID in the system view, refer to the *Command Reference*.
- If no interface of a router is configured with an IPv4 address, you must set a router ID for the router.

---End

## 9.2.3 Configuring an IPv6 Peer

Devices can exchange BGP4+ routing information only after BGP4+ peers are configured and the BGP4+ peer relationship is established.

### Procedure

- Configuring an IBGP Peer

Do as follows on the router on which the IBGP connection needs to be set up:

## 1. Run:

```
system-view
```

The system view is displayed.

## 2. Run:

```
bgp as-number
```

The BGP view is displayed.

## 3. Run:

```
peer ipv6-address as-number as-number
```

The peer address and the AS where the peer resides are configured.

The AS number of the specified peer must be the same as the local AS number.

When the IPv6 address of a specified peer is a loopback address or a sub-interface address, you need to perform [Configuring the Local Interfaces Used for BGP4+ Connections](#) to ensure the establishment of the peer.

## 4. (Optional) Run:

```
peer { ipv6-address | group-name } listen-only
```

A peer (group) is configured only to listen to connection requests, but not to send connection requests.

After this command is used, the existing peer relationship is interrupted. The peer on which this command is used waits for the connection request from its peer to reestablish the neighbor relationship. This configuration can prevent the conflict of sending connection requests.

 **NOTE**

This command can be used on only one of two peers. If this command is used on the two peers, the connection between the two peers cannot be established.

5. Run:  
`ipv6-family [ unicast ]`

The BGP IPv6 unicast address family view is displayed.

6. Run:  
`peer ipv6-address enable`

The IPv6 peers are enabled.

After configuring the BGP4+ peers in the BGP view, you need to enable these peers in the BGP IPv6 unicast address family view.

● **Configuring an EBGP Peer**

Do as follows on the router on which the EBGP connection needs to be set up:

1. Run:  
`system-view`  
 The system view is displayed.
2. Run:  
`bgp as-number`  
 The BGP view is displayed.
3. Run:  
`peer ipv6-address as-number as-number`

The IP address and the AS number of a specified BGP peer are specified.

The AS number of the specified BGP peer should be different from the local AS number.

If the IP address of the specified peer is that of a loopback interface on the reachable peer or that of a sub-interface on the directly connected peer, you need to complete the task of [Configuring the Local Interfaces Used for BGP4+ Connections](#) to ensure that the peer is correctly established.

4. Run:  
`peer { ipv6-address | group-name } ebgp-max-hop [ hop-count ]`

The maximum number of hops in the EBGP connections is set.

Usually, a direct physical link should be available between the EBGP peers. If this requirement cannot be met, you can use the `peer ebgp-max-hop` command to configure the EBGP peers to establish the TCP connections through multiple hops.

 **NOTE**

When establishing the EBGP connection through loopback interfaces, you must use the `peer ebgp-max-hop` command specifying that *hop-count* is greater than or equal to 2. Otherwise, BGP cannot set up the EBGP connection with the peer.

5. (Optional) Run:  
`peer { ipv6-address | group-name } listen-only`

The peer or peer group is configured only to listen to connection requests, but not to send any connection request.

After this command is used, the existing peer relationship is removed. The peer on which this command is used reestablishes the peer relationship after receiving the connection request from its peer. After this configuration is done, the conflict of connection requests is avoided.

 **NOTE**

This command can be used on only one of two peers. If this command is used on the two peers, the connection between the two peers cannot be established.

6. Run:

```
ipv6-family [unicast]
```

The BGP IPv6 unicast address family view is displayed.

7. Run:

```
peer ipv6-address enable
```

An IPv6 peer is enabled.

After configuring a BGP4+ peer in the BGP view, enable the peer in the BGP IPv6 unicast address family view.

---End

## 9.2.4 (Optional) Configuring the Local Interfaces Used for BGP4+ Connections

When establishing multiple peers between two devices through various links, you need to specify the local interface during the setup of a BGP4+ session on the devices.

### Context

Do as follows on the BGP4+ router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
peer { ipv6-address | group-name } connect-interface interface-type interface-
number [ipv6-source-address]
```

The source interface and source address used to set up a TCP connection are specified.

Usually, BGP4+ uses the physical interface that is directly connected with the peer as the session interface used for the TCP connection.

To increase the reliability and stability of the BGP4+ connections, configure the local interface used for the BGP4+ connection as the loopback interface. In this way, when there are redundant



links on the network, the BGP4+ connections are not interrupted due to the failure of a certain interface or a link.

----End

## 9.2.5 Checking the Configuration

After basic BGP4+ functions are configured, you can check BGP4+ peer information.

### Prerequisite

The configurations of basic BGP4+ functions are complete.

### Procedure

- Run the **display bgp ipv6 peer ipv4-address verbose** command to check information about the BGP4+ peers.
- Run the **display bgp ipv6 peer ipv6-address { log-info | verbose }** command to check information about the BGP4+ peers.

----End

## 9.3 Configuring BGP4+ Route Attributes

BGP4+ has many route attributes. By configuring these attributes, you can change BGP4+ routing policies.

### 9.3.1 Establishing the Configuration Task

Before controlling BGP4+ route selection, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

### Applicable Environment

You can change the BGP4+ routing policies by configuring the route attributes.

- BGP4+ priority  
After the BGP4+ priority is configured, Route Management (RM) is affected in routing between BGP4+ and the other routing protocols.
- Preferred value of BGP4+ routing information  
After the preferred value of BGP4+ routing information is configured, the route with the greatest preferred value is selected when multiple routes to the same destination exist in the BGP4+ routing table.
- Local\_Pref attribute  
The function of the Local\_Pref attribute is similar to that of the preferred value of BGP4+ routing information. The preferred value of BGP4+ routing information takes precedence over the Local\_Pref attribute.
- MED attribute  
After the MED attribute is configured, EBGP peers select the route with the smallest MED value when the traffic enters an AS.

- Next\_Hop attribute  
 A route with an unreachable next hop is ignored.
- Community attribute  
 The community attribute can simplify the management of routing policies. The management range of the community attribute is wider than that of the peer group. The community attribute can control the routing policies of multiple BGP4+ routers.
- AS\_Path attribute  
 After the AS\_Path attribute is configured, the route with a shorter AS path is selected.

## Pre-configuration Tasks

Before configuring BGP4+ route attributes, complete the following tasks:

- [Configuring Basic BGP4+ Functions](#)

## Data Preparation

To configure BGP4+ route attributes, you need the following data.

| No. | Data                                                         |
|-----|--------------------------------------------------------------|
| 1   | AS number                                                    |
| 2   | Protocol priority                                            |
| 3   | Local_Pref                                                   |
| 4   | MED                                                          |
| 5   | Name of the routing policy for using the community attribute |

### 9.3.2 Configuring the BGP4+ Preference

Setting the BGP4+ preference can affect route selection between BGP4+ and another routing protocol.

#### Context

Do as follows on the BGP4+ router:

#### Procedure

- Step 1** Run:  
`system-view`  
 The system view is displayed.
- Step 2** Run:  
`bgp as-number`  
 The BGP view is displayed.

**Step 3** Run:

```
ipv6-family [unicast]
```

The BGP IPv6 unicast address family view is displayed.

**Step 4** Run:

```
preference { external internal local | route-policy route-policy-name }
```

The BGP4+ preference is set.

 **NOTE**

Using `peer route-policy` command to configure the preference of the BGP protocol on the peers is not currently supported.

----End

### 9.3.3 Configuring BGP4+ Preferred Value for Routing Information

After the preferred value is configured for routing information, the route with the largest preferred value is selected when multiple routes to the same destination exist in the BGP4+ routing table.

#### Context

Do as follows on the BGP4+ router:

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family [unicast]
```

The BGP IPv6 unicast address family view is displayed.

**Step 4** Run:

```
peer { group-name | ipv4-address | ipv6-address } preferred-value value
```

The preferred value of a peer is configured.

By default, the preferred value of the route learned from a neighbor is 0.

----End

### 9.3.4 Configuring the Default Local\_Pref Attribute of the Local Router

The Local\_Pref attribute is used to determine the optimal route for the traffic that leaves an AS. When a BGP4+ router obtains multiple routes to the same destination address but with different next hops from different IBGP peers, the route with the largest Local\_Pref value is selected.

## Context

Do as follows on the BGP4+ router:

## Procedure

- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`bgp as-number`  
The BGP view is displayed.
- Step 3** Run:  
`ipv6-family [ unicast ]`  
The BGP IPv6 unicast address family view is displayed.
- Step 4** Run:  
`default local-preference preference`  
The default Local\_Pref of the local router is configured.
- End

## 9.3.5 Configuring the MED Attribute

The MED attribute serves as the metric used by an IGP. After MED attributes are set, EBGP peers select the route with the smallest MED value for the traffic that enters an AS.

## Context

Do as follows on the BGP4+ router:

## Procedure

- Step 1** Run:  
`system-view`  
The system view is displayed.
- Step 2** Run:  
`bgp as-number`  
The BGP view is displayed.
- Step 3** Run:  
`ipv6-family [ unicast ]`  
The BGP IPv6 unicast address family view is displayed.
- Step 4** Run the following commands to configure the BGP4+ MED attribute as required:
- Run:  
`default med med`

The default MED attribute is configured.

- Run:

```
compare-different-as-med
```

The MED values from different ASs are compared.

- Run:

```
deterministic-med
```

Deterministic-MED is enabled.

If this command is not configured, when an optimal route is to be selected from among routes which are received from different ASs and which carry the same prefix, the sequence in which routes are received is relevant to the result of route selection. After the command is configured, however, when an optimal route is to be selected from among routes which are received from different ASs and which carry the same prefix, routes are first grouped according to the leftmost AS in the AS\_Path. Routes with the same leftmost AS are grouped together, and after comparison, an optimal route is selected for the group. The group optimal route is then compared with optimal routes from other groups to determine the final optimal route. This mode of route selection ensures that the sequence in which routes are received is no longer relevant to the result of route selection.

- Run:

```
bestroute med-none-as-maximum
```

The maximum MED value is used when the current MED is not available.

- Run:

```
bestroute med-confederation
```

The MED values of routes advertised in the local confederation are compared.

The commands in Step 4 can be used regardless of the order.

----End

## 9.3.6 Configuring the Next\_Hop Attribute

By setting the Next\_Hop attribute, you can flexibly control BGP4+ route selection.

### Procedure

- Modifying the Next Hop When Advertising a Route to an IBGP Peer

Do as follows on the IBGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

4. Run:

```
peer { ipv6-address | group-name } next-hop-local
```

The local address is configured as the next hop when routes are advertised.

In some networking environments, to ensure that the IBGP neighbors find the correct next hop, configure the next hop address as its own address when routes are advertised to the IBGP peers.

 **NOTE**

If BGP load balancing is configured, the local router changes the next hop address to its own address when advertising routes to the IBGP peer groups, regardless of whether the **peer next-hop-local** command is used.

- The next-hop iteration based on the routing policy

Do as follows on the BGP router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv6-family unicast
```

The BGP-IPv6 unicast address family view is displayed.

4. Run:

```
nexthop recursive-lookup route-policy route-policy-name
```

The next-hop iteration based on the specified routing policy is enabled.

By default, the next-hop iteration based on the specified routing policy is disabled.

The next-hop iteration based on the specified routing policy can control the iterated route according to certain conditions. The route that fails to pass the policy is ignored.

----End

## 9.3.7 Configuring the AS-Path Attribute

The AS\_Path attribute is used to avoid routing loops and control route selection.

### Procedure

- Configuring the AS\_Path Attribute in the IPv6 Address Family View

Do as follows on the BGP4+ router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

4. Run the following commands to configure the AS-Path attribute as required:

- Run:

```
peer { ipv4-address | ipv6-address | group-name } allow-as-loop
[number]
```

The local AS number can be used repeatedly.

- Run:

```
bestroute as-path-ignore
```

The AS-Path attribute is not configured as one of the route selection rules.

- Run:

```
peer { ipv6-address | group-name } public-as-only
```

The AS-Path attribute is configured to carry only the public AS number.

The commands in Step 4 can be used regardless of the order.

- Configuring the Fake AS Number

Do as follows on the BGP4+ router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
peer { ipv6-address | group-name } fake-as fake-as-number
```

The fake AS number is set.

You can hide the actual AS number of the local router by using this command. EBGP peers in other ASs can only see this fake AS number. That is, peers in other ASs need to specify the number of the AS where the local peer resides as this fake AS number.

 **NOTE**

This command is applicable only to EBGP peers.

- Substituting the AS Number in the AS-Path Attribute

Do as follows on the BGP4+ router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv6-family vpn-instance vpn-instance-name
```

The BGP-VPN instance IPv6 address family view is displayed.

4. Run:

```
peer { ipv6-address | group-name } substitute-as
```

The AS number in the AS-Path attribute is substituted.

After this command is used, if the AS-Path attribute contains the AS number of the peer, you can substitute the local AS number for the AS number of the peer before advertising routes to the peer.



## CAUTION

If the configuration is not correct, the command may cause routing loops.

---

----End

## 9.3.8 Configuring the BGP4+ Community Attribute

The community attribute is used to simplify the management of routing policies. The management scope of the community attribute is far larger than that of the peer group. The community attribute can control the routing policies of multiple BGP4+ routers.

### Procedure

- Configuring the routers to Advertise the Community Attribute to the Peers

Do as follows on the BGP4+ router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

4. Run the following commands to advertise community attributes to the peer group:

- Run:

```
peer { ipv4-address | ipv6-address | group-name } advertise-community
```

Routers are configured to advertise the standard community attribute to a peer group.

- Run:

```
peer { ipv4-address | ipv6-address | group-name } advertise-ext-community
```

Routers are configured to advertise the extended community attribute to a peer group.

- Applying the Routing Policies to the Advertised Routing Information



Do as follows on the BGP4+ router:

1. Run:  
`system-view`  
 The system view is displayed.
2. Run:  
`bgp as-number`  
 The BGP view is displayed.
3. Run:  
`ipv6-family unicast`  
 The BGP IPv6 unicast address family view is displayed.
4. Run:  
`peer { ipv4-address | ipv6-address | group-name } route-policy route-policy-name export`  
 The outbound routing policies are configured.

 NOTE

- When configuring a BGP4+ community, you should define the specific community attribute by using the routing policies. Then, apply these routing policies to the advertisement of routing information.
- For the configuration of routing policies, refer to [Routing Policy Configuration](#). For the configuration of community attributes, refer to [BGP Configuration](#).

---End

## 9.3.9 Checking the Configuration

After BGP4+ route attributes are configured, you can check information about route attributes.

### Prerequisite

The configurations of BGP4+ route attributes are complete.

### Procedure

- Run the `display bgp ipv6 paths [ as-regular-expression ]` command to check the AS-Path information.
- Run the `display bgp ipv6 routing-table different-origin-as` command to check the route with the different source AS.
- Run the `display bgp ipv6 routing-table regular-expression as-regular-expression` command to check the routing information matching the regular expression of the AS.
- Run the `display bgp ipv6 routing-table community [ aa:nn <1-29> ] [ internet | no-advertise | no-export | no-export-subconfed ] * [ whole-match ]` command to check routing information about the specified BGP4+ community.
- Run the `display bgp ipv6 routing-table community-filter { { community-filter-name | basic-community-filter-number } [ whole-match ] | advanced-community-filter-number }` command to check information about the routes matching the specified BGP4+ community attribute filter.

---End

## 9.4 Controlling the Advertising and Receiving of BGP4+ Routing Information

BGP4+ can perform routing policies on or filter only the routes to be advertised to a certain peer.

### 9.4.1 Establishing the Configuration Task

Before controlling the advertisement of BGP4+ routes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

This section describes the following:

- Controlling the advertising and receiving of BGP4+ routing information, which includes the filtering of routing information and the application of the routing policies.
- Soft resetting the BGP4+ connections

In the NE80E/40E, BGP4+ supports the route-refresh capability. When the policies are changed, the system can refresh the BGP4+ routing table automatically without interrupting the BGP4+ connections.

If there are routers that do not support route-refresh in the network, you can run the **peer keep-all-routes** command to save all route refreshment locally. Then, you can run the **refresh bgp** command to soft reset the BGP4+ connections manually.

#### Pre-configuration Tasks

Before controlling the advertising and receiving of BGP4+ routing information, complete the following tasks:

- **Configuring Basic BGP4+ Functions**

#### Data Preparation

To control the advertising and receiving of BGP4+ routing information, you need the following data.

| No. | Data                                                                                                                                                                                                                          |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Name and process ID of the external route to be imported                                                                                                                                                                      |
| 2   | Name of the filtering list used in the routing policies                                                                                                                                                                       |
| 3   | Various parameters of route dampening, including half-life of a reachable route, half-life of an unreachable route, threshold for freeing suppressed routes, threshold for suppressing routes, and upper limit of the penalty |

## 9.4.2 Configuring BGP4+ to Advertise Local IPv6 Routes

The local routes to be advertised must be in the local IP routing table. You can use routing policies to control the routes to be advertised.

### Context

Do as follows on the BGP4+ router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 4** Run:

```
network ipv6-address prefix-length [route-policy route-policy-name]
```

The exactly-matched local IPv6 routes are advertised.

You can use the **network** command to statically inject the IPv6 routes to the BGP4+ routing table.

To be specific, the command can be used to advertise the routes only with the exactly-matched address prefix and mask. If the mask is not designated, the routes are exactly matched based on the natural network segment.

The local routes to be advertised should be in the local IPv6 routing table. You can use routing policies to control the routes to be advertised more flexibly.

---End

## 9.4.3 Configuring BGP4+ Route Aggregation

By configuring route aggregation, you can reduce the size of the routing table of a peer. BGP4+ supports automatic aggregation and manual aggregation.

### Context

Do as follows on the router enabled with BGP4+:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family unicast
```

The IPv6 unicast address family view is displayed.

**Step 4** Run:

```
aggregate ipv6-address prefix-length [as-set | attribute-policy route-policy-name1 | detail-suppressed | origin-policy route-policy-name2 | suppress-policy route-policy-name3] *
```

Manual aggregation of routes is configured.

Manual aggregation is valid for the routing entries in the local BGP4+ routing table. For example, if 9:3::1/64 does not exist in the BGP routing table, BGP4+ does not advertise the aggregated route even after the **aggregate 9:3::1 64** command is run to aggregate this route.

When configuring manual aggregation of routes, you can apply various routing policies and set the route attributes.

----End

## 9.4.4 Configuring BGP4+ to Import and Filter External Routes

After BGP4+ filters the imported routes, only the eligible routes are added to the local BGP4+ routing table and advertised to BGP4+ peers.

### Context

Do as follows on the BGP4+ router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 4** Run:

```
default-route imported
```

BGP4+ is configured to import the default routes.

If the **default-route imported** command is not used, you cannot import the default routes from other protocols by using the **import-route** command.

**Step 5** Run:

```
import-route protocol [process-id] [med med | route-policy route-policy-name] *
```

BGP4+ is configured to import routes of other protocols.

 **NOTE**

Specify the process ID when the routes of a dynamic routing protocol are imported.

**Step 6** Run:

```
filter-policy { acl6-number | acl6-name acl6-name | ipv6-prefix ipv6-prefix-name }

export [protocol [process-id]]
```

Imported routes are filtered.

After BGP4+ filters the imported routes, only the eligible routes are added to the BGP4+ local routing table and advertised to BGP4+ peers. If *protocol [ process-id ]* is specified, the routes of the specific routing protocol are filtered. If *protocol [ process-id ]* is not specified, all the local BGP routes to be advertised are filtered, including the imported routes and the local routes advertised through the **network** command.

----End

## 9.4.5 Configuring Routers to Advertise Default Routes to Peers

A router sends a default route with the local address being the next hop to the specified peer, regardless of whether there are default routes in the local routing table.

### Context

Do as follows on the BGP4+ router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 4** Run:

```
peer { ipv6-address | group-name } default-route-advertise [route-policy route-policy-name]
```

Default routes are advertised to peers (or a peer group).

 **NOTE**

After the command `peer default-route-advertise` is run, the router sends a default route with the local address as the next hop to the specified peer, regardless of whether there are default routes in the routing table.

----End

## 9.4.6 Configuring the Policy for Advertising BGP4+ Routing Information

After the policy for advertising routes is configured, only the routes that match the policy can be added to the local BGP4+ routing table and advertised to BGP4+ peers.

### Context

Do as follows on the BGP4+ router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 4** Run the following command to configure the outbound routing policy based on the following different filters:

- Based on the routing policy

Run:

```
peer { ipv4-address | ipv6-address | group-name } route-policy route-policy-name export
```

- Based on the ACL

Run:

```
peer { ipv4-address | ipv6-address | group-name } filter-policy { acl6-number | acl6-name acl6-name } export
```

- Based on the AS\_Path list

Run:

```
peer { ipv4-address | ipv6-address | group-name } as-path-filter { as-path-filter-number | as-path-filter-name } export
```

- Based on the prefix list

Run:

```
peer { ipv4-address | ipv6-address | group-name } ipv6-prefix ip-prefix-name export
```

The commands in Step 4 can be run regardless of the order.

The outbound routing updates policies used by the members of a peer group can be different from that used by the group. That is, members of each peer group can select their policies when advertising routes externally.

---End

## 9.4.7 Configuring the Policy for Receiving BGP4+ Routing Information

Only the routes that match the policy for receiving routes can be received by BGP4+ peers and added to the routing table.

### Context

Do as follows on the BGP4+ router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 4** Run:

```
filter-policy { acl6-number | acl6-name acl6-name | ipv6-prefix ipv6-prefix-name }
import
```

The imported global routes are filtered.

**Step 5** Run:

```
peer { ipv4-address | ipv6-address | group-name } route-policy route-policy-name
import
```

BGP is configured to filter the routes imported from the specified peers.

**Step 6** Run:

```
peer { ipv4-address | ipv6-address | group-name } filter-policy { acl6-number |
acl6-name acl6-name } import
```

BGP is configured to filter the routes based on the ACL.

**Step 7** Run:

```
peer { ipv4-address | ipv6-address | group-name } as-path-filter { as-path-filter-
number | as-path-filter-name } import
```

BGP is configured to filter the routes based on the AS path list.

**Step 8** Run:

```
peer { ipv4-address | ipv6-address | group-name } ipv6-prefix ipv6-prefix-name
import
```

BGP is configured to filter the routes based on the prefix list.

The commands in Steps 4 to 8 can be run regardless of the order.

The routes imported by BGP can be filtered, and only those routes that meet certain conditions are received by BGP and added to the routing table.

The inbound routing policies used by the members in a peer group can be different from that used by the group. That is, each peer can select its policy when importing routes.

----End

## 9.4.8 Configuring BGP4+ Soft Resetting

When routing policies are changed, the system can refresh the BGP4+ routing table dynamically without interrupting BGP4+ connections.

