



Quidway S5300 Series Ethernet Switches
V100R002C02

Configuration Guide – IP Routing

Issue	01
Date	2008-12-26
Part Number	

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. For any assistance, please contact our local office or company headquarters.

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

Copyright © Huawei Technologies Co., Ltd. 2008. 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 the property of Huawei Technologies Co., Ltd.

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

Notice

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 the statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

About This Document.....	1
1 Static Route Configuration.....	1-1
1.1 Introduction.....	1-2
1.1.1 Static Routes.....	1-2
1.1.2 Default Static Routes.....	1-2
1.1.3 BFD for Static Routes.....	1-2
1.1.4 Static Routes Supported by the Interface of the S-switch.....	1-3
1.1.5 Logical Relationships Between the Configuration Tasks.....	1-3
1.1.6 Update History.....	1-3
1.2 Configuring a Static Route.....	1-3
1.2.1 Establishing the Configuration Task.....	1-3
1.2.2 (Optional) Setting the Default Preference of a Static Route.....	1-4
1.2.3 Configuring a Static Route.....	1-4
1.2.4 Checking the Configuration.....	1-5
1.3 Configuring BFD for Static Routes in the Public Network.....	1-5
1.3.1 Establishing the Configuration Task.....	1-6
1.3.2 (Optional) Configuring a Static Route.....	1-6
1.3.3 Creating a BFD Session.....	1-7
1.3.4 Binding a Static Route to a BFD Session.....	1-7
1.3.5 Checking the Configuration.....	1-7
1.4 Configuration Examples.....	1-8
1.4.1 Example for Configuring Static Routes.....	1-8
1.4.2 Example for Configuring BFD for Static Routes.....	1-11
2 OSPF Configuration.....	2-1
2.1 Overview.....	2-3
2.1.1 Introduction.....	2-3
2.1.2 OSPF Features Supported by the S-switch.....	2-6
2.1.3 Logical Relationships Between the Configuration Tasks.....	2-8
2.1.4 Update History.....	2-8
2.1.5 References.....	2-8
2.2 Configuring Basic OSPF Functions.....	2-8
2.2.1 Establishing the Configuration Task.....	2-9

2.2.2 Enabling OSPF and Entering the OSPF View.....	2-9
2.2.3 Configuring Network Segments That Each Area Includes.....	2-10
2.2.4 Checking the Configuration.....	2-11
2.3 Setting Up and Maintaining the OSPF Neighbor Relationship or the Adjacency.....	2-11
2.3.1 Establishing the Configuration Task.....	2-12
2.3.2 (Optional) Setting the Interval for Sending Hello Packets.....	2-13
2.3.3 (Optional) Setting the Dead Interval of the Neighbor.....	2-13
2.3.4 (Optional) Setting the Interval for Retransmitting LSAs.....	2-14
2.3.5 (Optional) Setting Retransmission Limitation for OSPF Packets.....	2-14
2.3.6 (Optional) Suppressing an Interface from Receiving and Sending OSPF Packets.....	2-15
2.3.7 Checking the Configuration.....	2-15
2.4 Configuring OSPF Area Features.....	2-16
2.4.1 Establishing the Configuration Task.....	2-16
2.4.2 Configuring an OSPF Stub Area.....	2-17
2.4.3 Configuring an OSPF NSSA Area.....	2-18
2.4.4 Checking the Configuration.....	2-18
2.5 Configuring OSPF Attributes in Different Network Types.....	2-19
2.5.1 Establishing the Configuration Task.....	2-19
2.5.2 Configuring Network Types for an Interface Enabled with OSPF.....	2-20
2.5.3 (Optional) Setting the DR Priority for an Interface Enabled with OSPF.....	2-20
2.5.4 Configuring a Neighbor for an NBMA Network.....	2-21
2.5.5 (Optional) Setting the Interval for Sending Poll Packets on an NBMA Network.....	2-21
2.5.6 Checking the Configuration.....	2-21
2.6 Configuring OSPF Route Attributes.....	2-22
2.6.1 Establishing the Configuration Task.....	2-22
2.6.2 (Optional) Setting the Link Cost of OSPF.....	2-23
2.6.3 (Optional) Setting the Preference for an OSPF Route.....	2-24
2.6.4 (Optional) Setting the Maximum Number of OSPF Routes.....	2-25
2.6.5 Checking the Configuration.....	2-25
2.7 Configuring OSPF Route Aggregation.....	2-26
2.7.1 Establishing the Configuration Task.....	2-26
2.7.2 Configuring ABR Route Aggregation.....	2-26
2.7.3 Configuring ASBR Route Aggregation.....	2-27
2.7.4 Checking the Configuration.....	2-27
2.8 Configuring an OSPF Process to Filter Routes.....	2-28
2.8.1 Establishing the Configuration Task.....	2-28
2.8.2 Configuring an OSPF Process to Filter Type3 LSAs.....	2-29
2.8.3 Configuring an OSPF Process to Filter the Received Routes.....	2-29
2.8.4 Configuring an OSPF Process to Import External Routes.....	2-30
2.8.5 Checking the Configuration.....	2-31
2.9 Adjusting and Optimizing an OSPF Network.....	2-32
2.9.1 Establishing the Configuration Task.....	2-32

2.9.2 (Optional) Setting the Delay for Transmitting LSAs on an Interface.....	2-33
2.9.3 (Optional) Setting the Interval for LSAs.....	2-34
2.9.4 (Optional) Setting the Interval for the SPF Calculation.....	2-34
2.9.5 (Optional) Configuring a Stub Router.....	2-35
2.9.6 (Optional) Setting the MTU of DD Packets.....	2-35
2.9.7 (Optional) Setting the Maximum Number of External LSAs in an LSDB.....	2-36
2.9.8 (Optional) Configuring Selection Rules of External Routes That Are Compatible with RFC 1583	2-36
2.9.9 Checking the Configuration.....	2-37
2.10 Improving the Security of an OSPF Network.....	2-38
2.10.1 Establishing the Configuration Task.....	2-38
2.10.2 Configuring Authentication Mode for OSPF Areas.....	2-38
2.10.3 Configuring Interface Authentication.....	2-39
2.10.4 Checking the Configuration.....	2-39
2.11 Configuring OSPF Network Management.....	2-40
2.11.1 Establishing the Configuration Task.....	2-40
2.11.2 Configuring OSPF MIB Binding.....	2-41
2.11.3 Configuring the TRAP Function.....	2-41
2.11.4 Configuring the Log Function.....	2-41
2.11.5 Checking the Configuration.....	2-42
2.12 Maintaining OSPF.....	2-42
2.12.1 Resetting OSPF.....	2-43
2.12.2 Clearing OSPF.....	2-43
2.12.3 Debugging OSPF.....	2-43
2.13 Configuring Examples.....	2-44
2.13.1 Example for Configuring Basic OSPF Functions.....	2-44
2.13.2 Example for Configuring a Stub Area of OSPF.....	2-50
2.13.3 Example for Configuring an OSPF NSSA Area.....	2-55
2.13.4 Example for Configuring DR Election of an OSPF Process.....	2-59
2.13.5 Example for Configuring OSPF Load Balancing.....	2-64
3 IS-IS Configuration.....	3-1
3.1 Introduction.....	3-3
3.1.1 Basic Concepts of IS-IS.....	3-3
3.1.2 IS-IS Features Supported by the S-switch.....	3-4
3.1.3 Logical Relationships Between the Configuration Tasks.....	3-8
3.1.4 Update History.....	3-8
3.1.5 References.....	3-8
3.2 Configuring Basic IS-IS Functions.....	3-9
3.2.1 Establishing the Configuration Task.....	3-9
3.2.2 Enabling an IS-IS Process.....	3-10
3.2.3 Configuring a NET.....	3-10
3.2.4 (Optional) Configuring the Level of the S-switch.....	3-10

3.2.5 Starting the Corresponding IS-IS Process on the Specified Interface.....	3-11
3.2.6 Checking the Configuration.....	3-11
3.3 Establishing or Maintaining IS-IS Neighbor Relationships or Adjacencies.....	3-12
3.3.1 Establishing the Configuration Task.....	3-12
3.3.2 (Optional) Configuring Timers of IS-IS Packets.....	3-13
3.3.3 Configuring LSP Parameters.....	3-16
3.3.4 (Optional) Disable the Padding of Hello Packets on the Specified Interface.....	3-19
3.3.5 Checking the Configuration.....	3-20
3.4 Configuring the IS-IS Attributes in Different Types of Networks.....	3-21
3.4.1 Establishing the Configuration Task.....	3-21
3.4.2 Configuring the Network Type of an IS-IS Interface.....	3-22
3.4.3 (Optional) Configuring the DIS Priority of an Interface.....	3-22
3.4.4 Checking the Configuration.....	3-23
3.5 Configuring the Attributes of IS-IS Routes.....	3-23
3.5.1 Establishing the Configuration Task.....	3-24
3.5.2 Configuring the Cost of an IS-IS Interface.....	3-24
3.5.3 Configuring the Priority of IS-IS.....	3-27
3.5.4 Checking the Configuration.....	3-28
3.6 Controlling the Advertisement of IS-IS Routing Information.....	3-29
3.6.1 Establishing the Configuration Task.....	3-30
3.6.2 Configuring IS-IS Route Aggregation.....	3-30
3.6.3 Configuring IS-IS to Generate Default Routes.....	3-31
3.6.4 Configuring IS-IS Route Leaking from Level-2 to Level-1.....	3-31
3.6.5 Checking the Configuration.....	3-31
3.7 Controlling the Receiving of IS-IS Routing Information.....	3-32
3.7.1 Establishing the Configuration Task.....	3-32
3.7.2 Configuring IS-IS to Filter the Received Routing Information.....	3-33
3.7.3 Configuring IS-IS to Import External Routes.....	3-33
3.7.4 Checking the Configuration.....	3-33
3.8 Adjusting and Optimizing IS-IS.....	3-34
3.8.1 Establishing the Configuration Task.....	3-35
3.8.2 (Optional) Configuring the Level of an IS-IS Interface.....	3-35
3.8.3 Setting the Status of an IS-IS Interface to Suppressed.....	3-36
3.8.4 Configuring SPF Parameters.....	3-36
3.8.5 Enabling LSP Fast Flooding.....	3-37
3.8.6 Configuring IS-IS Dynamic Hostname Mapping.....	3-38
3.8.7 Configuring the LSP Overload Bit.....	3-39
3.8.8 Configuring Output of the Adjacency Status.....	3-39
3.8.9 Checking the Configuration.....	3-40
3.9 Improving the Security of an IS-IS Network.....	3-40
3.9.1 Establishing the Configuration Task.....	3-40
3.9.2 Configuring Area Authentication and Routing Domain Authentication.....	3-41

3.9.3 Configuring the Authentication on an Interface.....	3-41
3.9.4 Checking the Configuration.....	3-42
3.10 Maintaining IS-IS.....	3-42
3.10.1 Resetting the IS-IS Data Structure.....	3-42
3.10.2 Resetting a Specific IS-IS Neighbor.....	3-43
3.10.3 Debugging IS-IS.....	3-43
3.11 Configuration Examples.....	3-45
3.11.1 Example for Configuring Basic IS-IS Functions.....	3-45
3.11.2 Example for Configuring IS-IS Route Aggregation.....	3-51
3.11.3 Example for Configuring the DIS Election of IS-IS.....	3-55
3.11.4 Example for Configuring IS-IS Load Balancing.....	3-61
4 RIP Configuration.....	4-1
4.1 Introduction.....	4-2
4.1.1 Overview of RIP.....	4-2
4.1.2 RIP Features Supported by S-switch.....	4-2
4.2 Configuring Basic RIP Functions.....	4-2
4.2.1 Establishing the Configuration Task.....	4-3
4.2.2 Enabling RIP.....	4-3
4.2.3 Enabling RIP on the Specified Network Segment.....	4-4
4.2.4 Configuring RIP Version Number.....	4-4
4.2.5 Checking the Configuration.....	4-5
4.3 Configuring RIP Route Attributes.....	4-6
4.3.1 Establishing the Configuration Task.....	4-6
4.3.2 Configuring Additional Metrics of an Interface.....	4-7
4.3.3 Configuring RIP Preference.....	4-8
4.3.4 Setting the Maximum Number of Equal-Cost Routes.....	4-8
4.3.5 Checking the Configuration.....	4-9
4.4 Controlling the Advertising of RIP Routing Information.....	4-9
4.4.1 Establishing the Configuration Task.....	4-9
4.4.2 Configuring RIP to Advertise Default Routes.....	4-10
4.4.3 Disabling an Interface from Sending Update Packets.....	4-11
4.4.4 Configuring RIP to Import External Routes.....	4-12
4.4.5 Checking the Configuration.....	4-12
4.5 Controlling the Receiving of RIP Routing Information.....	4-13
4.5.1 Establishing the Configuration Task.....	4-13
4.5.2 Disabling an Interface from Receiving RIP Update Packets.....	4-14
4.5.3 Disabling RIP from Receiving Host Routes.....	4-14
4.5.4 Configuring RIP to Filter the Received Routes.....	4-15
4.5.5 Checking the Configuration.....	4-16
4.6 Configuring RIP-2 Features.....	4-16
4.6.1 Establishing the Configuration Task.....	4-17
4.6.2 Configuring RIP-2 Route Aggregation.....	4-17

4.6.3 Configuring Packet Authentication of RIP-2.....	4-18
4.6.4 Checking the Configuration.....	4-19
4.7 Optimizing a RIP Network.....	4-19
4.7.1 Establishing the Configuration Task.....	4-19
4.7.2 Configuring RIP Timers.....	4-20
4.7.3 Setting the Interval for Sending Packets and the Number of the Sent Packets.....	4-21
4.7.4 Configuring Split Horizon and Poison Reverse.....	4-22
4.7.5 Configuring RIP to Check the Validity of the Update Packets.....	4-22
4.7.6 Configuring RIP Neighbors.....	4-23
4.7.7 Checking the Configuration.....	4-24
4.8 Configuring the Network Management Function in RIP.....	4-24
4.8.1 Establishing the Configuration Task.....	4-24
4.8.2 Configuring RIP and MIB Binding.....	4-25
4.8.3 Checking the Configuration.....	4-25
4.9 Maintaining RIP.....	4-25
4.10 Configuration Examples.....	4-26
4.10.1 Example for Configuring RIP Version.....	4-26
4.10.2 Example for Configuring RIP to Import External Routes.....	4-29
5 BGP Configuration.....	5-1
5.1 Introduction.....	5-3
5.1.1 BGP Overview.....	5-3
5.1.2 BGP Features Supported by the S-switch.....	5-3
5.1.3 Update History.....	5-7
5.2 Configuring Basic BGP Functions.....	5-7
5.2.1 Establishing the Configuration Task.....	5-7
5.2.2 Starting a BGP Process.....	5-8
5.2.3 Configuring a BGP Peer.....	5-8
5.2.4 (Optional) Configuring a Local Interface for a BGP Connection.....	5-10
5.2.5 Checking the Configuration.....	5-10
5.3 Configuring BGP Route Attributes.....	5-10
5.3.1 Establishing the Configuration Task.....	5-11
5.3.2 Setting the BGP Preference.....	5-12
5.3.3 Setting the PrefVal for a BGP Peer.....	5-12
5.3.4 Setting the Default Local_Pref for the Local Device.....	5-13
5.3.5 Setting the MED.....	5-13
5.3.6 Configuring the Next_Hop.....	5-14
5.3.7 Setting the AS_Path.....	5-15
5.3.8 Checking the Configuration.....	5-17
5.4 Configuring BGP Filters.....	5-18
5.4.1 Establishing the Configuration Task.....	5-18
5.4.2 Configuring a Routing Policy for Advertising BGP Routes.....	5-19
5.4.3 Configuring a Routing Policy for Receiving BGP Routes.....	5-20

5.4.4 Configuring BGP Soft Resetting.....	5-22
5.4.5 Checking the Configuration.....	5-23
5.5 Controlling the Route Advertisement.....	5-24
5.5.1 Establishing the Configuration Task.....	5-24
5.5.2 Configuring BGP to Advertise Local Routes.....	5-25
5.5.3 Configuring BGP Route Aggregation.....	5-25
5.5.4 Configuring BGP to Advertise Default Routes to the Peers.....	5-26
5.5.5 Configuring Split Horizon Between EBGPeers.....	5-27
5.5.6 Checking the Configuration.....	5-27
5.6 Controlling BGP to Import Routes.....	5-28
5.6.1 Establishing the Configuration Task.....	5-28
5.6.2 Configuring BGP to Import Default Routes.....	5-28
5.6.3 Configuring BGP to Import Routes.....	5-29
5.6.4 Checking the Configuration.....	5-29
5.7 Configuring Parameters for a BGP Connection.....	5-29
5.7.1 Establishing the Configuration Task.....	5-30
5.7.2 Configuring BGP Timers.....	5-30
5.7.3 Setting the Interval for Sending Update Messages.....	5-31
5.7.4 Enabling Fast Resetting for EBGPeer Relationships.....	5-32
5.7.5 Checking the Configuration.....	5-32
5.8 Configuring BFD for BGP.....	5-32
5.8.1 Establishing the Configuration Task.....	5-33
5.8.2 Configuring BFD for BGP in the Public Network Instance.....	5-33
5.8.3 Configuring BFD for BGP in a Private Network.....	5-34
5.8.4 Checking the Configuration.....	5-34
5.9 Configuring BGP Load Balancing.....	5-34
5.9.1 Establishing the Configuration Task.....	5-35
5.9.2 Setting the Number of Routes for Load Balancing.....	5-35
5.9.3 Checking the Configuration.....	5-35
5.10 Configuring BGP Security.....	5-36
5.10.1 Establishing the Configuration Task.....	5-36
5.10.2 Configuring the MD5 Authentication.....	5-36
5.10.3 Checking the Configuration.....	5-37
5.11 Maintaining BGP.....	5-37
5.11.1 Resetting BGP Connections.....	5-37
5.11.2 Debugging BGP.....	5-38
5.12 Configuration Examples.....	5-38
5.12.1 Example for Configuring Basic BGP Functions.....	5-39
5.12.2 Example for Configuring BGP to Interact with an IGP.....	5-44
5.12.3 Example for Configuring BGP Load Balancing and the MED.....	5-48
6 Routing Policy Configuration.....	6-1
6.1 Introduction.....	6-2

6.1.1 Overview of the Routing Policy.....	6-2
6.1.2 Routing Policy Features Supported by the S-switch.....	6-3
6.1.3 Logical Relationships Between Configuration Tasks.....	6-4
6.1.4 Update History.....	6-4
6.2 Configuring an IP Prefix List.....	6-4
6.2.1 Establishing the Configuration Task.....	6-4
6.2.2 Configuring an IPv4 Prefix List.....	6-5
6.2.3 Checking the Configuration.....	6-6
6.3 Configuring a Route-Policy.....	6-6
6.3.1 Establishing the Configuration Task.....	6-6
6.3.2 Creating a Route-Policy.....	6-7
6.3.3 (Optional) Setting an if-match Clause.....	6-7
6.3.4 (Optional) Setting an apply Clause.....	6-8
6.3.5 Checking the Configuration.....	6-9
6.4 Applying Filters to Received Routes.....	6-9
6.4.1 Establishing the Configuration Task.....	6-9
6.4.2 Filtering Routes Received by OSPF.....	6-10
6.4.3 Filtering Routes Received by IS-IS.....	6-11
6.4.4 Filtering Routes Received by BGP.....	6-11
6.4.5 Checking the Configuration.....	6-12
6.5 Applying Filters to Advertised Routes.....	6-12
6.5.1 Establishing the Configuration Task.....	6-12
6.5.2 Filtering Routes Advertised by OSPF.....	6-13
6.5.3 Filtering Routes Advertised by IS-IS.....	6-14
6.5.4 Filtering Routes Advertised by BGP.....	6-14
6.5.5 Checking the Configuration.....	6-15
6.6 Applying Filters to Imported Routes.....	6-15
6.6.1 Establishing the Configuration Task.....	6-16
6.6.2 Applying a Route-Policy to Routes Imported by OSPF.....	6-16
6.6.3 Applying a Route-Policy to Routes Imported by IS-IS.....	6-17
6.6.4 Apply a Route-Policy to Routes Imported by BGP.....	6-17
6.6.5 Checking the Configuration.....	6-17
6.7 Controlling the Valid Time of a Routing Policy.....	6-18
6.7.1 Establishing the Configuration Task.....	6-18
6.7.2 Setting the Delay for Applying the Routing Policy.....	6-19
6.7.3 Checking the Configuration.....	6-19
6.8 Configuration Examples.....	6-19
6.8.1 Example for Filtering Received and Advertised Routes.....	6-19
7 MCE Configuration.....	7-1
7.1 Introduction to MCE.....	7-2
7.1.1 MCE Overview.....	7-2
7.1.2 MCE Functions Supported by the S-switch.....	7-3

7.1.3 Logical Relationships Between Configuration Tasks.....	7-4
7.1.4 Update History.....	7-4
7.2 Configuring a VPN Instance.....	7-5
7.2.1 Establishing the Configuration Task.....	7-5
7.2.2 Creating a VPN instance.....	7-5
7.2.3 Binding a VPN Instance to a VLANIF Interface.....	7-6
7.2.4 Checking the Configuration.....	7-7
7.3 Configuring a Route Multi-Instance Between an MCE and a Site.....	7-8
7.3.1 Establishing the Configuration Task.....	7-8
7.3.2 (Optional) Configuring a Static Route Between an MCE and a Site.....	7-9
7.3.3 (Optional) Configuring RIP Between an MCE and a Site.....	7-9
7.3.4 (Optional) Configuring OSPF Between an MCE and a Site.....	7-10
7.3.5 (Optional) Configuring IS-IS Between an MCE and a Site.....	7-10
7.3.6 (Optional) Configuring BGP Between an MCE and a Site.....	7-11
7.3.7 Checking the Configuration.....	7-12
7.4 Configuring a Route Multi-Instance Between an MCE and a PE.....	7-12
7.4.1 Establishing the Configuration Task.....	7-13
7.4.2 (Optional) Configuring a Static Route Between an MCE and a PE.....	7-14
7.4.3 (Optional) Configuring RIP Between an MCE and a PE.....	7-14
7.4.4 (Optional) Configuring OSPF Between an MCE and a PE.....	7-15
7.4.5 (Optional) Configuring IS-IS Between an MCE and a PE.....	7-15
7.4.6 (Optional) Configuring BGP Between an MCE and a PE.....	7-16
7.4.7 Checking the Configuration.....	7-16
7.5 MCE Configuration Examples.....	7-17
7.5.1 Example for Configuring MCE.....	7-17

Figures

Figure 1-1 Networking diagram of configuring static routes.....	1-8
Figure 1-2 Networking diagram of configuring BFD for static routes.....	1-12
Figure 2-1 OSPF area partition.....	2-4
Figure 2-2 OSPF device types.....	2-5
Figure 2-3 Changes of neighbor state machines.....	2-7
Figure 2-4 Networking diagram of basic OSPF configurations.....	2-45
Figure 2-5 Configuring OSPF stub areas.....	2-51
Figure 2-6 Configuring OSPF NSSA areas.....	2-56
Figure 2-7 Networking diagram of configuring DR election of an OSPF process.....	2-60
Figure 2-8 Networking diagram of configuring OSPF load balancing.....	2-65
Figure 3-1 IS-IS topology I.....	3-3
Figure 3-2 IS-IS topology II.....	3-4
Figure 3-3 Networking diagram for configuring basic IS-IS functions.....	3-46
Figure 3-4 Networking diagram for configuring IS-IS route convergence.....	3-52
Figure 3-5 Networking diagram for configuring the DIS election of IS-IS.....	3-56
Figure 3-6 Networking diagram for configuring IS-IS load balancing.....	3-61
Figure 4-1 Networking diagram of configuring the RIP version number.....	4-26
Figure 4-2 Networking diagram of configuring RIP to import external routes.....	4-29
Figure 5-1 Networking diagram of configuring basic BGP functions.....	5-39
Figure 5-2 Networking diagram of configuring BGP to interact with an IGP.....	5-44
Figure 5-3 Networking diagram of BGP route selection.....	5-48
Figure 6-1 Networking diagram for filtering received and advertised routes.....	6-20
Figure 7-1 Traditional BGP or MPLS IP VPN model.....	7-2
Figure 7-2 Typical MCE networking diagram.....	7-3
Figure 7-3 Networking diagram for configuring MCE.....	7-18

Tables

Table 3-1 Relationship between interface costs and the bandwidth.....3-26

Table 6-1 Differences between the routing policy and PBR.....6-2

About This Document

Purpose

This document provides configuration procedures and examples for the IP Routing features of the S-switch.