### Procedure

- Enabling the Route-refresh Capability

Do as follows on the BGP4+ router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
peer { ipv4-address | ipv6-address | group-name } capability-advertise
{ route-refresh | 4-byte-as }
```

The route-refresh capability is enabled.

By default, the route-refresh capability is enabled.

If the route-refresh capability is enabled on all the BGP4+ routers, the local router advertises the route-refresh messages to its peer if the BGP4+ route policies change. The peer receiving this message sends its routing information to the local router again. In this way, the BGP4+ routing table is updated dynamically and the new policies are applied without interrupting the BGP4+ connections.

- Keeping All Route Updates of Peers

Do as follows on the BGP4+ router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```



The BGP view is displayed.

3. Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

4. Run:

```
peer { ipv4-address | ipv6-address | group-name } keep-all-routes
```

All route updates of the peers are kept.

After this command is run, all the route updates of the specified peer are kept regardless of whether the filtering policies are used. When the BGP connections are soft reset, this information can be used to generate the BGP4+ routes.

- Soft Resetting a BGP4+ Connection Manually

Do as follows on the BGP4+ router:

1. Run:

```
refresh bgp ipv6 { all | ipv4-address | ipv6-address | group group-name |
external | internal } { export | import }
```

A BGP4+ connection is soft reset.

A BGP4+ connection must be soft reset in the user view.

----End

## 9.4.9 Checking the Configuration

After the advertising and receiving of BGP4+ routes are controlled, you can check the advertised routes that match the specified filter.

### Prerequisite

The configurations of controlling the advertising and receiving of BGP4+ routing information are complete.

### Procedure

- Run the **display bgp ipv6 network** command to check the routes advertised through the **network** command.
- Run the **display bgp ipv6 routing-table as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } command to check the routes matching the specified AS-Path filter.
- Run the **display bgp ipv6 routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [ **whole-match** ] | *advanced-community-filter-number* } command to check the routes matching the specified BGP4+ community filter.
- Run the **display bgp ipv6 routing-table peer** { *ipv4-address* | *ipv6-address* } { **advertised-routes** | **received-routes** } [ **statistics** ] command to check the routing information advertised or received by the BGP4+ peers.

----End

## 9.5 Configuring Parameters of a Connection Between BGP4+ Peers

By setting parameters of a connection between BGP4+ peers, you can adjust and optimize the BGP4+ network performance.

### 9.5.1 Establishing the Configuration Task

Before configuring parameters of a connection between BGP4+ peers, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

After a BGP4+ connection is set up between peers, the peers periodically send Keepalive messages to each other. This prevents the routers from considering that the BGP4+ connection is closed. If a router does not receive any Keepalive message or any type of packets from the peer within the specified Hold time, the BGP4+ connection is considered as closed.

When a router sets up a BGP4+ connection with its peer, the router and the peer need negotiation with each other. The Hold time after negotiation is the shorter one between the Hold time of the router and that of its peer. If the negotiation result is 0, no Keepalive message is transmitted and whether the Hold timer expires is not detected.

If the value of the timer changes, the BGP4+ connection is interrupted for a short time as the router and its peer need negotiate again.

A ConnectRetry timer is used to set the interval between BGP4+ attempts to initiate TCP connections. After BGP4+ initiates a TCP connection, the ConnectRetry timer is stopped if the TCP connection is established successfully. If the first attempt to establish a TCP connection fails, BGP4+ tries again to establish the TCP connection after the ConnectRetry timer expires.

You can speed up or slow down the establishment of BGP4+ peer relationships by changing the BGP4+ ConnectRetry interval. For example, if the ConnectRetry interval is reduced, BGP4+ will wait less time to retry establishing a TCP connection when an earlier attempt fails. This speeds up the establishment of the TCP connection. If a BGP4+ peer flaps constantly, the ConnectRetry interval can be increased to suppress route flapping caused by BGP4+ peer flapping. This speeds up route convergence.

#### Pre-configuration Tasks

Before configuring the parameters of a connection between BGP4+ peers, complete the following tasks:

- [Configuring Basic BGP4+ Functions](#)

#### Data Preparation

To configure the parameters of a connection between BGP4+ peers, you need the following data.

| No. | Data                                    |
|-----|-----------------------------------------|
| 1   | Values of the BGP4+ timers              |
| 2   | Interval for sending the update packets |
| 3   | BGP4+ ConnectRetry interval             |

## 9.5.2 Configuring BGP4+ Timers

Configuring timers properly can improve network performance. Changing the values of BGP4+ timers will interrupt the peer relationship.

### Context



#### CAUTION

As the change of the timer (with the **peer timer** command) tears down the BGP peer relationship between routers. So, confirm the action before you use the command.

Do as follows on the BGP4+ router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
peer { ipv6-address | group-name } timer keepalive keepalive-time hold hold-time
```

The interval for sending Keepalive messages and the Hold time of a peer (or peer group) are set.

In actual applications, the value of *hold-time* is at least three times that of *keepalive-time*.

By default, the Keepalive time is 60s and the Hold time is 180s.

#### NOTE

Setting the hold interval of a BGP peer to be longer than 20s is recommended. If the hold interval of a BGP peer is shorter than 20s, the session may be closed.

Note the following when you set the values of *keepalive-time* and *hold-time*:

- When the values of *keepalive-time* and *hold-time* are 0 at the same time, the BGP timer becomes invalid. That is, BGP does not detect link faults according to the timer.

- The value of *hold-time* is far greater than that of *keepalive-time*, such as, **timer keepalive 1 hold 65535**. If the Hold time is too long, the link fault cannot be detected on time.

----End

### 9.5.3 Configuring the Interval for Sending Update Packets

When a route changes, a router sends an Update packet to notify its peer. If a route changes frequently, to prevent the router from sending Update packets for every change, you can set the interval for sending Update packets for changes of this route.

#### Context

Do as follows on the BGP4+ router:

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 4** Run:

```
peer ipv6-address route-update-interval interval
```

The interval for sending update packets is set.

By default, the update interval is 15 seconds for the IBGP peers and the update interval is 30 seconds for the EBGp peers.

----End

### 9.5.4 Setting the BGP4+ ConnectRetry Interval

You can speed up or slow down the establishment of BGP4+ peer relationships to adapt the network changes by changing the BGP4+ ConnectRetry interval.

#### Context

When BGP4+ initiates a TCP connection, the ConnectRetry timer is stopped if the TCP connection is established successfully. If the first attempt to establish a TCP connection fails, BGP4+ tries again to establish the TCP connection after the ConnectRetry timer expires. The ConnectRetry interval can be adjusted as needed.

- The ConnectRetry interval can be reduced in order to lessen the time BGP4+ waits to retry establishing a TCP connection after the first attempt fails.

- To suppress route flapping caused by constant peer flapping, the ConnectRetry interval can be increased to speed up route convergence.

Do as follows on the BGP4+ router:

## Procedure

- Set a ConnectRetry interval globally.

Do as follows on the BGP4+ router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
timer connect-retry connect-retry-time
```

A BGP4+ ConnectRetry interval is set globally.

By default, the ConnectRetry interval is 32s.

- Set a ConnectRetry interval on a peer or peer group.

Do as follows on the BGP4+ router:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
peer { group-name | ipv6-address } timer connect-retry connect-retry-time
```

A ConnectRetry interval is set on a peer or peer group.

By default, the ConnectRetry interval is 32s.

The ConnectRetry interval configured on a peer or peer group takes precedence over a global ConnectRetry interval.

----End

## 9.5.5 Checking the Configuration

After parameters of a connection between BGP4+ peers are configured, you can check BGP4+ peers and peer groups.

## Prerequisite

The configurations of parameters of a connection between BGP4+ peers are complete.

## Procedure

- Run the **display bgp ipv6 peer *ipv4-address* verbose** command to check detailed information about the BGP4+ peers.
- Run the **display bgp ipv6 peer *ipv6-address* { log-info | verbose }** command to check information about the BGP4+ peers.

----End

## Example

Run the **display bgp ipv6 peer *ipv6-address* verbose** command in the system view. You can view the configured Keepalive period, holdtime, ConnectRetry interval, and interval at which Update packets are sent.

```
<RouterB> display bgp peer 9:1::1 verbose

 BGP Peer is 9:1::1, remote AS 100
 Type: IBGP link
 BGP version 4, Remote router ID 1.1.1.1
 Update-group ID: 1
 BGP current state: Established, Up for 00h01m05s
 BGP current event: KATimerExpired
 BGP last state: OpenConfirm
 BGP Peer Up count: 2
 Received total routes: 0
 Received active routes total: 0
 Advertised total routes: 0
 Port: Local - 49153 Remote - 179
 Configured: Connect-retry Time: 20 sec
 Configured: Active Hold Time: 150 sec Keepalive Time:40 sec
 Received : Active Hold Time: 180 sec
 Negotiated: Active Hold Time: 150 sec Keepalive Time:40 sec
 Peer optional capabilities:
 Peer supports bgp multi-protocol extension
 Peer supports bgp route refresh capability
 Peer supports bgp 4-byte-as capability
 Address family IPv6 Unicast: advertised and received
 Received: Total 3 messages
 Update messages 0
 Open messages 1
 KeepAlive messages 2
 Notification messages 0
 Refresh messages 0
 Sent: Total 4 messages
 Update messages 0
 Open messages 1
 KeepAlive messages 3
 Notification messages 0
 Refresh messages 0
 Authentication type configured: None
 Last keepalive received: 2010/11/17 16:11:42 UTC-08:00
 Minimum route advertisement interval is 20 seconds
 Optional capabilities:
 Route refresh capability has been enabled
 4-byte-as capability has been enabled
 Peer Preferred Value: 0
 Routing policy configured:
 No routing policy is configured
```

## 9.6 Configuring BFD for BGP4+

By configuring BFD for BGP4+, you can provide a fast fault detection mechanism for BGP4+, and thus speed up network convergence.

## 9.6.1 Establishing the Configuration Task

Before configuring BFD for BGP4+, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

### Applicable Environment

BFD can rapidly detect IPv6 forwarding failures. By adopting the BFD fast detection mechanism, an IPv6 network can transmit voice services, video services, and VoD services with high QoS. This enables service providers to provide their customers with highly available and reliable VoIP and other real-time services.

BGP periodically sends Keepalive messages to the peer to detect faults on the neighbor. This mechanism, however, takes more than one second to detect a fault. When the data rate is up to Gbit/s, the detection mechanism causes a great packet loss. This mechanism fails to meet the requirement on the reliability of core networks.

BGP introduces BFD for BGP4+. The fast detection mechanism of BFD can faster detect faults on the links between BGP peers. The convergence of networks thus speeds up.

### Pre-configuration Tasks

Before configuring BFD for BGP4+, complete the following tasks:

- Configuring link layer protocol parameters and assigning IP addresses to the interfaces to ensure that the status of the link layer protocol of the interface is Up
- [Configuring Basic BGP4+ Functions](#)

### Data Preparation

To configure BFD for BGP4+, you need the following data.

| No. | Data                                                                                                                                                           |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Type and number of the interface on which BFD is enabled                                                                                                       |
| 2   | Related BFD detection parameters, including the minimum interval and the maximum interval for receiving BFD control packets, and the detection time multiplier |

## 9.6.2 Configuring BFD for BGP4+ in the Public Network Instance

By configuring BFD for BGP4+, you can fast detect the BGP4+ route status. A BFD session can be established only when two BGP4+ peers are in the Established state.

### Context

Do as follows on BGP4+ routers at the two ends of a link on which a BFD session needs to be set up:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bfd
```

Global BFD is enabled on the node.

**Step 3** Run:

```
quit
```

Back to the system view.

**Step 4** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 5** (Optional) Run:

```
peer { group-name | ipv6-address } bfd { min-tx-interval min-tx-interval | min-rx-interval min-rx-interval | detect-multiplier multiplier } *
```

The parameters used to set up a BFD session are specified.

**Step 6** Run:

```
peer { group-name | ipv6-address } bfd enable
```

BFD is configured for a peer or a peer group and the BFD session is set up.

If BFD is configured on a peer group, peers that belong to the group set up BFD sessions when the **peer bfd block** command is not used on the peers.

 **NOTE**

- A BFD session is set up only when the BGP session is in the Established state.
- If BFD parameters of a peer are set, the BFD session is set up by using BFD parameters of the peer.

**Step 7** (Optional) Run:

```
peer ipv6-address bfd block
```

The peer is prevented from inheriting BFD of its group.

If a peer joins a group enabled with BFD, the peer inherits BFD of the group and creates a BFD session. If you do not want the peer to inherit BFD of the group, you can prevent the peer from inheriting BFD of its group.

 **NOTE**

The **peer bfd block** command is exclusive with the **peer bfd enable** command. After the **peer bfd block** command is used, the BFD session is automatically deleted.

----End

## 9.6.3 Configuring BFD for BGP4+ in a Private Network

On an IPv6 VPN network, configuring BFD for BGP4+ can fast detect the status of VPN BGP4+ routes. A BFD session can be established only when two BGP4+ peers are in the Established state.



## Context

Do as follows on the BGP routers at the both ends of the link that needs to set up a BFD session:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bfd
```

Global BFD is enabled on the node.

**Step 3** Run:

```
quit
```

Back to the system view.

**Step 4** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 5** Run:

```
ipv6-family vpn-instance vpn-instance-name
```

The BGP-VPN6 instance view is displayed.

**Step 6** (Optional) Run:

```
peer { group-name | ipv6-address } bfd { min-tx-interval min-tx-interval | min-rx-interval min-rx-interval | detect-multiplier multiplier } *
```

The parameters used to set up a BFD session are specified.

**Step 7** Run:

```
peer { group-name | ipv6-address } bfd enable
```

BFD is configured for a peer or a peer group and the BFD session is set up.

If BFD is configured on a peer group, peers that belong to the group set up BFD sessions when the **peer bfd block** command is not used on the peers.

### NOTE

- A BFD session is set up only when the BGP session is in the Established state.
- If BFD parameters of a peer are set, the BFD session is set up by using BFD parameters of the peer.

**Step 8** (Optional) Run:

```
peer ipv6-address bfd block
```

The peer is prevented from inheriting BFD of its group.

If a peer joins a group enabled with BFD, the peer inherits BFD of the group and creates a BFD session. If you do not want the peer to inherit BFD of the group, you can prevent the peer from inheriting BFD of its group.

 NOTE

The **peer ipv6-address bfd block** command is exclusive with the **peer { group-name | ipv6-address } bfd enable** command. After the **peer bfd block** command is used, the BFD session is automatically deleted.

----End

## 9.6.4 Checking the Configuration

After BFD for BGP4+ is configured, you can check the BFD sessions established by BGP4+.

### Prerequisite

The configurations of BFD for BGP4+ are complete.

### Procedure

- Run the **display bgp ipv6 bfd session** { [ **vpn6 vpn-instance vpn-instance-name** ] **peer ipv6-address | all** } command to check the BFD sessions established by BGP4+.
- Run the **display bgp** [ **vpn6 vpn-instance vpn-instance-name** ] **peer** [ [ **ipv6-address** ] **verbose** ] command to check BGP4+ peers.
- Run the **display bgp ipv6 group** [ **group-name** ] command to check BGP peer groups.
- Run the **display bgp vpn6** { **all | vpn-instance vpn-instance-name** } **group** [ **group-name** ] command to check BGP4+ peer groups.

----End

## 9.7 Configuring BGP4+ Tracking

On a network where BFD is unsuitable to deploy, you can configure BGP4+ tracking to implement the fast convergence of IBGP routes.

### 9.7.1 Establishing the Configuration Task

Before configuring BGP4+ tracking, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

Since BFD is difficult to deploy and is of poor scalability, in a network where BFD is unsuitable to be deployed, you can configure BGP4+ tracking as a substitution for BFD to implement the fast convergence of BGP4+ routes.

BGP4+ tracking is easy to deploy because it needs to be configured only on the local device, without the need of configuring it on the peer device. However, BGP4+ route convergence in a network configured with BGP4+ tracking is slower than that in a network enabled with BFD; therefore, BGP4+ tracking cannot meet the requirement of voice services that demand high convergence speed.

#### Pre-configuration Tasks

Before configuring BGP4+ tracking, complete the following tasks:

- **Configuring basic BGP4+ functions**

## Data Preparation

To configure BGP4+ tracking, you need the following data.

| No. | Data                                           |
|-----|------------------------------------------------|
| 1   | (Optional) Delay for tearing down a connection |

## 9.7.2 Enabling BGP4+ Tracking

Easy to deploy, BGP4+ tracking can speed up network convergence and adjust the interval between a peer's being discovered unreachable and the connection's being torn down.

### Context

Do as follows on the router enabled with BGP4+:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
peer { group-name | ipv6-address } tracking [delay delay-time]
```

BGP4+ tracking is enabled for the specified peer.

By default, BGP4+ tracking is disabled.

A proper value of *delay-time* can ensure network stability when a peer is detected unreachable.

- If *delay-time* is set to 0, BGP immediately tears down the connection between the local device and its peer after the peer is detected unreachable.
- If IGP route flapping occurs and *delay-time* for an IBGP peer is set to 0, the peer relationship between the local device and the peer alternates between Up and Down. Therefore, *delay-time* for an IBGP peer should be set to a value greater than the actual IGP route convergence time.
- When BGP neighbors successfully perform the GR negotiation, the active/standby switchover occurs on the BGP neighbors, to prevent the failure of GR, *delay-time* should be set to a value greater than GR period. If *delay-time* is set to be smaller than the GR period, the connection between the local device and the BGP peer will be torn down, which leads to the failure of GR.

----End

## 9.7.3 Checking the Configuration

After BGP4+ tracking is configured, you can check the configuration of BGP4+ tracking by viewing detailed information about the BGP peer or peer group.

### Prerequisite

All BGP4+ tracking configurations are complete.

### Checking the Configuration

Run the following commands to check the previous configuration.

- Run the **display bgp ipv6 peer** [ *ipv4-address* ] [ **verbose** ] command to check information about the BGP4+ peer.
- Run the **display bgp ipv6 group** [ *group-name* ] command to check information about the BGP4+ peer group.

## 9.8 Configuring BGP4+ Route Dampening

By configuring BGP4+ route dampening, you can suppress unstable BGP4+ routes.

### 9.8.1 Establishing the Configuration Task

Before configuring BGP4+ route dampening, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

### Applicable Environment

BGP4+ dampening can suppress unstable routes. BGP4+ neither adds the unstable routes to the routing table nor advertises them to other BGP peers.

### Pre-configuration Tasks

Before configuring BGP4+ route dampening, complete the following task:

- **Configuring Basic BGP4+ Functions**

### Data Preparation

To configure BGP4+ route dampening, you need the following data.

| No. | Data                                                                                                                                                                                                                        |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Various parameters of dampening, including half-life of a reachable route, half-life of an unreachable route, threshold for freeing the suppressed routes, threshold for suppressing routes, and upper limit of the penalty |

## 9.8.2 Configuring BGP4+ Route Dampening

BGP4+ route dampening can improve network stability. You can flexibly use routing policies for route dampening.

### Context

Do as follows on the BGP4+ router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 4** Run:

```
dampening [half-life-reach reuse suppress ceiling | route-policy route-policy-name] *
```

The parameters are configured for BGP4+ route dampening.

----End

## 9.8.3 Checking the Configuration

After BGP4+ route dampening is configured, you can check BGP4+ suppressed routes, parameters of BGP4+ route dampening, and flapped routes.

### Prerequisite

The configurations of BGP4+ route dampening are complete.

### Procedure

- Run the **display bgp ipv6 routing-table dampened** command to check BGP4+ dampened routes.
- Run the **display bgp ipv6 routing-table dampening parameter** command to check the configuration parameters of BGP4+ dampening.
- Run the **display bgp ipv6 routing-table flap-info [ regular-expression as-regular-expression | as-path-filter { as-path-filter-number | as-path-filter-name } | network-address [ prefix-length [ longer-match ] ] ]** command to check the statistics of BGP4+ route flapping.

----End

## 9.9 Configuring BGP4+ Load Balancing

By configuring BGP4+ load balancing, you can properly use network resources.

### 9.9.1 Establishing the Configuration Task

Before configuring BGP4+ load balancing, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

Load balancing can be performed among equal-cost BGP4+ routes whose first eight attributes described in "Principles of Route Selection" of [8.1.2 BGP Features Supported by the NE80E/40E](#) are the same and AS\_Path attributes are the same.

#### Pre-configuration Tasks

Before configuring BGP4+ load balancing, complete the following task:

- [Configuring Basic BGP4+ Functions](#)

#### Data Preparation

To configure BGP4+ load balancing, you need the following data.

| No. | Data                                    |
|-----|-----------------------------------------|
| 1   | The number of routes for load balancing |

### 9.9.2 Setting the Number of Routes for BGP4+ Load Balancing

Load balancing can be implemented among multiple equal-cost links between BGP4+ peers.

#### Context

Do as follows on the BGP4+ router:

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 4** Run:

```
maximum load-balancing [ebgp | ibgp] number
```

The maximum number of equal-cost routes for BGP4+ load balancing is set.

By default, the number of equal-cost routes for BGP4+ load balancing is 1.

----End

## 9.9.3 Checking the Configuration

After BGP4+ load balancing is configured, you can check information about load balancing.

### Prerequisite

The configurations of BGP4+ load balancing are complete.

### Procedure

- Run the **display bgp ipv6 routing-table** [ *ipv6-address prefix-length* ] command to check information about the BGP4+ routing table.
- Run the **display ipv6 routing-table** [ *verbose* ] command to check information about the IPv6 routing table.

----End

## 9.10 Configuring a BGP4+ Peer Group

By configuring a BGP4+ peer group, you can simplify the management of routing policies, and thus improve the efficiency of route advertisement.

### 9.10.1 Establishing the Configuration Task

Before configuring a BGP4+ peer group, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

### Applicable Environment

A great number of peers exist in a large-scale BGP4+ network, which is not convenient for configuration and maintenance. In this case, you can configure peer groups to simplify the management and improve the efficiency of route advertisement. According to the AS where the peers reside, you can classify peer groups into IBGP peer groups and EBGP peer groups. You can classify EBGP peer groups into pure EBGP peer groups and mixed EBGP peer groups. This classification is performed according to the position of the peers in the same external AS.

### Pre-configuration Tasks

Before configuring a BGP4+ peer group, complete the following task:

- **Configuring Basic BGP4+ Functions**

## Data Preparation

To configure a BGP4+ peer group, you need the following data.

| No. | Data                                               |
|-----|----------------------------------------------------|
| 1   | Type, name of the peer group, and the member peers |

## 9.10.2 Creating an IBGP Peer Group

When BGP4+ has multiple IBGP peers, you can create an IBGP peer group to simplify the management of routing policies. When creating an IBGP peer group, you do not need to specify the AS number.

### Context

Do as follows on the BGP4+ router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
group group-name [internal]
```

A peer group is created.

**Step 4** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 5** Run:

```
peer group-name enable
```

The peer group is enabled.

**Step 6** Run:

```
peer { ipv4-address | ipv6-address } group group-name
```

The IPv6 peers are added to the peer group.



 **NOTE**

After an IBGP peer is added to a peer group, the system automatically creates the IPv6 peer in the BGP view. Besides, the system enables this IBGP peer in the IPv6 address family view.

----End

## 9.10.3 Creating a Pure EBGP Peer Group

When BGP4+ has multiple EBGP peers that belong to the same AS, you can create an EBGP peer group to simplify the management of routing policies. All the peers in a pure EBGP peer group must have the same AS number.

### Context

Do as follows on the BGP4+ router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
group group-name external
```

A pure EBGP peer group is configured.

**Step 4** Run:

```
peer group-name as-number as-number
```

The AS number of the peer group is set.

**Step 5** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 6** Run:

```
peer group-name enable
```

The peer group is enabled.

**Step 7** Run:

```
peer ipv6-address group group-name
```

The IPv6 peer is added to the peer group.

After an EBGP peer is added to the peer group, the system automatically creates the EBGP peer in the BGP view. Besides, the system enables this EBGP peer in the IPv6 address family view.

When creating a pure EBGP peer group, you need to specify the AS number of the peer group.

If there are peers in the peer group, you cannot specify the AS number for this peer group.

----End

## 9.10.4 Creating a Mixed EBGP Peer Group

When BGP4+ has multiple EBGP peers that belong to different ASs, you can create a mixed EBGP peer group to simplify the management of routing policies. When creating a mixed EBGP peer group, you need to specify the AS number for each peer.

### Context

Do as follows on the BGP4+ router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
group group-name external
```

A mixed EBGP peer group is created.

**Step 4** Run:

```
peer ipv6-address as-number as-number
```

The AS number of the IPv6 peer is set.

**Step 5** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 6** Run:

```
peer group-name enable
```

The peer group is enabled.

**Step 7** Run:

```
peer ipv6-address group group-name
```

The IPv6 peers created are added to this peer group.

After an EBGP peer is added to the peer group, the system automatically enables each EBGP peer in the IPv6 address family view.

When creating a mixed EBGP peer group, you need to create peers separately, and you can configure different AS numbers for them, but cannot configure the AS number for the peer group.

----End

## 9.10.5 Checking the Configuration

After a BGP4+ peer group is configured, you can check detailed information about the BGP4+ peer and information about the BGP4+ peer group.

### Prerequisite

The configurations of a BGP4+ peer group are complete.

### Procedure

- Run the **display bgp ipv6 group** [ *group-name* ] command to check information about the IPv6 peer group.

---End

## 9.11 Configuring a BGP4+ Route Reflector

By configuring a BGP4+ route reflector, you can solve the problem of establishing fully meshed connections between multiple IBGP peers.

### 9.11.1 Establishing the Configuration Task

Before configuring a BGP4+ route reflector, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

### Applicable Environment

To ensure the connectivity between IBGP peers inside an AS, you need to establish full-meshed IBGP peers. When there are many IBGP peers, establishing a full-meshed network costs a lot. The route reflector or the confederation can be used to solve this problem.

### Pre-configuration Tasks

Before configuring a BGP4+ route reflector, complete the following task:

- [9.2 Configuring Basic BGP4+ Functions](#)

### Data Preparation

To configure a BGP4+ route reflector, you need the following data.

| No. | Data                                                     |
|-----|----------------------------------------------------------|
| 1   | Roles of each router (reflector, client, and non-client) |

### 9.11.2 Configuring a Route Reflector and Specifying Clients

A route reflector and clients need to be configured in a specified address family.

## Context

Do as follows on the BGP4+ router:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family [unicast]
```

The BGP IPv6 unicast address family view is displayed.

**Step 4** Run:

```
peer { ipv4-address | ipv6-address | group-name } reflect-client
```

The route reflector and its clients are configured.

The router on which this command is run serves as the route reflector. In addition, this command specifies the peers that serve as its clients.

---End

### 9.11.3 (Optional) Disabling a Route Reflection Between Clients

If the clients of a route reflector are fully meshed, you can disable route reflection between clients to reduce the cost.

## Context

Do as follows on the BGP4+ router:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 4** Run:

```
undo reflect between-clients
```

Route reflection between clients is disabled.

If the clients of the route reflector are full-meshed, you can use the **undo reflect between-clients** command to disable the route reflection between the clients. This reduces cost.

By default, the route reflection between clients is enabled.

This command is used only on the reflector.

---End

## 9.11.4 (Optional) Configuring the Cluster ID for a Route Reflector

When there are multiple route reflectors in a cluster, you need to configure the same cluster ID for all the route reflectors in this cluster to avoid routing loops.

### Context

Do as follows on the BGP4+ router:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 4** Run:

```
reflector cluster-id cluster-id
```

The cluster ID of the route reflector is set.

 **TIP**

When there are multiple route reflectors in a cluster, you can use the command to configure all the route reflectors in this cluster with the same cluster ID. This avoids routing loops.

---End

## 9.11.5 Checking the Configuration

After a BGP4+ route reflector is configured, you can check BGP4+ route information and peer group information.

### Prerequisite

The configurations of a BGP4+ route reflector are complete.

## Procedure

- Run the **display bgp ipv6 peer [ verbose ]** command to check information about BGP4+ peers.
- Run the **display bgp ipv6 peer ipv4-address verbose** command to check information about BGP4+ peers.
- Run the **display bgp ipv6 peer ipv6-address { log-info | verbose }** command to check information about BGP4+ peers.

----End

## 9.12 Configuring a BGP4+ Confederation

On a large-scale BGP4+ network, configuring a BGP4+ confederation can simplify the management of routing policies and improve the efficiency of route advertisement.

### 9.12.1 Establishing the Configuration Task

Before configuring a BGP4+ confederation, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

The confederation is a method of handling the abrupt increase of IBGP connections in an AS. The confederation divides an AS into multiple sub-ASs. In each sub-AS, IBGP peers can be full-meshed or be configured with a route reflector. EBGP connections are set up between sub-ASs.

#### Pre-configuration Tasks

Before configuring a BGP4+ confederation, complete the following task:

- **Configuring Basic BGP4+ Functions**

#### Data Preparation

To configure a BGP4+ confederation, you need the following data.

| No. | Data                                   |
|-----|----------------------------------------|
| 1   | Confederation ID and the sub-AS number |

### 9.12.2 Configuring a BGP Confederation

BGP4+ confederations deal with increasing IBGP connections in an AS.

#### Procedure

- Configuring a BGP Confederation

Do as follows on the BGP4+ router:

1. Run:  
`system-view`  
The system view is displayed.

2. Run:  
`bgp as-number`  
The BGP view is displayed.

3. Run:  
`confederation id as-number`  
The confederation ID is set.

4. Run:  
`confederation peer-as as-number <1-32>`  
The sub-AS number of other EBGP peers connected with the local AS is set.

A confederation includes up to 32 sub-ASs. *as-number* is valid for the confederation that it belongs to.

You must run the `confederation id` and `confederation peer-as` commands for all the EBGP peers that belong to a confederation, and specify the same confederation ID for them.

 **NOTE**

The old speaker with 2-byte AS numbers and the new speaker with 4-byte AS numbers cannot exist in the same confederation. Otherwise, routing loops may occur because AS4\_Path does not support confederations.

● **Configuring the Compatibility of a Confederation**

Do as follows on the BGP4+ router:

1. Run:  
`system-view`  
The system view is displayed.

2. Run:  
`bgp as-number`  
The BGP view is displayed.

3. Run:  
`confederation nonstandard`  
The compatibility of the confederation is configured.

When the confederation of other routers does not conform to the RFC, you can use this command to make standard devices be compatible with nonstandard devices.

---End

## 9.12.3 Checking the Configuration

After a BGP4+ confederation is configured, you can check BGP4+ route information and detailed peer information.

### Prerequisite

The configurations of a BGP4+ confederation are complete.

## Procedure

- Run the **display bgp ipv6 peer [ verbose ]** command to check detailed information about BGP4+ peers.

----End

## 9.13 Configuring BGP4+ 6PE

By configuring BGP4+ 6PE, you can connect separated IPv6 networks through the MPLS tunneling technology.

### 9.13.1 Establishing the Configuration Task

Before configuring BGP4+ 6PE, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

6PE interconnects separated IPv6 networks at different locations by using the MPLS technology in an IPv4 network. Multiple modes are used to connect separated IPv6 networks by using the tunnel technology. The tunnel in 6PE mode supports the IPv4/IPv6 dual stacks on PEs of the ISP. It identifies IPv6 routes by using the label assigned by MP-BGP, and implements IPv6 interworking through LSPs between PEs.

#### Pre-configuration Tasks

Before configuring BGP4+ 6PE, complete the following task:

- Establishing LSPs between PEs

#### Data Preparation

To configure BGP4+ 6PE, you need the following data.

| No. | Data                             |
|-----|----------------------------------|
| 1   | IP address and AS number of a PE |

### 9.13.2 Configuring a 6PE Peer

6PE interconnects separated IPv6 networks at different locations by using the MPLS tunneling technology in an existing IPv4 network.

#### Context

Do as follows on the PE supporting the IPv4/IPv6 dual stacks:



## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
peer ipv4-address as-number as-number
```

The IP address and AS number of a PE that needs to be configured with 6PE are specified.

**Step 4** Run:

```
ipv6-family unicast
```

The BGP IPv6 unicast address family view is displayed.

**Step 5** Run:

```
peer ipv4-address enable
```

A 6PE peer is configured in the IPv6 unicast address family view.

**Step 6** Run:

```
peer ipv4-address label-route-capability
```

The capability of sending labeled routes is enabled.

----End

### 9.13.3 (Optional) Enabling 6PE Routes Sharing the Explicit Null Label

By enabling 6PE routes sharing the explicit null label, you can save label resources on 6PE routers.

#### Context

By default, the 6PE router applies for a label for each 6PE route. When a large number of 6PE routes need to be sent, a large number of labels are required. This greatly wastes label resources and causes IPv6 routes unable to be advertised due to the shortage of label resources.

After 6PE routes sharing the explicit null label is enabled, all 6PE routes to be sent to the same 6PE peer share the explicit null label 2.

Do as follows on the 6PE router:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family unicast
```

The BGP-IPv6 unicast address family view is displayed.

**Step 4** Run:

```
apply-label explicit-null
```

All 6PE routes to be sent to the same 6PE peer share the explicit null label.

If you run this command after a 6PE peer relationship is established, temporary packet loss occurs.

---End

## 9.13.4 Checking the Configuration

After BGP4+ 6PE is configured, you can check BGP4+ peer information.

### Prerequisite

The configurations of BGP4+ 6PE are complete.

### Procedure

- Run the **display bgp ipv6 peer [ verbose ]** command to check detailed information about BGP4+ peers.

---End

## 9.14 Configuring BGP4+ 6PE FRR

After you configure 6PE FRR on a router, the router can select a backup next hop for received 6PE routes. When the next hop of the primary route between PEs becomes unreachable, traffic will be quickly switched to the backup next hop.

### 9.14.1 Establishing the Configuration Task

Before configuring BGP4+ 6PE FRR, familiarize yourself with the applicable environment, pre-configuration tasks, and required data. This can help you complete the configuration task quickly and accurately.

### Applicable Environment

6PE services are sensitive to the packet loss and delay. If high requirements are imposed on the reliability of the IPv4/MPLS network that carries the 6PE services, you can enable 6PE FRR on 6PE routers.

Enabled with 6PE FRR, a 6PE router selects an optimal route and a sub-optimal route among the routes with the same IP prefix from different 6PE peers. The optimal route serves as the

primary route, and the sub-optimal route serves as the backup route. When traffic forwarding on the primary route fails, 6PE services can be quickly redirected to the backup next hop.

## Pre-configuration Tasks

Before configuring 6PE FRR, complete the following tasks:

- Configuring a routing protocol on 6PE routers to enable the connectivity between devices on the IPv4/MPLS network
- Configuring different IGP metrics on the IPv4/MPLS network to ensure that two routes of different costs are generated between 6PE routers

## Data Preparation

To configure 6PE FRR, you need the following data.

| No. | Data                                                                   |
|-----|------------------------------------------------------------------------|
| 1   | IP address of each 6PE router and the number of AS to which it belongs |

### 9.14.2 Configuring BGP 6PE Peers

You need to configure BGP 6PE peers to transmit 6PE routes on the IPv4/MPLS network.

#### Context

For details, see [Configuring BGP4+ 6PE](#).

### 9.14.3 Enabling 6PE FRR

After 6PE FRR is enabled, the system automatically selects the backup next hop for 6PE routes. So, When the next hop of the primary route between PEs becomes unreachable, the traffic can be quickly redirected to the backup next hop.

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv6-family unicast
```

The BGP-IPv6 unicast address family view is displayed.

**Step 4** Run:

```
auto-frr
```

The 6PE FRR function is enabled.

The function of the **auto-frr** command varies with the command configuration view. At present, the **auto-frr** command configured in the BGP-IPv6 unicast address family view is valid only for 6PE FRR.

----End

## 9.14.4 Checking the Configuration

After 6PE FRR is configured, you can view information about the backup next hop and backup label of the 6PE routes on 6PE routers.

### Prerequisite

The configurations of 6PE FRR are complete.

### Procedure

- Run the **display ipv6 routing-table** *ipv6-address* [*prefix-length*] [**longer-match**] **verbose** command to check the backup next hop, backup tunnel, and backup label in the routing table.

----End

### Example

Run the **display ipv6 routing-table** *ipv6-address* [*prefix-length*] [**longer-match**] **verbose** command on the 6PE routers enabled with 6PE FRR to check the backup next hop, backup tunnel, and backup label of 6PE routes in the routing table.

```
<HUAWEI> display ipv6 routing-table 2003::1 verbose
Routing Table :
Summary Count : 1

Destination : 2003::1 PrefixLength : 128
NextHop : ::FFFF:2.2.2.2 Preference : 255
Neighbour : ::2.2.2.2 ProcessID : 0
Label : 1033 Protocol : IBGP
State : Active Adv Relied Cost : 0
Entry ID : 3 EntryFlags : 0x80024900
Reference Cnt: 2 Tag : 0
Priority : medium Age : 173sec
IndirectID : 0x4
RelayNextHop : :: TunnelID : 0x9
Interface : Pos2/0/0 Flags : RD
BkNextHop : ::FFFF:3.3.3.3 BkInterface :
BkLabel : 1029 BkTunnelID : 0x0
BkPETunnelID : 0xd BkIndirectID : 0x3
```

## 9.15 Configuring BGP4+ Security

To improve BGP4+ security, you can perform TCP connection authentication.

### 9.15.1 Establishing the Configuration Task

Before configuring BGP4+ network security, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

## Applicable Environment

- BGP4+ authentication

BGP4+ uses TCP as the transport layer protocol. To enhance BGP4+ security, you can perform the Message Digest 5 (MD5) authentication when TCP connections are created. The MD5 authentication, however, does not authenticate BGP4+ packets. Instead, it sets MD5 authentication passwords for TCP connections, and the authentication is then completed by TCP. If the authentication fails, TCP connections cannot be established.

- BGP4+ GTSM

The Generalized TTL Security Mechanism (GTSM) is used to prevent attacks by using the TTL detection. If an attack simulates BGP4+ packets and sends a large number of packets to a router, an interface through which the router receives the packets directly sends the packets to BGP4+ of the control layer, without checking the validity of the packets. In this manner, routers on the control layer process the packets as valid packets. As a result, the system becomes busy, and CPU usage is high.

In this case, you can configure GTSM to solve the preceding problem. After GTSM is configured on a router, the router checks whether the TTL value in the IP header of a packet is in the pre-defined range after receiving the packet. If yes, the router forwards the packet; if not, the router discards the packet. This enhances the security of the system.

### NOTE

- The NE80E/40E supports BGP4+ GTSM.
- GTSM supports only unicast addresses; therefore, GTSM needs to be configured on all the routers configured with routing protocols.

## Pre-configuration Tasks

Before configuring BGP4+ security, complete the following task:

- [Configuring Basic BGP4+ Functions](#)

## Data Preparation

Before configure BGP4+ security, you need the following data.

| No. | Data                                                        |
|-----|-------------------------------------------------------------|
| 1   | BGP4+ peer address or name of the peer group of each router |
| 2   | MD5 authentication password                                 |
| 3   | Key-Chain authentication name                               |

### 9.15.2 Configuring MD5 Authentication

In MD5 authentication of BGP4+, you only need to set MD5 authentication passwords for TCP connections, and the authentication is performed by TCP. If the authentication fails, TCP connections cannot be established.

## Context

Do as follows on the BGP4+ router:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
peer { ipv6-address | group-name } password { cipher cipher-password | simple
simple-password }
```

The MD5 authentication password is configured.

### NOTE

When this command is used in the BGP4+ view, the extensions on VPNv6 of MP-BGP are also valid because they use the same TCP connection.

Characters ^#^# and \$@\$@ are used to identify passwords with variable lengths. Characters ^#^# are the prefix and suffix of a new password, and characters \$@\$@ are the prefix and suffix of an old password. Neither of them can be both configured at the beginning and end of a plain text password.

The BGP MD5 authentication and BGP Keychain authentication are mutually exclusive.

----End

## 9.15.3 Configuring Keychain Authentication

You need to configure Keychain authentication on both BGP4+ peers, and ensure that encryption algorithms and passwords configured for Keychain authentication on both peers are the same. Otherwise, TCP connections cannot be established between BGP4+ peers, and BGP4+ messages cannot be exchanged.

### Context

Do as follows on the BGP4+ router:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
peer { ipv6-address | group-name } keychain keychain-name
```

The Keychain authentication is configured.

You must configure Keychain authentication on both BGP peers. Note that encryption algorithms and passwords configured for the Keychain authentication on both peers must be the

same; otherwise, the TCP connection cannot be set up between BGP peers and BGP messages cannot be transmitted.

Before configuring the BGP Keychain authentication, configure a Keychain in accordance with the configured *keychain-name*. Otherwise, the TCP connection cannot be set up.

 **NOTE**

- When this command is used in the BGP view, the extensions on VPNv6 of MP-BGP are also valid because they use the same TCP connection.
- The BGP MD5 authentication and BGP Keychain authentication are mutually exclusive.

----End

## 9.15.4 Configuring Basic BGP4+ GTSM Functions

The GTSM mechanism protects a router by checking whether the TTL value in the IP header is in a pre-defined range.

### Procedure

- Configuring Basic BGP4+ GTSM Functions

Do as follows on the two peers:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run

```
peer { group-name | ipv6-address } valid-ttl-hops [hops]
```

Basic BGP4+ GTSM functions are configured.

The range of TTL values of packets is [ 255-hops+1, 255 ]. By default, the value of *hops* is 255. That is, the valid TTL range is [ 1, 255 ]. For example, for the direct EBGP route, the value of *hops* is 1. That is, the valid TTL value is 255.

 **NOTE**

- The configuration in the BGP view is also valid for the VPNv6 extension of MP-BGP. This is because they use the same TCP connection.
- GSTM is exclusive with EBGP-MAX-HOP; therefore, you can enable only one of them on the same peer or the peer group.

After the BGP4+ GTSM policy is configured, an interface board checks the TTL values of all BGP4+ packets. According to the actual networking requirements, you can configure GTSM to discard or process the packets that do not match the GTSM policy. If you configure GTSM to discard the packets that do not match the GTSM policy by default, you can configure the range of finite TTL values according to the network topology; therefore, the interface board directly discards the packets with the TTL value not in the configured range. Thus, the attackers cannot simulate valid BGP4+ packets to occupy CPU resources.

- Performing the Default GTSM Action

Do as follows on the router configured with GTSM:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
gtsm default-action { drop | pass }
```

The default action is configured for the packets that do not match the GTSM policy.

By default, the packets that do not match the GTSM policy can pass the filtering.

 **NOTE**

If only the default action is configured and the GTSM policy is not configured, GTSM does not take effect.

---End

## 9.15.5 Checking the Configuration

After BGP4+ network security is configured, you can check authentication information of BGP4+ peers.

### Prerequisite

The configurations of BGP4+ security are complete.

### Procedure

- Run the **display gtsm statistics** { *slot-id* | **all** } command to check the statistics of GTSM.

Run the **display gtsm statistics** command. You can view GTSM statistics on each board, including the total number of BGP4+ packets, the total number of OSPF packets, the number of packets that match the GTSM policy, and the number of discarded packets.

- Run the **display bgp ipv6 peer** *ipv6-address* **verbose** command to check information about BGP4+ GTSM.
- Run the **display bgp group** [ *group-name* ] command to check GTSM of a BGP4+ peer group.

---End

## 9.16 Maintaining BGP4+

Maintaining BGP4+ involves resetting a BGP4+ connection and clearing BGP4+ statistics.

### 9.16.1 Resetting BGP4+ Connections

This section describes how to clear the statistics of BGP4+ accounting, flapped routes, and suppressed routes.



## Context



### CAUTION

The peer relationship is broken after you reset the BGP4+ connections with the **reset bgp ipv6** command. So, confirm the action before you use the command.

---

After the BGP4+ configuration changes, reset the BGP4+ connections to validate the modification.

To reset the BGP4+ connections, run the following **reset** command in the user view.

## Procedure

- To validate the new configuration, run the **reset bgp ipv6 all** command in the user view to reset all the BGP4+ connections.
- To validate the new configuration, run the **reset bgp ipv6 as-number** command in the user view to reset the BGP+4 connections between the peers in a specified AS.
- To validate the new configuration, run the **reset bgp ipv6 { ipv4-address | ipv6-address | group group-name }** command in the user view to reset the BGP+4 connections with the specified peer (or peer group).
- To validate the new configuration, run the **reset bgp ipv6 external** command in the user view to reset the external BGP4+ connections.
- To validate the new configuration, run the **reset bgp ipv6 internal** command in the user view to reset the internal BGP4+ connections.

---End

## 9.16.2 Clearing BGP4+ Statistics

Devices can generate debugging information after the debugging of a module is enabled in the user view. Debugging information shows the contents of the packets sent or received by the debugged module.

## Context



### CAUTION

The BGP4+ statistics cannot be restored after you clear it. So, confirm the action before you use the command.

---

## Procedure

- Run the **reset bgp ipv6 dampening [ ipv6-address prefix-length ]** command in the user view to clear information about route dampening and release the suppressed routes.

- Run the **reset bgp ipv6 flap-info** [ *ipv6-address prefix-length* | **regexp** *as-path-regexp* | **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } ] command in the user view to clear the statistics of route flapping.

---End

## 9.17 Configuration Examples

BGP4+ configuration examples explain networking requirements, networking diagram, configuration notes, configuration roadmap, and configuration procedure.

### NOTE

This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.

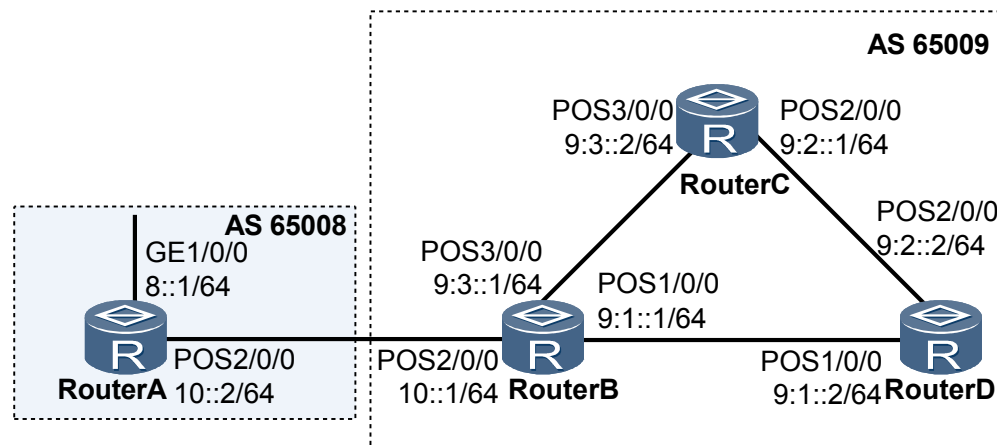
### 9.17.1 Example for Configuring Basic BGP4+ Functions

Before building BGP4+ networks, you need to configure basic BGP4+ functions.

#### Networking Requirement

As shown in **Figure 9-1**, there are two ASs: 65008 and 65009. Router A belongs to AS 65008; Router B, Router C, and Router D belong to AS65009. BGP4+ is required to exchange the routing information between the two ASs.

**Figure 9-1** Networking diagram of configuring basic BGP4+ functions



#### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the IBGP connections among Router B, Router C, and Router D.
2. Configure the EBGP connection between Router A and Router B.

#### Data Preparation

To complete the configuration, you need the following data:

- The router ID of Router A is 1.1.1.1. Its AS number is 65008.
- The router IDs of Router B, Router C, and Router D are 2.2.2.2, 3.3.3.3, and 4.4.4.4 respectively. Their AS number is 65009.

## Procedure

**Step 1** Assign an IPv6 address for each interface.

The details are not mentioned here.

**Step 2** Configure the IBGP.

# Configure Router B.

```
[RouterB] ipv6
[RouterB] bgp 65009
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 9:1::2 as-number 65009
[RouterB-bgp] peer 9:3::2 as-number 65009
[RouterB-bgp] ipv6-family unicast
[RouterB-bgp-af-ipv6] peer 9:1::2 enable
[RouterB-bgp-af-ipv6] peer 9:3::2 enable
[RouterB-bgp-af-ipv6] network 9:1:: 64
[RouterB-bgp-af-ipv6] network 9:3:: 64
```

# Configure Router C.