This document covers the following topics:

- Feature description
- Data preparations
- Pre-configuration tasks
- Configuration procedures
- Checking the configuration
- Configuration examples

This document helps you grasp the configuration procedures and application scenarios of the IP Routing features of the S-switch.

Related Versions

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

Product Name	Version
S5300	V100R002C02

Intended Audience

This document is intended for:

- Commissioning engineers
- Data configuration engineers
- Network administrators
- System maintenance engineers

Organization






This document provides basic knowledge of the software and hardware of the S-switch and describes user login procedures.

Chapter	Description
1 Static Route Configuration	This chapter describes the fundamentals of static route and configuration steps for static routes, along with typical examples.
2 OSPF Configuration	This chapter describes the OSPF fundamentals and configuration steps for basic OSPF functions, OSPF area features, OSPF network types, controlling OSPF routing information and adjusting and optimizing OSPF networks, along with typical examples.
3 IS-IS Configuration	This chapter describes the IS-IS fundamentals and configuration steps for basic IS-IS functions, controlling IS-IS routing information, adjusting and optimizing IS-IS, along with typical examples.
4 RIP Configuration	This chapter describes the RIP fundamentals and configuration steps for basic RIP functions, controlling BGP routing information, adjusting and optimizing RIP, along with typical examples.
5 BGP Configuration	This chapter describes the BGP fundamentals and configuration steps for basic BGP functions, controlling BGP routing information, adjusting and optimizing BGP, along with typical examples.
6 Routing Policy Configuration	This chapter describes the fundamentals of the routing policy and configuration steps for filtering lists, the routing policy, along with typical examples.
7 MCE Configuration	This chapter describes the MCE fundamentals and configuration steps for basic MCE functions, controlling BGP routing information, adjusting and optimizing MCE, along with typical examples.

Conventions

Symbol Conventions

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

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injuries.
 CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 TIP	Indicates a tip that may help you address a problem or save your time.
 NOTE	Provides additional information to emphasize or supplement important points of the main text.

General Conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Boldface	Names of files, directories, folders, and users are in Boldface . For example, log in as user Root .
<i>Italic</i>	Book titles are in <i>Italics</i> .
Courier New	Examples of information displayed on the screen are in Courier New.

Command Conventions

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.

Convention	Description
{ x y ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x y ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none 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 alternative items are grouped in square brackets and separated by vertical bars. Several or none is selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

GUI Conventions

Convention	Description
boldface	Buttons, menus, parameters, tabs, windows, and dialog titles are in boldface . For example, click OK .
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose File > Create > Folder .

Keyboard Operations

Convention	Description
Key	Press the key. For example, press Enter and press Tab .
Key 1+Key 2	Press the keys concurrently. For example, pressing Ctrl+Alt+A means the three keys should be pressed concurrently.
Key 1, Key 2	Press the keys in turn. For example, pressing Alt, F means the two keys should be pressed in turn.

Mouse Operations

Convention	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.

Convention	Description
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

Update History

Updates between document issues are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Updates in Issue 01 (12.26.08)

This is the first release.

1 Static Route Configuration

About This Chapter

This section describes how to configure IS-IS to generate routes based on specified rules and set the rules for route leaking.

[1.1 Introduction](#)

This section describes basic concepts of static routes.

[1.2 Configuring a Static Route](#)

This section describes how to configure a static route.

[1.3 Configuring BFD for Static Routes in the Public Network](#)

This section describes how to configure BFD for static routes.

[1.4 Configuration Examples](#)

This section provides several configuration examples of static routes and BFD for static routes.

1.1 Introduction

This section describes basic concepts of static routes.

1.1.1 Static Routes

1.1.2 Default Static Routes

1.1.3 BFD for Static Routes

1.1.4 Static Routes Supported by the Interface of the S-switch

1.1.5 Logical Relationships Between the Configuration Tasks

1.1.6 Update History

1.1.1 Static Routes

Static routes refer to the routes that are configured manually.

When the network is simple or the topology seldom changes, you need to configure only static routes to make the network run normally. Proper configuration and usage of static routes can improve the network performance and provide fixed routes for important applications.

The advantages of static routes are as follows:

- Static routes can be easily implemented.
- Static routes occupy less network resources.
- Static routes can be used to control routing selection.

The disadvantage of static routes is as follows:

- When a fault occurs in the network or the topology changes, static routes cannot automatically change and must be changed by an administrator.

1.1.2 Default Static Routes

The default route is a special route. The administrators can manually configure a default route. The default route, however, can also be generated through dynamic routing protocols, such as the Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) protocols.

The default route is used when no routing entry is matched. In a routing table, the destination address of the default route is 0.0.0.0 with the mask being 0.0.0.0. You can check whether the default route is configured by using the **display ip routing-table** command.

If the destination IP address of a packet does not match any entry in the routing table, the default route is selected to forward this packet. If neither the default route nor the destination address of the packet exists in the routing table, the packet is discarded. An Internet Control Message Protocol (ICMP) packet is then sent, reporting that the destination address or the destination network is unreachable.

1.1.3 BFD for Static Routes

Compared with the dynamic routing protocol, static routes do not have a detection mechanism. When a fault occurs in the network, the administrator needs to reconfigure static routes.

BFD for static routes is used to bind a BFD session to each static route.

- When the BFD session that is bound to a static route detects a fault, that is, the link changes from Up to Down, BFD reports the fault to the Routing Management (RM). Then, RM sets the route to inactive. That is, the route is unavailable and is deleted from the routing table.
- When the BFD session that is bound to a static route is set up, that is, the link changes from Down to Up, BFD reports the event to RM. Then, RM sets the route to active. That is, the route is available and is added to the routing table.

1.1.4 Static Routes Supported by the Interface of the S-switch

Before configuring static routes, you need assign IP addresses to interfaces so that the networks can interconnect. The physical interface except the MEth interface of the S-switch is a Layer 2 interface; therefore, it cannot be assigned an IP address. In this case, you can configure the S-switch through the following methods:

- Creating a VLAN to which the Layer 2 interface belongs and assigning an IP address to the VLANIF interface
- Assigning an IP address to the loopback interface

1.1.5 Logical Relationships Between the Configuration Tasks

Setting the default preference of the static route is optional.

1.1.6 Update History

Version	Revision
V100R002C01B050	This is the first release.

1.2 Configuring a Static Route

This section describes how to configure a static route.

[1.2.1 Establishing the Configuration Task](#)

[1.2.2 \(Optional\) Setting the Default Preference of a Static Route](#)

[1.2.3 Configuring a Static Route](#)

[1.2.4 Checking the Configuration](#)

1.2.1 Establishing the Configuration Task

Applicable Environment

When the network is simple or the topology seldom changes, you can configure static routes to make the network run normally.

Static routes can be set with different preferences, so routing management policies are flexibly applied. For example, when you configure multiple routes to the same destination, load balancing can be performed, if you set the same preference for the routes; route backup can be carried out, if you set different preferences for the routes.

A default route exists in a routing table. In this manner, the packet is not discarded and is forwarded according to the default route when no routing entry is matched.

Pre-configuration Tasks

Before configuring a static route, complete the following tasks:

- Configuring physical parameters of interfaces
- Creating a VLAN to which each interface belongs
- Assigning an IP address to each VLANIF interface to make the network layer reachable between the interfaces

Data Preparation

To configure a static route, you need the following data.

No.	Data
1	(Optional) Default preference of a default route
2	Destination IP address and sub-net mask, IP address of the next hop, or local outbound interface

1.2.2 (Optional) Setting the Default Preference of a Static Route

Context

By default, the preference of a static route is 60.

When a static route is configured, the default preference is used, if the preference is not re-set. After the default preference is re-set, the re-set one is valid for new static routes only.

Do as follows on the S-switchs that need be configured with the default preferences of static routes.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ip route-static default-preference preference** command to set the default preference of a static route.

----End

1.2.3 Configuring a Static Route

Context

You should specify the next hop address when configuring a static route on the S-switch. This is because the physical interfaces of the S-switch are Ethernet interfaces of the broadcast type and can be associated with multiple next hop addresses for the same outbound interface. The next hop thus fails to be uniquely identified. If the outbound interface must be specified, you must specify the next hop address of the outbound interface.

Do as follows on the S-switches that need forward data across multiple network segments.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ip route-static** *ip-address* { *mask* | *mask-length* } [**vpn-instance** *vpn-instance-name*] { *nexthop-address* | *interface-type interface-number* [*nexthop-address*] } [**preference** *preference*] * [**track bfd-session** *cfg-name*] [**description** *text*] command to set a static route. If the **ip route-static** command is used to configure a static route and the destination address and the mask are set to 0.0.0.0 0.0.0.0, it indicates that default route is configured.

----End

1.2.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the summary of the IP routing table.	display ip routing-table
Check detailed information about the IP routing table.	display ip routing-table verbose

Run the **display ip routing-table** command. You can view information about the routing table and the configured static route in the routing table.

```
<Quidway> display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 4          Routes : 4

Destination/Mask    Proto  Pre  Cost    FlagsNextHop        Interface
-----
0.0.0.0/0           Static 60   0        RD    1.1.4.2      Vlanif10
1.1.1.0/24          Direct 0     0         D    1.1.1.1      Vlanif30
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      Vlanif1
```

1.3 Configuring BFD for Static Routes in the Public Network

This section describes how to configure BFD for static routes.

1.3.1 Establishing the Configuration Task

[1.3.2 \(Optional\) Configuring a Static Route](#)[1.3.3 Creating a BFD Session](#)[1.3.4 Binding a Static Route to a BFD Session](#)[1.3.5 Checking the Configuration](#)

1.3.1 Establishing the Configuration Task

Applicable Environment

The configured static route does not change automatically regardless of the link changes. When a packet is transmitted according to the set static route, the packet may be lost or a loop may occur.

BFD for static routes in the public network provides fast detection. The BFD session can detect the connectivity of the network automatically. When BFD detects a link failure, it sets the static route bound to the BFD session to invalid, if the static route is bound to the BFD session. After the link is recovered, the static route bound to the BFD session is enabled automatically.

Pre-configuration Tasks

Before configuring BFD for static routes, complete the following tasks:

- Configuring physical parameters of interfaces
- Creating a VLAN to which each interface belongs
- Assigning an IP address to each VLANIF interface to make the network layer reachable between the interfaces

Data Preparation

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

No.	Data
1	Destination network address and mask, IP address of the next hop, or local outbound interface
2	IP address of the peer device detected by BFD, and local and remote discriminators of the BFD session

1.3.2 (Optional) Configuring a Static Route

Context

To run a BFD session, the reachable forwarding path should exist in the routing table. When you set up the BFD session on both ends of the non-directly-connected network, you should first configure a static route. Then, the BFD session can run normally. The BFD session that is set up at both ends of the directly connected network need not be configured with static routes.

Procedure

1.2 Configuring a Static Route

----End

1.3.3 Creating a BFD Session

Procedure

Refer to the *Quidway S5300 Series Ethernet Switches Configuration Guide - Reliability*.

----End

1.3.4 Binding a Static Route to a BFD Session

Context

When a static route is bound to a BFD session, ensure that the BFD session and the static route reside on the same link. A static route can be bound to only one BFD session.

Do as follows on the S-switches at both ends of the link that need be bound to the BFD session.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ip route-static** *ip-address { mask | mask-length } [vpn-instance vpn-instance-name] { nexthop-address | interface-type interface-number [nexthop-address] } [preference preference] * [track bfd-session cfg-name] [description text]* command to bind the static route in the public network to the BFD session.

----End

1.3.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the BFD session.	display bfd session { all discriminator <i>discriminator</i> peer-ip <i>peer-ip</i> } [verbose]
Check the configuration of BFD for static routes.	display current-configuration include bfd

Run the **display bfd session** command. If you can view information about the BFD session and the state field is Up, it means that the configuration succeeds.

```
<Quidway> display bfd session all
```

```
-----
Local      Remote    PeerIPAddress  Interface Name  State      Type
-----
```

```
10      20      1.1.1.2      --      Up      S_IP
-----
Total UP/DOWN Session Number : 1/0
```

Run the **display current-configuration | include bfd** command in the system view. You can view that the BFD session is bound to the static route.

```
<Quidway> 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
```

1.4 Configuration Examples

This section provides several configuration examples of static routes and BFD for static routes.

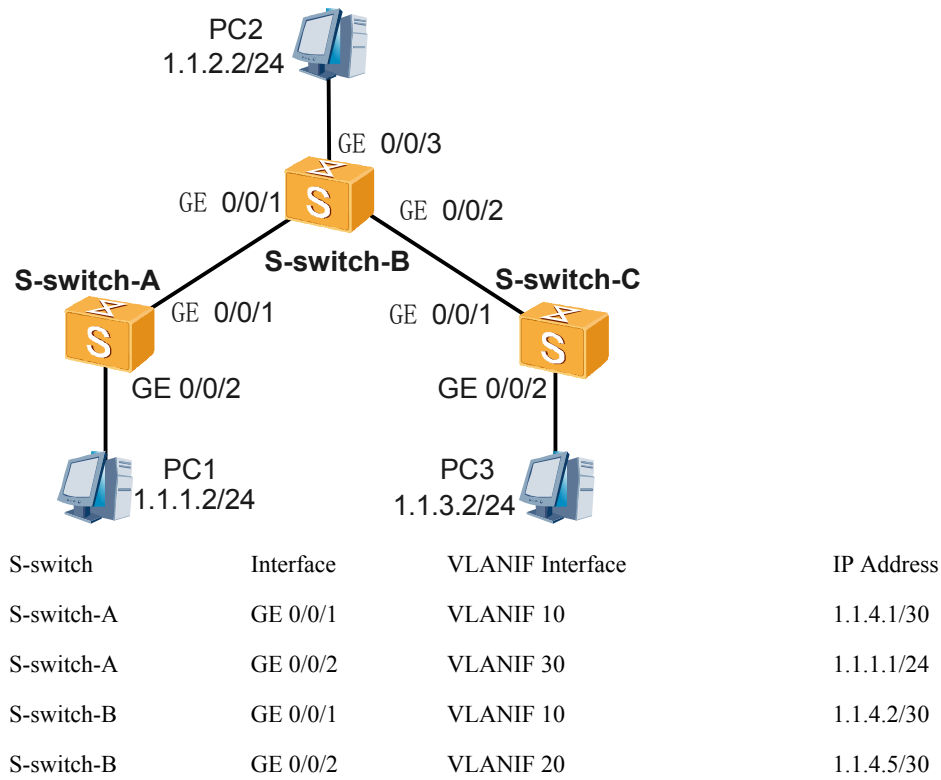
- 1.4.1 Example for Configuring Static Routes
- 1.4.2 Example for Configuring BFD for Static Routes

1.4.1 Example for Configuring Static Routes

Networking Requirements

The PCs that belong to different network segments are connected through several S-switchs. Static routes should be used so that any two PCs in different network segments can communicate with each other.

Figure 1-1 Networking diagram of configuring static routes



S-switch-B	GE 0/0/3	VLANIF 40	1.1.2.1/24
S-switch-C	GE 0/0/1	VLANIF 20	1.1.4.6/30
S-switch-C	GE 0/0/2	VLANIF 50	1.1.3.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN to which each interface belongs.
2. Assign an IP address to each VLANIF interface.
3. Configure a default IP gateway on each host.
4. Configure static routes and default routes on each S-switch.

Data Preparation

To complete the configuration, you need the following data:

- The IDs of the VLANs to which the interfaces belong are shown in [Figure 1-1](#).
- The VLANIF interfaces and the IP addresses of the hosts are shown in [Figure 1-1](#).
- The next hop address of the default route on S-switch-A is 1.1.4.2.
- The destination address of S-switch-B is 1.1.1.0, and the next hop address of the static route is 1.1.4.1.
- The destination address of S-switch-B is 1.1.3.0, and the next hop address of the static route is 1.1.4.6.
- The next hop address of the default route on S-switch-C is 1.1.4.5.

Configuration Procedure

1. Create a VLAN to which each interface belongs.
The configuration details are not mentioned here.
2. Assign an IP address to each interface.
The configuration details are not mentioned here.
3. Configure the hosts.
Configure default gateways of the hosts PC1, PC2, and PC3 as 1.1.1.1, 1.1.2.1, and 1.1.3.1 respectively.
4. Configure static routes.
Configure a default route on S-switch-A.

```
<S-switch-A> system-view
[S-switch-A] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
```


Configure two static routes on S-switch-B.

```
<S-switch-B> system-view
[S-switch-B] ip route-static 1.1.1.0 255.255.255.0 1.1.4.1
[S-switch-B] ip route-static 1.1.3.0 255.255.255.0 1.1.4.6
```


Configure a default route on S-switch-C.

```
<S-switch-C> system-view
[S-switch-C] ip route-static 0.0.0.0 0.0.0.0 1.1.4.5
```
5. Verify the configuration.

Check the routing table of S-switch-A.

[S-switch-A] **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
0.0.0.0/0	Static	60	0	RD	1.1.4.2	Vlanif10
1.1.1.0/24	Direct	0	0	D	1.1.1.1	Vlanif30
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	Vlanif10
1.1.4.1/32	Direct	0	0	D	127.0.0.1	InLoopBack
1.1.4.2/32	Direct	0	0	D	1.1.4.2	Vlanif10
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.

[S-switch-A] **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.

[S-switch-A] **tracert 1.1.3.1**

traceroute to 1.1.3.1(1.1.3.1) 30 hops max, 40 bytes packet

1 1.1.4.2 31 ms 32 ms 31 ms

2 1.1.4.6 62 ms 63 ms 62 ms

Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
vlan batch 10 30
#
interface Vlanif10
ip address 1.1.4.1 255.255.255.252
#
interface Vlanif30
ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 30
#
ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
```

```

vlan batch 10 20 40
#
interface Vlanif10
 ip address 1.1.4.2 255.255.255.252
#
interface Vlanif20
 ip address 1.1.4.5 255.255.255.252
#
interface Vlanif40
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/3
 port trunk allow-pass vlan 40
#
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 S-switch-C

```

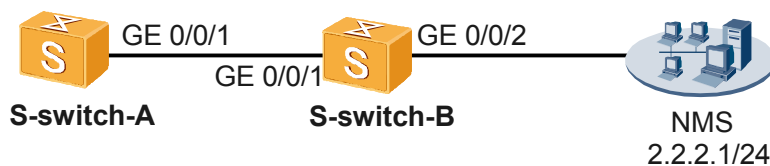
#
sysname S-switch-C
#
vlan batch 20 50
#
interface Vlanif20
 ip address 1.1.4.6 255.255.255.252
#
interface Vlanif40
 ip address 1.1.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 50
#
ip route-static 0.0.0.0 0.0.0.0 1.1.4.5
#
return

```

1.4.2 Example for Configuring BFD for Static Routes

Networking Requirements

As shown in [Figure 1-2](#), S-switch-A is connected to the Network Management System (NMS) through S-switch-B. You can configure static routes on S-switch-A so that S-switch-A can communicate with the NMS. A BFD session is set up between S-switch-A and S-switch-B to detect link failures.

Figure 1-2 Networking diagram of configuring BFD for static routes

S-switch	Interface	VLANIF Interface	IP Address
S-switch-A	GE 0/0/1	VLANIF 10	1.1.1.1/24
S-switch-B	GE 0/0/1	VLANIF 10	1.1.1.2/24
S-switch-B	GE 0/0/2	VLANIF 20	2.2.2.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a BFD session on S-switch-A and S-switch-B to detect the link between S-switch-A and S-switch-B.
2. Configure a static route from S-switch-A to the NMS and bind the static route to the BFD session.

Data Preparation

To complete the configuration, you need the following data:

- The IDs of the VLANs to which the interfaces belong are shown in [Figure 1-2](#).
- The VLANIF interfaces and the IP addresses of the hosts are shown in [Figure 1-2](#).
- IP address of the peer detected by BFD.
- Local and remote discriminators of the BFD session.
- Static route from S-switch-A to the NMS.

Configuration Procedure

The following lists the configuration procedure of the S-switch. For the configuration procedure of other devices shown in [Figure 1-2](#), refer to the related configuration guides.

1. Configure the VLAN that each interface belongs to.
The configuration details are not mentioned here.
2. Configure the IP address for each interface.
The configuration details are not mentioned here.
3. Create a BFD session between S-switch-A and S-switch-B.

On S-switch-A, create a BFD session with S-switch-B.

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

On S-switch-B, create a BFD session with S-switch-A.

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

4. Configure a default static route and bind a BFD session to the default static route.

On S-switch-A, configure a default static route to the external network and bind the default static route to a BFD session named aa.

```
[S-switch-A] ip route-static 2.2.2.1 24 1.1.1.2 track bfd-session aa
[S-switch-A] quit
```

5. Verify the configuration.

Run the **display bfd session all** command on S-switch-A and S-switch-B. You can view that the BFD session is set up and its status is Up.

Take the display on S-switch-A as an example.

```
<S-switch-A> display bfd session all
-----
--
Local      Remote    PeerIPAddress      Interface Name      State      Type
-----
--
10         20         1.1.1.2            --                  Up
S_IP
-----
--
Total UP/DOWN Session Number : 1/0
```

Run the **display ip routing-table** command on S-switch-A. You can view that the static route exists in the routing table.

```
<S-switch-A> 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
1.1.1.0/24            Direct 0    0     D      1.1.1.1      Vlanif10
1.1.1.1/32            Direct 0    0     D      127.0.0.1    InLoopBack0
1.1.1.2/32            Direct 0    0     D      1.1.1.2      Vlanif10
2.2.2.0/24            Static 60   0     RD     1.1.1.2      Vlanif10
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
```

On S-switch-A, enable the debugging on the terminal.

```
<S-switch-A> terminal monitor
<S-switch-A> terminal debugging
```

Run the **shutdown** command on VLANIF 10 of S-switch-B to simulate a link fault.

```
[S-switch-B] interface vlanif 10
[S-switch-B-Vlanif10] shutdown
```

You can view the following debugging information on S-switch-A. The information indicates that BFD detects a link fault.

```
<S-switch-A>
*0.27708400 S-switch-A RM/3/RMDEBUG:
RM_USR_BFDRefreshRT_H:
BfdSessionID = 10
BfdEvent      = 0X0
USR : UsrDbID = 0X6, DestAdd = 0X0, Mask = 0X0, NextHop = 0X1010102
URT : TableID = 0X1, EntryID = 0XB, ProcID = 0X2, FLAG = 0X8114000
```

Run the **display ip routing-table** command on S-switch-A. You can view that default route 2.2.2.0/24 does not exist. This is because the BFD session is bound to the default static route. When BFD detects a fault, it rapidly notifies that the bound static route is unavailable.

```
<S-switch-A> display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 5          Routes : 5
Destination/Mask    Proto   Pre  Cost   Flags  NextHop    Interface
1.1.1.0/24         Direct  0    0      D      1.1.1.1     Vlanif10
1.1.1.1/32         Direct  0    0      D      127.0.0.1   InLoopBack0
1.1.1.2/32         Direct  0    0      D      1.1.1.2     Vlanif10
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 **undo shutdown** command on VLANIF 10 of S-switch-B to simulate link recovery.

```
[S-switch-B-Vlanif10] undo shutdown
```

Run the **display ip routing-table** command on S-switch-A. You can view that default route 2.2.2.0/24 exists. When BFD detects link recovery, it rapidly notifies that the bound static route is available.

```
<S-switch-A> 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
1.1.1.0/24         Direct  0    0      D      1.1.1.1     Vlanif10
1.1.1.1/32         Direct  0    0      D      127.0.0.1   InLoopBack0
1.1.1.2/32         Direct  0    0      D      1.1.1.2     Vlanif10
2.2.2.0/24         Static  60    0      RD     1.1.1.2     Vlanif10
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
```

Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
vlan batch 10
#
bfd
#
interface Vlanif10
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
bfd aa bind peer-ip 1.1.1.2
 discriminator local 10
 discriminator remote 20
 commit
#
ip route-static 2.2.2.0 255.255.255.0 1.1.1.2 track bfd-session aa
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
vlan batch 10 20
```

```
#
bfd
#
interface Vlanif10
 ip address 1.1.1.2 255.255.255.0
#
interface Vlanif20
 ip address 2.2.2.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 20
#
bfd bb bind peer-ip 1.1.1.1
 discriminator local 20
 discriminator remote 10
 commit
#
return
```


2 OSPF Configuration

About This Chapter

This chapter describes the OSPF fundamentals, configuration steps for OSPF functions, and typical examples.

[2.1 Overview](#)

This section describes the principle and concepts of OSPF.

[2.2 Configuring Basic OSPF Functions](#)

This section describes how to configure basic OSPF functions.

[2.3 Setting Up and Maintaining the OSPF Neighbor Relationship or the Adjacency](#)

This section describes how to set up and maintain the OSPF neighbor relationship or the adjacency.

[2.4 Configuring OSPF Area Features](#)

This section describes how to configure OSPF area features.

[2.5 Configuring OSPF Attributes in Different Network Types](#)

This section describes how to change the network type of the interface forcibly as required and configure DR election of OSPF in broadcast and NBMA networks.

[2.6 Configuring OSPF Route Attributes](#)

This section describes how to set the link cost, the priority, and the maximum number of equal-cost routes of OSPF.

[2.7 Configuring OSPF Route Aggregation](#)

This section describes how to configure route aggregation of OSPF.

[2.8 Configuring an OSPF Process to Filter Routes](#)

This section describes how to configure the filtering for OSPF routes and import routes of other routing protocols.

[2.9 Adjusting and Optimizing an OSPF Network](#)

This section describes how to adjust and optimize the OSPF network as required.

[2.10 Improving the Security of an OSPF Network](#)

This section describes how to configure the OSPF area authentication and interface authentication.

[2.11 Configuring OSPF Network Management](#)

This section describes how to configure the OSPF MIB binding, OSPF Trap function, and log function.

[2.12 Maintaining OSPF](#)

This section describes how to maintain OSPF.

[2.13 Configuring Examples](#)

This section provides several configuration examples of OSPF.

2.1 Overview

This section describes the principle and concepts of OSPF.

[2.1.1 Introduction](#)

[2.1.2 OSPF Features Supported by the S-switch](#)

[2.1.3 Logical Relationships Between the Configuration Tasks](#)

[2.1.4 Update History](#)

[2.1.5 References](#)

2.1.1 Introduction

The Open Shortest Path First (OSPF) protocol, developed by the Internet Engineering Task Force (IETF), is an internal gateway protocol based on the link state. At present, OSPF version 2, as explained in RFC 2328, is used for IPv4.



NOTE

In this document, OSPF refers to OSPFv2, unless otherwise stated.

OSPF Features

OSPF has the following features:

- Wide applications: OSPF is applicable to a network in which hundreds of S-switches and routers are connected.
- Fast convergence: When the network topology changes, LSU packets are transmitted to synchronize the LSDBs of all the devices in an AS.
- Loop-free: According to the collected link status, OSPF calculates routes through the SPF algorithm. This algorithm ensures the generation of loop-free routes.
- Area partition: An AS is partitioned into areas to simplify the AS management. Less bandwidth is consumed by the aggregated routes transmitted within the AS.
- Equal-cost route: OSPF allows multiple equal-cost routes to the same destination.
- Routing hierarchy: Four types of routes are available. They are listed in a descending order of the preference: intra-area, inter-area, Type 1 external, and Type 2 external routes.
- Authentication: Area authentication and interface authentication are used to ensure the security of packet exchange.
- Multicast: Protocol packets are transmitted in multicast mode only on certain types of links to reduce the interference for some devices that are not enabled with OSPF.

Calculation of OSPF Routes

OSPF routes are calculated in the following methods:

- Based on the surrounding network topology, each OSPF device generates an LSA. The OSPF device sends LSU packets containing the LSA to other OSPF devices.

- Each OSPF device collects the LSAs from other devices in the same AS, and all these LSAs constitute the LSDB. An LSA describes the network topology around a S-switch, whereas an LSDB describes the network topology of the entire AS.
- OSPF devices transform the LSDB into a directed map based on weights. The directed map based on weights reflects the topology of the AS. All devices of the same area have the same map.
- According to the directed map, each S-switch uses the SPF algorithm to calculate the shortest path tree with itself being the root. The tree shows the routes to each node in the area.

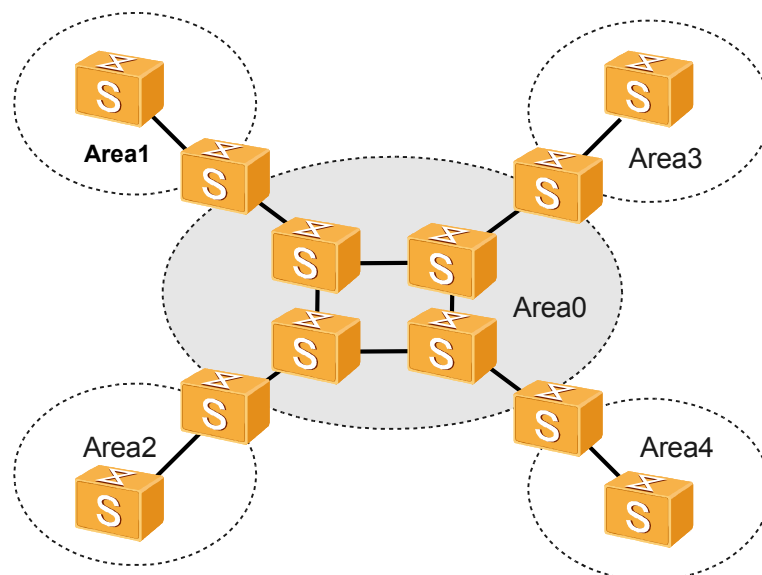
OSPF Area Partition

Suppose that all routers in a large-scale network run OSPF and the nodes increase with the expansion of the network. This leads to a large LSDB on each node. Such a Link State Database (LSDB) occupies a great amount of memory, complicates the calculation of the Shortest Path First (SPF) algorithm, and increases the burden of the CPU.

Due to the network expansion, the network topology is prone to changes. That is, the route flapping often occurs. A great number of OSPF packets are transmitted on the network, and the utilization of the bandwidth is reduced. In addition, each change in topology requires all the nodes to recalculate the routes.

OSPF addresses the preceding problem by partitioning an Autonomous System (AS) into areas. The area is regarded as a logical group. Each area is identified uniquely by an area ID. At the border of an area resides a S-switch rather than a link. A network segment or a link can belong to only one area. That is, each interface enabled with OSPF must specify to which area it belongs, as shown in [Figure 2-1](#).

Figure 2-1 OSPF area partition



After area partition, route aggregation can be enabled on the Area Border Routers (ABRs) to reduce the Link State Advertisements (LSAs) advertised to other areas. Route aggregation also minimizes the impact caused by topology changes.

Types of the S-switchs in an AS

Based on their locations in an AS, the S-switchs that run OSPF are classified into the following types:

- Internal routers

All interfaces of the S-switchs belong to the same OSPF area.

- ABRs

The S-switchs can belong to over two areas, but one of the areas must be a backbone area. An ABR is used to connect the backbone area and the non-backbone areas. An ABR is physically or logically connected to the backbone area.

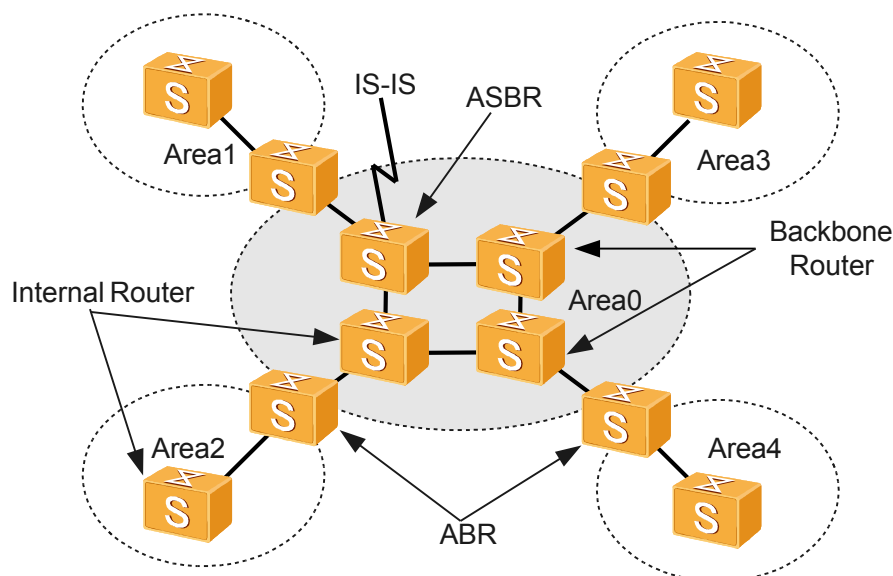
- Backbone routers

A minimum of one interface on the S-switch of this type must belong to the backbone area. All ABRs and internal nodes in Area 0, therefore, are backbone routers.

- ASBRs

The S-switch exchanges routing information with other ASs. An AS Boundary Router (ASBR) is not necessarily on the AS border. It can be an internal router or an ABR. When an OSPF device imports some external routes, it becomes an ASBR.

Figure 2-2 OSPF device types



OSPF Network Types

When OSPF is enabled, the networks are classified into the following 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 network, Hello packets, LSU packets, and LSAck packets are transmitted in multicast mode (224.0.0.5: the reserved IP broadcast address of the OSPF node; 224.0.0.6: the reserved IP multicast address of the OSPF DR), and DD packets and LSR packets are transmitted in unicast mode.

- NBMA: If the link layer protocol is Frame Relay, ATM, or X.25, OSPF defaults the network type to NBMA. In this type of network, the protocol packets, such as Hello packets, Database Description (DD) packets, Link State Request (LSR) packets, Link State Update (LSU) packets, and Link State Acknowledgement (LSAck) packets, are transmitted in unicast mode.
- P2MP: Regardless of link layer protocols, OSPF does not default the network type to P2MP. A P2MP network must be changed from other network types. Generally, a non-fully connected NBMA network is changed to P2MP. In this type of network, the protocol packets, such as Hello packets, DD packets, LSR packets, LSU packets, and LSAck packets, are transmitted in multicast mode.
- P2P: If the link layer protocol is the Point-to-Point Protocol (PPP), the High-level Data Link Control (HDLC), or the Link Access Procedure, Balanced (LAPB), OSPF defaults the network to P2P. In the P2P network, the protocol packets, such as Hello packets, DD packets, LSR packets, LSU packets, and LSAck packets, are transmitted in multicast mode (224.0.0.5).

The link layer protocol of the physical interface of the S-switch is Ethernet, so OSPF defaults the network of the S-switch interface to broadcast.

2.1.2 OSPF Features Supported by the S-switch

Interfaces That Supports OSPF

The S-switch need set up the OSPF routing table and configure all features on Layer 3 interfaces, but most physical interfaces of the S-switch are Layer 2 interfaces. In this case, use the following methods to configure the S-switch:

- Configure a VLAN to which the Layer 2 interface belongs, assign an IP address to the VLANIF interface, and enable OSPF.
- Assign an IP address to a loopback interface and enable OSPF.

Multi-Process

OSPF supports multi-process. A maximum of 50 OSPF processes can be run on the same S-switch, and is independent of each other. The route interaction between different OSPF processes is similar to the interaction between different routing protocols.

An interface of a S-switch can belong to only one OSPF process.

Authentication

OSPF supports packet authentication. Only the OSPF packets that pass the authentication are received. Otherwise, the neighbor relationship cannot be set up. The S-switch supports the following authentication modes:

- Area authentication
- Interface authentication

If both modes are available, the latter is preferred.

OSPF HSB

The S-switch, in a distributed structure, supports OSPF hot standby (HSB). OSPF backs up necessary information from the Main Processing Unit (MPU) to the Service Interface Card (SIC). When the MPU fails, the SIC replaces it to ensure normal operation of OSPF.

OSPF supports the following HSB modes:

- Backing up all OSPF data: When the switching between the MPU and the SIC occurs, OSPF can be restored immediately.
- Backing up only the OSPF configuration: When the switching between the MPU and the SIC occurs, OSPF performs GR, obtains the adjacency from its neighbors, and synchronizes the LSDBs.

Smart-Discover

Generally, the S-switch sends Hello packets periodically from the interface on which OSPF is run. Through Hello packets, the S-switches can set up and maintain the neighbor relationship, and elect a Designated Router (DR) and a Backup Designated Router (BDR) on the multi-address network of broadcast or Non-Broadcast Multi-Access (NBMA). When the neighbor relationship is set up and the DR and BDR are elected on the multi-address network, the interface sends Hello packets only when the Hello timer expires. This affects the speed of setting up the neighbor relationship and electing the DR and BDR.

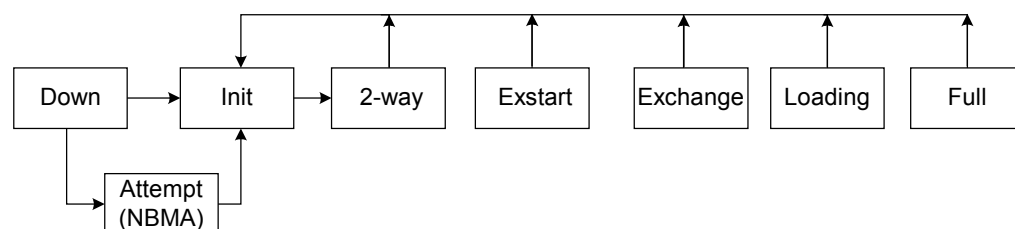
NOTE

- The interval for sending Hello packets on an interface depends on that set on the interface.
- The default interval for sending Hello packets varies with network types.

The smart-discover function can solve the preceding problems:

- In broadcast and NBMA networks, set up the neighbor relationship rapidly and elect a DR and a BDR on the networks.
 - When the neighbor status first reaches 2-way or changes from 2-way or higher to Init, the interface enabled with smart-discover sends Hello packets to neighbors immediately after it receives Hello packets of neighbors and finds that the neighbor status changes, as shown in [Figure 2-3](#). At this time, the interface need not wait for the timeout of the Hello timer.

Figure 2-3 Changes of neighbor state machines



- When the status of an interface of the DR and BDR on the multi-address network changes, the interface enabled with smart-discover sends Hello packets on the network segment and participates in the election of a DR or BDR.

On Point-to-Point (P2P) or Point-to-Multipoint (P2MP) networks, the principle of setting up the adjacency fast is the same as that of broadcast and NBMA networks.

OSPF GR

Graceful Restart (GR) is used to restart the device gracefully. It does not affect the forwarding of the traffic, or causes route flapping due to short restart of the S-switch.

If a S-switch does not restart OSPF in GR mode, its adjacent device removes it from the neighbor list and notifies other devices. This leads to the SPF recalculation. When a S-switch needs to be shut down for a very short time, it does not affect the topology of the whole network. When the S-switch is restored within a few seconds, the adjacency is established and the SPF is recalculated.

To prevent unnecessary SPF calculation, when a S-switch restarts OSPF in GR mode, it notifies its adjacent nodes that it is shut down just for a few minutes and is restored soon. The adjacent node, therefore, does not remove the S-switch in GR mode from the neighbor list. Other devices do not know that the router restarts. This avoids route flapping caused by changes of the neighbor relationship.

NOTE

"Protocol restart" stated in this manual refers to OSPF restarted in GR mode, unless otherwise stated.

When a S-switch 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 certain period. This ensures that the traffic forwarding is not interrupted when a protocol restart occurs.

2.1.3 Logical Relationships Between the Configuration Tasks

[2.2 Configuring Basic OSPF Functions](#) is the prerequisite and basis of other configurations.

2.1.4 Update History

Version	Revision
V100R002C01B050	This is the first release.

2.1.5 References

For more information about OSPF, refer to the following document.

Document No.	Description
RFC 2328	OSPF Version 2

2.2 Configuring Basic OSPF Functions

This section describes how to configure basic OSPF functions.

[2.2.1 Establishing the Configuration Task](#)

[2.2.2 Enabling OSPF and Entering the OSPF View](#)

2.2.3 Configuring Network Segments That Each Area Includes

2.2.4 Checking the Configuration

2.2.1 Establishing the Configuration Task

Applicable Environment

If OSPF need be configured on the S-switch in the network, configure basic OSPF functions on each device, enable OSPF, specify the interface enabled with OSPF and the area number, and then configure other functions of OSPF.

When multiple devices are configured in the same area, most configuration data, such as timer, filter, and aggregation, should be kept consistent in the area. Incorrect configuration may make neighboring nodes fail to send messages to each other, and even lead to path congestion or self-loop.

Pre-configuration Tasks

Before configuring basic OSPF functions, complete the following tasks:

- Configuring a link layer protocol
- Configuring a VLAN to which each interface belongs
- Assigning network layer addresses to VLANIF interfaces to ensure the network layer connectivity between OSPF neighbors



NOTE

An interface can be added to a VLAN through the default method or by running the **port trunk allow-pass vlan** command. When the interface is added to the VLAN through the **port trunk allow-pass vlan** command, the directly connected physical interfaces of the same network segment must be added to the same VLAN. The S-switch can then implement interconnection at the network layer between VLANIF interfaces. The interface that is added to the VLAN at both ends of a link must be the same.

Data Preparation

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

No.	Data
1	Router ID
2	OSPF process ID
3	Area to which each interface belongs

2.2.2 Enabling OSPF and Entering the OSPF View

Context

Do as follows on each S-switch in an area.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf [vpn-instance vpn-instance-name] [process-id | router-id router-id] *** command to start an OSPF process, enter the OSPF view, and set the router ID of the local device.

To ensure the stability of OSPF, you should determine the router ID of each device during network planning. You should also manually set the router ID for each device by running the **ospf [vpn-instance vpn-instance-name] [process-id | router-id router-id] *** command. When you manually configure the router ID of the S-switch, ensure that IDs of any two devices in an AS are different.



TIP

Generally, the configured router ID is the same as the IP address of a certain interface of the S-switch.

----End

2.2.3 Configuring Network Segments That Each Area Includes

Context

Do as follows on each S-switch in an area.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf [process-id]** command to start an OSPF process and enter the OSPF view.

Step 3 Run the **area area-id** command to enter the OSPF area view.

Step 4 Run the **network ip-address wildcard-mask** command to configure the network segments for the area.

This network segment refers to one of the IP addresses of the interface enabled with OSPF.

A network segment can belong to only one area; that is, you must specify an area for each interface enabled with OSPF.

OSPF can be run on an interface only when the following situations occur:

- The mask length of the IP address of an interface is greater than or equal to that in the **network** command.
- The primary IP address of an interface should be in the range of the network segment specified through the **network** command.

For a loopback interface, by default, the OSPF process advertises its IP address in 32-bit host route, which is irrelevant to the mask length of the IP address on the interface. To advertise the segment route of loopback interface, configure the network type as non-broadcast in the interface view, such as P2P. For details, see [2.5.2 Configuring Network Types for an Interface Enabled with OSPF](#).

----End

2.2.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the statistics of an OSPF process.	display ospf [<i>process-id</i>] cumulative
Check information about the LSDB of an OSPF process.	display ospf [<i>process-id</i>] lsdb [brief] display ospf [<i>process-id</i>] lsdb [router network summary asbr ase nssa] [<i>link-state-id</i>] [originate-router [<i>advertising-router-id</i>] self-originate]
Check information about neighboring nodes of an OSPF process.	display ospf [<i>process-id</i>] peer [{ [<i>interface-type</i> <i>interface-number</i>] [<i>neighbor-id</i>] } brief]
Check the routing table of an OSPF process.	display ospf [<i>process-id</i>] routing [<i>ip-address</i> [<i>mask</i> <i>mask-length</i>]] [interface <i>interface-type</i> <i>interface-number</i>] [nexthop <i>nexthop-address</i>]

Run the **display ospf peer** command. If you can view that the status of OSPF neighbor is **Full**, it means that the configuration succeeds.

```
<Quidway> display ospf peer

      OSPF Process 1 with Router ID 10.1.1.2
      Neighbors

Area 0.0.0.0 interface 10.1.1.2(Vlanif10)'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
  Neighbor is up for 00:00:05
  Authentication Sequence: [ 0 ]
```

2.3 Setting Up and Maintaining the OSPF Neighbor Relationship or the Adjacency

This section describes how to set up and maintain the OSPF neighbor relationship or the adjacency.