```
[RouterC] ipv6
[RouterC] bgp 65009
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 9:3::1 as-number 65009
[RouterC-bgp] peer 9:2::2 as-number 65009
[RouterC-bgp] ipv6-family unicast
[RouterC-bgp-af-ipv6] peer 9:3::1 enable
[RouterC-bgp-af-ipv6] peer 9:2::2 enable
[RouterC-bgp-af-ipv6] network 9:3:: 64
[RouterC-bgp-af-ipv6] network 9:2:: 64
```

# Configure Router D.

```
[RouterD] ipv6
[RouterD] bgp 65009
[RouterD-bgp] router-id 4.4.4.4
[RouterD-bgp] peer 9:1::1 as-number 65009
[RouterD-bgp] peer 9:2::1 as-number 65009
[RouterD-bgp] ipv6-family unicast
[RouterD-bgp-af-ipv6] peer 9:1::1 enable
[RouterD-bgp-af-ipv6] peer 9:2::1 enable
[RouterD-bgp-af-ipv6] network 9:2:: 64
[RouterD-bgp-af-ipv6] network 9:1:: 64
```

**Step 3** Configure the EBGP.

# Configure Router A.

```
[RouterA] ipv6
[RouterA] bgp 65008
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 10::1 as-number 65009
[RouterA-bgp] ipv6-family unicast
[RouterA-bgp-af-ipv6] peer 10::1 enable
[RouterA-bgp-af-ipv6] network 10:: 64
[RouterA-bgp-af-ipv6] network 8:: 64
```

# Configure Router B.

```
[RouterB] bgp 65009
```

```
[RouterB-bgp] peer 10::2 as-number 65008
[RouterB-bgp] ipv6-family unicast
[RouterB-bgp-af-ipv6] peer 10::2 enable
[RouterB-bgp-af-ipv6] network 10:: 64
```

# Check the connection status of BGP4+ peers.

```
[RouterB] display bgp ipv6 peer
BGP local router ID : 2.2.2.2
Local AS number : 65009
Total number of peers : 3 Peers in established state : 3
Peer V AS MsgRcvd MsgSent OutQ Up/Down State PrefRcv
9:1::2 4 65009 8 9 0 00:05:37 Established 2
9:3::2 4 65009 2 2 0 00:00:09 Established 2
10::2 4 65008 9 7 0 00:05:38 Established 2
```

The routing table shows that Router B has set up BGP4+ connections with other routers.

# Display the routing table of Router A.

```
[RouterA] display bgp ipv6 routing-table
BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete
Total Number of Routes: 6
*> Network : 8::: PrefixLen : 64
 NextHop : ::: LocPrf :
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : i
*> Network : 9:1::: PrefixLen : 64
 NextHop : 10::1 LocPrf :
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : 65009 i
*> Network : 9:2::: PrefixLen : 64
 NextHop : 10::1 LocPrf :
 MED : PrefVal : 0
 Label :
 Path/Ogn : 65009 i
*> Network : 9:3::: PrefixLen : 64
 NextHop : 10::1 LocPrf :
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : 65009 i
*> Network : 10::: PrefixLen : 64
 NextHop : ::: LocPrf :
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : i
*
 NextHop : 10::1 LocPrf :
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : 65009 i
```

The routing table shows that Router A has learned the route from AS 65009. AS 65008 and AS 65009 can exchange their routing information.

----End

## Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
```

```
 ipv6
 #
 interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 8::1/64
 #
 interface Pos2/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 10::2/64
 #
 bgp 65008
 router-id 1.1.1.1
 peer 10::1 as-number 65009
 #
 ipv4-family unicast
 undo synchronization
 #
 ipv6-family unicast
 network 8:: 64
 network 10:: 64
 peer 10::1 enable
 #
 return
```

- Configuration file of Router B

```
 #
 sysname RouterB
 #
 ipv6
 #
 interface Pos1/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 9:1::1/64
 #
 interface Pos2/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 10::1/64
 #
 interface Pos3/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 9:3::1/64
 #
 bgp 65009
 router-id 2.2.2.2
 peer 10::2 as-number 65008
 peer 9:1::2 as-number 65009
 peer 9:3::2 as-number 65009
 #
 ipv4-family unicast
 undo synchronization
 #
 ipv6-family unicast
 network 9:1:: 64
 network 9:3:: 64
 network 10:: 64
 peer 9:3::2 enable
 peer 9:1::2 enable
 peer 10::2 enable
 #
 return
```

- Configuration file of Router C

```
 #
 sysname RouterC
 #
 ipv6
```

```
#
interface Pos2/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 9:2::1/64
#
interface Pos3/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 9:3::2/64
#
bgp 65009
 router-id 3.3.3.3
 peer 9:3::1 as-number 65009
 peer 9:2::2 as-number 65009
#
 ipv4-family unicast
 undo synchronization
#
 ipv6-family unicast
 network 9:2:: 64
 network 9:3:: 64
 peer 9:3::1 enable
 peer 9:2::2 enable
#
return
```

- Configuration file of Router D

```
#
 sysname RouterD
#
 ipv6
#
interface Pos1/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 9:1::2/64
#
interface Pos2/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 9:2::2/64
#
bgp 65009
 router-id 4.4.4.4
 peer 9:1::1 as-number 65009
 peer 9:2::1 as-number 65009
#
 ipv4-family unicast
 undo synchronization
#
 ipv6-family unicast
 network 9:1:: 64
 network 9:2:: 64
 peer 9:2::1 enable
 peer 9:1::1 enable
#
return
```

## 9.17.2 Example for Configuring a BGP4+ Route Reflection

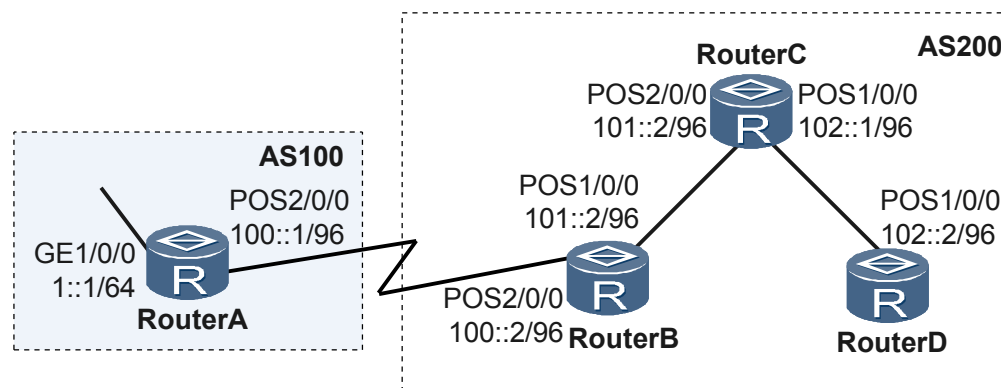
A BGP4+ route reflector avoids fully meshed connections between IBGP peers and thus simplifies the network.

## Networking Requirements

As shown in **Figure 9-2**, Router B receives an update packet from the EBGP peer and forwards it to Router C. Router C is configured as a route reflector with two clients, Router B and Router D.

Router B and Router D need not set up an IBGP connection. When Router C receives the route update packet from Router B, it reflects the information to Router D. Similarly, when Router C receives the route update packet from Router D, it reflects the information to Router B.

**Figure 9-2** Networking diagram of configuring BGP4+ route reflection



## Configuration Roadmap

The configuration roadmap is as follows:

1. Establish an IBGP connection between the client and the route reflector.
2. Configure Router C as the route reflector and check the routing information.

## Preparation Data

To complete the configuration, you need the following data:

- The AS numbers are AS 100 and AS 200.
- The router IDs of Router A, Router B, Router C, and Router D are 1.1.1.1, 2.2.2.2, 3.3.3.3, and 4.4.4.4 respectively.

## Procedure

**Step 1** Assign an IPv6 address for each interface.

The details are not mentioned here.

**Step 2** Configure basic BGP4+ functions.

# Configure Router A.

```
[RouterA] ipv6
[RouterA] bgp 100
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 100::2 as-number 200
```

```
[RouterA-bgp] ipv6-family unicast
[RouterA-bgp-af-ipv6] peer 100::2 enable
[RouterA-bgp-af-ipv6] network 1::64
[RouterA-bgp-af-ipv6] quit
[RouterA-bgp]
```

### # Configure Router B.

```
[RouterB] ipv6
[RouterB] bgp 200
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 100::1 as-number 100
[RouterB-bgp] peer 101::1 as-number 200
[RouterB-bgp] ipv6-family unicast
[RouterB-bgp-af-ipv6] peer 100::1 enable
[RouterB-bgp-af-ipv6] peer 101::1 enable
```

### # Configure Router C.

```
[RouterC] ipv6
[RouterC] bgp 200
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 101::2 as-number 200
[RouterC-bgp] peer 102::2 as-number 200
[RouterC-bgp] ipv6-family unicast
[RouterC-bgp-af-ipv6] peer 101::2 enable
[RouterC-bgp-af-ipv6] peer 102::2 enable
```

### # Configure Router D.

```
[RouterD] ipv6
[RouterD] bgp 200
[RouterD-bgp] router-id 4.4.4.4
[RouterD-bgp] peer 102::1 as-number 200
[RouterD-bgp] ipv6-family unicast
[RouterD-bgp-af-ipv6] peer 102::1 enable
```

## Step 3 Configure the route reflector.

# Configure Router C as a route reflector, and Router B and Router D serve as its clients.

```
[RouterC-bgp] ipv6-family unicast
[RouterC-bgp-af-ipv6] peer 101::2 reflect-client
[RouterC-bgp-af-ipv6] peer 102::2 reflect-client
```

# Check the routing table of Router B.

```
[RouterB]display bgp ipv6 routing-table

BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 6
*> Network : 1::: PrefixLen : 64
 NextHop : 100::1 LocPrf :
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : 100 i
*> Network : 100::: PrefixLen : 96
 NextHop : ::: LocPrf :
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : i
*
 NextHop : 100::1 LocPrf :
 MED : 0 PrefVal : 0
 Label :
```



```

 Path/Ogn : 100 i
 *> Network : 101::: PrefixLen : 96
 NextHop : :: LocPrf :
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : i
 i
 NextHop : 101::1 LocPrf : 100
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : i
 *>i Network : 102::: PrefixLen : 96
 NextHop : 101::1 LocPrf : 100
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : i

```

# Check the routing table of Router D.

[RouterD]display bgp ipv6 routing-table

```

BGP Local router ID is 4.4.4.4
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

```

```

Total Number of Routes: 5
 *>i Network : 1::: PrefixLen : 64
 NextHop : 100::1 LocPrf : 100
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : 100 i
 *>i Network : 100::: PrefixLen : 96
 NextHop : 101::2 LocPrf : 100
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : i
 *>i Network : 101::: PrefixLen : 96
 NextHop : 102::1 LocPrf : 100
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : i
 *> Network : 102::: PrefixLen : 96
 NextHop : :: LocPrf :
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : i
 i
 NextHop : 102::1 LocPrf : 100
 MED : 0 PrefVal : 0
 Label :
 Path/Ogn : i

```

The routing table shows that Router D and Router B learn the routing information advertised by Router A from Router C.

----End

## Configuration Files

- Configuration file of Router A

```

#
 sysname RouterA
#
 ipv6
#
 interface GigabitEthernet1/0/0

```

```
 ipv6 enable
 ipv6 address 1::1/64
#
interface Pos2/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 100::1/96
#
bgp 100
 router-id 1.1.1.1
 peer 100::2 as-number 200
#
 ipv6-family unicast
 undo synchronization
 network 1:: 64
 network 100:: 96
 peer 100::2 enable
#
return
```

● Configuration file of Router B

```
#
sysname RouterB
#
ipv6
#
interface Pos1/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 101::2/96
#
interface Pos2/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 100::2/96
#
bgp 200
 router-id 2.2.2.2
 peer 100::1 as-number 100
 peer 101::1 as-number 200
#
 ipv6-family unicast
 undo synchronization
 network 100:: 96
 network 101:: 96
 peer 100::1 enable
 peer 101::1 enable
#
return
```

● Configuration file of Router C

```
#
sysname RouterC
#
ipv6
#
interface Pos1/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 102::1/96
#
interface Pos2/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 101::1/96
#
bgp 200
 router-id 3.3.3.3
 peer 101::2 as-number 200
 peer 102::2 as-number 200
```

```
#
ipv6-family unicast
undo synchronization
network 101:: 96
network 102:: 96
peer 101::2 enable
peer 101::2 reflect-client
peer 102::2 enable
peer 102::2 reflect-client
#
return
```

- Configuration file of Router D

```
#
sysname RouterD
#
ipv6
#
interface Pos1/0/0
link-protocol ppp
ipv6 enable
ipv6 address 102::2/96
#
bgp 200
router-id 4.4.4.4
peer 102::1 as-number 200
#
ipv4-family unicast
undo synchronization
#
ipv6-family unicast
undo synchronization
network 102:: 96
peer 102::1 enable
#
Return
```

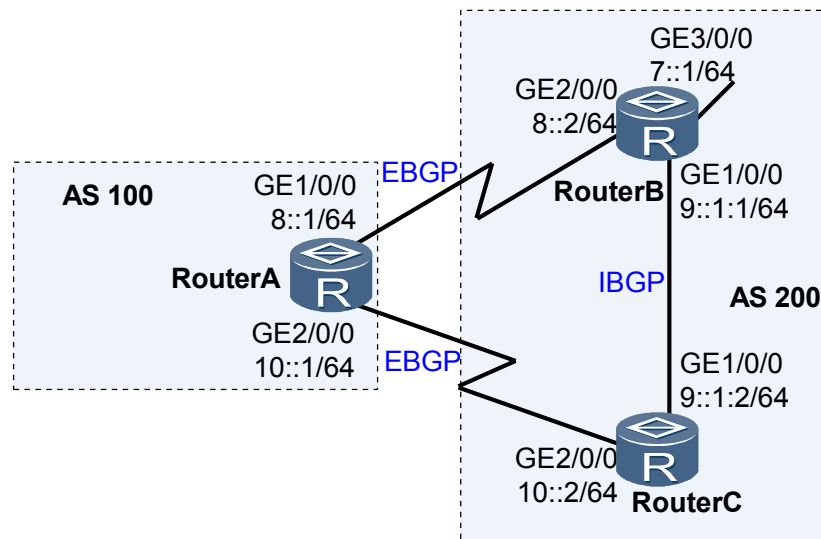
### 9.17.3 Example for Configuring BFD for BGP4+

After BFD for BGP4+ is configured, BFD can fast detect the fault on the link between BGP4+ peers and notify it to BGP4+ so that service traffic can be transmitted through the backup link.

#### Networking Requirements

- As shown in [Figure 9-3](#), Router A belongs to AS 100, Router B to AS 200, and Router C to AS 200. Establish an EBGP connection between Router A and Router B and that between Router A and Router C.
- Traffic is transmitted on the active link Router A → Router B. The link Router A → Router C → Router B acts as the standby link.
- Use BFD to detect the BGP session between Router A and Router B. When the link between Router A and Router B fails, BFD can rapidly detect the failure and notify BGP of the failure. Traffic is transmitted on the standby link.

**Figure 9-3** Networking diagram of configuring BFD for BGP4+



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the basic BGP4+ functions on each router.
2. Configure MED attributes to control the routing selection of the routers.
3. Enable the BFD on Router A and Router B.

## Data Preparation

To complete the configuration, you need the following data:

- Router IDs and AS numbers of Router A, Router B and Router C
- Peer IPv6 address detected by BFD
- Minimum interval for sending the packets, minimum interval for receiving the packets, and local detection time multiplier controlled by BFD

## Procedure

**Step 1** Assign an IPv6 address to each interface.

The detailed configuration is not mentioned here.

**Step 2** Configure the basic BGP4+ functions. Establish an EBGp connection between Router A and Router B, that between Router A and Router C. Establish an IBGP connection between Router B and Router C.

# Configure Router A.

```
[RouterA] bgp 100
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 8::2 as-number 200
[RouterA-bgp] peer 10::2 as-number 200
[RouterA-bgp] ipv6-family unicast
```

```
[RouterA-bgp-af-ipv6] peer 8::2 enable
[RouterA-bgp-af-ipv6] peer 10::2 enable
[RouterA-bgp-af-ipv6] quit
[RouterA-bgp] quit
```

### # Configure Router B.

```
[RouterB] bgp 200
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 8::1 as-number 100
[RouterB-bgp] peer 9::1:2 as-number 200
[RouterB-bgp] ipv6-family unicast
[RouterB-bgp-af-ipv6] peer 8::1 enable
[RouterB-bgp-af-ipv6] peer 9::1:2 enable
[RouterB-bgp-af-ipv6] network 7::1 64
[RouterB-bgp-af-ipv6] quit
[RouterB-bgp] quit
```

### # Configure Router C.

```
[RouterC] bgp 200
[RouterC-bgp] router-id 3.3.3.3
[RouterC-bgp] peer 10::1 as-number 100
[RouterC-bgp] peer 9::1:1 as-number 200
[RouterC-bgp] ipv6-family unicast
[RouterC-bgp-af-ipv6] peer 10::1 enable
[RouterC-bgp-af-ipv6] peer 9::1:1 enable
[RouterC-bgp-af-ipv6] quit
[RouterC-bgp] quit
```

### # Display the established BGP neighbors on Router A.

```
<RouterA> display bgp ipv6 peer
```

```
BGP local router ID : 1.1.1.1
Local AS number : 100
Total number of peers : 2 Peers in established state : 2
```

| Peer  | V | AS  | MsgRcvd | MsgSent | OutQ | Up/Down  | State       | PrefRcv |
|-------|---|-----|---------|---------|------|----------|-------------|---------|
| 8::2  | 4 | 200 | 12      | 11      | 0    | 00:07:26 | Established | 0       |
| 10::2 | 4 | 200 | 12      | 12      | 0    | 00:07:21 | Established | 0       |

## Step 3 Configure MED attributes.

Set the value of MED sent by Router B and Router C to Router A by using the policy.

### # Configure Router B.

```
[RouterB] route-policy 10 permit node 10
[RouterB-route-policy] apply cost 100
[RouterB-route-policy] quit
[RouterB] bgp 200
[RouterB-bgp] ipv6-family unicast
[RouterB-bgp-af-ipv6] peer 8::1 route-policy 10 export
[RouterB-bgp-af-ipv6] quit
[RouterB-bgp] quit
```

### # Configure Router C.

```
[RouterC] route-policy 10 permit node 10
[RouterC-route-policy] apply cost 150
[RouterC-route-policy] quit
[RouterC] bgp 200
[RouterC-bgp] ipv6-family unicast
[RouterC-bgp-af-ipv6] peer 10::1 route-policy 10 export
[RouterC-bgp-af-ipv6] quit
[RouterC-bgp] quit
```

# Display all BGP routing information on Router A.

```
<RouterA> display bgp ipv6 routing-table

BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 2
*> Network : 7:: PrefixLen : 64
 NextHop : 8::2 LocPrf :
 MED : 100 PrefVal : 0
 Label :
 Path/Ogn : 200 i
*
 NextHop : 10::2 LocPrf :
 MED : 150 PrefVal : 0
 Label :
 Path/Ogn : 200 i
```

As shown in the BGP routing table, the next hop address of the route to 7::1/64 is 8::2 and traffic is transmitted on the active link Router A → Router B.

**Step 4** Configure the BFD detection function, the interval for sending the packets, the interval for receiving the packets, and the local detection time multiple.

# Enable BFD on Router A, set the minimum interval for sending the packets and the minimum interval for receiving the packets to 100 ms, and set the local detection time multiple to 4.

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bgp 100
[RouterA-bgp] peer 8::2 bfd enable
[RouterA-bgp] peer 8::2 bfd min-tx-interval 100 min-rx-interval 100 detect-
multiplier 4
```

# Enable BFD on Router B, set the minimum interval for sending the packets and the minimum interval for receiving the packets to 100 ms, and set the local detection time multiple to 4.

```
[RouterB] bfd
[RouterB-bfd] quit
[RouterB] bgp 200
[RouterB-bgp] peer 8::1 bfd enable
[RouterB-bgp] peer 8::1 bfd min-tx-interval 100 min-rx-interval 100 detect-
multiplier 4
```

# Display all BFD sessions set up by BGP on Router A.

```
<RouterA> display bgp ipv6 bfd session all

Local_Address : 8::1
Peer_Address : 8::2
Tx-interval(ms) : 100 Rx-interval(ms) : 100
Multiplier : 4 Interface : GigabitEthernet1/0/0
LD/RD : 8192/8192 Session-State : Up

```

**Step 5** Verify the Configuration.

# Run the **shutdown** command on GE 2/0/0 of Router B to simulate the active link failure.

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] shutdown
```

**Step 6** # Display the routing table on Router A.

```
<RouterA> display bgp ipv6 routing-table
```

```

BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 1
*> Network : 7::: PrefixLen : 64
 NextHop : 10::2 LocPrf :
 MED : 150 PrefVal : 0
 Label :
 Path/Ogn : 200 i

```

As shown in the BGP routing table, the standby link Router A → Router C → Router B takes effect after the active link fails. The next hop address of the route to 7::1/64 becomes 10::2.

----End

## Configuration Files

- Configuration file of Router A

```

#
 sysname RouterA
#
 ipv6
#
 bfd
#
 interface GigabitEthernet1/0/0
 undo shutdown
 ipv6 enable
 ipv6 address 8::1/64
#
 interface GigabitEthernet2/0/0
 undo shutdown
 ipv6 enable
 ipv6 address 10::1/64
#
 interface NULL0
#
 interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
 bgp 100
 router-id 1.1.1.1
 peer 8::2 as-number 200
 peer 8::2 bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 4
 peer 8::2 bfd enable
 peer 10::2 as-number 200
#
 ipv4-family unicast
 undo synchronization
#
 ipv6-family unicast
 undo synchronization
 peer 8::2 enable
 peer 10::2 enable
#
 return

```

- Configuration file of Router B

```

#
 sysname RouterB
#
 sysname RouterB
#
 ipv6

```

```
#
bfd
#
interface interface GigabitEthernet2/0/0
shutdown
ipv6 enable
ipv6 address 8::2/64
#
interface GigabitEthernet1/0/0
undo shutdown
ipv6 enable
ipv6 address 9::1:1/64
#
interface GigabitEthernet3/0/0
undo shutdown
ipv6 enable
ipv6 address 7::1/64
#
interface NULL0
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
#
bgp 200
router-id 2.2.2.2
peer 8::1 as-number 100
peer 8::1 bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 4
peer 8::1 bfd enable
peer 9::1:2 as-number 200
#
ipv4-family unicast
undo synchronization
#
ipv6-family unicast
undo synchronization
network 7:: 64
peer 8::1 enable
peer 8::1 route-policy 10 export
peer 9::1:2 enable
#
route-policy 10 permit node 10
apply cost 100
#
return
```

● Configuration file of Router C

```
#
sysname RouterC
#
ipv6
#
interface interface GigabitEthernet1/0/0
undo shutdown
ipv6 enable
ipv6 address 9::1:2/64
#
interface interface GigabitEthernet2/0/0
undo shutdown
ipv6 enable
ipv6 address 10::2/64
#
interface LoopBack0
ip address 3.3.3.3 255.255.255.255
#
bgp 200
router-id 3.3.3.3
peer 9::1:1 as-number 200
peer 10::1 as-number 100
#
ipv4-family unicast
```



```

undo synchronization
#
ipv6-family unicast
undo synchronization
peer 9::1:1 enable
peer 10::1 enable
peer 10::1 route-policy 10 export
#
route-policy 10 permit node 10
apply cost 150
#
return

```

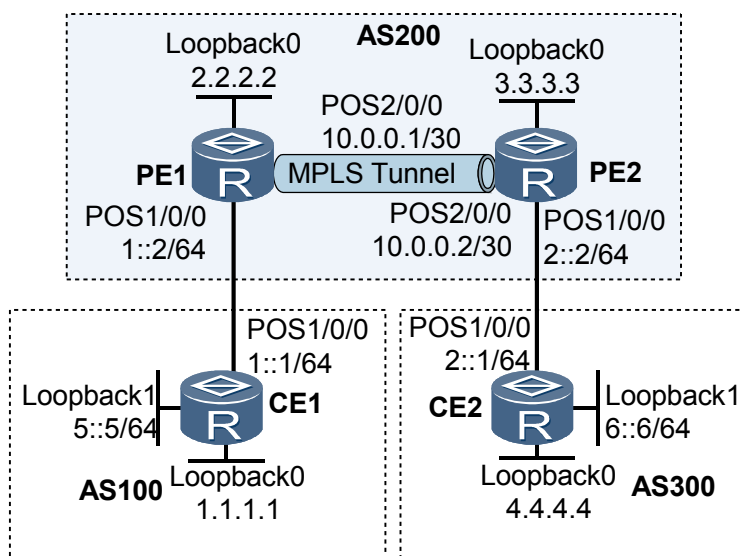
## 9.17.4 Example for Configuring BGP4+ 6PE

By configuring BGP4+ 6PE, you can connect separated IPv6 networks through the MPLS tunneling technology.