[2.3.1 Establishing the Configuration Task](#)

[2.3.2 \(Optional\) Setting the Interval for Sending Hello Packets](#)

[2.3.3 \(Optional\) Setting the Dead Interval of the Neighbor](#)

[2.3.4 \(Optional\) Setting the Interval for Retransmitting LSAs](#)

[2.3.5 \(Optional\) Setting Retransmission Limitation for OSPF Packets](#)

[2.3.6 \(Optional\) Suppressing an Interface from Receiving and Sending OSPF Packets](#)

2.3.7 Checking the Configuration

2.3.1 Establishing the Configuration Task

Applicable Environment

After an OSPF process is enabled, Hello packets are sent periodically through OSPF interfaces to discover and maintain the OSPF neighbor relationship. After an OSPF device receives these Hello packets, it checks some parameters carried in the packets. If the parameters of the two neighboring nodes are the same, they establish the neighbor relationship. If the S-switch does not receive Hello packets from the neighbor within the dead interval, the S-switch considers the neighbor as invalid.

By setting the interval for sending Hello packets and dead interval, the S-switch can improve the network convergence speed and utilize network bandwidth resources properly.

After the adjacency is established, both peers send LSU packets to synchronize the LSDBs. When a S-switch sends an LSA to its neighbor, it need wait for the LSAck packet of the peer. If the S-switch does not receive the LSAck packet within the interval for retransmitting LSAs, it retransmits the LSA. The S-switch can improve the convergence speed of OSPF network by setting the interval for retransmitting LSAs on the interface.

You can restrict the number of retransmission times of OSPF packets by configuring Retransmission Limitation for OSPF (RL-OSPF). If the number of transmission times expires, OSPF disconnects the neighbor. This avoids the infinite loop caused by continuous retransmission when the neighbor does not receive the packet.

If a certain interface of the S-switch need be isolated from the OSPF process, you can suppress the interface from receiving and sending OSPF packets.

Pre-configuration Tasks

Before setting up and maintain the OSPF neighbor relationship or the adjacency, complete the following tasks:

- Configuring a VLAN to which each interface belongs
- Assigning an IP address to each VLANIF interface to ensure the network layer connectivity between OSPF neighbors
- [2.2 Configuring Basic OSPF Functions](#)

Data Preparation

To set up and maintain the OSPF neighbor relationship or the adjacency, you need the following data.

No.	Data
1	(Optional) Interval for sending Hello packets
2	(Optional) Dead interval of the neighbor
3	(Optional) Interval for retransmitting LSAs
4	(Optional) Retransmission limitation count for OSPF packets

2.3.2 (Optional) Setting the Interval for Sending Hello Packets

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **ospf timer hello interval** command to set the interval for sending Hello packets for the interface.

By default, the interval for sending Hello packets on P2P and broadcast interfaces is 10s, and the interval for sending Hello packets on P2MP and NBMA interfaces is 30s.

The smaller the interval for sending Hello packets is, the faster the network topology changes and the greater the bandwidth cost of the network is.

The interval for sending Hello packets on the interface and that on the connected interface of the neighboring S-switch should be the same.

----End

Postrequisite

If the network type changes, the interval for sending Hello packets on the interface restores to the default value.

2.3.3 (Optional) Setting the Dead Interval of the Neighbor

Context

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **ospf timer dead interval** command to set the dead interval of the neighbor for the interface.

By default, the dead interval of an OSPF neighbor on P2P and broadcast interfaces is 40s, and the dead interval of an OSPF neighbor on P2MP and NBMA interfaces is 120s.

The dead interval of an OSPF neighbor: During the dead interval, if the device does not receive the Hello packet from the neighbor, it considers the neighbor as invalid.

The dead interval should be at least four times the interval for sending Hello packets. The dead interval of S-switch neighbors on the same network segment should be the same.

----End

Postrequisite

If the network type changes, the dead interval of the neighbor restores to the default value.

2.3.4 (Optional) Setting the Interval for Retransmitting LSAs

Context

When a S-switch sends an LSA to its neighbor, it need wait for the LSAck packet of the peer. If the S-switch does not receive the LSAck packet within the interval for retransmitting LSAs, it retransmits the LSA.

On a low-speed network, the interval for retransmitting LSAs on the interface should not be set small. Otherwise, unnecessary retransmission occurs. The interval is greater than the roundtrip of one packet transmitted on two nodes.

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **ospf timer retransmit interval** command to set the interval for retransmitting LSAs for the interface.

By default, the interval for retransmitting LSAs on an interface is 5s.

----End

2.3.5 (Optional) Setting Retransmission Limitation for OSPF Packets

Context

The OSPF packet retransmission mechanism is applied to DD packets, Update packets, and Request packets. When a S-switch sends these three packets to its neighbor, it need wait for the LSAck packet of the neighbor. If the S-switch does not receive response packets, it retransmits the packets. After the retransmission function is enabled and the number of retransmission times is set, the S-switch disconnects the neighbor after the specified number of retransmission times expires to prevent unnecessary retransmission.

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.

Step 2 Run the **ospf** [*process-id*] command to enter the OSPF view.

Step 3 Run the **retransmission-limit** [*max-number*] command to enable the retransmission limitation and set the maximum number of retransmission times.

If only the **retransmission-limit** command is configured and the optional parameter *max-number* is not configured, the number of retransmission times is 30.

By default, an OSPF process does not enable retransmission limitation.

----End

2.3.6 (Optional) Suppressing an Interface from Receiving and Sending OSPF Packets

Context

After an OSPF interface is set in the silent state, the interface can still advertise its direct route. The Hello packets on the interface, however, are blocked, and no neighbor relationship can be set up on the interface. This can enhance the OSPF capability to adapt to the networking and reduce the consumption of system resources.

Do as follows on the S-switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf** [*process-id*] command to start an OSPF process and enter the OSPF view.

Step 3 Run the **silent-interface** { **all** | *interface-type interface-number* } command to suppress the interface from receiving and sending OSPF packets.

If OSPF routing information need not be obtained by the device of a certain network and the local S-switch does not receive routing updates from other devices, you can run the **silent-interface** command to suppress an 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 a specified process is enabled, and is invalid for the interfaces of other processes.

----End

2.3.7 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the OSPF interface.	display ospf [<i>process-id</i>] interface [all <i>interface-type interface-number</i>] [verbose]
Check information about the OSPF neighboring node.	display ospf [<i>process-id</i>] peer [{ [<i>interface-type interface-number</i>] [<i>neighbor-id</i>] } brief]

Action	Command
Check information about the retransmission list of an OSPF process.	display ospf [<i>process-id</i>] retrans-queue [<i>interface-type interface-number</i>] [<i>neighbor-id</i>]
Check the summary of an OSPF process.	display ospf [<i>process-id</i>] brief
Check the statistics of an OSPF process.	display ospf [<i>process-id</i>] cumulative

Run the **display ospf interface** command. You can view detailed information about OSPF packet timer and the delay for transmitting LSAs on an interface.

```
<Quidway> display ospf interface vlanif 40

      OSPF Process 1 with Router ID 192.168.32.11
      Interfaces

Interface: 40.0.0.2 (Vlanif40)
Cost: 100      State: DR      Type: Broadcast      MTU: 1500
Priority: 1
Designated Router: 40.0.0.2
Backup Designated Router: 40.0.0.1
Timers: Hello 10 , Dead 40 , Poll 120 , Retransmit 5 , Transmit Delay 1
```

2.4 Configuring OSPF Area Features

This section describes how to configure OSPF area features.

[2.4.1 Establishing the Configuration Task](#)

[2.4.2 Configuring an OSPF Stub Area](#)

[2.4.3 Configuring an OSPF NSSA Area](#)

[2.4.4 Checking the Configuration](#)

2.4.1 Establishing the Configuration Task

Applicable Environment

After area partition, OSPF routes between non-backbone areas are updated by the backbone area. OSPF defines that all non-backbone areas should maintain the connectivity with the backbone area and the backbone area should maintain its own connectivity.

After area partition, the number of LSAs on the network is reduced and the expansibility of OSPF is enhanced. To reduce the size of routing tables and the number of LSAs, configure some non-backbone areas that reside at the AS border as stub areas.

The NSSA area is imported because stub areas cannot import external routes. In the NSSA area, transmitting Type7 LSAs is allowed. Generated by an ASBR in the NSSA area, a Type7 LSA is transformed to a Type5 LSA when it reaches the ABR of the NSSA area, and is advertised to other areas.

Pre-configuration Tasks

Before configuring OSPF area features, complete the following tasks:

- Configuring a VLAN to which each interface belongs
- Assigning an IP address to each VLANIF interface to ensure the network layer connectivity between OSPF neighbors
- [2.2 Configuring Basic OSPF Functions](#)

Data Preparation

To configure OSPF areas, you need the following data.

No.	Data
1	Type of the area
2	Interfaces included in the area
3	Default routes advertised to the area

2.4.2 Configuring an OSPF Stub Area

Context

Do as follows on the S-switches of the area that need not import external routes.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf [process-id]** command to enter the OSPF view.

Step 3 Run the **area area-id** command to enter the OSPF area view.

Step 4 Run the **stub [no-summary]** command to configure the current area as a stub area.

All nodes connected to a stub area must configure the current area as the stub area through the **stub** command.

When you run the **stub** command on an ABR, you can configure **no-summary**. By configuring **no-summary**, you can forbid Type3 LSAs instead of default routes to enter the stub area connected to the ABR Network-Summary-LSA. The routing entries of devices in the stub area are thus further reduced.

Step 5 (Optional) Run the **default-cost cost** command to set the cost of default routes sent to the stub area.

By default, the cost of default routes sent to the stub area is 1.

The command is applicable to only the ABR that is connected to a stub area.

----End

2.4.3 Configuring an OSPF NSSA Area

Context

Do as follows on the S-switch of the area that denies Type5 LSAs.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf** [*process-id*] command to start an OSPF process and enter the OSPF view.
- Step 3** Run the **area** *area-id* command to enter the OSPF area view.
- Step 4** Run the **nssa** [**default-route-advertise**] [**no-import-route**] [**no-summary**] command to configure the area as an NSSA area.

All nodes connected to an NSSA area must configure the current area as the NSSA area through the **nssa** command.

When you use the **nssa** command on an ABR, the optional parameters can be configured.

- Step 5** (Optional) Run the **default-cost** *cost* command to set the cost of the default route sent to the NSSA area.

By default, the cost of default routes sent to an NSSA area is 1.

The command is applicable to only the ABR that is connected to an NSSA area.

----End

2.4.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the LSDB of an OSPF process.	display ospf [<i>process-id</i>] lsdb [brief] display ospf [<i>process-id</i>] lsdb [router network summary asbr ase nssa] [link-state-id] [originate-router [<i>advertising-router-id</i>] self-originate]
Check information about the routing table of an OSPF process.	display ospf [<i>process-id</i>] routing [interface <i>interface-type interface-number</i>] [nexthop <i>nexthop-address</i>]
Check information about ABRs and ASBRs of an OSPF process.	display ospf [<i>process-id</i>] abr-asbr
Check information about interfaces of an OSPF process.	display ospf [<i>process-id</i>] interface [all <i>interface-type interface-number</i>]

2.5 Configuring OSPF Attributes in Different Network Types

This section describes how to change the network type of the interface forcibly as required and configure DR election of OSPF in broadcast and NBMA networks.

[2.5.1 Establishing the Configuration Task](#)

[2.5.2 Configuring Network Types for an Interface Enabled with OSPF](#)

[2.5.3 \(Optional\) Setting the DR Priority for an Interface Enabled with OSPF](#)

[2.5.4 Configuring a Neighbor for an NBMA Network](#)

[2.5.5 \(Optional\) Setting the Interval for Sending Poll Packets on an NBMA Network](#)

[2.5.6 Checking the Configuration](#)

2.5.1 Establishing the Configuration Task

Applicable Environment

After OSPF is enabled, the network is classified into four types according to the link layer protocols. The link layer protocol of a physical interface of the S-switch is Ethernet and the default type of the interface is broadcast; therefore, you should change the network type forcibly through the command when the S-switch and routers constitute the networking.

For NBMA networks, if there is no reachable link between some nodes, the interface should be set to P2MP. If the S-switch has only one peer in the NBMA network, you can also change the interface to P2P.

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. Generally, you should choose the device with high performance and reliability as the DR and BDR.

Pre-configuration Tasks

Before configuring OSPF attributes, complete the following tasks:

- Configuring a VLAN to which each interface belongs
- Assigning an IP address to each VLANIF interface to ensure the network layer connectivity between OSPF neighbors
- [2.2 Configuring Basic OSPF Functions](#)

Data Preparation

To configure OSPF attributes, you need the following data.

No.	Data
1	Network types to be used

No.	Data
2	IP addresses of the neighbors (for NBMA networks)
3	(Optional) DR priority of an interface
4	(Optional) Interval for sending Poll packets in NBMA networks

2.5.2 Configuring Network Types for an Interface Enabled with OSPF

Context

If the network types of the interfaces enabled with OSPF that are used to set up the neighbor relationship are different, the local S-switch may not learn correct routes. After you configure the new network type for an interface, the previous network type is overridden.

Do as follows on the S-switch.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **ospf network-type { broadcast | nbma | p2mp | p2p }** command to configure a network types for an interface enabled with OSPF.

----End

2.5.3 (Optional) Setting the DR Priority for an Interface Enabled with OSPF

Context

When configuring broadcast networks or NBMA networks, you can set the DR priorities of interfaces to affect the DR/BDR election in a network.

Do as follows on the S-switches that need change the election priority.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **ospf dr-priority priority** command to set the DR priority for an interface enabled with OSPF.

By default, the DR priority is 1.

----End

Postrequisite

After the DR priority is set, the configuration is valid only when you run the **reset ospf** [*process-id*] **process** command to restart an OSPF process.

2.5.4 Configuring a Neighbor for an NBMA Network

Context

Some special configurations are required for NBMA networks. Neighboring nodes cannot be discovered by broadcasting Hello packets. Therefore, you should manually assign IP addresses and configure election right of the neighboring node for an interface.

Do as follows on the S-switchs in an NBMA network.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf** [*process-id*] command to start an OSPF process and enter the OSPF view.
- Step 3** Run the **peer ip-address** [**dr-priority** *priority*] command to configure a neighbor for the NBMA network.

----End

2.5.5 (Optional) Setting the Interval for Sending Poll Packets on an NBMA Network

Context

On an NBMA network, after the neighbor is invalid, Hello packets are sent periodically according to the interval set through the **ospf timer poll** command. The poll interval should be at least four times the interval for sending Hello packets.

Do as follows on the S-switchs in an NBMA network.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **ospf timer poll** *interval* command to set the interval for sending poll Hello packets on an NBMA network.

By default, the interval for sending poll Hello packets is 120s.

----End

2.5.6 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the LSDB of an OSPF process.	display ospf [<i>process-id</i>] lsdb [brief] display ospf [<i>process-id</i>] lsdb [router network summary asbr ase nssa] [<i>link-state-id</i>] [originate-router [<i>advertising-router-id</i>] self-originate]
Check information about neighbors of an OSPF process.	display ospf [<i>process-id</i>] peer [{ [<i>interface-type interface-number</i>] [<i>neighbor-id</i>] } brief]
Check information about the next hop of an OSPF process.	display ospf [<i>process-id</i>] nexthop
Check information about the routing table of an OSPF process.	display ospf [<i>process-id</i>] routing [interface <i>interface-type interface-number</i>] [nexthop <i>nexthop-address</i>]
Check information about interfaces of an OSPF process.	display ospf [<i>process-id</i>] interface [all <i>interface-type interface-number</i>]
Check the summary of an OSPF process.	display ospf [<i>process-id</i>] brief

2.6 Configuring OSPF Route Attributes

This section describes how to set the link cost, the priority, and the maximum number of equal-cost routes of OSPF.

2.6.1 Establishing the Configuration Task

2.6.2 (Optional) Setting the Link Cost of OSPF

2.6.3 (Optional) Setting the Preference for an OSPF Route

2.6.4 (Optional) Setting the Maximum Number of OSPF Routes

2.6.5 Checking the Configuration

2.6.1 Establishing the Configuration Task

Applicable Environment

In a network with complex topology, there may be multiple different routes to the same destination. The routes can be discovered by the same or different routing protocols. You can learn how to choose different routes to the same destination through the configuration in this section.

Pre-configuration Tasks

Before configuring OSPF route attributes, complete the following tasks:

- Configuring a VLAN to which each interface belongs

- Assigning an IP address to each VLANIF interface to ensure the network layer connectivity between OSPF neighbors
- [2.2 Configuring Basic OSPF Functions](#)

Data Preparation

To configuring OSPF route attributes, you need the following data.

No.	Data
1	(Optional) Link cost
2	(Optional) Priority of OSPF
3	(Optional) Number of maximum equal-cost routes of OSPF

2.6.2 (Optional) Setting the Link Cost of OSPF

Setting the Cost for an Interface Enabled with OSPF

Context

Do as follows on the S-switchs in an area.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **ospf cost** *cost* command to set the cost for an interface enabled with OSPF.

If the cost of an interface is not set, OSPF calculates the cost automatically according to the bandwidth of the interface.

During the configuration, ensure that the cost of interfaces of the S-switchs in the area should be the same. Otherwise, a routing loop occurs.

----End

Setting the Bandwidth Reference Value

Context

Do as follows on the S-switch in an area.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf** [*process-id*] command to start an OSPF process and enter the OSPF view.

Step 3 Run the **bandwidth-reference value** command to set the bandwidth reference value.

By default, the bandwidth reference value is 100 Mbit/s.

If the cost of an interface is not set through the **ospf cost** command in the interface view, OSPF calculates the cost of the interface according to the bandwidth of the interface. The calculation formula is: the cost of the interface = bandwidth reference value/the interface bandwidth. If the cost is smaller than 1, the cost value is 1. You can directly change the cost of the interface by changing the bandwidth reference value.

During the configuration, ensure that the bandwidth reference value of the S-switches in the area should be the same. Otherwise, a routing loop occurs.

----End

2.6.3 (Optional) Setting the Preference for an OSPF Route

Setting the Preference for an OSPF Route

Context

Do as follows on the S-switches that run OSPF.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf [process-id]** command to start an OSPF process and enter the OSPF view.

Step 3 Run the **preference [ase] [route-policy route-policy-name] preference** command to set the preference for an OSPF route.

Multiple routing protocols can be enabled on a S-switch at the same time, so there is the problem about routing information sharing and selection among routing protocols. The system sets the priority for each routing protocol. When different protocols find routes to the same destination, the route with a higher preference is selected. The smaller the value is, the higher the preference is.

----End

Setting the Preference for an OSPF Equal-Cost Route

Context

Do as follows on the S-switches that run OSPF.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf [process-id]** command to start an OSPF process and enter the OSPF view.

Step 3 Run the **nexthop ip-address weight value** command to set the preference for an OSPF equal-cost route.

Using the **nexthop** command selects the next hop with the highest preference from the equal-cost routes calculated by OSPF. The smaller the weight is, the higher the preference is. By default, the weight value is 255, indicating that load balancing is performed among the equal-cost routes.

----End

2.6.4 (Optional) Setting the Maximum Number of OSPF Routes

Context

Do as follows on the S-switchs in an area.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf** [*process-id*] command to start an OSPF process and enter the OSPF view.
- Step 3** Run the **maximum load-balancing** *number* command to set the maximum number of equal-cost routes.

By default, the maximum number of equal-cost routes is 2.

----End

2.6.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the routing table of an OSPF process.	display ospf [<i>process-id</i>] routing [<i>ip-address</i> [<i>mask</i> <i>mask-length</i>]] [interface <i>interface-type</i> <i>interface-number</i>] [nexthop <i>nexthop-address</i>] display ospf [<i>process-id</i>] routing router-id [<i>router-id</i>]
Check information about interfaces of an OSPF process.	display ospf [<i>process-id</i>] interface [all <i>interface-type</i> <i>interface-number</i>] [verbose]

Run the **display ospf interface** command. You can view the link cost and the preference of an OSPF route.

```
<Quidway> display ospf interface vlanif 40
```

```
OSPF Process 1 with Router ID 192.168.32.11
Interfaces
```

```
Interface: 40.0.0.2 (Vlanif40)
Cost: 100      State: DR      Type: Broadcast      MTU: 1500
Priority: 1
Designated Router: 40.0.0.2
Backup Designated Router: 40.0.0.1
```

Timers: Hello 10 , Dead 40 , Poll 120 , Retransmit 5 , Transmit Delay 1

2.7 Configuring OSPF Route Aggregation

This section describes how to configure route aggregation of OSPF.

[2.7.1 Establishing the Configuration Task](#)

[2.7.2 Configuring ABR Route Aggregation](#)

[2.7.3 Configuring ASBR Route Aggregation](#)

[2.7.4 Checking the Configuration](#)

2.7.1 Establishing the Configuration Task

Applicable Environment

When network devices maintain routing entries to all network segments, the devices should have powerful capabilities of storage and calculation. To reduce the burden of storage and calculation of network devices, you can configure route aggregation on ABRs and ASBRs. The transmission of routing information is reduced without affecting the previous forwarding path.

Pre-configuration Tasks

Before configuring OSPF route aggregation, complete the following tasks:

- Configuring a VLAN to which each interface belongs
- Assigning an IP address to each VLANIF interface to ensure the network layer connectivity between OSPF neighbors
- [2.2 Configuring Basic OSPF Functions](#)

Data Preparation

To configure OSPF route aggregation, you need the following data.

No.	Data
1	Destination address and mask of the aggregated route
2	(Optional) Cost of the aggregated route and tag of the external LSA

2.7.2 Configuring ABR Route Aggregation

Context

Routes that are transmitted to a certain area are aggregated and an ABR sends only one aggregated route to the area.

The routes received from an indirectly connected area are not aggregated.

Do as follows on the ABRs that need reduce the transmission of routing entries.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf** [*process-id*] command to enter the OSPF view.
- Step 3** Run the **area** *area-id* command to enter the OSPF area view.
- Step 4** Run the **abr-summary** *ip-address mask* [{ **advertise** | **not-advertise** } | **cost** *cost*] * command to configure ABR route aggregation for the area.

You can set the cost for an aggregated route by specifying optional parameters.