### Networking Requirements

As shown in [Figure 9-4](#), the link between CE1 and PE1 is an IPv6 link; the link between PE1 and PE2 is an IPv4 link; the link between PE2 and CE2 is an IPv6 link. BGP4+ runs between CE1 and PE1 and between PE2 and CE2. MPLS runs between PE1 and PE2. 6PE is configured to implement interworking between IPv6 networks.

**Figure 9-4** Networking diagram of configuring BGP4+ 6PE



### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure OSPF on PE1 and PE2 to make them learn loopback interface addresses from each other.
2. Configure BGP4+ between CE1 and PE1 and between PE2 and CE2.
3. Configure MPLS on PE1 and PE2 and set up the LSP.

4. Configure 6PE on PE1 and PE2.

## Data Preparation

To complete the configuration, you need the following data:

- Router IDs of CE1, PE1, PE2, and CE2 as 1.1.1.1, 2.2.2.2, 3.3.3.3, and 4.4.4.4 respectively
- Number of the AS where each router resides

## Procedure

**Step 1** Configure the IPv4 and IPv6 addresses for each interface.

The configuration details are not mentioned here.

**Step 2** Configure OSPF on PE1 and PE2 to make them learn routes from each other.

The configuration details are not mentioned here.

**Step 3** Configure BGP4+.

# Configure CE1.

```
[CE1] bgp 100
[CE1-bgp] peer 1::2 as-number 200
[CE1-bgp] ipv6-family unicast
[CE1-bgp-af-ipv6] peer 1::2 enable
[CE1-bgp-af-ipv6] network 5::5 64
[CE1-bgp-af-ipv6] quit
[CE1-bgp] quit
```

# Configure PE1.

```
[PE1] bgp 200
[PE1-bgp] peer 1::1 as-number 100
[PE1-bgp] ipv6-family unicast
[PE1-bgp-af-ipv6] peer 1::1 enable
[PE1-bgp-af-ipv6] quit
[PE1-bgp] quit
```

# Configure PE2.

```
[PE2] bgp 200
[PE2-bgp] peer 2::1 as-number 300
[PE2-bgp] ipv6-family unicast
[PE2-bgp-af-ipv6] peer 2::1 enable
[PE2-bgp-af-ipv6] quit
[PE2-bgp] quit
```

# Configure CE2.

```
[CE2] bgp 300
[CE2-bgp] peer 2::2 as-number 200
[CE2-bgp] ipv6-family unicast
[CE2-bgp-af-ipv6] peer 2::2 enable
[CE2-bgp-af-ipv6] network 6::6 64
[CE2-bgp-af-ipv6] quit
[CE2-bgp] quit
```

# Check whether the neighbor relationship is set up on PE1 and PE2.

```
[PE1] display bgp ipv6 peer
BGP local router ID : 2.2.2.2
Local AS number : 200
Total number of peers : 1 Peers in established state : 1
Peer V AS MsgRcvd MsgSent OutQ Up/Down State PrefRcv
```

```

1::1 4 100 32 35 0 00:27:20 Established
1
[PE2] display bgp ipv6 peer
BGP local router ID : 3.3.3.3
Local AS number : 200
Total number of peers : 1 Peers in established state : 1
Peer V AS MsgRcvd MsgSent OutQ Up/Down State PrefRcv
2::1 4 300 31 37 0 00:28:08 Established
1

```

#### Step 4 Configure MPLS on PE1 and PE2 and set up the LSP.

# Configure PE1.

```

[PE1] mpls lsr-id 2.2.2.2
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface pos2/0/0
[PE1-Pos2/0/0] mpls
[PE1-Pos2/0/0] mpls ldp
[PE1-Pos2/0/0] quit

```

# Configure PE 2.

```

[PE2] mpls lsr-id 3.3.3.3
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface pos2/0/0
[PE2-Pos2/0/0] mpls
[PE2-Pos2/0/0] mpls ldp
[PE2-Pos2/0/0] quit

```

# Check whether the LSP is set up, taking PE1 as an example.

```

[PE1] display mpls lsp

 LSP Information: LDP LSP

FEC In/Out Label In/Out IF Vrf Name
3.3.3.3/32 NULL/3 -/Pos2/0/0
3.3.3.3/32 1027/3 -/Pos2/0/0

 LSP Information: BGP IPV6 LSP

FEC : 1::/64
In Label : 105472
In Interface : -----
Vrf Name :
FEC : 5::/64
In Label : 105475
In Interface : -----
Vrf Name :
Out Label : -----
OutInterface : -----

```

#### Step 5 Configure 6PE.

# Configure PE1.

```

[PE1] bgp 200
[PE1-bgp] peer 3.3.3.3 as-number 200
[PE1-bgp] peer 3.3.3.3 connect-interface LoopBack0
[PE1-bgp] ipv6-family unicast
[PE1-bgp-af-ipv6] peer 3.3.3.3 enable
[PE1-bgp-af-ipv6] peer 3.3.3.3 label-route-capability
[PE1-bgp-af-ipv6] import-route direct
[PE1-bgp-af-ipv6] quit
[PE1-bgp] quit

```

# Configure PE2.

```
[PE2] bgp 200
[PE2-bgp] peer 2.2.2.2 as-number 200
[PE2-bgp] peer 2.2.2.2 connect-interface LoopBack0
[PE2-bgp] ipv6-family unicast
[PE2-bgp-af-ipv6] peer 2.2.2.2 enable
[PE2-bgp-af-ipv6] peer 2.2.2.2 label-route-capability
[PE2-bgp-af-ipv6] import-route direct
[PE2-bgp-af-ipv6] quit
[PE2-bgp] quit
```

# Check the connection status of 6PE peers.

```
[PE1] display bgp ipv6 peer
BGP local router ID : 2.2.2.2
Local AS number : 200
Total number of peers : 2 Peers in established state : 2
Peer V AS MsgRcvd MsgSent OutQ Up/Down State PrefRcv
3.3.3.3 4 200 1248 1342 0 18:06:28 Established
1
1::1 4 100 32 35 0 00:27:20 Established
1
```

From the preceding display, you can view that the BGP 6PE connection between PE1 and PE2 is set up.

#### Step 6 Verify the configuration.

Take CE1 as an example.

CE1 can learn the address of Loopback 1 from CE2 and ping through CE2.

```
[CE1] display ipv6 routing-table
Routing Table : Public
Destinations : 8 Routes : 8

Destination : ::1 PrefixLength : 128
NextHop : ::1 Preference : 0
Cost : 0 Protocol : Direct
RelayNextHop : :: TunnelID : 0x0
Interface : InLoopBack0 Flags : D

Destination : 1:: PrefixLength : 64
NextHop : 1::1 Preference : 0
Cost : 0 Protocol : Direct
RelayNextHop : :: TunnelID : 0x0
Interface : Pos1/0/0 Flags : D

Destination : 1::1 PrefixLength : 128
NextHop : ::1 Preference : 0
Cost : 0 Protocol : Direct
RelayNextHop : :: TunnelID : 0x0
Interface : InLoopBack0 Flags : D

Destination : 2:: PrefixLength : 64
NextHop : 1::2 Preference : 255
Cost : 0 Protocol : EBGp
RelayNextHop : :: TunnelID : 0x0
Interface : Pos1/0/0 Flags : D

Destination : 5:: PrefixLength : 64
NextHop : 5::5 Preference : 0
Cost : 0 Protocol : Direct
RelayNextHop : :: TunnelID : 0x0
Interface : LoopBack1 Flags : D

Destination : 5::5 PrefixLength : 128
NextHop : ::1 Preference : 0
```

```

Cost : 0
RelayNextHop : ::
Interface : InLoopBack0
Protocol : Direct
TunnelID : 0x0
Flags : D

Destination : 6::
NextHop : 1::2
Cost : 0
RelayNextHop : ::
Interface : Pos1/0/0
PrefixLength : 64
Preference : 255
Protocol : EBGp
TunnelID : 0x0
Flags : D

Destination : FE80::
NextHop : ::
Cost : 0
RelayNextHop : ::
Interface : NULL0
PrefixLength : 10
Preference : 0
Protocol : Direct
TunnelID : 0x0
Flags : D

```

Ping the address of Loopback1 of CE2 on CE1.

```

[CE1] ping ipv6 -c 5 6::6
PING 6::6 : 56 data bytes, press CTRL_C to break
 Reply from 6::6:
 bytes=56 Sequence=1 hop limit=62 time = 80 ms
 Reply from 6::6:
 bytes=56 Sequence=2 hop limit=62 time = 80 ms
 Reply from 6::6:
 bytes=56 Sequence=3 hop limit=62 time = 90 ms
 Reply from 6::6:
 bytes=56 Sequence=4 hop limit=62 time = 90 ms
 Reply from 6::6:
 bytes=56 Sequence=5 hop limit=62 time = 60 ms
--- 6::6 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 60/80/90 ms

```

From the preceding display, you can view that 6PE connects the separated IPv6 networks and realizes interworking.

---End

## Configuration Files

- Configuration file of CE1

```

#
sysname CE1
#
ipv6
#
interface Pos1/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 1::1/64
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface LoopBack1
 ipv6 enable
 ipv6 address 5::5/64
#
bgp 100
 peer 1::2 as-number 200
#
 ipv4-family unicast
 undo synchronization
#
 ipv6-family unicast

```

```
 undo synchronization
 network 5:: 64
 peer 1::2 enable
 #
 return
```

● Configuration file of PE1

```
#
sysname PE1
#
ipv6
#
mpls lsr-id 2.2.2.2
mpls
#
mpls ldp
#
interface Pos1/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 1::2/64
#
interface Pos2/0/0
 link-protocol ppp
 ip address 10.0.0.1 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
bgp 200
 peer 1::1 as-number 100
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
#
 ipv4-family unicast
 undo synchronization
 peer 3.3.3.3 enable
#
 ipv6-family unicast
 undo synchronization
 import-route direct
 peer 3.3.3.3 enable
 peer 3.3.3.3 label-route-capability
 peer 1::1 enable
#
ospf 1
 area 0.0.0.0
 network 2.2.2.2 0.0.0.0
 network 10.0.0.0 0.0.0.3
#
return
```

● Configuration file of PE2

```
#
sysname PE2
#
ipv6
#
mpls lsr-id 3.3.3.3
mpls
#
mpls ldp
#
interface Pos2/0/0
 link-protocol ppp
 ip address 10.0.0.2 255.255.255.252
 mpls
 mpls ldp
```

```
#
interface Pos1/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 2::2/64
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
bgp 200
 peer 2::1 as-number 300
 peer 2.2.2.2 as-number 200
 peer 2.2.2.2 connect-interface LoopBack0
#
ipv4-family unicast
 undo synchronization
 peer 2.2.2.2 enable
#
ipv6-family unicast
 undo synchronization
 import-route direct
 peer 2.2.2.2 enable
 peer 2.2.2.2 label-route-capability
 peer 2::1 enable
#
ospf 1
 area 0.0.0.0
 network 3.3.3.3 0.0.0.0
 network 10.0.0.0 0.0.0.3
#
return
```

- Configuration file of CE2

```
#
sysname CE2
#
ipv6
#
interface Pos1/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 2::1/64
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface LoopBack1
 ipv6 enable
 ipv6 address 6::6/64
#
bgp 300
 peer 2::2 as-number 200
#
ipv4-family unicast
 undo synchronization
#
ipv6-family unicast
 undo synchronization
 network 6:: 64
 peer 2::2 enable
#
return
```

## 9.17.5 Example for Configuring BGP4+ 6PE FRR

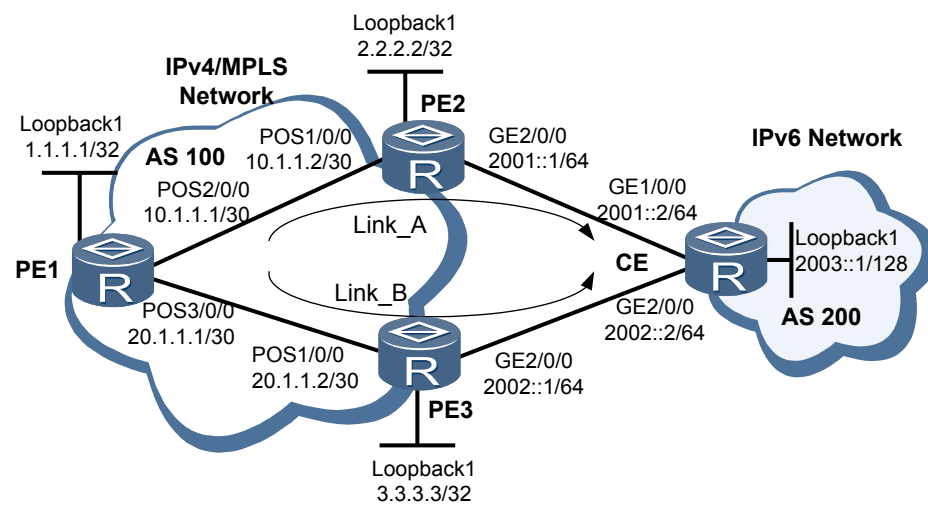
After you configure 6PE FRR, 6PE routers can select the backup next hop for received 6PE routes. When the next hop of the primary route between PEs becomes unreachable, traffic will be quickly redirected to the backup next hop.

## Networking Requirements

A 6PE router learns the 6PE routes with the same IP prefix from different 6PE peers. After BGP 6PE FRR is configured on the 6PE router, a backup link can be selected for the router. When the next hop of the primary route between PEs becomes unreachable, traffic can be quickly switched to the backup link.

As shown in **Figure 9-5**, 6PE peer relationships are established between PE1 and PE2, and between PE1 and PE3. PE1 receives the 6PE routes to the loopback interface on the CE from PE2 and PE3. On PE1, it is required to configure a primary 6PE route and a backup 6PE route to the loopback interface on the CE, with Link\_A serving as the primary link and Link\_B serving as the backup link.

**Figure 9-5** Networking diagram of configuring 6PE FRR



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IGP on the IPv4/MPLS network to enable the connectivity between network devices.
2. Enable MPLS and MPLS LDP globally and on the interfaces of the routers on the network and set up LDP LSPs.
3. Establish 6PE peer relationships between the PEs.
4. Establish EBGP peer relationships between the PEs and CE and import the address of the loopback interface on the CE into BGP.
5. Configure 6PE FRR on PE1.

## Data Preparation

To complete the configuration, you need the following data:

- IP or IPv6 addresses of the interfaces on the routers
- Numbers of the ASs where the PEs and CE reside
- Names of the routing policies used to affect route costs on the PEs



## Procedure

**Step 1** Configure IP or IPv6 addresses for the interfaces on the routers. For details, see the following configuration files.

**Step 2** Configure an IGP on the IPv4/MPLS network.

In this example, OSPF, as an IGP, is configured. For the configuration details, see the following configuration files.

After the configuration is complete, run the **display ip routing-table** command on the PEs, and you can see that the routers have learned the addresses of the loopback interfaces on the other routers. The following takes the display on PE1 as an example:

```
<PE1> display ip routing-table
Route Flags: R - relay, D - download to fib

Routing Tables: Public
 Destinations : 11 Routes : 11

Destination/Mask Proto Pre Cost Flags NextHop Interface

 1.1.1.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
 2.2.2.2/32 OSPF 10 1562 D 10.1.1.2 Pos2/0/0
 3.3.3.3/32 OSPF 10 1562 D 20.1.1.2 Pos3/0/0
 10.1.1.0/30 Direct 0 0 D 10.1.1.1 Pos2/0/0
 10.1.1.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
 10.1.1.2/32 Direct 0 0 D 10.1.1.2 Pos2/0/0
 20.1.1.0/30 Direct 0 0 D 20.1.1.1 Pos3/0/0
 20.1.1.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
 20.1.1.2/32 Direct 0 0 D 20.1.1.2 Pos3/0/0
 127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
 127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
```

**Step 3** Enable MPLS and MPLS LDP globally and on the interfaces of the routers on the network and set up LDP LSPs.

# Configure PE1.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface pos2/0/0
[PE1-Pos2/0/0] mpls
[PE1-Pos2/0/0] mpls ldp
[PE1-Pos2/0/0] quit
[PE1] interface pos3/0/0
[PE1-Pos3/0/0] mpls
[PE1-Pos3/0/0] mpls ldp
[PE1-Pos3/0/0] quit
```

The configurations of the PE2 and PE3 are similar to the configuration of PE1, and are not mentioned here. For details, see the following configuration files.

After the configuration is complete, run the **display mpls ldp lsp** command on the PEs, and you can find the labels allocated to the routes to the loopback interfaces on the other PEs.

```
<PE1> display mpls ldp lsp
LDP LSP Information

DestAddress/Mask In/OutLabel UpstreamPeer NextHop OutInterface

 1.1.1.1/32 3/NULL 2.2.2.2 127.0.0.1 InLoop0
 1.1.1.1/32 3/NULL 3.3.3.3 127.0.0.1 InLoop0
```

```
*1.1.1.1/32 Liberal/1024 DS/2.2.2.2
*1.1.1.1/32 Liberal/1024 DS/3.3.3.3
2.2.2.2/32 NULL/3 - 10.1.1.2 Pos2/0/0
2.2.2.2/32 1024/3 2.2.2.2 10.1.1.2 Pos2/0/0
2.2.2.2/32 1024/3 3.3.3.3 10.1.1.2 Pos2/0/0
*2.2.2.2/32 Liberal/1025 DS/3.3.3.3
3.3.3.3/32 NULL/3 - 20.1.1.2 Pos3/0/0
3.3.3.3/32 1025/3 2.2.2.2 20.1.1.2 Pos3/0/0
3.3.3.3/32 1025/3 3.3.3.3 20.1.1.2 Pos3/0/0
*3.3.3.3/32 Liberal/1025 DS/2.2.2.2
```

```

TOTAL: 8 Normal LSP(s) Found.
TOTAL: 4 Liberal LSP(s) Found.
TOTAL: 0 Frr LSP(s) Found.
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
A '*' before a UpstreamPeer means the session is in GR state
A '*' before a NextHop means the LSP is FRR LSP
```

#### Step 4 Establish 6PE peer relationships between the PEs.

Establish 6PE peer relationships between PE1 and PE2, and between PE1 and PE3.

# Configure PE1.

```
[PE1] bgp 100
[PE1-bgp] peer 2.2.2.2 as-number 100
[PE1-bgp] peer 2.2.2.2 connect-interface LoopBack1
[PE1-bgp] peer 3.3.3.3 as-number 100
[PE1-bgp] peer 3.3.3.3 connect-interface LoopBack1
[PE1-bgp] ipv6-family unicast
[PE1-bgp-af-ipv6] peer 2.2.2.2 enable
[PE1-bgp-af-ipv6] peer 2.2.2.2 label-route-capability
[PE1-bgp-af-ipv6] peer 3.3.3.3 enable
[PE1-bgp-af-ipv6] peer 3.3.3.3 label-route-capability
[PE1-bgp-af-ipv6] quit
[PE1-bgp] quit
```

# Configure PE2.

```
[PE2] bgp 100
[PE2-bgp] peer 1.1.1.1 as-number 100
[PE2-bgp] peer 1.1.1.1 connect-interface LoopBack1
[PE2-bgp] ipv6-family unicast
[PE2-bgp-af-ipv6] peer 1.1.1.1 enable
[PE2-bgp-af-ipv6] peer 1.1.1.1 label-route-capability
[PE2-bgp-af-ipv6] quit
[PE2-bgp] quit
```

# Configure PE3.

```
[PE3] bgp 100
[PE3-bgp] peer 1.1.1.1 as-number 100
[PE3-bgp] peer 1.1.1.1 connect-interface LoopBack1
[PE3-bgp] ipv6-family unicast
[PE3-bgp-af-ipv6] peer 1.1.1.1 enable
[PE3-bgp-af-ipv6] peer 1.1.1.1 label-route-capability
[PE3-bgp-af-ipv6] quit
[PE3-bgp] quit
```

After the configuration is complete, run the **display bgp ipv6 peer** command on the PEs, and you can find that the status of the peer relationships is **Established**. The following takes the display on PE1 as an example:

```
<PE1> display bgp ipv6 peer

BGP local router ID : 10.1.1.1
Local AS number : 100
Total number of peers : 2 Peers in established state : 2
```

| Peer PrefRcv | V | AS  | MsgRcvd | MsgSent | OutQ | Up/Down  | State       |   |
|--------------|---|-----|---------|---------|------|----------|-------------|---|
| 2.2.2.2      | 4 | 100 | 19      | 20      | 0    | 00:12:53 | Established | 1 |
| 3.3.3.3      | 4 | 100 | 16      | 18      | 0    | 00:12:13 | Established | 1 |

**Step 5** Establish EBGP peer relationships between PE2 and the CE, and between PE3 and the CE, and import the address of the loopback interface on the CE into BGP.

# Configure PE2.

```
[PE2] bgp 100
[PE2-bgp] peer 2001::2 as-number 200
[PE2-bgp] ipv6-family unicast
[PE2-bgp-af-ipv6] peer 2001::2 enable
[PE2-bgp-af-ipv6] quit
[PE2-bgp] quit
```

# Configure PE3.

```
[PE3] bgp 100
[PE3-bgp] peer 2002::2 as-number 200
[PE3-bgp] ipv6-family unicast
[PE3-bgp-af-ipv6] peer 2002::2 enable
[PE3-bgp-af-ipv6] quit
[PE3-bgp] quit
```

# Configure the CE.