----End

2.7.3 Configuring ASBR Route Aggregation

Context

Routes imported to a certain area are aggregated.

Do as follows on the ASBRs that need reduce the transmission of routing entries.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf** [*process-id*] command to enter the OSPF view.
- Step 3** Run the **asbr-summary** *ip-address mask* [**cost** *cost*] [**not-advertise**] [**tag** *tag*] command to configure ASBR route aggregation for OSPF routes.

You can set the cost for an aggregated route and the tag of an external LSA by specifying optional parameters.

----End

2.7.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the routing table of an OSPF process.	display ospf [<i>process-id</i>] routing [<i>ip-address</i> [<i>mask</i> <i>mask-length</i>]] [interface <i>interface-type</i> <i>interface-number</i>] [nexthop <i>nexthop-address</i>]
Check information about the ABR aggregation of an OSPF process.	display ospf [<i>process-id</i>] asbr-summary [<i>ip-address mask</i>]

Run the **display ospf asbr-summary** command. You can view information about route aggregation imported by OSPF.

```

<Quidway> display ospf asbr-summary
      OSPF Process 1 with Router ID 192.168.32.11
      Summary Addresses
Total summary address count: 1
      Summary Address
net      : 10.0.0.0
mask     : 255.0.0.0
tag      : 0 (Not Configured)
status   : Advertise
Cost     : 0 (Not Configured)
The Count of Route is : 2

```

Destination	Net Mask	Proto	Process	Type	Metric
10.0.0.0	255.255.255.0	Static	1	2	1
10.1.0.0	255.255.255.0	Static	1	2	1

2.8 Configuring an OSPF Process to Filter Routes

This section describes how to configure the filtering for OSPF routes and import routes of other routing protocols.

[2.8.1 Establishing the Configuration Task](#)

[2.8.2 Configuring an OSPF Process to Filter Type3 LSAs](#)

[2.8.3 Configuring an OSPF Process to Filter the Received Routes](#)

[2.8.4 Configuring an OSPF Process to Import External Routes](#)

[2.8.5 Checking the Configuration](#)

2.8.1 Establishing the Configuration Task

Applicable Environment

When network devices maintain routing entries to all network segments, the devices should have powerful capabilities of storage and calculation. To reduce the burden of storage and calculation of network devices, you can configure filtering rules for inbound or outbound routes on the S-switch. In this manner, the S-switch can filter routes that do not need be received or sent and reduce the burden to maintained routing entries.

Pre-configuration Tasks

Before configuring an OSPF process to filter routes, complete the following tasks:

- Configuring a VLAN to which each interface belongs
- Assigning an IP address to each VLANIF interface to ensure the network layer connectivity between OSPF neighbors
- [2.2 Configuring Basic OSPF Functions](#)

Data Preparation

To configure an OSPF process to filter routes, you need the following data.

No.	Data
1	ACL number, name of an IP prefix list, and name of a Route-Policy
2	Name, process ID, and default value of the imported routing protocol

2.8.2 Configuring an OSPF Process to Filter Type3 LSAs

Context

Do as follows on the ABRs.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf** [*process-id*] command to start an OSPF process and enter the OSPF view.
- Step 3** Run the **area** *area-id* command to enter the OSPF area view.
- Step 4** Run the **filter** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } { **export** | **import** } command to configure the OSPF process to filter ABR Type3 LSAs.

----End

2.8.3 Configuring an OSPF Process to Filter the Received Routes

Context

Do as follows on the S-switchs.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf** [*process-id*] command to start an OSPF process and enter the OSPF view.
- Step 3** Run the **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **import** command to configure the OSPF process to filter the received routes.

Because OSPF is a dynamic routing protocol based on the link state, it does not filter the advertised and received LSAs because the routing information is not displayed in the link state.

You can run the **filter-policy import** command to filter the routes calculated by OSPF. Only the routes filtered are added to the routing table.

This command is used to filter only the routes that are added to the local routing table, without affecting the OSPF routing table and the advertised routes.

----End

2.8.4 Configuring an OSPF Process to Import External Routes

Configuring an OSPF Process to Import Routes of Other Protocols

Context

Do as follows on the ASBRs according to the filtering rules.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf** [*process-id*] command to enter the OSPF view.
- Step 3** Run the **import-route protocol** [*process-id*] [**cost** *cost* | **tag** *tag* | **type** *type*] * [**route-policy** *route-policy-name*] command to import routes of other protocols to the OSPF process.
- Step 4** (Optional) Run the **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]] command to filter the imported routes in step 3.

Only the routes that meet matching rules can be sent.

The S-switch can filter routes of the specific protocol or process by specifying *protocol* [*process-id*]. If *protocol* [*process-id*] is not specified, an OSPF process filters all the imported routes.

NOTE

- Running the import-route command cannot import the default routes.
- An OSPF process filters the imported routes; that is, OSPF transforms only the external routes satisfying the requirements to Type5 LSAs and advertises them

----End

Configuring an OSPF Process to Import Default Routes

Context

Do as follows on the S-switches that run OSPF.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf** [*process-id*] command to enter the OSPF view.
- Step 3** Run the **default-route-advertise default-route-advertise** [**always** | **cost** *cost* | **type** *type* | **route-policy** *route-policy-name*] * command to import default routes to the OSPF process.

When you configure **always** through the command, you can import a default route forcibly. Otherwise, routes can be imported only when the local default routes exist.

 **NOTE**

If a default route is imported to an OSPF routing area and some OSPF routers within the area is configured with a static default route, you need set the preference of the static default route lower than that of the imported default route. Otherwise, the default route may not be assigned the highest preference in the routing table.

----End

Configuring Related Parameters for an OSPF Process to Import Routes

Context

Do as follows on the S-switchs that run OSPF.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf** [*process-id*] command to start an OSPF process and enter the OSPF view.
- Step 3** Run the **default** { **cost** *cost* | **limit** *limit* | **tag** *tag* | **type** *type* } * command to set the default values of **cost**, **limit**, **tag**, and **type** related to imported routes.

When an OSPF process imports external routes, you can configure the default values for some additional parameters, such as **cost**, **limit**, **tag**, and **type**. The route tag is used to mark the protocol related information. For example, it is used to differentiate the number of ASs when an OSPF process receives BGP routes.

----End

2.8.5 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about the routing table of an OSPF process.	display ospf [<i>process-id</i>] routing [<i>ip-address</i> [<i>mask</i> <i>mask-length</i>]] [interface <i>interface-type</i> <i>interface-number</i>] [nexthop <i>nexthop-address</i>]

Run the **display ospf routing** command. You can view information about the routes that meet matching rules and are imported from other routing protocols.

<Quidway> **display ospf routing**

OSPF Process 1 with Router ID 192.168.32.10
Routing Tables

Routing for Network

Destination	Cost	Type	NextHop	AdvRouter	Area
30.1.0.0/24	1	Transit	30.1.0.1	192.168.32.10	0.0.0.1
50.0.0.0/24	2	Inter-area	30.1.0.2	192.168.32.11	0.0.0.1

Routing for ASEs

Destination	Cost	Type	Tag	NextHop	AdvRouter
-------------	------	------	-----	---------	-----------

```
10.0.0.0/24      1      Type2      1      30.1.0.2      192.168.32.11

Total Nets: 3
Intra Area: 1  Inter Area: 1  ASE: 1  NSSA: 0
```

2.9 Adjusting and Optimizing an OSPF Network

This section describes how to adjust and optimize the OSPF network as required.

[2.9.1 Establishing the Configuration Task](#)

[2.9.2 \(Optional\) Setting the Delay for Transmitting LSAs on an Interface](#)

[2.9.3 \(Optional\) Setting the Interval for LSAs](#)

[2.9.4 \(Optional\) Setting the Interval for the SPF Calculation](#)

[2.9.5 \(Optional\) Configuring a Stub Router](#)

[2.9.6 \(Optional\) Setting the MTU of DD Packets](#)

[2.9.7 \(Optional\) Setting the Maximum Number of External LSAs in an LSDB](#)

[2.9.8 \(Optional\) Configuring Selection Rules of External Routes That Are Compatible with RFC 1583](#)

[2.9.9 Checking the Configuration](#)

2.9.1 Establishing the Configuration Task

Applicable Environment

The LSDB of LSAs on the S-switch ages with time. It is increased by one every second, but the LSDB is not increased during transmission. To reduce the error between the aging time and lifetime of LSAs, an interface can be configured with the delay for transmitting LSAs plus the aging time of LSAs.

The delay for transmitting LSAs depends on the network, and the configuration is important for a low-speed network.

To avoid too much usage of network and device resources due to the network connection or frequent route flapping, the S-switch sets the interval for updating and receiving LSAs. The S-switch can improve the convergence speed of an OSPF network by adjusting the interval for updating and receiving LSAs.

The OSPF process calculates the LSDB through the SPF algorithm. By adjusting the interval for the SPF calculation, you can reduce resource waste due to frequent network changes.

If the S-switch need restrict the traffic, you can configure stub routers to increase the link cost and reduce the forwarding traffic.

Pre-configuration Tasks

Before adjusting and optimizing an OSPF network, complete the following tasks:

- Configuring a VLAN to which each interface belongs

- Assigning an IP address to each VLANIF interface to ensure the network layer connectivity between OSPF neighbors
- [2.2 Configuring Basic OSPF Functions](#)

Data Preparation

To adjust and optimize OSPF networks, you need the following data.

No.	Data
1	(Optional) Delay for transmitting LSAs
2	(Optional) Interval for LSAs
3	(Optional) Interval for the SPF calculation
4	(Optional) Maximum number of external LSAs in an LSDB

2.9.2 (Optional) Setting the Delay for Transmitting LSAs on an Interface

Context

The LSDB of LSAs on the S-switch ages with the time. The LSDB is increased by one every second, but it is not increased during transmission. To reduce the error between the aging time and lifetime of LSAs, an interface can be configured with the delay for transmitting LSAs on the interface plus the aging time of LSAs.

The delay for transmitting LSAs depends on the network, and the configuration is important for a low-speed network.

Do as follows on the S-switchs according to the actual bandwidth rate.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **ospf trans-delay interval** command to set the delay for transmitting LSAs on the interface.

By default, the delay for transmitting LSAs on an interface is 1s.

----End

2.9.3 (Optional) Setting the Interval for LSAs

Setting the Interval for Updating LSAs

Context

OSPF defines that the interval for updating LSAs is 5s. This avoids too much usage of network bandwidth and device resource due to network connections or frequent route flapping.

For a stable networking with high requirements on route convergence time, you can set the interval for updating LSAs to 0 to cancel the interval. In this manner, the change of the topology or routes can be advertised to the network through LSAs. The route convergence speed in the network is thus increased.

Do as follows on the S-switchs in the AS according to the actual bandwidth rate.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf [process-id]** command to enter the OSPF view.

Step 3 Run the **lsa-originate-interval 0** command to set the interval for updating LSAs to 0.

By default, the interval for updating LSAs is 5s.

----End

Setting the Interval for Receiving LSAs

Context

For a stable networking with high requirements on the route convergence time, you can set the interval for receiving LSAs to 0. In this manner, the change of the topology or the network can be detected immediately.

Do as follows on the S-switchs in the AS according to the actual bandwidth rate.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf [process-id]** command to enter the OSPF view.

Step 3 Run the **lsa-arrival-interval 0** command to set the interval for receiving LSAs.

By default, the interval for receiving LSAs is 1s.

----End

2.9.4 (Optional) Setting the Interval for the SPF Calculation

Context

When the LSDB of an OSPF process changes, the SPF calculation is performed again. When a change occurs, calculating the shortest path consumes resources and affects the performance of the device.

Adjusting the interval for the SPF calculation, however, can reduce the resource consumption caused by frequent network changes.

Do as follows on the S-switchs in an area according to the rate of the change of the network topology.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf** [*process-id*] command to start an OSPF process and enter the OSPF view.

Step 3 Run the **spf-schedule-interval** { *interval1* | **millisecond** *interval2* } command to set the interval for the SPF calculation.

By default, the interval for the SPF calculation is 5s.

----End

2.9.5 (Optional) Configuring a Stub Router

Context

A stub router can control the traffic and informs other OSPF devices of not using it to forward data, but they can own a route to the stub router.

Among Router-LSAs generated by a stub router, the metric of all links is set to 65535.

Do as follows on the S-switchs.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf** [*process-id*] command to enter the OSPF view.

Step 3 Run the **stub-router** command to configure a stub router.



NOTE

A stub router is not related to the stub area.

----End

2.9.6 (Optional) Setting the MTU of DD Packets

Context

Different device manufacturers may use different default MTUs. To ensure the consistency, the MTU is often set to 0 when an interface sends DD packets. By default, an interface does not use the actual MTU when it sends DD packets. Instead, the interface uses 0.

After this command is used, the interface fills the MTU field of the DD packets in the actual MTU.

Do as follows on the S-switchs.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
 - Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
 - Step 3** Run the **ospf mtu-enable** command to enable the interface to fill the MTU in DD packets when DD packets are sent.
- End

2.9.7 (Optional) Setting the Maximum Number of External LSAs in an LSDB

Context

Through the configuration, the S-switch can control the number of external LSAs in its LSDB and reduce the burden of storage and calculation. By default, the maximum number of external LSAs in an LSDB is 1000000.

Do as follows on the S-switchs.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
 - Step 2** Run the **ospf** [*process-id*] command to start an OSPF process and enter the OSPF view.
 - Step 3** Run the **lsdb-overflow-limit** *number* command to set the maximum number of external LSAs in an LSDB.
- End

2.9.8 (Optional) Configuring Selection Rules of External Routes That Are Compatible with RFC 1583

Context

If multiple AS-External-LSAs send routes to the same destination, you can choose the optimal route according to the preference rule defined by RFC 1583.

By default, the function is disabled.

Do as follows on the S-switchs.

Procedure

- Step 1** Run the **system-view** command to enter the system view.

Step 2 Run the **ospf** [*process-id*] command to start an OSPF process and enter the OSPF view..

Step 3 Run the **rfc1583 compatible** command to configure the selection rules of external routes that are compatible with RFC 1583.

----End

2.9.9 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the summary of an OSPF process.	display ospf [<i>process-id</i>] brief
Check the statistics of an OSPF process.	display ospf [<i>process-id</i>] cumulative

Run the **display ospf brief** command. You can view that the interface is suppressed.

```
<Quidway> display ospf brief
      OSPF Process 1 with Router ID 192.168.32.11
      OSPF Protocol Information
RouterID: 192.168.32.11   Border Router:  AREA
Route Tag: 0
Multi-VPN-Instance is not enabled
Spf-schedule-interval: 5s
Default ASE parameters: Metric: 1 Tag: 1 Type: 2
Route Preference: 10
ASE Route Preference: 150
SPF Computation Count: 20
RFC 1583 Compatible
Retransmission limitation is disabled
Area Count: 2   Nssa Area Count: 0
ExChange/Loading Neighbors: 0

Area: 0.0.0.0
Authtype: None   Area flag: Normal
SPF scheduled Count: 20
ExChange/Loading Neighbors: 0

Interface: 50.0.0.1 (Vlanif50)
Cost: 1           State: DR           Type: Broadcast   MTU: 1500
Priority: 1
Designated Router: 50.0.0.1
Backup Designated Router: 0.0.0.0
Timers: Hello 10 , Dead 40 , Poll 120 , Retransmit 5 , Transmit Delay 1
Silent interface, No hellos

Area: 0.0.0.1           (MPLS TE not enabled)
Authtype: None   Area flag: Normal
SPF scheduled Count: 20
ExChange/Loading Neighbors: 0

Interface: 30.1.0.2 (Vlanif40)
Cost: 1           State: BDR          Type: Broadcast   MTU: 1500
Priority: 1
Designated Router: 30.1.0.1
Backup Designated Router: 30.1.0.2
Timers: Hello 10 , Dead 40 , Poll 120 , Retransmit 5 , Transmit Delay 1
```

2.10 Improving the Security of an OSPF Network

This section describes how to configure the OSPF area authentication and interface authentication.

[2.10.1 Establishing the Configuration Task](#)

[2.10.2 Configuring Authentication Mode for OSPF Areas](#)

[2.10.3 Configuring Interface Authentication](#)

[2.10.4 Checking the Configuration](#)

2.10.1 Establishing the Configuration Task

Applicable Environment

For a network with higher requirements on security, you can configure OSPF authentication to improve the security of the OSPF network.

Pre-configuration Tasks

Before improving the security of an OSPF network, complete the following tasks:

- Configuring a VLAN to which each interface belongs
- Assigning an IP address to each VLANIF interface to ensure the network layer connectivity between OSPF neighbors
- [2.2 Configuring Basic OSPF Functions](#)

Data Preparation

To improve the security of an OSPF network, you need the following data.

No.	Data
1	Authentication type and password

2.10.2 Configuring Authentication Mode for OSPF Areas

Context

OSPF supports packet authentication. Only the OSPF packets passing the authentication can be received; otherwise, the neighbor relationship cannot be set up.

When you use area authentication, the authentication mode and password of all devices in an area should be the same. For example, the authentication mode of all devices in Area 0 is simple authentication and the password is **abc**.

Do as follows on all S-switches in an area.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf** [*process-id*] command to start an OSPF process and enter the OSPF view.
- Step 3** Run the **area** *area-id* command to enter the OSPF area view.
- Step 4** Run the following command as required.
- Run the **authentication-mode simple** { [**plain**] *plain-text* | **cipher** *cipher-text* } command to set the simple authentication for an OSPF area.
 - Run the **authentication-mode** { **md5** | **hmac-md5** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }] command to set the MD5 authentication for an OSPF area.
- End

2.10.3 Configuring Interface Authentication

Context

Interface authentication is used between neighboring devices and takes precedence over area authentication.

The authentication mode and password of interfaces in the same area should be the same, but they can be different in different areas.

Do as follows on all S-switches in an area.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type* *interface-number* command to enter the interface view.
- Step 3** Run the following command as required.
- Run the **ospf authentication-mode simple** { [**plain**] *plain-text* | **cipher** *cipher-text* } command to set the simple authentication and the password for an interface enabled with OSPF.
 - Run the **ospf authentication-mode** { **md5** | **hmac-md5** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }] command to set the MD5 authentication and the password for an interface enabled with OSPF.
 - Run the **ospf authentication-mode null** command to set the authentication for an interface enabled with OSPF.
- End

2.10.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the summary of an OSPF process.	display ospf [<i>process-id</i>] brief

Run the **display ospf brief** command. You can view the configuration of area authentication.

```
<Quidway> display ospf brief

      OSPF Process 1 with Router ID 192.168.32.11
      OSPF Protocol Information

RouterID: 192.168.32.11   Border Router:
Route Tag: 0
Multi-VPN-Instance is not enabled
Spf-schedule-interval: 5s
Default ASE parameters: Metric: 1 Tag: 1 Type: 2
Route Preference: 10
ASE Route Preference: 150
SPF Computation Count: 77
RFC 1583 Compatible
Retransmission limitation is disabled
Area Count: 1   Nssa Area Count: 0
ExChange/Loading Neighbors: 0

Area: 0.0.0.0
Authtype: Simple   Area flag: Normal
SPF scheduled Count: 77
ExChange/Loading Neighbors: 0

Interface: 20.0.0.1 (Vlanif20)
Cost: 1   State: BDR   Type: Broadcast   MTU: 1500
Priority: 1
Designated Router: 20.0.0.2
Backup Designated Router: 20.0.0.1
Timers: Hello 10 , Dead 40 , Poll 120 , Retransmit 5 , Transmit Delay 1
```

2.11 Configuring OSPF Network Management

This section describes how to configure the OSPF MIB binding, OSPF Trap function, and log function.

[2.11.1 Establishing the Configuration Task](#)

[2.11.2 Configuring OSPF MIB Binding](#)

[2.11.3 Configuring the TRAP Function](#)

[2.11.4 Configuring the Log Function](#)

[2.11.5 Checking the Configuration](#)

2.11.1 Establishing the Configuration Task

Applicable Environment

OSPF supports network management, so you can bind the OSPF MIB to a certain process, and configure the functions of sending Trap messages and logs.

Pre-configuration Tasks

Before configuring OSPF network management, complete the following tasks:

- Creating a VLAN to which each interface belongs

- Assigning an IP address to each VLANIF interface to ensure the network layer connectivity between OSPF neighbors
- [2.2 Configuring Basic OSPF Functions](#)

Data Preparation

To configure OSPF network management, you need the following data.

No.	Data
1	OSPF process ID
2	(Optional) Parameters of Trap messages

2.11.2 Configuring OSPF MIB Binding

Context

Do as follows on the S-switchs.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf mib-binding process-id** command to bind the OSPF MIB to a certain process.
- End

2.11.3 Configuring the TRAP Function

Context

Do as follows on the S-switchs.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **snmp-agent trap enable ospf** command to enable the Trap function.
- OSPF can be configured to forward SNMP TRAP messages and a certain OSPF process can be specified to send SNMP TRAP messages.
- If *process-id* is not specified during the configuration, all OSPF processes send Trap messages.
- End

2.11.4 Configuring the Log Function

Context

Do as follows on the S-switchs.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf [process-id]** command to start an OSPF process and enter the OSPF view.

Step 3 Run the **enable log [config | state | error]** command to enable the log function.

----End

2.11.5 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the summary of an OSPF process.	display ospf [process-id] brief

Run the **display ospf brief** command. You can view the configuration of OSPF network management.

<Quidway> **display ospf brief**

```
OSPF Process 1 with Router ID 192.168.32.11
  OSPF Protocol Information
```

```
RouterID: 192.168.32.11   Border Router:
Route Tag: 0
Multi-VPN-Instance is not enabled
Spf-schedule-interval: 5s
Default ASE parameters: Metric: 1 Tag: 1 Type: 2
Route Preference: 10
ASE Route Preference: 150
SPF Computation Count: 87
RFC 1583 Compatible
Retransmission limitation is disabled
This process is currently bound to MIB
This process is currently bound to SNMP trap
Area Count: 1   Nssa Area Count: 0
ExChange/Loading Neighbors: 0

Area: 0.0.0.0           (MPLS TE not enabled)
AuthType: None   Area flag: Normal
SPF scheduled Count: 87
ExChange/Loading Neighbors: 0

Interface: 20.0.0.1 (Vlanif20)
Cost: 1           State: BDR           Type: Broadcast   MTU: 1500
Priority: 1
Designated Router: 20.0.0.2
Backup Designated Router: 20.0.0.1
Timers: Hello 10 , Dead 40 , Poll 120 , Retransmit 5 , Transmit Delay 1
```

2.12 Maintaining OSPF

This section describes how to maintain OSPF.

[2.12.1 Resetting OSPF](#)

[2.12.2 Clearing OSPF](#)

[2.12.3 Debugging OSPF](#)

2.12.1 Resetting OSPF



CAUTION

The OSPF adjacency of S-switchs is disconnected after you reset the OSPF connection. So, confirm the action before you use the command.

After modifying the OSPF routing policy or protocol, you need to reset the OSPF connections to validate the modification.

To reset OSPF connections, run the following **reset** commands in the user view.

Action	Command
Restart an OSPF process.	reset ospf [<i>process-id</i>] process

2.12.2 Clearing OSPF



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** commands in the user view.

Action	Command
Clear OSPF counters.	reset ospf [<i>process-id</i>] counters [neighbor [<i>interface-type interface-number</i>] [<i>router-id</i>]]
Clear routes imported by OSPF.	reset ospf [<i>process-id</i>] redistribution

2.12.3 Debugging OSPF

**CAUTION**

Debugging affects the performance of the system. So, after debugging, run the **undo debugging all** command to disable it immediately.

When an OSPF fault occurs, run the following **debugging** commands in the user view to locate the fault.

Action	Command
Enable the debugging of OSPF packets.	debugging ospf [<i>process-id</i>] packet [ack dd hello request update] [brief] [filter { src nbr } { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> }]
Enable the debugging of OSPF events.	debugging ospf [<i>process-id</i>] event
Enable the debugging of OSPF LSAs.	debugging ospf [<i>process-id</i>] lsa-originate
Enable the debugging of OSPF SPF.	debugging ospf [<i>process-id</i>] spf { all brief intra } debugging ospf [<i>process-id</i>] spf { asbr-summary ase net-summary nssa } [filter { acl <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> }]

2.13 Configuring Examples

This section provides several configuration examples of OSPF.

[2.13.1 Example for Configuring Basic OSPF Functions](#)

[2.13.2 Example for Configuring a Stub Area of OSPF](#)

[2.13.3 Example for Configuring an OSPF NSSA Area](#)

[2.13.4 Example for Configuring DR Election of an OSPF Process](#)

[2.13.5 Example for Configuring OSPF Load Balancing](#)

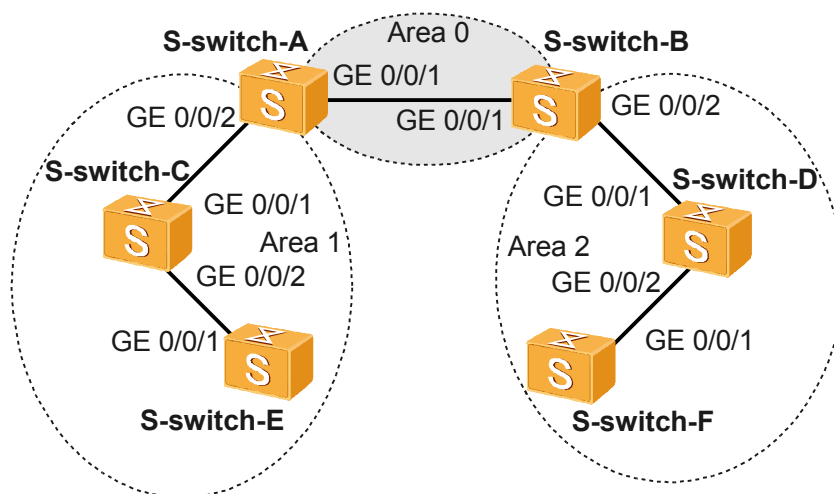
2.13.1 Example for Configuring Basic OSPF Functions

Networking Requirements

As shown in [Figure 2-4](#), all S-switchs run OSPF, and the entire AS is partitioned into three areas. S-switch-A and S-switch-B serve as ABRs to forward routes between areas.

After the configuration, each S-switch should learn the routes to all network segments from the AS.

Figure 2-4 Networking diagram of basic OSPF configurations



S-switch	Interface	VLANIF Interface	IP Address
S-switch-A	GE 0/0/1	VLANIF 10	192.168.0.1/24
S-switch-A	GE 0/0/2	VLANIF 20	192.168.1.1/24
S-switch-B	GE 0/0/1	VLANIF 10	192.168.0.2/24
S-switch-B	GE 0/0/2	VLANIF 30	192.168.2.1/24
S-switch-C	GE 0/0/1	VLANIF 20	192.168.1.2/24
S-switch-C	GE 0/0/2	VLANIF 40	172.16.1.1/24
S-switch-D	GE 0/0/1	VLANIF 30	192.168.2.2/24
S-switch-D	GE 0/0/2	VLANIF 50	172.17.1.1/24
S-switch-E	GE 0/0/1	VLANIF 40	172.16.1.2/24
S-switch-F	GE 0/0/1	VLANIF 50	172.17.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create the ID of a VLAN to which each interface belongs.
2. Assign an IP address to each VLANIF interface.
3. Enable OSPF on each S-switch and specify network segments in different areas.
4. Check the routing table and LSDB.

Data Preparation

To complete the configuration, you need the following data:

- The ID of the VLAN that each interface belongs to is shown in [Figure 2-4](#).
- The IP address of each interface is shown in [Figure 2-4](#).
- The router ID of each S-switch, the OSPF process ID, and the area to which each interface belongs are as follows.

- The router ID of S-switch-A is 1.1.1.1, the OSPF process ID 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 S-switch-B is 2.2.2.2, the OSPF process ID 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 S-switch-C is 3.3.3.3, the OSPF process ID is 1, the network segments of Area 1 are 192.168.1.0/24 and 172.16.1.0/24.
- The router ID of S-switch-D is 4.4.4.4, the OSPF process ID 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 S-switch-E is 5.5.5.5, the OSPF process ID is 1, and the network segment of Area 1 is 172.16.1.0/24.
- The router ID of S-switch-F is 6.6.6.6, the OSPF process ID is 1, and the network segment of Area 2 is 172.17.1.0/24.

Configuration Procedure

1. Create a VLAN to which each interface belongs.
The configuration details are not mentioned here.
2. Assign an IP address to each interface.
The configuration details are not mentioned here.
3. **2.2 Configuring Basic OSPF Functions.**

Configure S-switch-A.

```
[S-switch-A] router id 1.1.1.1
[S-switch-A] ospf
[S-switch-A-ospf-1] area 0
[S-switch-A-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[S-switch-A-ospf-1-area-0.0.0.0] quit
[S-switch-A-ospf-1] area 1
[S-switch-A-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[S-switch-A-ospf-1-area-0.0.0.1] quit
[S-switch-A-ospf-1] quit
```

Configure S-switch-B.

```
[S-switch-B] router id 2.2.2.2
[S-switch-B] ospf
[S-switch-B-ospf-1] area 0
[S-switch-B-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[S-switch-B-ospf-1-area-0.0.0.0] quit
[S-switch-B-ospf-1] area 2
[S-switch-B-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[S-switch-B-ospf-1-area-0.0.0.2] quit
[S-switch-B-ospf-1] quit
```

Configure S-switch-C.

```
[S-switch-C] router id 3.3.3.3
[S-switch-C] ospf
[S-switch-C-ospf-1] area 1
[S-switch-C-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[S-switch-C-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[S-switch-C-ospf-1-area-0.0.0.1] quit
[S-switch-C-ospf-1] quit
```

Configure S-switch-D.

```
[S-switch-D] router id 4.4.4.4
[S-switch-D] ospf
[S-switch-D-ospf-1] area 2
[S-switch-D-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[S-switch-D-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[S-switch-D-ospf-1-area-0.0.0.2] quit
[S-switch-D-ospf-1] quit
```

Configure S-switch-E.

```
[S-switch-E] router id 5.5.5.5
[S-switch-E] ospf
[S-switch-E-ospf-1] area 1
[S-switch-E-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[S-switch-E-ospf-1-area-0.0.0.1] quit
[S-switch-E-ospf-1] quit
```

Configure S-switch-F.

```
[S-switch-F] router id 6.6.6.6
[S-switch-F] ospf
[S-switch-F-ospf-1] area 2
[S-switch-F-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[S-switch-F-ospf-1-area-0.0.0.2] quit
[S-switch-F-ospf-1] quit
```

4. Verify the configuration.

Check OSPF neighbors of S-switch-A.

```
[S-switch-A] display ospf peer
      OSPF Process 1 with Router ID 1.1.1.1
      Neighbors

Area 0.0.0.0 interface 192.168.0.1(Vlanif10)'s neighbors
Router ID: 2.2.2.2      Address: 192.168.0.2      GR State: Normal
  State: Full Mode:Nbr is Master Priority: 1
    DR: 192.168.0.1 BDR: 192.168.0.2 MTU: 0
    Dead timer due in 36 sec
    Neighbor is up for 00:15:04
    Authentication Sequence: [ 0 ]

      Neighbors

Area 0.0.0.1 interface 192.168.1.1(Vlanif20)'s neighbors
Router ID: 3.3.3.3      Address: 192.168.1.2      GR State: Normal
  State: Full Mode:Nbr is Master Priority: 1
    DR: 192.168.1.1 BDR: 192.168.1.2 MTU: 0
    Dead timer due in 39 sec
    Neighbor is up for 00:07:32
    Authentication Sequence: [ 0 ]
```

Check OSPF routing information of S-switch-A.

```
[S-switch-A] 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      Transit     192.168.0.1    1.1.1.1        0.0.0.0
192.168.1.0/24   1      Transit     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 S-switch-A.

```
[S-switch-A] 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
Network   192.168.0.1   1.1.1.1        316  32   80000001      0
```

```

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 192.168.1.2 192.168.1.2 188 48 80000002 1
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
Sum-Net 172.17.1.0 1.1.1.1 202 28 80000002 3
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

```

Check the routing table of S-switch-D and perform the ping operation to test the connectivity.

```
[S-switch-D] 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 Transit 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

```

```
[S-switch-D] 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

```

Configuration Files

- Configuration file of S-switch-A

```

#
sysname S-switch-A
#
router id 1.1.1.1
#
vlan batch 10 20
#
interface Vlanif10
ip address 192.168.0.1 255.255.255.0
#
interface Vlanif20
ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2

```

```
port trunk allow-pass vlan 20
#
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 S-switch-B

```
#
sysname S-switch-B
#
router id 2.2.2.2
#
vlan batch 10 30
#
interface Vlanif10
ip address 192.168.0.2 255.255.255.0
#
interface Vlanif30
ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 30
#
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 S-switch-C

```
#
sysname S-switch-C
#
router id 3.3.3.3
#
vlan batch 20 40
#
interface Vlanif20
ip address 192.168.1.2 255.255.255.0
#
interface Vlanif40
ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 40
#
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 S-switch-D

```
#
sysname S-switch-D
#
router id 4.4.4.4
#
```

```

    vlan batch 30 50
    #
    interface Vlanif30
    ip address 192.168.2.2 255.255.255.0
    #
    interface Vlanif50
    ip address 172.17.1.1 255.255.255.0
    #
    interface GigabitEthernet0/0/1
    port trunk allow-pass vlan 30
    #
    interface GigabitEthernet0/0/2
    port trunk allow-pass vlan 50
    #
    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 S-switch-E

```

    #
    sysname S-switch-E
    #
    router id 5.5.5.5
    #
    vlan batch 40
    #
    interface Vlanif40
    ip address 172.16.1.2 255.255.255.0
    #
    interface GigabitEthernet0/0/1
    port trunk allow-pass vlan 40
    #
    ospf 1
    area 0.0.0.1
    network 172.16.1.0 0.0.0.255
    #
    return

```

- Configuration file of S-switch-F

```

    #
    sysname S-switch-F
    #
    router id 6.6.6.6
    #
    vlan batch 50
    #
    interface Vlanif50
    ip address 172.17.1.2 255.255.255.0
    #
    interface GigabitEthernet0/0/1
    port trunk allow-pass vlan 50
    #
    ospf 1
    area 0.0.0.2
    network 172.17.1.0 0.0.0.255
    #
    return

```

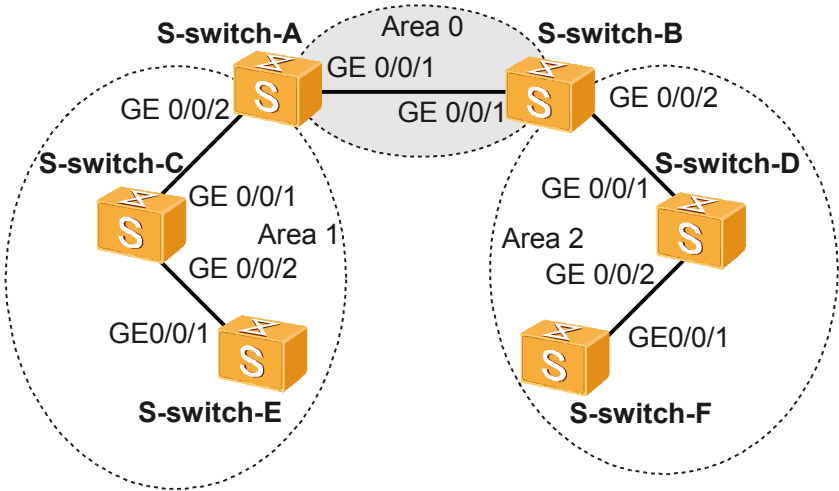
2.13.2 Example for Configuring a Stub Area of OSPF

Networking Requirements

As shown in [Figure 2-5](#), OSPF is enabled on all S-switchs and the entire AS is partitioned into three areas. S-switch-A and S-switch-B function as ABRs to forward routes between areas. S-switch-D functions as the ASBR to import static routes.

The requirement is to configure Area 1 as the stub area, thus reducing the LSAs advertised to this area without affecting the route reachability.

Figure 2-5 Configuring OSPF stub areas



S-switch	Interface	VLANIF Interface	IP Address
S-switch-A	GE 0/0/1	VLANIF 10	192.168.0.1/24
S-switch-A	GE 0/0/2	VLANIF 20	192.168.1.1/24
S-switch-B	GE 0/0/1	VLANIF 10	192.168.0.2/24
S-switch-B	GE 0/0/2	VLANIF 30	192.168.2.1/24
S-switch-C	GE 0/0/1	VLANIF 20	192.168.1.2/24
S-switch-C	GE 0/0/2	VLANIF 40	172.16.1.1/24
S-switch-D	GE 0/0/1	VLANIF 30	192.168.2.2/24
S-switch-D	GE 0/0/2	VLANIF 50	172.17.1.1/24
S-switch-E	GE 0/0/1	VLANIF 40	172.16.1.2/24
S-switch-F	GE 0/0/1	VLANIF 50	172.17.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable OSPF on each S-switch and configure basic OSPF functions.
2. Configure static routes on S-switch-D and import them.
3. Configure Area 1 as a stub area. You need to run the **stub** command on all S-switchs in Area 1.
4. Do not advertise Type3 LSAs to the stub area on S-switch-A.

Data Preparation

To complete the configuration, you need the following data:

- The ID of the VLAN to which each interface belongs is shown in [Figure 2-5](#).
- The IP address of each interface is shown in [Figure 2-5](#).
- The router ID of each S-switch, the OSPF process ID, and the area to which each interface belongs are as follows:
 - The router ID of S-switch-A is 1.1.1.1, the OSPF process ID 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 S-switch-B is 2.2.2.2, the OSPF process ID 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 S-switch-C is 3.3.3.3, the OSPF process ID 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 S-switch-D is 4.4.4.4, the OSPF process ID 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 S-switch-E is 5.5.5.5, the OSPF process ID is 1, and the network segment of Area 1 is 172.16.1.0/24.
 - The router ID of S-switch-F is 6.6.6.6, the OSPF process ID is 1, and the network segment of Area 2 is 172.17.1.0/24.

Configuration Procedure

1. [2.13.1 Example for Configuring Basic OSPF Functions](#).
2. Configure S-switch-D to import static routes.

Import static routes on S-switch-D, as follows:

```
[S-switch-D] ip route-static 200.0.0.0 8 null 0
[S-switch-D] ospf
[S-switch-D-ospf-1] import-route static type 1
[S-switch-D-ospf-1] quit
```

Display the ABR or ASBR of S-switch-C.

```
[S-switch-C] display ospf abr-asbr
```

```
OSPF Process 1 with Router ID 3.3.3.3
Routing Table to ABR and ASBR
```

Type	Destination	Area	Cost	NextHop	RtType
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

Check the routing table of an OSPF process of S-switch-C.

```
[S-switch-C] display ospf routing
```

```
OSPF Process 1 with Router ID 3.3.3.3
Routing Tables
```

Routing for Network

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	Transit	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
```

If the area where S-switch-C resides is the common area, you can view that AS external routes exist in the routing table.

3. Configure Area 1 as a stub area.

Configure S-switch-A.

```
[S-switch-A] ospf
[S-switch-A-ospf-1] area 1
[S-switch-A-ospf-1-area-0.0.0.1] stub
[S-switch-A-ospf-1-area-0.0.0.1] quit
[S-switch-A-ospf-1] quit
```

Configure S-switch-C.

```
[S-switch-C] ospf
[S-switch-C-ospf-1] area 1
[S-switch-C-ospf-1-area-0.0.0.1] stub
[S-switch-C-ospf-1-area-0.0.0.1] quit
[S-switch-C-ospf-1] quit
```

Configure S-switch-E.

```
[S-switch-E] ospf
[S-switch-E-ospf-1] area 1
[S-switch-E-ospf-1-area-0.0.0.1] stub
[S-switch-E-ospf-1-area-0.0.0.1] quit
[S-switch-E-ospf-1] quit
```

Check the routing table of S-switch-C.

```
[S-switch-C] 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	Transit	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
```

When the area where S-switch-C resides is configured as a stub area, you may not find the AS external route but a default route external to the AS.

Disable Router A from advertising Type3 LSAs to the stub area.

```
[S-switch-A] ospf
[S-switch-A-ospf-1] area 1
[S-switch-A-ospf-1-area-0.0.0.1] stub no-summary
[S-switch-A-ospf-1-area-0.0.0.1] quit
[S-switch-A-ospf-1] quit
```

4. Verify the configuration.

Check the OSPF routing table of S-switch-C.

```
[S-switch-C] 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      Transit      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
```

After the advertisement of Summary-LSA to the stub area is disabled, the route entries are further reduced. The AS external routers are invisible in the routing table. Instead, there is a default route.

Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
router id 1.1.1.1
#
vlan batch 10 20
#
interface Vlanif10
 ip address 192.168.0.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet0/0/1
 port trunk allow-pass vlan 10
#
interface Ethernet0/0/2
 port trunk allow-pass vlan 20
#
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
```

NOTE

Configuration files of S-switch-B and S-switch-F are the same as the configuration file of S-switch-A, and are not mentioned here.

- Configuration file of S-switch-C

```
#
sysname S-switch-C
# router id 3.3.3.3
#
vlan batch 20 40
#
interface Vlanif20
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif40
 ip address 172.16.1.1 255.255.255.0
#
interface Ethernet0/0/1
 port trunk allow-pass vlan 20
#
interface Ethernet0/0/2
 port trunk allow-pass vlan 40
#
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 S-switch-D


```
#
sysname S-switch-D
#
vlan batch 30 50
#
router id 4.4.4.4
#
interface Vlanif30
ip address 192.168.2.2 255.255.255.0
#
interface Vlanif50
ip address 172.17.1.1 255.255.255.0
#
interface Ethernet0/0/1
port trunk allow-pass vlan 30
#
interface Ethernet0/0/2
port trunk allow-pass vlan 50
#
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 S-switch-E

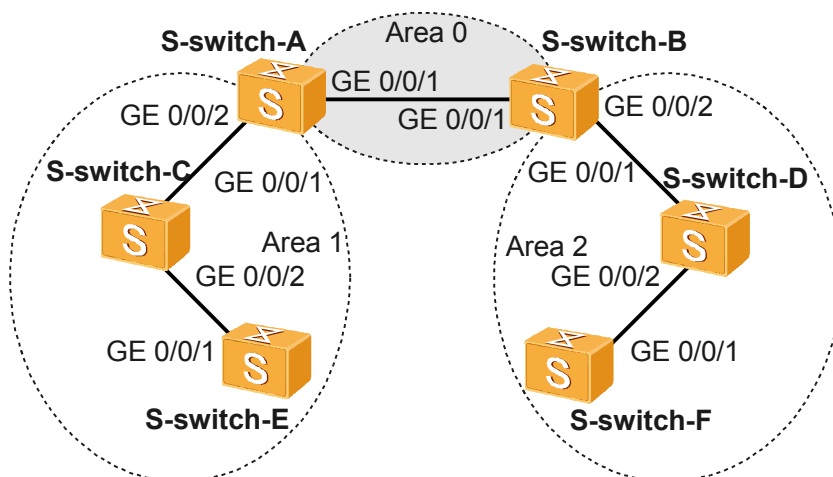

```
#
sysname S-switch-E
#
router id 5.5.5.5
#
vlan batch 40
#
interface Vlanif40
ip address 172.16.1.2 255.255.255.0
#
interface Ethernet0/0/1
port trunk allow-pass vlan 40
#
ospf 1
area 0.0.0.1
network 172.16.1.0 0.0.0.255
stub
#
return
```

2.13.3 Example for Configuring an OSPF NSSA Area

Networking Requirements

As shown in [Figure 2-6](#), OSPF is enabled on all S-switchs and the entire AS is partitioned into three areas. S-switch-A and S-switch-B function as ABRs to forward routes between areas. S-switch-D functions as the ASBR to import external routes (static routes).

The requirement is to configure Area 1 as an NSSA area and configure S-switch-C as an ASBR to import external routes (static routes). The routing information can be transmitted correctly in the AS.

Figure 2-6 Configuring OSPF NSSA areas

S-switch	Interface	VLANIF Interface	IP Address
S-switch-A	GE 0/0/1	VLANIF 10	192.168.0.1/24
S-switch-A	GE 0/0/2	VLANIF 20	192.168.1.1/24
S-switch-B	GE 0/0/1	VLANIF 10	192.168.0.2/24
S-switch-B	GE 0/0/2	VLANIF 30	192.168.2.1/24
S-switch-C	GE 0/0/1	VLANIF 20	192.168.1.2/24
S-switch-C	GE 0/0/2	VLANIF 40	172.16.1.1/24
S-switch-D	GE 0/0/1	VLANIF 30	192.168.2.2/24
S-switch-D	GE 0/0/2	VLANIF 50	172.17.1.1/24
S-switch-E	GE 0/0/1	VLANIF 40	172.16.1.2/24
S-switch-F	GE 0/0/1	VLANIF 50	172.17.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable OSPF on each S-switch and configure basic OSPF functions.
2. Configure static routes on S-switch-D and import them into OSPF.
3. Configure Area 1 as an NSSA area (run the **nssa** command on all routers in Area 1) and check the OSPF routing information of S-switch-C.
4. Configure static routes on S-switch-C, import them into OSPF, and check the OSPF routing information of S-switch-D.

Data Preparation

To complete the configuration, you need the following data:

- The ID of the VLAN to which each interface belongs is shown in [Figure 2-6](#).
- The IP address of each interface is shown in [Figure 2-6](#).
- The router ID of each S-switch, the OSPF process ID, and the area to which each interface belongs are as follows:

- The router ID of S-switch-A is 1.1.1.1, the OSPF process ID 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 S-switch-B is 2.2.2.2, the OSPF process ID 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 S-switch-C is 3.3.3.3, the OSPF process ID is 1, and the network segments of Area 2 are 192.168.1.0/24 and 172.16.1.0/24.
- The router ID of S-switch-D is 4.4.4.4, the OSPF process ID is 1, and the network segments of Area 2 are 192.168.2.0/24 and 172.16.1.0/24.
- The router ID of S-switch-E is 5.5.5.5, the OSPF process ID is 1, and the network segment of Area 1 is 172.16.1.0/24.
- The router ID of S-switch-F is 6.6.6.6, the OSPF process ID is 1, and the network segment of Area 2 is 172.17.1.0/24.

Configuration Procedure

1. [2.13.1 Example for Configuring Basic OSPF Functions.](#)
2. Configure S-switch-D to import static routes. See [2.13.2 Example for Configuring a Stub Area of OSPF.](#)
3. Configure Area 1 as an NSSA area.

Configure S-switch-A.