```
[CE] bgp 200
[CE-bgp] peer 2001::1 as-number 100
[CE-bgp] peer 2002::1 as-number 100
[CE-bgp] ipv6-family unicast
[CE-bgp-af-ipv6] peer 2001::1 enable
[CE-bgp-af-ipv6] peer 2002::1 enable
[CE-bgp-af-ipv6] network 2003::1 128
[CE-bgp-af-ipv6] quit
[CE-bgp] quit
```

After the configuration is complete, run the **display ipv6 routing-table** command on the PEs, and you can find that the PEs have received the routes to the loopback interface on the CE. The following takes the display on PE2 as an example:

```
<PE2> display ipv6 routing-table
Routing Table : Public
Destinations : 5 Routes : 5

Destination : ::1 PrefixLength : 128
NextHop : ::1 Preference : 0
Cost : 0 Protocol : Direct
RelayNextHop : :: TunnelID : 0x0
Interface : InLoopBack0 Flags : D

Destination : 2001:: PrefixLength : 64
NextHop : 2001::1 Preference : 0
Cost : 0 Protocol : Direct
RelayNextHop : :: TunnelID : 0x0
Interface : GigabitEthernet2/0/0 Flags : D

Destination : 2001:::1 PrefixLength : 128
NextHop : ::1 Preference : 0
Cost : 0 Protocol : Direct
RelayNextHop : :: TunnelID : 0x0
Interface : InLoopBack0 Flags : D

Destination : 2003::1 PrefixLength : 128
NextHop : 2001::2 Preference : 255
Cost : 0 Protocol : EBGP
```

```

RelayNextHop : :: TunnelID : 0x0
Interface : GigabitEthernet2/0/0 Flags : D

Destination : FE80:: PrefixLength : 10
NextHop : :: Preference : 0
Cost : 0 Protocol : Direct
RelayNextHop : :: TunnelID : 0x0
Interface : NULL0 Flags : D

```

**Step 6** Configure a routing policy on PE3 and apply this policy to make the cost of the route sent from PE3 to PE1 greater than the cost of the route sent from PE2 to PE1. In this case, PE1 later will select the route sent from PE2.

```

Configure PE3.
[PE3] route-policy addcost permit node 10
[PE3-route-policy] apply cost 20
[PE3-route-policy] quit
[PE3] bgp 100
[PE3-bgp] ipv6-family unicast
[PE3-bgp-af-ipv6] peer 1.1.1.1 route-policy addcost export
[PE3-bgp-af-ipv6] quit
[PE3-bgp] quit

```

**Step 7** Enable 6PE FRR on PE1.

```

Configure PE1.

[PE1] bgp 100
[PE1-bgp] ipv6-family unicast
[PE1-bgp-af-ipv6] auto-frr
[PE1-bgp-af-ipv6] quit

```

**Step 8** Verify the configuration.

Run the **display ipv6 routing-table** command on PE1. You can find that PE2 is the next hop of PE1 on the route to the loopback interface on the CE and there are also a backup next hop and a backup label on PE1.

```

<PE1> display ipv6 routing-table 2003::1 verbose
Routing Table :
Summary Count : 1

Destination : 2003::1 PrefixLength : 128
NextHop : ::FFFF:2.2.2.2 Preference : 255
Neighbour : ::2.2.2.2 ProcessID : 0
Label : 1033 Protocol : IBGP
State : Active Adv Relied Cost : 0
Entry ID : 3 EntryFlags : 0x80024900
Reference Cnt: 2 Tag : 0
Priority : medium Age : 173sec
IndirectID : 0x4
RelayNextHop : :: TunnelID : 0x9
Interface : Pos2/0/0 Flags : RD
BkNextHop : ::FFFF:3.3.3.3 BkInterface :
BkLabel : 1029 BkTunnelID : 0x0
BkPETunnelID : 0xd BkIndirectID : 0x3

```

After running the **undo ipv6 enable** command on GE 2/0/0 of PE2, run the **display ipv6 routing-table** command on PE1. You can find that PE3 is the next hop of PE1 on the route to the loopback interface on the CE and there is no backup next hop for PE1.

```

<PE1> display ipv6 routing-table 2003::1 verbose
Routing Table :
Summary Count : 1

Destination : 2003::1 PrefixLength : 128
NextHop : ::FFFF:3.3.3.3 Preference : 255
Neighbour : ::3.3.3.3 ProcessID : 0
Label : 1029 Protocol : IBGP

```

```
State : Active Adv Relied Cost : 20
Entry ID : 3 EntryFlags : 0x80024900
Reference Cnt : 2 Tag : 0
Priority : medium Age : 6sec
IndirectID : 0x3 TunnelID : 0xd
RelayNextHop : :: Flags : RD
Interface : Pos3/0/0
```

----End

## Configuration Files

- Configuration file of PE1

```
#
sysname PE1
#
mpls lsr-id 1.1.1.1
mpls
#
mpls ldp
#
interface Pos2/0/0
link-protocol ppp
ip address 10.1.1.1 255.255.255.252
mpls
mpls ldp
#
interface Pos3/0/0
link-protocol ppp
ip address 20.1.1.1 255.255.255.252
mpls
mpls ldp
#
interface LoopBack1
ip address 1.1.1.1 255.255.255.255
#
bgp 100
router-id 1.1.1.1
peer 2.2.2.2 as-number 100
peer 2.2.2.2 connect-interface LoopBack1
peer 3.3.3.3 as-number 100
peer 3.3.3.3 connect-interface LoopBack1
#
ipv4-family unicast
undo synchronization
peer 2.2.2.2 enable
peer 3.3.3.3 enable
#
ipv6-family unicast
undo synchronization
auto-frr
peer 2.2.2.2 enable
peer 2.2.2.2 label-route-capability
peer 3.3.3.3 enable
peer 3.3.3.3 label-route-capability
#
ospf 1
area 0.0.0.0
network 1.1.1.1 0.0.0.0
network 10.1.1.0 0.0.0.3
network 20.1.1.0 0.0.0.3
#
return
```

- Configuration file of PE2

```
#
sysname PE2
#
ipv6
```

```

#
 mpls lsr-id 2.2.2.2
 mpls
#
 mpls ldp
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.252
 mpls
 mpls ldp
#
 interface GigabitEthernet2/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 2001::1 64
#
 interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
 bgp 100
 router-id 2.2.2.2
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack1
 peer 2001::2 as-number 200
#
 ipv4-family unicast
 undo synchronization
 peer 1.1.1.1 enable
#
 ipv6-family unicast
 undo synchronization
 peer 1.1.1.1 enable
 peer 1.1.1.1 label-route-capability
 peer 2001::2 enable
#
 ospf 1
 area 0.0.0.0
 network 2.2.2.2 0.0.0.0
 network 10.1.1.0 0.0.0.3
#
 return

```

● Configuration file of PE3

```

#
 sysname PE3
#
 ipv6
#
 mpls lsr-id 3.3.3.3
 mpls
#
 mpls ldp
#
 interface Pos1/0/0
 link-protocol ppp
 ip address 20.1.1.2 255.255.255.252
 mpls
 mpls ldp
#
 interface GigabitEthernet2/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 2002::1/64
#
 interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
 bgp 100
 router-id 3.3.3.3

```

```
peer 1.1.1.1 as-number 100
peer 1.1.1.1 connect-interface LoopBack1
peer 2002::2 as-number 200
#
ipv4-family unicast
 undo synchronization
 peer 1.1.1.1 enable
#
ipv6-family unicast
 undo synchronization
 peer 1.1.1.1 enable
 peer 1.1.1.1 route-policy addcost export
 peer 1.1.1.1 label-route-capability
 peer 2002::2 enable
#
ospf 1
 area 0.0.0.0
 network 3.3.3.3 0.0.0.0
 network 20.1.1.0 0.0.0.3
#
route-policy addcost permit node 10
 apply cost 20
#
return
```

- Configuration file of CE1

```
#
sysname CE
#
ipv6
#
interface GigabitEthernet1/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 2001::2/64
#
interface GigabitEthernet2/0/0
 link-protocol ppp
 ipv6 enable
 ipv6 address 2002::2/64
#
interface LoopBack1
 ipv6 enable
 ipv6 address 2003::1/128
#
bgp 200
 peer 2001::1 as-number 100
 peer 2002::1 as-number 100
#
 ipv4-family unicast
 undo synchronization
#
 ipv6-family unicast
 undo synchronization
 network 2003::1 128
 peer 2001::1 enable
 peer 2002::1 enable
#
return
```

# 10 Routing Policy Configuration

---

## About This Chapter

Routing policies are used to filter routes to change the path through which network traffic passes.

### [10.1 Introduction of Routing Policy](#)

By configuring routing policies, you can properly use network resources.

### [10.2 Configuring the IP-Prefix List](#)

An IP prefix list filters routes according to the destination addresses of the routes.

### [10.3 Configuring the Route-Policy](#)

Each node of a Route-Policy consists of a set of if-match and apply clauses.

### [10.4 Applying Filters to Received Routes](#)

By applying the related filters of routing policies to routing protocols, you can filter the received routes.

### [10.5 Applying Filters to Advertised Routes](#)

By applying the related filters of routing policies to routing protocols, you can filter advertised routes.

### [10.6 Applying Filters to Imported Routes](#)

By applying the related filters of routing policies to routing protocols, you can filter imported routes.

### [10.7 Controlling the Valid Time of the Routing policy](#)

To ensure network stability, you need to configure the delay for applying a routing policy when modifying the routing policy.

### [10.8 Maintaining the Routing Policy](#)

Maintaining routing policies involves clearing the statistics of the IP prefix list and debugging routing policies.

### [10.9 Configuration Examples](#)

Routing policy configuration examples explain networking requirements, networking diagram, configuration notes, configuration roadmap, and configuration procedure.



## 10.1 Introduction of Routing Policy

By configuring routing policies, you can properly use network resources.

### 10.1.1 Overview of the Routing Policy

By using routing policies, you can flexibly control the routes to be sent or received.

#### Routing Policy

Routing policies are used to filter routes and control the receiving and advertising of routes. By changing the route attributes such as reachability, you can change the path that the traffic passes through.

When a router sends or receives routes, it may use certain policies to filter routes. The policies are used in the following situations:

- Send or receive routes that meet the matching rules.
- A routing protocol such as the Routing Information Protocol (RIP) needs to import the routes discovered by other routing protocols to enrich its routing information. When importing routes from other routing protocols, the router may import certain routes that meet the matching rules, and set attributes of the routes imported to meet the requirement.

To implement a routing policy, you must:

- Define a set of matching rules and setting rules. The policy is applied to the routing information to meet the requirements of the matching rules.
- Apply the matching rules to the routing policies for route advertisement, reception, and import.

#### Differences Between Routing Policy and PBR

Different from the forwarding by searching the Forwarding information base (FIB) according to the destination address of a packet, Policy-based routing (PBR) is a route selection mechanism based on policies set by users. PBR supports the information based on the source address and the length of a packet. PBR selects routes according to the set policy. PBR can be applicable to security and load balancing.

Routing policies and PBR are different concepts. [Table 10-1](#) shows the differences between the two concepts.

**Table 10-1** Differences between routing policy and PBR

| Routing policy                                                                | Policy-based routing                                                                                                               |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Forwards packets based on the destination address in the routing table.       | Forwards packets based on the policy. If packets fail to be forwarded, the device forwards packets by searching the routing table. |
| Based on the control plane and serves the routing protocol and routing table. | Based on forwarding plane and serves for the forwarding policy.                                                                    |

| Routing policy                     | Policy-based routing                                                                                  |
|------------------------------------|-------------------------------------------------------------------------------------------------------|
| Combines with the routing protocol | Needs to be manually configured hop by hop to ensure that the packet is forwarded through the policy. |

## 10.1.2 Routing Policy Features Supported by the NE80E/40E

When configuring routing policies, you can use these filters: ACL, IP prefix list, AS-Path filter, community filter, extended community filter, RD filter, and Route-Policy.

### Filters

The NE80E/40E provides several types of filters for routing protocols, such as Access Control Lists (ACLs), IP prefix lists, AS-Path filters, community filters, extended community filters (Extcommunity-filters), and Route-Policies.

- **ACL**

The ACL consists of the ACL for IPv4 packets and the ACL for IPv6 packets. According to the usage, ACLs are classified into three types, that is, interface-based ACLs, basic ACLs, and advanced ACLs. When defining an ACL, you can specify the IP address and subnet range to match the destination network segment address or the next hop address of a route.

For details of the ACL configuration, refer to the *HUAWEI NetEngine80E/40E Router Configuration Guide - IP Services*.
- **IP-Prefix List**

The IP-prefix list consists of IPv4 prefix list and IPv6 prefix list. The implementation of the IP-prefix is flexible.

An IP-prefix list is identified by its list name. Each prefix list includes multiple entries. Each entry can independently specify the matching range in the form of the network prefix. The matching range is identified by an index number that designates the sequence of the matching check.

During the matching, the router checks entries identified by index numbers in an ascending order. When a route matches an entry, the system does not search the next entry matching the route. For the detailed configuration, refer to [Configuring the IP-Prefix List](#).
- **AS-Path Filter**

Border Gateway Protocol (BGP) routing information packet includes an autonomous system (AS) path domain. The AS-Path filter specifies the matching condition for the AS path domain.

For the configuration of AS-Path filter, refer to [BGP Configuration](#).
- **Community Filter**

The community filter is used only in BGP. The BGP routing information includes a community attribute domain. It is used to identify a community. The community filter specifies the matching condition for the community attribute domain.

For the configuration of community filter, refer to [BGP Configuration](#).
- **Extcommunity-Filter**

The Extcommunity-filter is used only in BGP. The extended community of BGP supports only the Router-Target (RT) extended community of Virtual Private Network (VPN). The Extcommunity-filter specifies matching rules for the extended community attribute.

For the configuration of excommunity-filter, refer to [BGP Configuration](#).

- RD Filter

Through Route Distinguisher (RD), the VPN instance implements the independency of address space and identifies the IPv4 and IPv6 prefixes of the same address space. The RD attribute filter specifies matching conditions for different RDs.

For the configuration of the RD attribute filter, refer to the HUAWEI NetEngine80E/40E Router *Configuration Guide - VPN*.

- Route-Policy

The Route-Policy is a complex filter. A Route-Policy is used to match certain route attributes, and to change the route attributes when certain matching rules are met. The Route-Policy uses the preceding filters to define its filtering rules.

A Route-Policy consists of multiple nodes. The relationship between the nodes is "OR". The system checks the nodes in the routing policy, the node with the smaller value of node is checked first. When the route matches a node in the routing policy, it passes the Route-Policy and the system does not search the next matching node.

Each node comprises a set of **if-match** and **apply** clauses. The **if-match** clauses define the matching rules. The matching objects are certain route attributes. The relationship between **if-match** clauses in a node is "AND". A matching succeeds only when all the matching rules specified by the **if-match** clauses in the same node are matched.

The **apply** clauses specify actions. When a route matches a rule, the **apply** clause sets certain attributes for the route. For the detailed configuration, refer to [Configuring the Route-Policy](#).

## Application of the Routing Policy

The routing policy is used in the following situations:

- Import routes that meet the matching rules through filters when a routing protocol imports routes discovered by other protocols.
- Filter routes that a routing protocol advertises or receives. Only the routes that meet the matching rules are received or advertised.

For the configuration of routing policy applications, refer to the related routing protocol configurations.

 **NOTE**

After the routing policy changes, RM immediately notifies various protocols for processing by default.

## 10.2 Configuring the IP-Prefix List

An IP prefix list filters routes according to the destination addresses of the routes.

### 10.2.1 Establishing the Configuration Task

Before configuring the IP prefix list, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

## Applicable Environment

Before applying a routing policy, you should set the matching rules, that is, filters. Compared with an ACL, an IP prefix list is more flexible. When the IP prefix list is used to filter routes, it matches the destination address of a route.

## Pre-configuration Tasks

None.

## Data Preparation

To configure an IP prefix list, you need the following data.

| No. | Data                   |
|-----|------------------------|
| 1   | Name of IP prefix list |
| 2   | Matched address range  |

## 10.2.2 Configuring an IPv4 Prefix List

An IP prefix list filters routes according to IP address prefixes. An IP address prefix is defined by the IP address and mask length.

### Context

Do as follows on the router to which the IP prefix list is applied:

### Procedure

#### Step 1 Run:

```
system-view
```

The system view is displayed.

#### Step 2 Run:

```
ip ip-prefix ip-prefix-name [index index-number] { permit | deny } ip-address
mask-length [greater-equal greater-equal-value] [less-equal less-equal-value]
```

An IPv4 prefix list is configured.

The range of the mask length can be specified as  $mask-length \leq greater-equal-value \leq less-equal-value \leq 32$ . If only **greater-equal** is specified, the range of the prefix is [*greater-equal-value*, 32]; if only **less-equal** is specified, the range of the prefix is [*mask-length*, *less-equal-value*].

An IPv4 prefix list is identified by its list name. Each prefix list contains multiple entries. Each entry can independently specify the matching range in the form of the network prefix and identify it with an index number. For example, the following shows an IPv4 prefix list named **abcd**:

```

ip ip-prefix abcd index 10 permit 1.0.0.0 8
ip ip-prefix abcd index 20 permit 2.0.0.0 8
```

During the matching, the system checks the entries identified by the index numbers in an ascending order. When a route matches an entry, it does not match other entries.

In the NE80E/40E and NE80E/40EHI, all unmatched routes cannot pass the filtering list. If all entries are in **deny** mode, all routes are filtered. It is recommended that you define a **permit 0.0.0.0 0 less-equal 32** entry after multiple entries in **deny** mode, thus allowing all the other IPv4 routes to pass the IP prefix list.

 **NOTE**

If more than one IP-prefix entry is defined, at least one entry should be in the **permit** mode.

----End

## 10.2.3 Configuring an IPv6 Prefix List

An IPv6 prefix list filters routes according to IPv6 address prefixes. An IPv6 address prefix is defined by the IPv6 address and mask length.

### Context

Do as follows on the router to which the IP prefix list is applied:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
ip ipv6-prefix ipv6-prefix-name [index index-number] { permit | deny } ipv6-
address prefix-length [greater-equal greater-equal-value] [less-equal less-
equal-value]
```

An IPv6 prefix list is configured.

An IPv6 prefix list is identified by its list name. Each prefix list can include multiple entries. Each entry can independently specify the matching range in the form of the network prefix and identify it with an index number. For example, the following shows an IPv6 prefix list named **abcd**:

```

ip ipv6-prefix abcd index 10 permit 1:: 64
ip ipv6-prefix abcd index 20 permit 2:: 64
```

During the matching, the system checks the entries identified by the index numbers in an ascending order. When a route matches an entry, it does not match other entries.

In NE80E/40E, all unmatched routes are filtered. If all entries are in **deny** mode, all routes are filtered. It is recommended that you define a **permit :: 0 less-equal 128** after multiple entries in **deny** mode, thus allowing all the other IPv6 routes to pass the IP prefix list.

----End

## 10.2.4 Checking the Configuration

After an IP prefix list is configured, you can check information about the IP prefix list.

## Prerequisite

The configurations of the IP-Prefix list are complete.

## Procedure

- Run the **display ip ip-prefix** [ *ip-prefix-name* ] command to check information about the IPv4 prefix list.
- Run the **display ip ipv6-prefix** [ *ipv6-prefix-name* ] command to check information about the IPv6 prefix list.

---End

## Example

Run the **display ip ip-prefix p1** command. You can view information about the prefix list named **p1**.

```
<HUAWEI> display ip ip-prefix p1
Prefix-list p1
Permitted 5
Denied 2
index: 10 permit 192.168.0.0/16 ge 17 le 18
```

# 10.3 Configuring the Route-Policy

Each node of a Route-Policy consists of a set of if-match and apply clauses.

## 10.3.1 Establishing the Configuration Task

Before configuring the Route-Policy, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

### Applicable Environment

A Route-Policy is used to match routes or certain route attributes, and to change these attributes when the matching rules are met.

A Route-Policy consists of multiple nodes. Each node is classified into the following clauses:

- **if-match** clauses: define the matching rules. The matching rules are used by the routes that match the Route-Policy. The matching objects refer to some attributes of the route.
- **apply** clauses: specify actions, that is, configuration commands used to modify certain attributes.

For more information about Route-Policy, refer to the *HUAWEI NetEngine80E/40E Router Feature Description - IP Routing*.

### Pre-configuration Tasks

To configure a Route-Policy, complete the following tasks:

- [10.2 Configuring the IP-Prefix List](#)
- Configuring routing protocols

## Data Preparation

To configure a Route-Policy, you need the following data.

| No. | Data                                     |
|-----|------------------------------------------|
| 1   | Name and node number of the Route-Policy |
| 2   | Matching rule                            |
| 3   | Route attributes to be modified          |

### 10.3.2 Creating a Route-Policy

By applying a Route-Policy, you can set attributes for the imported routes according to networking requirements.

#### Context

Do as follows on the router to which the Route-Policy is applied:

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
route-policy route-policy-name { permit | deny } node node
```

A node of the Route-Policy is created and the Route-Policy view is displayed.

- The parameter **permit** specifies a node in a Route-Policy in **permit** mode. If a route matches the node, the router performs actions defined by the **apply** clauses and the matching is complete. Otherwise, the route continues to match the next node.
- The parameter **deny** specifies a node in a Route-Policy in **deny** mode. In **deny** mode, the **apply** clauses are not used. If a route entry matches all the **if-match** clauses of the node, the route is denied by the node and the next node is not matched. If the entry does not match all the clauses, the next node is matched.

 **NOTE**

In the NE80E/40E and NE80E/40EHI, by default, the unmatched routes are denied. If multiple nodes are defined in a Route-Policy, at least one of them should be in **permit** mode.

When the parameter **route-policy** is used to filter routes, note the following:

- If a route does not match any node, it is denied by the Route-Policy.
- If all the nodes in the routing policy are in **deny** mode, all the routes are denied by the Route-Policy.

When a Route-Policy is used to filter the routing information, the node with the smaller value of *node* is tested first.

**Step 3** (Optional) Run:

```
description text
```

The description of the routing policy is configured.

----End

### 10.3.3 (Optional) Configuring the If-Match Clause

The **if-match** clauses define the rules for matching certain route attributes.

#### Context

Do as follows on the router to which the Route-Policy is applied:

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
route-policy route-policy-name { permit | deny } node node
```

The Route-Policy view is displayed.

**Step 3** Run the following command as required:

## ● Run:

```
if-match acl { acl-number | acl-name }
```

The ACL is configured to match the routes.

## ● Run:

```
if-match cost cost
```

The cost is set to match the routes.

## ● Run:

```
if-match interface interface-type interface-number
```

The outbound interface is configured to match the routes.

## ● Run:

```
if-match ip { next-hop | route-source } { acl { acl-number | acl-name } | ip-prefix ip-prefix-name }
```

The next hop or the source address is configured to match the routes.

## ● Run:

```
if-match ip-prefix ip-prefix-name
```

The IP prefix list is configured to match the routes.

 **NOTE**

For the same Route-Policy node, you cannot run the **if-match acl** command and the **if-match ip-prefix** command at the same time. This is because the latest configuration overrides the previous configuration.

## ● Run:

```
if-match ipv6 { address | next-hop | route-source } prefix-list ipv6-prefix-name
```



The next hop or the source address is configured to match the routes.

- Perform as follows to match the type of the route:

– Run:

```
if-match route-type { external-type1 | external-type1or2 | external-type2 |
internal | nssa-external-type1 | nssa-external-type1or2 | nssa-external-
type2 }
```

The route type, OSPF in this case, is set to match the routes.

– Run:

```
if-match route-type { is-is-level-1 | is-is-level-2 }
```

The route type, IS-IS in this case, is set to match the routes.

- Run:

```
if-match tag tag
```

The tag is set to match the routes.

The commands in Step 3 can be used regardless of the order. A node can have multiple or no **if-match** clauses.

#### NOTE

- For the same node in a route-policy, the relationship between **if-match** clauses is "AND". The route must meet all the matching rules before the actions defined by the **apply** clauses are performed. In the **if-match route-type** and **if-match interface** commands, the relationship between the **if-match** clauses is "OR". In other commands, the relationship between **if-match** clauses is "AND".
- If no **if-match** clause is specified, all the routes meet the matching rules.

----End

## 10.3.4 (Optional) Configuring the Apply Clause

The **apply** clauses specify actions to set certain route attributes.