```
[S-switch-A] ospf
[S-switch-A-ospf-1] area 1
[S-switch-A-ospf-1-area-0.0.0.1] nssa default-route-advertise no-summary
[S-switch-A-ospf-1-area-0.0.0.1] quit
[S-switch-A-ospf-1] quit
```

Configure S-switch-C.

```
[S-switch-C] ospf
[S-switch-C-ospf-1] area 1
[S-switch-C-ospf-1-area-0.0.0.1] nssa
[S-switch-C-ospf-1-area-0.0.0.1] quit
[S-switch-C-ospf-1] quit
```

Configure S-switch-E.

```
[S-switch-E] ospf
[S-switch-E-ospf-1] area 1
[S-switch-E-ospf-1-area-0.0.0.1] nssa
[S-switch-E-ospf-1-area-0.0.0.1] quit
[S-switch-E-ospf-1] quit
```

NOTE

You should run the **default-route-advertise no-summary** command on S-switch-A. In this manner, the size of the routing table of devices in the NSSA area can be reduced. For other devices in the NSSA area, you need to use only the **nssa** command.

Check the OSPF routing table of S-switch-C.

```
[S-switch-C] 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	Transit	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
```

4. Configure S-switch-C to import static routes.

Import static routes on S-switch-C, as follows:

```
[S-switch-Cip route-static 100.0.0.0 8 null 0
[S-switch-C] ospf
[S-switch-C-ospf-1] import-route static
[S-switch-C-ospf-1] quit
```

5. Verify the configuration.

Check the OSPF routing table of S-switch-D.

```
[S-switch-D] 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	Transit	192.168.2.2	4.4.4.4	0.0.0.2

Routing for ASEs

Destination	Cost	Type	Tag	NextHop	AdvRouter
100.0.0.0/8	1	Type2	1	192.168.2.1	1.1.1.1

Total Nets: 6

```
Intra Area: 2   Inter Area: 3   ASE: 1   NSSA: 0
```

You can view one imported AS external route on S-switch-D in the NSSA area.

Configuration Files

- Configuration file of S-switch-A

```
#
 sysname S-switch-A
#
router id 1.1.1.1
#
vlan batch 10 20
#
interface Vlanif10
 ip address 192.168.0.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet0/0/1
 port trunk allow-pass vlan 10
#
interface Ethernet0/0/2
 port trunk allow-pass vlan 20
#
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
 nssa default-route-advertise no-summary
#
return
```

NOTE

Configuration files of S-switch-B, S-switch-D, and S-switch-F are the same as the configuration file of S-switch-A, and are not mentioned here.

- Configuration file of S-switch-C

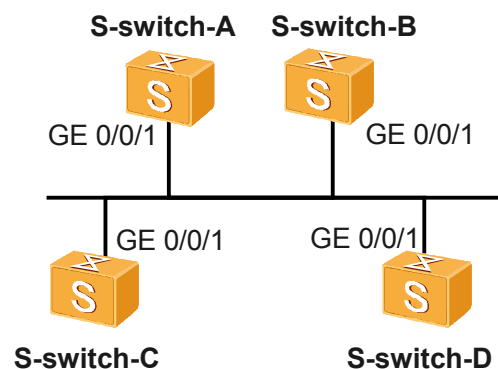

```
#
sysname S-switch-C
#
router id 3.3.3.3
#
vlan batch 20 40
#
interface Vlanif20
ip address 192.168.1.2 255.255.255.0
#
interface Vlanif40
ip address 172.16.1.1 255.255.255.0
#
interface Ethernet0/0/1
port trunk allow-pass vlan 20
#
interface Ethernet0/0/2
port trunk allow-pass vlan 40
#
ospf 1
import-route static
area 0.0.0.1
network 192.168.1.0 0.0.0.255
network 172.16.1.0 0.0.0.255
nssa
#
ip route-static 100.0.0.0 255.0.0.0 NULL0
#
return
```
- Configuration file of S-switch-E


```
#
sysname S-switch-E
#
router id 5.5.5.5
#
vlan batch 40
#
interface Vlanif40
ip address 172.16.1.2 255.255.255.0
#
interface Ethernet0/0/1
port trunk allow-pass vlan 40
#
ospf 1
area 0.0.0.1
network 172.16.1.0 0.0.0.255
nssa
#
return
```

2.13.4 Example for Configuring DR Election of an OSPF Process

Networking Requirements

As shown in [Figure 2-7](#), S-switch-A has the highest priority of 100 in the network and is selected as DR. S-switch-C has the second highest priority, and is selected as BDR. The priority of S-switch-B is 0, so S-switch-B cannot be selected as DR. The priority of S-switch-D is not configured and its default value is 1.

Figure 2-7 Networking diagram of configuring DR election of an OSPF process

S-switch	Interface	VLANIF	IP address
S-switch-A	FE 0/0/1	VLANIF 10	192.168.1.1/24
S-switch-B	FE 0/0/1	VLANIF 10	192.168.1.2/24
S-switch-C	FE 0/0/1	VLANIF 10	192.168.1.3/24
S-switch-D	FE 0/0/1	VLANIF 10	192.168.1.4/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create the ID of a VLAN to which each interface belongs.
2. Assign an IP address to each VLANIF interface.
3. Configure the router ID of each S-switch, enable OSPF, and specify network segments.
4. Check the DR or BDR status of each S-switch.
5. Set the DR priority of the interface and check the DR or BDR status.

Data Preparation

To complete the configuration, you need the following data:

- The ID of the VLAN to which each interface belongs is shown in [Figure 2-7](#).
- The IP address of each interface is shown in [Figure 2-7](#).
- The router ID of each S-switch, the OSPF process ID, the area to which each interface belongs, and DR priority are as follows:
 - The router ID of S-switch-A is 1.1.1.1, the OSPF process ID is 1, the network segment of Area 0 is 192.168.1.0/24, and the DR priority is 100.
 - The router ID of S-switch-B is 2.2.2.2, the OSPF process ID is 1, the network segment of Area 0 is 192.168.1.0/24, and the DR priority is 0.
 - The router ID of S-switch-C is 3.3.3.3, the OSPF process ID is 1, the network segment of Area 0 is 192.168.1.0/24, and the DR priority is 2.
 - The router ID of S-switch-B is 4.4.4.4, the OSPF process ID is 1, the network segment of Area 0 is 192.168.1.0/24, and the DR priority is 1.

Configuration Procedure

1. Create a VLAN to which each interface belongs.
The configuration details are not mentioned here.
2. Assign an IP address to each interface.
The configuration details are not mentioned here.
3. [2.13.1 Example for Configuring Basic OSPF Functions.](#)

Configure S-switch-A.

```
[S-switch-A] router id 1.1.1.1
[S-switch-A] ospf
[S-switch-A-ospf-1] area 0
[S-switch-A-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[S-switch-A-ospf-1-area-0.0.0.0] quit
[S-switch-A-ospf-1] quit
```

Configure S-switch-B.

```
[S-switch-B] router id 2.2.2.2
[S-switch-B] ospf
[S-switch-B-ospf-1] area 0
[S-switch-B-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[S-switch-B-ospf-1-area-0.0.0.0] quit
[S-switch-B-ospf-1] quit
```

Configure S-switch-C.

```
[S-switch-C] router id 3.3.3.3
[S-switch-C] ospf
[S-switch-C-ospf-1] area 0
[S-switch-C-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[S-switch-C-ospf-1-area-0.0.0.0] quit
[S-switch-C-ospf-1] quit
```

Configure S-switch-D.

```
[S-switch-D] router id 4.4.4.4
[S-switch-D] ospf
[S-switch-D-ospf-1] area 0
[S-switch-D-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[S-switch-D-ospf-1-area-0.0.0.0] quit
[S-switch-D-ospf-1] quit
```

Check the DR or BDR status.

```
[S-switch-A] display ospf peer
```

```
OSPF Process 1 with Router ID 1.1.1.1
Neighbors
```

```
Area 0.0.0.0 interface 192.168.1.1(Vlanif10)'s neighbors
Router ID: 2.2.2.2      Address: 192.168.1.2      GR State: Normal
  State: 2-Way  Mode:Nbr is Master  Priority: 1
  DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
  Dead timer due in 32 sec
  Neighbor is up for 00:00:00
  Authentication Sequence: [ 0 ]
```

```
Router ID: 3.3.3.3      Address: 192.168.1.3      GR State: Normal
  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
  Neighbor is up for 00:04:06
  Authentication Sequence: [ 0 ]
```

```
Router ID: 4.4.4.4      Address: 192.168.1.4      GR State: Normal
  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
  Neighbor is up for 00:03:53
```

Authentication Sequence: [0]

Check information about the neighbor of S-switch-A. You can view the DR priority and neighbor status. By default, the DR priority is 1. Now S-switch-D is a DR and S-switch-C is a BDR.

NOTE

When the priority is the same, the S-switch with a higher router ID is selected as DR. If one Ethernet interface of the S-switch becomes DR, the other broadcast interfaces of the S-switch have a high priority of being selected as DRs in future DR selection. That is, select the DR S-switch as DR. DR cannot be preempted.

4. Configure DR priorities on the interfaces.

Configure S-switch-A.

```
[S-switch-A] interface Vlanif 10
[S-switch-A-Vlanif10] ospf dr-priority 100
[S-switch-A-Vlanif10] quit
```

Configure S-switch-B.

```
[S-switch-B] interface Vlanif 10
[S-switch-B-Vlanif10] ospf dr-priority 0
[S-switch-B-Vlanif10] quit
```

Configure S-switch-C.

```
[S-switch-C] interface Vlanif 10
[S-switch-C-Vlanif10] ospf dr-priority 2
[S-switch-C-Vlanif10] quit
```

View the DR or BDR status.

```
[S-switch-D] display ospf peer

      OSPF Process 1 with Router ID 4.4.4.4
      Neighbors

Area 0.0.0.0 interface 192.168.1.4(Vlanif10)'s neighbors
Router ID: 1.1.1.1      Address: 192.168.1.1      GR State: Normal
  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
  Neighbor is up for 00:11:17
  Authentication Sequence: [ 0 ]
Router ID: 2.2.2.2      Address: 192.168.1.2      GR State: Normal
  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
  Neighbor is up for 00:11:19
  Authentication Sequence: [ 0 ]

Router ID: 3.3.3.3      Address: 192.168.1.3      GR State: Normal
  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
  Neighbor is up for 00:11:15
  Authentication Sequence: [ 0 ]
```

NOTE

The DR priority on the interface is invalid after it is configured.

5. Restart OSPF processes.

On each S-switch, run the **reset ospf 1 process** command in the user view to restart the OSPF process.

6. Verify the configuration.

Check the status of OSPF neighbors.

```
[S-switch-D] display ospf peer
```

```

OSPF Process 1 with Router ID 4.4.4.4
  Neighbors

Area 0.0.0.0 interface 192.168.1.4(Vlanif10)'s neighbors
Router ID: 1.1.1.1      Address: 192.168.1.1      GR State: Normal
  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
  Neighbor is up for 00:07:19
  Authentication Sequence: [ 0 ]

Router ID: 2.2.2.2      Address: 192.168.1.2      GR State: Normal
  State: 2-Way Mode:Nbr is Master Priority: 0
  DR: 192.168.1.1 BDR: 192.168.1.3 MTU: 0
  Dead timer due in 35 sec
  Neighbor is up for 00:00:00
  Authentication Sequence: [ 0 ]

Router ID: 3.3.3.3      Address: 192.168.1.3      GR State: Normal
  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
  Neighbor is up for 00:07:17
  Authentication Sequence: [ 0 ]

# Check the status of an interface enabled with OSPF.
[S-switch-A] 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

[S-switch-B] 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

```

All neighbors are in the full state. This indicates that S-switch-A sets up neighbor relationships with all its neighbors. If the neighbor remains "2-Way", it indicates both of them are not DRs or BDRs. Thus, they need not exchange LSAs.

All other neighbors are DR Others. This indicates that they are neither DRs nor BDRs.

Configuration Files

- Configuration file of S-switch-A


```

#
sysname S-switch-A
#
router id 1.1.1.1
#
vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
 ospf dr-priority 100
#
interface Ethernet0/0/1
 port trunk allow-pass vlan 10
#

```

```
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of S-switch-B

```
#
 sysname S-switch-B
#
router id 2.2.2.2
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.2 255.255.255.0
 ospf dr-priority 0
#
interface Ethernet0/0/1
 port trunk allow-pass vlan 10
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of S-switch-C

```
#
 sysname S-switch-C
#
router id 3.3.3.3
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.3 255.255.255.0
 ospf dr-priority 2
#
interface Ethernet0/0/1
 port trunk allow-pass vlan 10
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of S-switch-D

```
#
 sysname S-switch-D
#
router id 4.4.4.4
#
 vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.4 255.255.255.0
#
interface Ethernet0/0/1
 port trunk allow-pass vlan 10
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

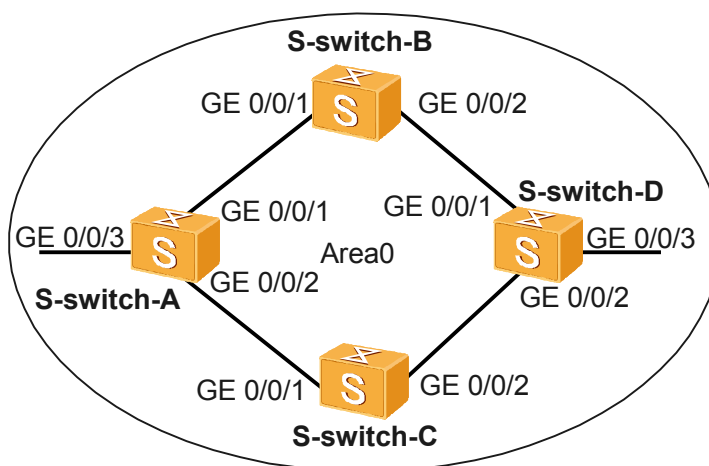
2.13.5 Example for Configuring OSPF Load Balancing

Networking Requirements

As shown in [Figure 2-8](#):

- S-switch-A, S-switch-B, S-switch-C, and S-switch-D connect to each other through OSPF.
- S-switch-A, S-switch-B, S-switch-C, and S-switch-D belong to Area 0.
- Load balancing is performed between S-switch-B and S-switch-C. The traffic of S-switch-A is sent to S-switch-D by S-switch-B and S-switch-C.

Figure 2-8 Networking diagram of configuring OSPF load balancing



S-switch	Interface	VLANIF Interface	IP Address
S-switch-A	GE 0/0/1	VLANIF 10	10.1.1.1/24
S-switch-A	GE 0/0/2	VLANIF 20	10.1.2.1/24
S-switch-A	GE 0/0/3	VLANIF 50	172.16.1.1/24
S-switch-B	GE 0/0/1	VLANIF 10	10.1.1.2/24
S-switch-B	GE 0/0/2	VLANIF 30	192.168.0.1/24
S-switch-C	GE 0/0/1	VLANIF 20	10.1.2.2/24
S-switch-C	GE 0/0/2	VLANIF 40	192.168.1.1/24
S-switch-D	GE 0/0/1	VLANIF 30	192.168.0.2/24
S-switch-D	GE 0/0/2	VLANIF 40	192.168.1.2/24
S-switch-D	GE 0/0/3	VLANIF 60	172.17.1.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable OSPF on each S-switch to implement interconnection.
2. Cancel load balancing and check the routing table.
3. (Optional) Set the preferences for equal-cost routes on S-switch-A.

Data Preparation

To configure OSPF load balancing, you need the following data:

- The ID of the VLAN to which each interface belongs is shown in [Figure 2-8](#).
- The IP address of each interface is shown in [Figure 2-8](#).
- The router ID of each S-switch, the OSPF process ID, and the area to which each interface belongs are as follows:
 - The router ID of S-switch-A is 1.1.1.1, the OSPF process ID is 1, and the network segments of Area 1 are 10.1.1.0/24, 10.1.2.0/24, and 172.16.1.0/24.
 - The router ID of S-switch-B is 2.2.2.2, the OSPF process ID is 1, and the network segments of Area 0 are 10.1.1.0/24 and 192.168.0.0/24.
 - The router ID of S-switch-C is 3.3.3.3, the OSPF process ID is 1, and the network segments of Area 0 are 10.1.2.0/24 and 192.168.1.0/24.
 - The router ID of S-switch-D is 4.4.4.4, the OSPF process ID is 1, and the network segments of Area 0 are 172.17.1.0/24, 192.168.0.0/24, and 192.168.1.0/24.
 - The number of routes for load balancing on S-switch-A is 1.
 - The preference of the equal-cost route of S-switch-C is 1.

Configuration Procedure

1. Create a VLAN to which each interface belongs.
The configuration details are not mentioned here.
2. Assign an IP address to each interface.
The configuration details are not mentioned here.
3. [2.13.1 Example for Configuring Basic OSPF Functions](#).
4. Cancel load balancing on S-switch-A.

```
[S-switch-A] ospf
[S-switch-A-ospf-1] maximum load-balancing 1
[S-switch-A-ospf-1] quit
```

Check the routing table of S-switch-A.

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

Routing Tables: Public						
Destinations : 13			Routes : 13			
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.1.1.0/24	Direct	0	0	D	10.1.1.1	Vlanif10
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	Vlanif10
10.1.2.0/24	Direct	0	0	D	10.1.2.1	Vlanif20
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	Vlanif20
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	Vlanif50
172.16.1.1/32	Direct	0	0	D	127.0.0.1	
InLoopBack0						
172.17.1.0/24	OSPF	10	3	D	10.1.1.2	Vlanif10

192.168.0.0/24	OSPF	10	2	D	10.1.1.2	Vlanif10
192.168.1.0/24	OSPF	10	2	D	10.1.2.2	Vlanif20

As shown in the routing table, when the maximum number of the equal-cost routes is 1, the next hop to the destination network segment 172.17.1.0 is 10.1.1.2.

 **NOTE**

In the preceding example, 10.1.1.2 is selected as the optimal next hop. This is because OSPF selects the next hop of the equal-cost route randomly.

5. Restore the default number of routes for load balancing on S-switch-A.

```
[S-switch-A] ospf
[S-switch-A-ospf-1] undo maximum load-balancing
[S-switch-A-ospf-1] quit
```

Check the routing table of S-switch-A.

```
[S-switch-A] display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
  Destinations : 11          Routes : 12
Destination/Mask    Proto    Pre  Cost  Flags       NextHop         Interface
-----
10.1.1.0/24         Direct   0     0      D          10.1.1.1         Vlanif10
10.1.1.1/32         Direct   0     0          D          127.0.0.1
InLoopBack0
10.1.2.0/24         Direct   0     0      D          10.1.2.1         Vlanif20
10.1.2.1/32         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
172.16.1.0/24        Direct   0     0      D          172.16.1.1         Vlanif50
172.16.1.1/32        Direct   0     0          D          127.0.0.1
InLoopBack0
172.17.1.0/24        OSPF     10    3      D          10.1.1.2         Vlanif10
                        OSPF     10    3      D          10.1.2.2
Vlanif2
192.168.0.0/24       OSPF     10    2      D          10.1.1.2         Vlanif10
192.168.1.0/24       OSPF     10    2      D          10.1.2.2         Vlanif20
```

As shown in the routing table, when the default setting of load balancing is restored, the next hops of S-switch-A, that is, 10.1.1.2 (S-switch-B) and 10.1.2.2 (S-switch-C), become valid routes. This is because the default number of equal-cost routes is 6.

6. (Optional) Set the preferences for equal-cost routes on S-switch-A.

If you need not perform load balancing between S-switch-B and S-switch-C, set the preferences for equal-cost routes and specify the next hop.

```
[S-switch-A] ospf
[S-switch-A-ospf-1] nexthop 10.1.2.2 weight 1
[S-switch-A-ospf-1] quit
```

Check the routing table of S-switch-A.

```
[S-switch-A] 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
-----
10.1.1.0/24         Direct   0     0      D          10.1.1.1         Vlanif10
10.1.1.1/32         Direct   0     0          D          127.0.0.1
InLoopBack0
10.1.2.0/24         Direct   0     0      D          10.1.2.1         Vlanif20
10.1.2.1/32         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						
172.16.1.0/24	Direct	0	0	D	172.16.1.1	Vlanif50
172.16.1.1/32	Direct	0	0	D	127.0.0.1	
InLoopBack0						
172.17.1.0/24	OSPF	10	3	D	10.1.2.2	Vlanif20
192.168.0.0/24	OSPF	10	2	D	10.1.1.2	Vlanif10
192.168.1.0/24	OSPF	10	2	D	10.1.2.2	Vlanif20

As shown in the routing table, OSPF selects the next hop 10.1.2.2 as the unique optimal route. This is because the preference of the next hop 10.1.2.2 (S-switch-C) is higher than that of the next hop 10.1.1.2 (S-switch-B) after the preferences of the equal-cost routes are set.

Configuration Files

- Configuration file of S-switch-A

```
#
 sysname S-switch-A
#
 vlan batch 10 20 50
#
 interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
 interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
#
 interface Vlanif50
 ip address 172.16.1.1 255.255.255.0
#
 interface Ethernet0/0/1
 port trunk allow-pass vlan 10
#
 interface Ethernet0/0/2
 port trunk allow-pass vlan 20
#
 interface Ethernet0/0/3
 port trunk allow-pass vlan 50
#
 ospf 1 router-id 1.1.1.1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 10.1.2.0 0.0.0.255
 network 172.16.1.0 0.0.0.255
#
 return
```

- Configuration file of S-switch-B

```
sysname S-switch-B
#
 vlan batch 10 30
#
 interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
#
 interface Vlanif30
 ip address 192.168.0.1 255.255.255.0
#
 interface Ethernet0/0/1
 port trunk allow-pass vlan 10
#
 interface Ethernet0/0/2
 port trunk allow-pass vlan 30
#
 ospf 1 router-id 2.2.2.2
```

```
    area 0.0.0.0
      network 10.1.1.0 0.0.0.255
      network 192.168.0.0 0.0.0.255
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
vlan batch 20 40
#
interface Vlanif20
  ip address 10.1.2.2 255.255.255.0
#
interface Vlanif40
  ip address 192.168.1.1 255.255.255.0
#
interface Ethernet0/0/1
  port trunk allow-pass vlan 20
#
interface Ethernet0/0/2
  port trunk allow-pass vlan 40
#
ospf 1 router-id 3.3.3.3
  area 0.0.0.0
    network 10.1.2.0 0.0.0.255
    network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of S-switch-D

```
#
sysname S-switch-D
#
vlan batch 30 40 60
#
interface Vlanif30
  ip address 192.168.0.2 255.255.255.0
#
interface Vlanif40
  ip address 192.168.1.2 255.255.255.0
#
interface Vlanif60
  ip address 172.17.1.1 255.255.255.0
#
interface Ethernet0/0/1
  port trunk allow-pass vlan 30
#
interface Ethernet0/0/2
  port trunk allow-pass vlan 40
#
interface Ethernet0/0/3
  port trunk allow-pass vlan 60
#
ospf 1 router-id 4.4.4.4
  area 0.0.0.0
    network 192.168.0.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
return
```


3 IS-IS Configuration

About This Chapter

This chapter describes the IS-IS fundamentals, configuration steps for IS-IS functions, and typical examples.