### Context

Do as follows on the router to which the Route-Policy is applied:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
route-policy route-policy-name { permit | deny } node node
```

The Route-Policy view is displayed.

**Step 3** Run the following command as required:

- Run:

```
apply backup-interface interface-type interface-number
```

The backup outbound interface is set.

- Run:

```
apply backup-nexthop { ip-address | auto }
```

The backup next hop is set.

- Run:

```
apply cost [+ | -] cost
```

The cost of the route is set.

- Set the cost type of the route.

- Run the **apply cost-type** { **external** | **internal** } command to set the cost type of an IS-IS route.
- Run the **apply cost-type** { **type-1** | **type-2** } command to set the cost type of an OSPF route.

- Run:

```
apply ip-address next-hop { peer-address | ipv4-address }
```

The next hop address of the IPv4 route is set.

- Run:

```
apply ipv6 next-hop { peer-address | ipv6-address }
```

The next hop address of the IPv6 route is set.

- Run:

```
apply isis { level-1 | level-1-2 | level-2 }
```

The route level of IS-IS is set.

- Run:

```
apply ospf { backbone | stub-area }
```

The area of the OSPF route is set.

- Run:

```
apply preference preference
```

The preference of the routing protocol is set.

- Run:

```
apply tag tag
```

The tag of the route is set.

The commands in Step 3 can be used regardless of the order.

----End

## 10.3.5 Checking the Configuration

After the Route-Policy is configured, you can check information about the Route-Policy.

### Prerequisite

The configurations of the Route-Policy are complete.

### Procedure

- Run the **display route-policy** [ *route-policy-name* ] command to check the Route-Policy.

----End

## 10.4 Applying Filters to Received Routes

By applying the related filters of routing policies to routing protocols, you can filter the received routes.

### 10.4.1 Establishing the Configuration Task

Before applying filters to the received routes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

After defining the filters including the IP prefix list, ACL, and Route-Policy related to the routing policy, you need to import the filters to the protocols. The routing filters are used in the following situations:

- Filtering the received routes

Use the **filter-policy** command in the protocol view and apply an ACL or an IP prefix list to filter the received routes. Only the routes that meet the matching rules are received.

The **filter-policy import** command is used to filter the received routes.

For the distance vector (DV) protocol and the link state protocol, the procedures are different after the **filter-policy** command is run.

- DV protocol

A DV protocol generates routes based on the routing table. The filters affect the routes received from the neighbor and the routes to be sent to the neighbor.

- Link state protocol

A link state protocol generates routes based on the Link State Database. The **filter-policy** command does not affect the Link State Advertisements (LSAs) or the integrity of the LSDB. Therefore, the effect on the commands of **filter-policy import** and **filter-policy export** are different.

The **filter-policy import** command identifies the route that is added to a local routing table from a protocol routing table only. That is, this command affects the local routing table only, but does not affect the protocol routing table.

#### NOTE

- BGP has powerful filtering functions. For details of BGP configuration, refer to [BGP Configuration](#).
- You can run the **filter-policy** command and the **import-route** command with different parameters for RIP, OSPF, IS-IS, and BGP. For details, refer to related configurations.

#### Pre-configuration Tasks

Before applying filters to received routes, complete the following tasks:

- [10.2 Configuring the IP-Prefix List](#)
- Configuring an ACL
- [10.3 Configuring the Route-Policy](#)

## Data Preparation

To apply filters to received routes, you need the following data.

| No. | Data                                     |
|-----|------------------------------------------|
| 1   | Name of the IP prefix list               |
| 2   | Name of the ACL                          |
| 3   | Name of the Route-Policy and node number |

### 10.4.2 Filtering Routes Received by RIP

By applying filters, you can control the receiving of RIP routes.

#### Context

Do as follows on the router that runs RIP:

#### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
rip [process-id]
```

A RIP process is enabled and the RIP view is displayed.

**Step 3** Run either of the following commands as required:

- **filter-policy** { *acl-number* | **acl-name** *acl-name* } **import** [ *interface-type interface-number* ]
- **filter-policy gateway** *ip-prefix-name* **import**
- **filter-policy ip-prefix** *ip-prefix-name* [ **gateway** *ip-prefix-name* ] **import** [ *interface-type interface-number* ]

The filtering policy is configured for routes received by RIP.

----End

### 10.4.3 Filtering Routes Received by OSPF

By applying filters, you can control the receiving of OSPF routes.

#### Context

Do as follows on the router that runs OSPF:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
ospf [process-id]
```

An OSPF process is enabled and the OSPF view is displayed.

**Step 3** Run:

```
filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name } import
```

The filtering policy is configured for routes received by OSPF.

----End

## 10.4.4 Filtering Routes Received by IS-IS

By applying filters, you can control the receiving of IS-IS routes.

### Context

Do as follows on the router that runs IS-IS:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis [process-id]
```

An IS-IS process is enabled and the IS-IS view is displayed.

**Step 3** Run:

```
filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name | route-policy route-policy-name } import
```

The filtering policy is configured for routes received by IS-IS.

----End

## 10.4.5 Filtering Routes Received by BGP

By applying filters, you can control the receiving of BGP routes.

### Procedure

- Filtering the Received Routes

Do as follows on the router that runs BGP:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name } import
```

The filtering policy is configured for routes received by BGP.

- Filtering Routes Received from the Peers

Do as follows on the router that runs BGP:

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
bgp as-number
```

The BGP view is displayed.

3. Run:

```
ipv4-family unicast
```

The IPv4 unicast address family view is displayed.

4. Run:

```
peer { group-name | ipv4-address } filter-policy { acl-number | acl-name acl-name } import
```

The filtering policy is configured for routes received from peers.

----End

## 10.4.6 Checking the Configuration

After filters are applied to the received routes, you can check information about the routing table of each protocol.

### Prerequisite

The configurations of applying filters to received routes are complete.

### Procedure

- Run the **display rip route** *process-id* **route** command to check information about the RIP routing table.
- Run the **display ospf** [*process-id*] **routing** command to check information about the OSPF routing table.
- Run the **display isis** [*process-id*] **route** command to check information about the ISIS routing table.
- Run the **display bgp routing-table** command to check information about the BGP routing table.
- Run the **display ip routing-table** command to check information about the public IPv4 routing table.

Run the **display ip routing-table** command on the neighboring router. You can find that the routes that meet the matching rules set on the neighboring router are filtered or the actions defined by the **apply** clauses are performed.

----End

## 10.5 Applying Filters to Advertised Routes

By applying the related filters of routing policies to routing protocols, you can filter advertised routes.

### 10.5.1 Establishing the Configuration Task

Before applying filters to advertised routes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

After defining the filters including the IP prefix list, ACL, and Route-Policy related to the routing policy, you need to import the filters to the protocols.

- Filtering the advertised routes

Use the **filter-policy** command in the protocol view and import an ACL or an IP prefix list to filter the advertised routes. Only the routes that meet the matching rules are advertised.

The **filter-policy export** command is used to filter the advertised routes.

For the DV protocol and the link state protocol, the procedures are different after the **filter-policy** command is run.

- DV protocol

A DV protocol generates routes based on the routing table. The filters affect the route received from the neighbor and the route to be sent to the neighbor.

- Link state protocol

A link state protocol generates routes based on LSDBs. The **filter-policy** does not affect LSAs or the integrity of LSDBs. The commands of **filter-policy import** and **filter-policy export** are different.

To advertise routes, you can run the **filter-policy export** command to advertise routes imported by protocols, such as routes imported by RIP. Only the LSAs or Link Switched Paths (LSPs) that are imported by using the **import** command are added to the LSDB. This does not affect LSAs advertised by other routers.

 **NOTE**

- BGP has powerful filtering function. For details of BGP configuration, refer to [BGP Configuration](#).
- You can run the **filter-policy** command and the **import-route** command with different parameters for RIP, OSPF, IS-IS, and BGP. For details, refer to related configurations.

#### Pre-configuration Tasks

Before applying filters to advertised routes, complete the following tasks:

- [10.2 Configuring the IP-Prefix List](#)

- Configuring an ACL
- **10.3 Configuring the Route-Policy**

## Data Preparation

To apply filters to advertised routes, you need the following data.

| No. | Data                                     |
|-----|------------------------------------------|
| 1   | Name of the IP prefix list               |
| 2   | Name of the ACL                          |
| 3   | Name of the Route-Policy and node number |

## 10.5.2 Filtering Routes Advertised by RIP

By applying filters, you can control the advertisement of RIP routes.

### Context

Do as follows on the router that runs RIP:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
rip [process-id]
```

A RIP process is enabled and the RIP view is displayed.

**Step 3** Run

```
filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name } export
[protocol [process-id] | interface-type interface-number]
```

The filtering policy is configured for routes advertised by RIP.

----End

## 10.5.3 Filtering Routes Advertised by OSPF

By applying filters, you can control the advertisement of OSPF routes.

### Context

Do as follows on the router that runs OSPF:



## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
ospf [process-id]
```

An OSPF process is enabled and the OSPF view is displayed.

**Step 3** Run:

```
filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name } export
[protocol [process-id]]
```

The filtering policy is configured for routes advertised by OSPF.

----End

## 10.5.4 Filtering Routes Advertised by IS-IS

By applying filters, you can control the advertisement of IS-IS routes.

### Context

Do as follows on the router that runs IS-IS:

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis [process-id]
```

An IS-IS process is enabled and the IS-IS view is displayed.

**Step 3** Run:

```
filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name | route-
policy route-policy-name } export [protocol [process-id]]
```

The filtering policy is configured for routes advertised by IS-IS.

----End

## 10.5.5 Filtering Routes Advertised by BGP

By applying filters, you can control the advertisement of BGP routes.

### Procedure

- Filtering the Advertised Routes

Do as follows on the router that runs BGP:

1. Run:  
`system-view`  
The system view is displayed.
2. Run:  
`bgp as-number`  
The BGP view is displayed.
3. Run:  
`ipv4-family unicast`  
The IPv4 unicast address family view is displayed.
4. Run:  
`filter-policy { acl-number | acl-name acl-name | ip-prefix ip-prefix-name } export [ protocol [ process-id ] ]`

The filtering policy is configured for routes advertised by BGP.

For the routes imported by BGP, only the routes that meet matching rules can be added to the BGP local routing table and advertised to the BGP peers.

- If *protocol* is specified, only the routes of the specified protocol are filtered.
- If the parameter is not specified, all the routes advertised by BGP are filtered, including the imported routes and the local routes advertised through the `network` command.

 **NOTE**

The `filter-policy export` command of different protocols have different affect ranges on routes advertisement:

- For the link state protocol, only the routes imported are filtered.
  - For the DV protocol, the routes imported and the routes discovered by the protocols are filtered.
- Filtering Routes Advertised to the Peers

Do as follows on the router that runs BGP:

1. Run:  
`system-view`  
The system view is displayed.
2. Run:  
`bgp as-number`  
The BGP view is displayed.
3. Run:  
`ipv4-family unicast`  
The IPv4 unicast address family view is displayed.
4. Run:  
`peer { group-name | ipv4-address } filter-policy { acl-number | acl-name acl-name } export`

The filtering policy is configured for routes advertised to the peers.

----End

## 10.5.6 Checking the Configuration

After filters are applied to advertised routes, you can check information about the routing table of each protocol.

### Prerequisite

The configurations of applying filters to advertised routes are complete.

### Procedure

- Run the **display rip** *process-id* **route** command to check information about the RIP routing table.
- Run the **display ospf** [*process-id*] **routing** command to check information about the OSPF routing table.
- Run the **display isis** [*process-id*] **route** command to check information about the ISIS routing table.
- Run the **display bgp routing-table** command to check information about the BGP routing table.
- Run the **display ip routing-table** command to check information about the public IPv4 routing table.

Run the **display ip routing-table** command on the neighboring router. You can find that the routes that meets the matching rules set on the neighboring router are filtered or the actions defined by the **apply** clauses are performed.

----End

## 10.6 Applying Filters to Imported Routes

By applying the related filters of routing policies to routing protocols, you can filter imported routes.

### 10.6.1 Establishing the Configuration Task

Before applying filters to imported routes, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

After defining the filters including the IP prefix list, ACL, and Route-Policy related to the routing policy, you need to import the filters to the protocols.

- Applying the policy to import external routes
  - Use the **import-route** command in the protocol view. Import the required external routes to the protocols and apply a Route-Policy to the imported routes.
  - After the external routes are imported, run the **filter-policy export** to filter the routes. Only the routes that meet the matching rules are advertised.

 **NOTE**

- BGP has powerful filtering functions. For details of BGP configuration, refer to [BGP Configuration](#).
- You can run the **filter-policy** command and the **import-route** command with different parameters for RIP, OSPF, IS-IS, and BGP. For details, refer to related configurations.

## Pre-configuration Tasks

Before applying filters to imported routes, complete the following tasks:

- [Configuring the IP-Prefix List](#)
- Configuring an ACL
- [Configuring the Route-Policy](#)

## Data Preparation

To apply filters to imported routes, you need the following data.

| No. | Data                                     |
|-----|------------------------------------------|
| 1   | Name of the IP prefix list               |
| 2   | Name of the ACL                          |
| 3   | Name of the Route-Policy and node number |

## 10.6.2 Applying Route-Policy to Routes Imported by RIP

By applying filters, you can control the import of RIP routes.

### Context

Do as follows on the router that runs RIP:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
rip [process-id]
```

A RIP routing process is enabled and the RIP view is displayed.

**Step 3** Run:

```
import-route bgp [cost { cost | transparent } | route-policy route-policy-name]
* or import-route { { static | direct | unr } | { { rip | ospf | isis } [process-
id] } } [cost cost | route-policy route-policy-name] *
```

The external routes are imported.

----End

## 10.6.3 Applying Route-Policy to Routes Imported by OSPF

By applying filters, you can control the import of OSPF routes.

### Context

Do as follows on the router that runs OSPF:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
ospf [process-id]
```

An OSPF process is enabled and the OSPF view is displayed.

**Step 3** Run:

```
import-route { limit limit-number | protocol [process-id] [cost cost | route-policy route-policy-name | tag tag | type type] * }
```

The external routes are imported.

---End

## 10.6.4 Applying Route-Policy to Routes Imported by IS-IS

By applying filters, you can control the import of IS-IS routes.

### Context

Do as follows on the router that runs IS-IS:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
isis [process-id]
```

An IS-IS process is enabled and the IS-IS view is displayed.

**Step 3** Configuring IS-IS to Import External Routes

- If you want to set the cost for the imported route, you can run the **import-route protocol [ process-id ] [ cost-type { external | internal } | cost cost | tag tag | route-policy route-policy-name | [ level-1 | level-2 | level-1-2 ] ] \*** command to import the external routes.

- If you want to keep the original cost for the imported route, you can run the **import-route** { { **rip** | **isis** | **ospf** } [ *process-id* ] | **bgp** } **inherit-cost** [ **tag** *tag* | **route-policy** *route-policy-name* ] [ **level-1** | **level-2** | **level-1-2** ] ] \* command to import the external routes.

----End

## 10.6.5 Applying Route-Policy to Routes Imported by BGP

By applying filters, you can control the import of BGP routes.

### Context

Do as follows on the router that runs BGP:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
bgp as-number
```

The BGP view is displayed.

**Step 3** Run:

```
ipv4-family unicast
```

The IPv4 unicast address family view is displayed.

**Step 4** Run:

```
import-route protocol [process-id] [med med | route-policy route-policy-name] *
```

The external routes are imported.

----End

## 10.6.6 Checking the Configuration

After filters are applied to imported routes, you can check information about the routing table of each protocol.

### Prerequisite

The configurations of applying filters to imported routes are complete.

### Procedure

- Run the **display rip** *process-id* **route** command to check information about the RIP routing table.
- Run the **display ospf** [ *process-id* ] **routing** command to check information about the OSPF routing table.
- Run the **display isis** [ *process-id* ] **route** command to check information about the ISIS routing table.

- Run the **display bgp routing-table** command to check information about the BGP routing table.
- Run the **display ip routing-table** command to check information about the public IPv4 routing table.

Run the **display ip routing-table** command on the neighboring router. You can find that the routes that meet the matching rules on the neighboring router are filtered or the actions defined by the **apply** clauses are performed.

----End

## 10.7 Controlling the Valid Time of the Routing policy

To ensure network stability, you need to configure the delay for applying a routing policy when modifying the routing policy.

### 10.7.1 Establishing the Configuration Task

Before configuring the delay for applying a routing policy, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

#### Applicable Environment

In actual applications, when the configurations of multiple cooperative routing policies change, the Routing Management Module (RM) immediately notifies related protocols to apply a new routing policy, after the configuration of the routing policy is complete. An incomplete routing policy causes route flapping, instability of the network, and a waste of time during packet processing.

The NE80E/40E provides the following rules for processing changes of a routing policy:

- By default, the RM immediately notifies the protocol of applying the new policy when the routing policy changes.
- If the valid time of the routing policy is configured, when the commands used to configure the routing policy change, the RM does not notify various protocols of immediately processing the changes. Instead, the RM waits for a certain period, and then notifies various protocols of applying the changed routing policy.
- If the routing policy changes again during the waiting time, the RM resets the timer.

You can run related commands to set the waiting time as required.

#### Pre-configuration Tasks

None.

#### Data Preparation

To configure the valid time of the routing policy, you need the following data.

| No. | Data                                  |
|-----|---------------------------------------|
| 1   | Delay for applying the routing policy |

## 10.7.2 Configuring the Delay for Applying the Routing Policy

When modifying multiple cooperative routing policies, you need to configure the delay for applying a routing policy.

### Context

Do as follows on the router on which the delay for applying routing policy needs to be changed:

### Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Run:

```
route-policy-change notify-delay delay-time
```

The delay for applying the routing policy is set.

The delay ranges from 1 to 180, in seconds.

By default, the RM immediately notifies the protocol of applying the new policy when the routing policy changes.

**Step 3** Run:

```
quit
```

Back to the user view.

**Step 4** (Optional) Run:

```
refresh bgp all { export | import }
```

BGP is configured to apply the new routing policy.

After the command is used, the effect of the policy filtering can be found immediately. You can run the command to configure BGP to immediately apply new policies.

The policies affected by the timer are ACLs, IP prefix lists, AS-Path filters, community filters, extended community filters, RD filters, and Route-Policies.

---End

## 10.7.3 Checking the Configuration

After the delay for applying a routing policy is configured, you can check the configuration.

### Prerequisite

The configurations of controlling the valid time of the routing policy are complete.



## Procedure

- Run the **display current-configuration | include notify-delay** command to check the delay for applying the routing policy.

---End

## Example

Run the **display current-configuration** command. You can find the delay for applying the routing policy. For example:

```
<HUAWEI> display current-configuration | include notify-delay
route-policy-change notify-delay 10
```

# 10.8 Maintaining the Routing Policy

Maintaining routing policies involves clearing the statistics of the IP prefix list and debugging routing policies.

## Context



### CAUTION

The statistics of IP prefix lists cannot be restored after you clear it. So, confirm the action before you use the command.

---

By default, the statistics of IP prefix lists are not cleared.

## Procedure

- Run **reset ip ip-prefix** [ *ip-prefix-name* ] command in the user view to clear the IPv4 prefix list statistics.
- Run **reset ip ipv6-prefix** [ *ipv6-prefix-name* ] command in the user view to clear the IPv6 prefix list statistics.

---End

# 10.9 Configuration Examples

Routing policy configuration examples explain networking requirements, networking diagram, configuration notes, configuration roadmap, and configuration procedure.



### NOTE

This document takes interface numbers and link types of the NE40E-X8 as an example. In working situations, the actual interface numbers and link types may be different from those used in this document.

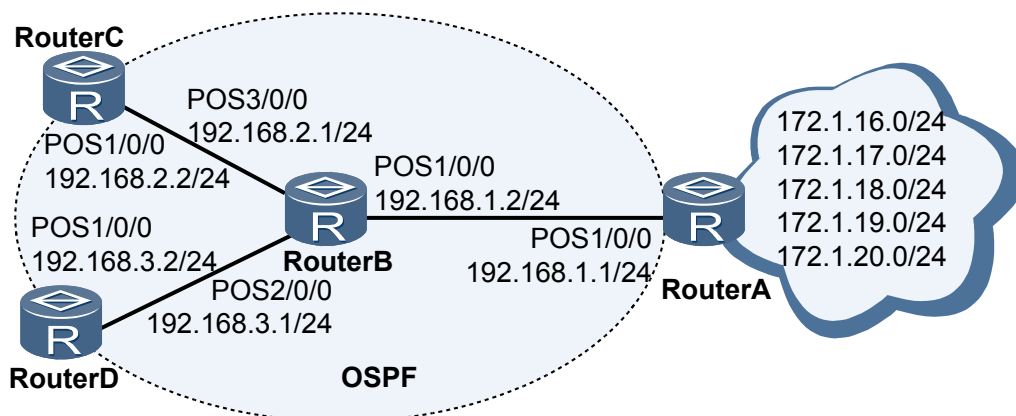
## 10.9.1 Example for Filtering Received and Advertised Routes

Filters can be applied to the received and advertised routes according to networking requirements.

## Networking Requirements

As shown in **Figure 10-1**, in the network that runs OSPF, Router A receives routes from the network, and provides some of these routes for Router B. Router A is required to provide only 172.1.17.0/24, 172.1.18.0/24 and 172.1.19.0/24 for Router B. Router C is required to receive only 172.1.18.0/24. Router D receives all the routes provided by Router B.

**Figure 10-1** Networking diagram for filtering received and advertised routes



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic OSPF functions on Router A, Router B, Router C, and Router D.
2. Configure static routes on Router A, and import these routes to OSPF.
3. Configure the policy for advertising routes on Router A, and check the filtering result on Router B.
4. Configure the policy for receiving routes on Router C, and check the filtering result on Router C.

## Data Preparation

To complete the configuration, you need the following data:

- Five static routes imported by Router A.
- Router A, Router B, Router C, and Router D that reside in Area 0, that is the backbone area.
- Name of the IP prefix list and route to be filtered.

## Procedure

**Step 1** Assign an IP address to each interface.

The configuration details are not mentioned here.

**Step 2** Configure basic OSPF functions.

# Configure Router A.

```
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

# Configure Router B.

```
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
```

# Configure Router C.

```
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

# Configure Router D.

```
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
```

### Step 3 Configure five static routes on Router A and import these routes to OSPF.

```
[RouterA] ip route-static 172.1.16.0 24 NULL 0
[RouterA] ip route-static 172.1.17.0 24 NULL 0
[RouterA] ip route-static 172.1.18.0 24 NULL 0
[RouterA] ip route-static 172.1.19.0 24 NULL 0
[RouterA] ip route-static 172.1.20.0 24 NULL 0
[RouterA] ospf
[RouterA-ospf-1] import-route static
[RouterA-ospf-1] quit
```

# Check the IP routing table on Router B. You can view that the five static routes are imported to OSPF.

```
[RouterB] display ip routing-table
Route Flags: R - relay, D - download to fib

Routing Tables: Public
 Destinations : 16 Routes : 16
Destination/Mask Proto Pre Cost Flags NextHop Interface
127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
172.1.16.0/24 O_ASE 150 1 D 192.168.1.1 Pos1/0/0
172.1.17.0/24 O_ASE 150 1 D 192.168.1.1 Pos1/0/0
172.1.18.0/24 O_ASE 150 1 D 192.168.1.1 Pos1/0/0
172.1.19.0/24 O_ASE 150 1 D 192.168.1.1 Pos1/0/0
172.1.20.0/24 O_ASE 150 1 D 192.168.1.1 Pos1/0/0
192.168.1.0/24 Direct 0 0 D 192.168.1.2 Pos1/0/0
192.168.1.1/32 Direct 0 0 D 192.168.1.1 Pos1/0/0
192.168.1.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0
192.168.2.0/24 Direct 0 0 D 192.168.2.1 Pos3/0/0
192.168.2.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
192.168.2.2/32 Direct 0 0 D 192.168.2.2 Pos3/0/0
192.168.3.0/24 Direct 0 0 D 192.168.3.1 Pos2/0/0
192.168.3.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
192.168.3.2/32 Direct 0 0 D 192.168.3.2 Pos2/0/0
```

### Step 4 Configure the policy for advertising routes.

# Configure the IP prefix list named **a2b** on Router A.

```
[RouterA] ip ip-prefix a2b index 10 permit 172.1.17.0 24
[RouterA] ip ip-prefix a2b index 20 permit 172.1.18.0 24
[RouterA] ip ip-prefix a2b index 30 permit 172.1.19.0 24
```

# Configure the policy for advertising routes on Router A and use the IP prefix list named **a2b** to filter routes.

```
[RouterA] ospf
[RouterA-ospf-1] filter-policy ip-prefix a2b export static
```

# Check IP routing table on Router B, and you can view the three routes received by Router B from **a2b**.

```
[RouterB] display ip routing-table
Route Flags: R - relay, D - download to fib

Routing Tables: Public
 Destinations : 14 Routes : 14
Destination/Mask Proto Pre Cost Flags NextHop Interface
 127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
 127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
 172.1.17.0/24 O_ASE 150 1 D 192.168.1.1 Pos1/0/0
 172.1.18.0/24 O_ASE 150 1 D 192.168.1.1 Pos1/0/0
 172.1.19.0/24 O_ASE 150 1 D 192.168.1.1 Pos1/0/0
 192.168.1.0/24 Direct 0 0 D 192.168.1.2 Pos1/0/0
 192.168.1.1/32 Direct 0 0 D 192.168.1.1 Pos1/0/0
 192.168.1.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0
 192.168.2.0/24 Direct 0 0 D 192.168.2.1 Pos3/0/0
 192.168.2.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
 192.168.2.2/32 Direct 0 0 D 192.168.2.2 Pos3/0/0
 192.168.3.0/24 Direct 0 0 D 192.168.3.1 Pos2/0/0
 192.168.3.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
 192.168.3.2/32 Direct 0 0 D 192.168.3.2 Pos2/0/0
```

### Step 5 Configure the policy for receiving routes.

# Configure the IP prefix list named **in** on Router C.

```
[RouterC] ip ip-prefix in index 10 permit 172.1.18.0 24
```

# Configure the policy for receiving routes on Router C, and use IP prefix list named **in** to filter routes.

```
[RouterC] ospf
[RouterC-ospf-1] filter-policy ip-prefix in import
```

# Check the IP routing table on Router C, and you can find that Router C in the local core routing table receives only one route from the IP prefix list named **in**.

```
[RouterC] display ip routing-table
Route Flags: R - relay, D - download to fib

Routing Tables: Public
 Destinations : 6 Routes : 6
Destination/Mask Proto Pre Cost Flags NextHop Interface
 127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0
 127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
 172.1.18.0/24 O_ASE 150 1 D 192.168.2.1 Pos1/0/0
 192.168.2.0/24 Direct 0 0 D 192.168.2.2 Pos1/0/0
 192.168.2.1/32 Direct 0 0 D 192.168.2.1 Pos1/0/0
 192.168.2.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0
```

# Check the OSPF routing table of Router C. You can find that three routes defined by the IP prefix list named **a2b** are in the OSPF routing table. In the link state protocol, you can run the **filter-policy import** command to filter the routes that joins the local core routing table from the protocol routing table.

```
[RouterC] display ospf routing
```

OSPF Process 1 with Router ID 192.168.2.2  
 Routing Tables

```

Routing for Network
Destination Cost Type NextHop AdvRouter Area
192.168.2.0/24 1 Stub 192.168.2.2 192.168.2.2 0.0.0.0
192.168.1.0/24 2 Stub 192.168.2.1 192.168.2.1 0.0.0.0
192.168.3.0/24 2 Stub 192.168.2.1 192.168.2.1 0.0.0.0

Routing for ASEs
Destination Cost Type Tag NextHop AdvRouter
172.1.17.0/24 1 Type2 1 192.168.2.1 192.168.1.1
172.1.18.0/24 1 Type2 1 192.168.2.1 192.168.1.1
172.1.19.0/24 1 Type2 1 192.168.2.1 192.168.1.1

Total Nets: 6
Intra Area: 3 Inter Area: 0 ASE: 3 NSSA: 0

```

----End

## Configuration Files

- Configuration file of Router A

```

#
 sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 filter-policy ip-prefix a2b export static
 import-route static
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
#
 ip ip-prefix a2b index 10 permit 172.1.17.0 24
 ip ip-prefix a2b index 20 permit 172.1.18.0 24
 ip ip-prefix a2b index 30 permit 172.1.19.0 24
#
 ip route-static 172.1.16.0 255.255.255.0 NULL0
 ip route-static 172.1.17.0 255.255.255.0 NULL0
 ip route-static 172.1.18.0 255.255.255.0 NULL0
 ip route-static 172.1.19.0 255.255.255.0 NULL0
 ip route-static 172.1.20.0 255.255.255.0 NULL0
#
return

```

- Configuration file of Router B

```

#
 sysname RouterB
#
interface Pos1/0/0
 link-protocol ppp
 ip address 192.168.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 192.168.3.1 255.255.255.0
#
interface Pos3/0/0
 link-protocol ppp
 ip address 192.168.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255

```

```

network 192.168.2.0 0.0.0.255
network 192.168.3.0 0.0.0.255
#
return

```

- Configuration file of Router C

```

#
sysname RouterC
#
interface Pos1/0/0
link-protocol ppp
ip address 192.168.2.2 255.255.255.0
#
ospf 1
filter-policy ip-prefix in import
area 0.0.0.0
network 192.168.2.0 0.0.0.255
#
ip ip-prefix in index 10 permit 172.1.18.0 24
#
return

```

- Configuration file of Router D

```

#
sysname RouterD
#
interface Pos1/0/0
link-protocol ppp
ip address 192.168.3.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 192.168.3.0 0.0.0.255
#
return

```

## 10.9.2 Example for Applying the Routing Policy When Importing Routes

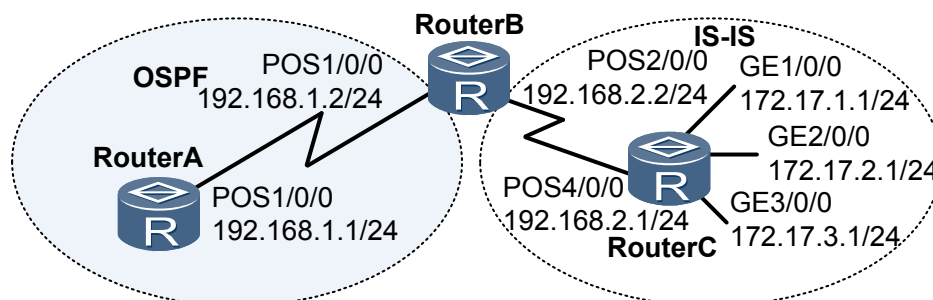
By applying routing policies, you can control the import of routes and set attributes for imported routes.

### Networking Requirements

As shown in [Figure 10-2](#), Router B exchanges routing information with Router A through OSPF and with Router C through IS-IS.

Router B is required to import IS-IS routes into OSPF and to use the routing policy to set the route attributes. The cost of the route 172.17.1.0/24 is set to 100, and the tag of the route 172.17.2.0/24 is set to 20.

**Figure 10-2** Networking diagram of applying a routing policy for imported routes



## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic IS-IS functions on Router B and Router C.
2. Configure OSPF on Router A and Router B and then import IS-IS routes.
3. Configure the routing policy on Router B and apply the routing policy when OSPF imports IS-IS routes, and verify the routes.

## Data Preparation

To complete the configuration, you need the following data:

- The IS-IS level of Router C is Level-2. The system ID is ID 0000.0000.0001. The IS-IS level of Router B is Level-2. The system ID is ID 0000.0000.0002. The area number of Router B and Router C is 10.
- Router A and Router B are located in Area 0, that is, the backbone area.
- Configure the name of the filtering list and IP prefix list. The cost of the route 172.17.1.0/24 is 100. The tag of the route 172.17.2.0/24 is 20.

## Procedure

**Step 1** Assign an IP address to each interface.

The configuration details are not mentioned here.

**Step 2** Configure IS-IS.

# Configure Router C.

```
[RouterC] isis
[RouterC-isis-1] is-level level-2
[RouterC-isis-1] network-entity 10.0000.0000.0001.00
[RouterC-isis-1] quit
[RouterC] interface pos 4/0/0
[RouterC-Pos4/0/0] isis enable
[RouterC-Pos4/0/0] quit
[RouterC] interface GigabitEthernet 1/0/0
[RouterC-GigabitEthernet1/0/0] isis enable
[RouterC-GigabitEthernet1/0/0] quit
[RouterC] interface GigabitEthernet 2/0/0
[RouterC-GigabitEthernet2/0/0] isis enable
[RouterC-GigabitEthernet2/0/0] quit
[RouterC] interface GigabitEthernet 3/0/0
[RouterC-GigabitEthernet3/0/0] isis enable
[RouterC-GigabitEthernet3/0/0] quit
```

# Configure Router B.

```
[RouterB] isis
[RouterB-isis-1] is-level level-2
[RouterB-isis-1] network-entity 10.0000.0000.0002.00
[RouterB-isis-1] quit
[RouterB] interface pos 2/0/0
[RouterB-Pos2/0/0] isis enable
[RouterB-Pos2/0/0] quit
```

**Step 3** Configure OSPF and import routes.

# Configure Router A and enable OSPF.

```
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
```

# Configure Router B. Enable OSPF and import IS-IS routes.

```
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] import-route isis 1
```

# Check the OSPF routing table of Router A. You can view the imported routes.

```
[RouterA] display ospf routing
 OSPF Process 1 with Router ID 192.168.1.1
 Routing Tables

Routing for Network
Destination Cost Type NextHop AdvRouter Area
192.168.1.0/24 1 Stub 192.168.1.1 192.168.1.1 0.0.0.0

Routing for ASEs
Destination Cost Type Tag NextHop AdvRouter
172.17.1.0/24 1 Type2 1 192.168.1.2 192.168.1.2
172.17.2.0/24 1 Type2 1 192.168.1.2 192.168.1.2
172.17.3.0/24 1 Type2 1 192.168.1.2 192.168.1.2
192.168.2.0/24 1 Type2 1 192.168.1.2 192.168.1.2
Total Nets: 5
Intra Area: 1 Inter Area: 0 ASE: 4 NSSA: 0
[RouterA]
```

#### Step 4 Configure the filtering list.

# Configure ACL 2002 to match 172.17.2.0/24.

```
[RouterB] acl number 2002
[RouterB-acl-basic-2002] rule permit source 172.17.2.0 0.0.0.255
[RouterB-acl-basic-2002] quit
```

# Configure the IP prefix list named **prefix-a** to match 172.17.1.0/24.

```
[RouterB] ip ip-prefix prefix-a index 10 permit 172.17.1.0 24
```

#### Step 5 Configure the Route-Policy.

```
[RouterB] route-policy isis2ospf permit node 10
[RouterB-route-policy] if-match ip-prefix prefix-a
[RouterB-route-policy] apply cost 100
[RouterB-route-policy] quit
[RouterB] route-policy isis2ospf permit node 20
[RouterB-route-policy] if-match acl 2002
[RouterB-route-policy] apply tag 20
[RouterB-route-policy] quit
[RouterB] route-policy isis2ospf permit node 30
[RouterB-route-policy] quit
```

#### Step 6 Apply the Route-Policy when the route is imported.

# Configure Router B and apply the Route-Policy as the route is imported.

```
[RouterB] ospf
[RouterB-ospf-1] import-route isis 1 route-policy isis2ospf
[RouterB-ospf-1] quit
```

# Check the OSPF routing table of Router A. You can view the cost of the route with the destination address as 172.17.1.0/24 is 100. The tag of the route with the destination address as 172.17.2.0/24 is 20. Other routing attributes do not change.



```
[RouterA] display ospf routing
OSPF Process 1 with Router ID 192.168.1.1
Routing Tables
Routing for Network
Destination Cost Type NextHop AdvRouter Area
192.168.1.0/24 1 Stub 192.168.1.1 192.168.1.1 0.0.0.0
Routing for ASEs
Destination Cost Type Tag NextHop AdvRouter
172.17.1.0/24 100 Type2 1 192.168.1.2 192.168.1.2
172.17.2.0/24 1 Type2 20 192.168.1.2 192.168.1.2
172.17.3.0/24 1 Type2 1 192.168.1.2 192.168.1.2
192.168.2.0/24 1 Type2 1 192.168.1.2 192.168.1.2
Total Nets: 5
Intra Area: 1 Inter Area: 0 ASE: 4 NSSA: 0
[RouterA]

----End
```

## Configuration Files

- Configuration file of Router A

```
#
 sysname RouterA
#
interface Pos1/0/0
 link-protocol ppp
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
acl number 2002
 rule 5 permit source 172.17.2.0 0.0.0.255
#
isis 1
 is-level level-2
 network-entity 10.0000.0000.0002.00
#
interface Pos1/0/0
 link-protocol ppp
 ip address 192.168.1.2 255.255.255.0
#
interface Pos2/0/0
 link-protocol ppp
 ip address 192.168.2.2 255.255.255.0
 isis enable 1
#
ospf 1
 import-route isis 1 route-policy isis2ospf
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
#
route-policy isis2ospf permit node 10
 if-match ip-prefix prefix-a
 apply cost 100
route-policy isis2ospf permit node 20
 if-match acl 2002
 apply tag 20
route-policy isis2ospf permit node 30
#
ip ip-prefix prefix-a index 10 permit 172.17.1.0 24
```

```
#
return
● Configuration file of Router C
#
sysname RouterC
#
isis 1
is-level level-2
network-entity 10.0000.0000.0001.00
#
interface GigabitEthernet1/0/0
ip address 172.17.1.1 255.255.255.0
isis enable 1
#
interface GigabitEthernet2/0/0
ip address 172.17.2.1 255.255.255.0
isis enable 1
#
interface GigabitEthernet3/0/0
ip address 172.17.3.1 255.255.255.0
isis enable 1
#
interface Pos4/0/0
link-protocol ppp
ip address 192.168.2.1 255.255.255.0
isis enable 1
#
return
```

---

# A Glossary

---

This appendix collates frequently used glossaries in this document.

## A

|                          |                                                                                                                                                                                                                                                                                       |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Control List      | A list that contains a group of rules that consist of <b>rule</b> { <b>deny</b>   <b>permit</b> } statements. In firewall, ACL is applied to an interface of a router. The router then decides which packets can be received or be rejected. In QoS, ACL is used to classify traffic. |
| Accounting               | To record the network resources used by users.                                                                                                                                                                                                                                        |
| Additional System ID     | A system ID assigned by the network manager. Each additional system ID can generate up to 256 additional or extended LSP fragments.                                                                                                                                                   |
| Area                     | A logical set of network segments and devices. Areas are connected through routers to form AS.                                                                                                                                                                                        |
| Area border router (ABR) | A router that can belong to more than two areas of which one area must be a backbone area.                                                                                                                                                                                            |
| AS Border Router (ASBR)  | A router that exchanges routing information with other ASs.                                                                                                                                                                                                                           |
| Autonomous System        | A network set that uses the same routing policy and is managed by the same technology administration department. Each AS has a unique identifier that is a integer. The identifier is assigned by IANA. An AS can be divided into areas.                                              |

## B

|                         |                                                                                                                         |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Backbone Area           | An area that is responsible for routing between areas and forwarding routing information of non-backbone areas.         |
| Backbone Router         | A router with a minimum of one interface connecting to the backbone area                                                |
| Border Gateway Protocol | A type of external gateway protocol used to exchange inter-AS routes with routing loop. BGP-4 becomes the ECP standard. |

## C

**Classless InterDomain Routing** To use IP address and mask to indicate network address and sub-network address. Through CIDR, routers can flexibly aggregate routes. This reduces the size of the routing table.

## E

**Extended Community Access List** A list that identifies a community, which is divided into standard community access list and extended community access list.

**Exterior Gateway Protocol (EGP)** A routing protocol that runs between different ASs.

## I

**Incremental SPF** To recalculate the routes that change but not to recalculate all routes.

**Interior Gateway Protocol (IGP)** A routing protocol that runs in an AS, including RIP, OSPF.

**Internet engineering task force** An organization engaged in the development and design of TCP/IP protocol suite.

**Intra-Domain Router** A router with all interfaces that belong to an OSPF area.

## M

**Multi-Exit-Disc (MED)** An attribute that is equivalent to the metrics used by IGP. It is only exchanged between two adjacent ASs. The AS that receives this attribute does not advertise it to any other ASs.

**Multiprotocol Border Gateway Protocol** A multiprotocol extension for BGP-4, which is also called BGP-4+. MP-BGP is the extended protocol of BGP-4. MP-BGP can carry both IPv4 unicast routing information and routing information of other network protocols, such as multicast and IPv6.  
NE80E/40E provides multiple types of MP-BGP applications, including extension of multicast and the extension of BGP/MPLS VPN.

## N

**Network Entity Title (NET)** Network layer information of an IS itself. It excludes the transport layer information (SEL = 0) and can be regarded as a special NSAP.

**Network Service Access Point (NSAP)** A network address defined by ISO, through which entities on the network layer can access OSI network services.

## O

**Originating System** A router that runs the IS-IS protocol

## P

**Partial Route Calculation** A type of route calculation that is similar to that of PRC. Only the routes that change are calculated. Instead of calculating the node path, PRC updates the leaf routes according to the SPT calculated by I-SPF.

**Path Attribute** A part of Update packet.

**Poison Reverse** A feature that RIP learns a route from the neighboring interface, sets its cost to 16, and advertises it to the neighboring routers.

**Pseudonode** A virtual node that is used to simulate broadcast network. It is generated by DIS.

## R

**Router ID** A unique identifier of a router in an AS, which is an integer of 32 bits.

## S

**Split Horizon** A feature that RIP does not send the route learned from the neighboring interface back to its neighboring router.

**Stub area** A specific area in which ABRs do not transmit the routes outside the AS.

**System ID** To uniquely identify a host or a router in an area.

**System ID** System ID of the originating system.

## T

**Transmit area** An area that provides an internal route of a non-backbone area for the both ends of a virtual link.

## V

**Versatile Routing Platform (VRP)** A versatile operation platform of Huawei data communication.

**Virtual Link** A logical channel that connects two ABRs through a non-backbone area.

---

|                |                                                                                                                                                                 |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Virtual System | The system, identified by an additional system ID, is used to generate extended LSP fragments. These fragments carry the additional system IDs in their LSP IDs |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

# B Acronyms and Abbreviations

---

This appendix collates frequently used acronyms and abbreviations in this document.

## A

|      |                                   |
|------|-----------------------------------|
| ABR  | Area Border Router                |
| ACL  | Access Control List               |
| ARP  | Address Resolution Protocol       |
| AS   | Autonomous System; Access Server  |
| ASBR | Autonomous System Boundary Router |
| ATM  | Asynchronous Transfer Mode        |

## B

|     |                          |
|-----|--------------------------|
| BDR | Backup Designated Router |
| BGP | Border Gateway Protocol  |
| BRI | Basic Rate Interface     |

## C

|      |                                 |
|------|---------------------------------|
| CE   | Customer Edge                   |
| CIDR | Classless Inter-Domain Routing  |
| CLNP | Connectionless Network Protocol |
| CPU  | Central Processing Unit         |
| CSNP | Complete Sequence Number PDUs   |

## D

|    |                      |
|----|----------------------|
| DD | Database Description |
|----|----------------------|

|          |                                                |
|----------|------------------------------------------------|
| DIS      | Designated Intermediate System                 |
| DR       | Designated Router                              |
| DVMRP    | Distance Vector Multicast Routing Protocol     |
| <b>E</b> |                                                |
| EBGP     | External BGP                                   |
| EGP      | Exterior Gateway Protocol                      |
| <b>F</b> |                                                |
| FDDI     | Fiber Distributed Digital Interface            |
| <b>H</b> |                                                |
| HDLC     | High level Data Link Control                   |
| <b>I</b> |                                                |
| IBGP     | Internal BGP                                   |
| ICMP     | Internet Control Message Protocol              |
| ID       | Identification                                 |
| IETF     | Internet Engineering Task Force                |
| IGP      | Interior Gateway Protocol                      |
| IP       | Internet Protocol                              |
| ISDN     | Integrated Services Digital Network            |
| IS-IS    | Intermediate System-Intermediate System        |
| ISO      | International Organization for Standardization |
| ISP      | Internet Service Provider                      |
| <b>L</b> |                                                |
| L2VPN    | Layer 2 VPN                                    |
| L3VPN    | Layer 3 VPN                                    |
| LAN      | Local Area Network                             |
| LAPB     | Link Access Procedure, Balanced                |
| LSA      | Link State Advertisement                       |



|          |                                       |
|----------|---------------------------------------|
| LSDB     | Link-State Data Base                  |
| LSP      | Label Switch Path                     |
| LSP      | Link State Protocol Data Unit         |
| LSR      | Label Switching Router                |
| LSR      | Link State Request Packet             |
| LSU      | Link State Update Packet              |
| <b>M</b> |                                       |
| MAC      | Medium Access Control                 |
| MD5      | Message Digest 5                      |
| MED      | Multi-Exit discrimination             |
| MIB      | Management Information Base           |
| MP       | Multilink PPP                         |
| MP-BGP   | Multiprotocol Border Gateway Protocol |
| MPLS     | Multi-Protocol Label Switching        |
| MTU      | Maximum Transmission Unit             |
| <b>N</b> |                                       |
| NBMA     | Non Broadcast Multiple Access         |
| NET      | Network Entity Title                  |
| NLRI     | Network Layer Reachable Information   |
| NSSA     | Not-So-Stubby Area                    |
| <b>O</b> |                                       |
| OSI      | Open System Interconnection           |
| OSPF     | Open Shortest Path First              |
| <b>P</b> |                                       |
| P2P      | Point to Point                        |
| PC       | Personal Computer                     |
| PDU      | Protocol Data Unit                    |
| PE       | Provider Edge                         |

|        |                                            |
|--------|--------------------------------------------|
| PIM    | Protocol Independent Multicast             |
| PIM-DM | Protocol Independent Multicast-Dense Mode  |
| PIM-SM | Protocol Independent Multicast-Sparse Mode |
| POS    | Packet Over SDH/SONET                      |
| PPP    | Point-to-Point Protocol                    |
| PRI    | Primary Rate Interface                     |
| PSNP   | Partial Sequence Number PDUs               |

**R**

|     |                              |
|-----|------------------------------|
| RD  | Route Distinguisher          |
| RIP | Routing Information Protocol |
| RM  | Routing Management           |
| RPF | Reverse Path Forwarding      |
| RPM | Routing Policy Management    |

**S**

|      |                                    |
|------|------------------------------------|
| SNMP | Simple Network Management Protocol |
| SPF  | Shortest Path First                |

**T**

|     |                               |
|-----|-------------------------------|
| TCP | Transmission Control Protocol |
| TE  | Traffic Engineering           |

**U**

|     |                        |
|-----|------------------------|
| UDP | User Datagram Protocol |
| UP  | User Plane             |

**V**

|     |                            |
|-----|----------------------------|
| VPN | Virtual Private Network    |
| VRP | Versatile Routing Platform |
| VT  | Virtual-Template           |

**W**

WAN                      Wide Area Network