[3.1 Introduction](#)

This section describes the principle and concepts of IS-IS.

[3.2 Configuring Basic IS-IS Functions](#)

This section describes how to start IS-IS and enable the S-switch to perform routing in the network by running the IS-IS protocol.

[3.3 Establishing or Maintaining IS-IS Neighbor Relationships or Adjacencies](#)

This section describes how to adjust the timers of IS-IS packets and configure LSP parameters.

[3.4 Configuring the IS-IS Attributes in Different Types of Networks](#)

This section describes how to change the network type of an IS-IS interface and configure the parameters of IS-IS in networks of different types.

[3.5 Configuring the Attributes of IS-IS Routes](#)

This section describes how to adjust the parameters of IS-IS routing entries and configure the link cost and priority of IS-IS.

[3.6 Controlling the Advertisement of IS-IS Routing Information](#)

This section describes how to configure IS-IS to generate routes based on specified rules and set the rules for route leaking.

[3.7 Controlling the Receiving of IS-IS Routing Information](#)

This section controls the routing information inside and outside the domain.

[3.8 Adjusting and Optimizing IS-IS](#)

This section describes how to configure the status of IS-IS interfaces and adjust LSP parameters.

[3.9 Improving the Security of an IS-IS Network](#)

This section describes how to configure the IS-IS authentication mode and password.

[3.10 Maintaining IS-IS](#)

This section describes how to reset IS-IS connections or debug IS-IS.

[3.11 Configuration Examples](#)

This section provides several configuration examples of IS-IS.

3.1 Introduction

This section describes the principle and concepts of IS-IS.

3.1.1 Basic Concepts of IS-IS

3.1.2 IS-IS Features Supported by the S-switch

3.1.3 Logical Relationships Between the Configuration Tasks

3.1.4 Update History

3.1.5 References

3.1.1 Basic Concepts of IS-IS

The intra-domain Intermediate System-to-Intermediate System (IS-IS) routing protocol is initially issued by the International Organization for Standardization (ISO) for its Connectionless Network Protocol (CLNP).

To support the IP routing, the International Engineering Task Force (IETF) extends and modifies IS-IS in RFC 1195. Thus, IS-IS can be applied to TCP/IP and OSI environments at the same time. 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 inside an Autonomous System (AS). IS-IS is a link state protocol. It uses the Shortest Path First (SPF) algorithm to calculate routes, which resembles the Open Shortest Path First (OSPF) protocol.

IS-IS Areas

To support large-scale routing networks, IS-IS adopts a two-level structure in a routing domain. A large routing domain is divided into one or more areas. The intra-area routing is managed by Level-1 devices, whereas the inter-area routing is managed by Level-2 devices.

Figure 3-1 shows an IS-IS network. Its topology is similar to that of a multi-area OSPF network. Area 1 is a backbone area. All S-switches in the area are Level-2 devices. The other four areas are non-backbone areas. They are connected to Area 1 through Level-1-2 S-switches.

Figure 3-1 IS-IS topology I

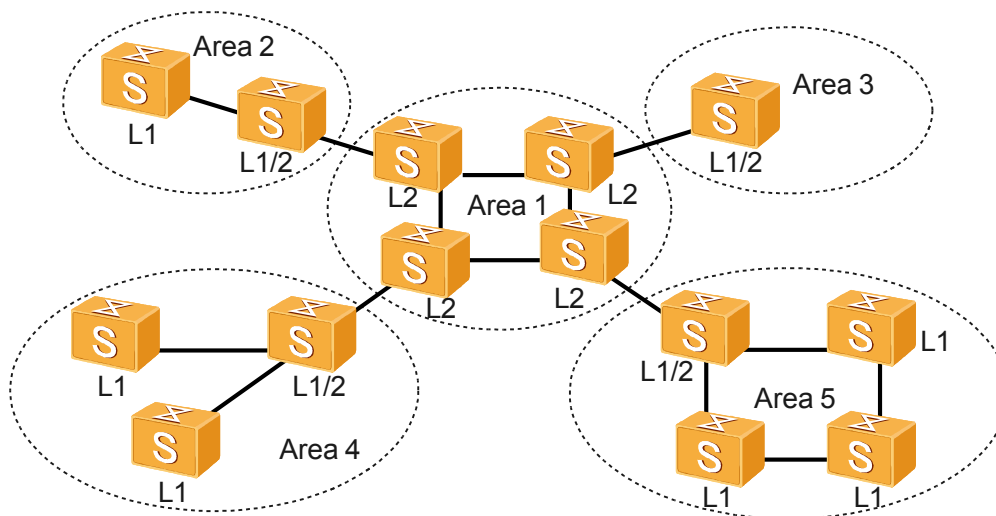
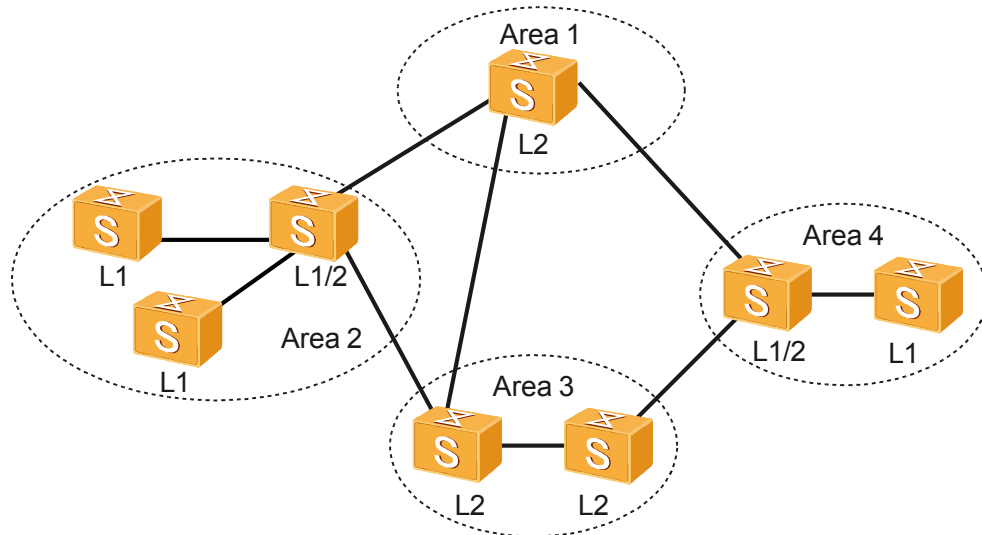


Figure 3-1 shows another IS-IS topology. The Level-1-2 S-switches are used to connect the Level-1 and Level-2 S-switches. In addition, the Level-1-2 S-switches constitute the backbone network together with the Level-2 S-switches. In this topology, no area is specified as the backbone area. All the Level-2 S-switches constitute an IS-IS backbone network. They may belong to different areas, but they must be successive.

Figure 3-2 IS-IS typology II



NOTE

An IS-IS backbone network does not refer to a specific area.

This networking scheme shows the difference 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 and Level-2 S-switches use the SPF algorithm to generate the Shortest Path Tree (SPT).

Network Types

IS-IS supports only two types of networks, which can be classified into the following categories based on physical links:

- Broadcast links such as Ethernet links
- Point-to-point (P2P) links

3.1.2 IS-IS Features Supported by the S-switch

IS-IS Interfaces

The creation of IS-IS routing tables and configurations of IS-IS functions and features must be done in Layer 3 interface views. Except the MEth interface, the physical interfaces on the S-switch, however, are Layer 2 interfaces. To facilitate the configurations, do as follows on the S-switch:

- Configure the VLAN to which a Layer 2 interface belongs, assign an IP address to the VLANIF interface of this VLAN, and enable the IS-IS functions and features on the interface.
- Assign an IP address to the sub-interface and enable IS-IS functions and features on the interface.
- Assign an IP address to the loopback interface and enable IS-IS functions and features on the interface.

The S-switch adds a 3-bit Logical-Link Control (LLC) field before an IS-IS PDU before encapsulating the PDU into an Ethernet frame. Then, the S-switch transmits the Ethernet frame. The LLC field does not belong to the head of the Ethernet frame but serves as a data field in the Ethernet frame. Therefore, the maximum length of an IS-IS PDU that can be transmitted by the S-switch equals the Maximum Transmission Unit (MTU) size of the physical interface minus 3. That is, the MTU value of an IS-IS interface equals the MTU value of a physical interface minus 3. The MTU value of a physical interface on the Quidway S5300 Series Ethernet Switches is 1500. Thus, the MTU value of an IS-IS interface on the Quidway S5300 Series Ethernet Switches is 1497.

Multi-process

For easy management and effective control, IS-IS provides the multi-process feature. The multi-process feature allows a group of interfaces to be associated with a specified IS-IS process. This ensures that the specific IS-IS process performs all the protocol operations only on the group of interfaces. Thus, multiple IS-IS processes can work on a single S-switch and each process is responsible for a unique group of interfaces.

Administrative Tags

The use of administrative tags simplifies management. Administrative tags can be controlled through the advertisement of IP prefixes in the IS-IS domain. An administrative tag carries information about the management of an IP address prefix. These tags are used to control the route importing between levels and areas and the bearing of different routing protocols, multiple IS-IS instances running on the same S-switch, BGP standard, and extended community attributes.

The value of an administrative tag is associated with certain attributes. When IS-IS advertises an IP address prefix with these attributes, it adds the administrative tag to the Type-Length-Value (TLV) in the prefix. In this manner, the tag is flooded with the prefix throughout the routing domain.

LSP Fragments Extension

If the link state Protocol Data Units (PDUs) to be advertised by IS-IS contain much information, they are advertised in multiple LSP fragments of the same system. Each LSP fragment is identified by the LSP identifier field of an LSP. The LSP identifier field is 1 byte long. Thus, the maximum number of fragments that can be generated by an IS-IS process is 256.

The IS-IS fragments extension feature allows an IS-IS process to generate more LSP fragments. To implement this feature, you can enable the network manager to configure additional system IDs for the S-switch. Each system ID represents a virtual system that can generate 256 LSP fragments. With more additional system IDs (up to 50 virtual systems), an IS-IS process can generate a maximum of 13056 LSP fragments.

- Related terms
 - Originating system
It is the S-switch that runs the IS-IS protocol. With the LSP fragments extension function, an LSP of an IS-IS S-switch can be sliced into multiple LSPs of pseudonodes before being advertised. The originating system refers to the actual IS-IS process.
 - Normal system ID
It is the system ID of the originating system.
 - Virtual System
This system is used to generate extended LSP fragments. After an LSP is sliced into more than 256 LSP fragments, the extra LSP fragments are advertised to the network by virtual systems. These fragments carry additional system IDs in their LSP ID fields.
 - Additional system ID
It is the system ID of a virtual system. The network manager assigns additional system IDs. Each additional system ID can generate up to 256 additional or extended LSP fragments. Like a normal system ID, an additional system ID must be unique in a routing domain.
- Operation modes
The S-switch can run the LSP fragments extension feature in the following modes:
 - mode-1: is adopted when certain nodes in the network do not support this feature. In this mode, the originating system advertises a link to each virtual system of which the additional system ID is in the LSPs. Similarly, each virtual system advertises a link to the originating system. The virtual systems look like the actual nodes that are connected to the originating system in the network. The one restriction in this mode is that only the leaf information can be advertised in the LSPs of the virtual systems.
 - mode-2: is adopted when all the nodes in the network support this feature. In this mode, all the nodes in the network can learn that the LSPs generated by the virtual systems actually belong to the originating system. There is no restriction on the link state information that can be advertised in the LSPs of the virtual systems.

Dynamic Hostname Exchange Mechanism

The dynamic hostname exchange mechanism is introduced to conveniently manage and maintain IS-IS networks. The mechanism provides a service of mapping hostnames to system IDs for the IS-IS S-switches. This dynamic name information is advertised in the form of a dynamic hostname TLV.

The dynamic hostname exchange mechanism also provides a service to associate a hostname with the Designated IS (DIS) in the broadcast network. Then, this mechanism advertises this association through the pseudonode LSP of the S-switch in the form of a dynamic hostname TLV.

It is easier to identify and memorize the hostname than the system ID. After this function is configured, the output of the **display** command run on the S-switch displays the hostname rather than the system ID of the S-switch.

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 adopted to calculate routes. When a node changes in the network, this algorithm is used to recalculate all routes. The calculation takes a long time and consumes too many CPU resources, which affects the convergence speed.

I-SPF improves this algorithm. Except for the first time, only changed nodes instead of all nodes are involved in calculation. The SPT generated at last is the same as that generated by the previous algorithm. This improves the CPU utilization and speeds up the network convergence.

- PRC

Similar to I-SPF, only changed nodes are involved in Partial Route Calculation (PRC). PRC, however, does not calculate the shortest path. It updates leaf routes based on the SPT calculated by I-SPF.

In route calculation, a leaf represents a route, and a node represents a device. If the SPT changes after I-SPF calculation, PRC processes all the leaves only on that changed node. If the SPT remains unchanged, PRC processes only the changed leaves.

For example, if IS-IS is enabled 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 consuming less CPU resources.

PRC working 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.

- LSP fast flooding

For the implementation of the RFC protocol, when the S-switch receives new LSPs from other S-switches, it floods out the LSPs in its own LSDB periodically according to a timer. This can speed up the network convergence, but the LSDB is synchronized slowly.

LSP fast flooding addresses the problem. When the S-switch configured with this feature receives one or more LSPs, it floods out the LSPs less than the specified number before route calculation. Thus, LSDB can 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 consume too many CPU resources. The SPF intelligent timer addresses these problems.

It responds to the burst events quickly, and avoids too much CPU consumption. An IS-IS network running normally is stable. The frequent changes on a network are rather rare, and the IS-IS S-switch does not calculate routes very often. Thus, set a short period (in milliseconds) for triggering the route calculation for the first time. If the topology of the network changes very often, the interval set by the intelligent timer increases with the calculation times to avoid too much CPU consumption.

The LSP generation intelligent timer is similar to the SPF intelligent timer. When the LSP generation intelligent timer expires, the system generates a new LSP based on the current topology. The original mechanism adopts a timer with uniform intervals, and thus fast convergence and low CPU consumption cannot be achieved. Thus, the LSP generation timer is designed as an intelligent timer to respond to the burst events (such as the interface is Up or Down) quickly and speed up the network convergence. In addition, when the network changes very often, the interval for the intelligent timer becomes longer to avoid too much CPU consumption.



Take care to configure the intelligent timers according to the actual conditions of the network.

BFD for IS-IS

On the VRP, static 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.

To configure static BFD, use command lines to manually configure the parameters of BFD sessions, including the local identifier and remote identifier, and then send requests to set up BFD sessions.

3.1.3 Logical Relationships Between the Configuration Tasks

[3.2 Configuring Basic IS-IS Functions](#) is the prerequisite and basis of other configurations.

3.1.4 Update History

Version	Revision
V100R002C01B050	This is the first release.

3.1.5 References

For more details of IS-IS, refer to the follow documents:

- ISO 10589: ISO IS-IS Routing Protocol
- ISO 9542: ES-IS Routing Protocol
- ISO 8348/Ad2: Network Services Access Points
- RFC 1195: Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
- RFC 2763: Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 2966: Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 2973: IS-IS Mesh Groups
- RFC 3277: IS-IS Transient Blackhole Avoidance
- RFC 3358: Optional Checksums in ISIS
- RFC 3373: Three-Way Handshake for IS-IS Point-to-Point Adjacencies
- RFC 3567: Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
- RFC 3719: Recommendations for Interoperable Networks using IS-IS
- RFC 3786: Extending the Number of IS-IS LSP Fragments Beyond the 256 Limit
- RFC 3787: Recommendations for Interoperable IP Networks using IS-IS
- RFC 3784: IS-IS extensions for Traffic Engineering
- RFC 3847: Restart signaling for IS-IS

- draft-ietf-isis-admin-tags-02: A Policy Control Mechanism in IS-IS Using Administrative Tags
- draft-ietf-isis-wg-multi-topology-11: M-ISIS: Multi Topology (MT) Routing in IS-IS

3.2 Configuring Basic IS-IS Functions

This section describes how to start IS-IS and enable the S-switch to perform routing in the network by running the IS-IS protocol.

3.2.1 Establishing the Configuration Task

3.2.2 Enabling an IS-IS Process

3.2.3 Configuring a NET

3.2.4 (Optional) Configuring the Level of the S-switch

3.2.5 Starting the Corresponding IS-IS Process on the Specified Interface

3.2.6 Checking the Configuration

3.2.1 Establishing the Configuration Task

Applicable Environment

Perform the configuration task on each S-switch in a network first when enabling IS-IS on the S-switches so that the S-switches can normally select routes.

Pre-configuration Tasks

Before configuring basic IS-IS functions, complete the following tasks:

- Configuring the link layer protocol
- Configuring the VLANs to which the physical interfaces belong
- Assigning IP addresses to VLANIF interfaces to ensure that the neighboring nodes are reachable



NOTE

To configure the VLANs to which the interfaces belong, you can adopt the default mode or run the **port trunk allow-pass vlan** command to add interfaces to VLANs. Both ends of a link should adopt the same mode to add interfaces to a VLAN.

If you run the **port trunk allow-pass vlan** command to add interfaces to VLANs, the directly connected physical interfaces in the same network segment should be added to the same VLAN. In this manner, the corresponding VLANIF interfaces can set up the direct connection at the network level.

Data Preparation

To configure basic IS-IS functions, you need the following data.

No.	Data
1	IS-IS process ID

No.	Data
2	NET
3	(Optional) Level of the S-switch

3.2.2 Enabling an IS-IS Process

Context

To enable IS-IS, you should create an IS-IS process and run the **isis enable** command to activate it on the interface that may be associated with other S-switchs.

Do as follows on each S-switch that needs to run IS-IS.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **isis** [*process-id*] command to enable an IS-IS process and enter the IS-IS view.

process-id specifies an IS-IS process. If no process ID is specified, IS-IS process 1 is started by default.

----End

3.2.3 Configuring a NET

Context

A NET specifies the current IS-IS area address and the system ID of the S-switch.

You can configure a maximum of three NETs on a process of a S-switch. The system IDs of the three NETs must be the same.

Do as follows on each S-switch that needs to run IS-IS.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **isis** [*process-id*] command to enter the IS-IS view.

Step 3 Run the **network-entity** *net* command to configure the Network Entity Title (NET).

----End

3.2.4 (Optional) Configuring the Level of the S-switch

Context

The IS-IS S-switch generates an LSDB for each level. If the level of the S-switch is Level-1-2, the S-switch generates a Level-1 LSDB and a Level-2 LSDB. If the level of the S-switch is Level-1 or Level-2, the S-switch generates an LSDB for the corresponding level. Creating and maintaining two LSDBs at the same time consume too many system resources. Thus, after the network structure is layered, set a proper level for the S-switch according to its position in the network.

Do as follows on each S-switch of which the level need be specified.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis [process-id]** command to enter the IS-IS view.
- Step 3** Run the **is-level { level-1 | level-1-2 | level-2 }** command to set the level of the S-switch.
- By default, the level of the S-switch is Level-1-2.
- End

3.2.5 Starting the Corresponding IS-IS Process on the Specified Interface

Context

Only one IS-IS process can be enabled on an interface.

Do as follows on each S-switch that needs to run IS-IS.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** to enter the interface view.
- Step 3** Run the **isis enable [process-id]** command to enable IS-IS on the specified interface.
- End

3.2.6 Checking the Configuration

Run the following commands to check the configuration.

Action	Command
Check information about the IS-IS interface.	display isis interface [verbose process-id] *
Check information about the LSDB.	display isis lsdb [{ level-1 level-2 } { local lsp-id is-name symbolic-name } process-id verbose] *

Action	Command
Check information about the IS-IS neighbors.	display isis peer [verbose] [<i>process-id</i>]
Check the IS-IS routing information.	display isis route [<i>process-id</i>] [ipv4] [{ <i>ip-address</i> [<i>mask</i> <i>mask-length</i>] } { level-1 level-2 } verbose] * display isis process-id route [ipv4] [{ <i>ip-address</i> [<i>mask</i> <i>mask-length</i>] } { level-1 level-2 } verbose] *
Check the statistics on the IS-IS process.	display isis statistics [level-1 level-2 level-1-2] [<i>process-id</i>]

Run the **display isis interface** command. If IS-IS neighbors are correctly established, you can find that the IPv4 neighbors of the local S-switch are in the Up state.

<Quidway> **display isis interface**

```

                                Interface information for ISIS(1)
                                -----
Interface      Id      IPV4.State      MTU    Type    DIS
Vlanif10      001      Up              Down   1497    L1/L2    No/No

```

3.3 Establishing or Maintaining IS-IS Neighbor Relationships or Adjacencies

This section describes how to adjust the timers of IS-IS packets and configure LSP parameters.

3.3.1 Establishing the Configuration Task

3.3.2 (Optional) Configuring Timers of IS-IS Packets

3.3.3 Configuring LSP Parameters

3.3.4 (Optional) Disable the Padding of Hello Packets on the Specified Interface

3.3.5 Checking the Configuration

3.3.1 Establishing the Configuration Task

Applicable Environment

After an IS-IS process is started, the S-switch sends IS-IS packets to neighbors through IS-IS interfaces. This section describes how to configure the parameters of IS-IS packets. You can adjust the configurations according to the actual conditions of different networks. The configurations are performed to:

- Adjust the timers of IS-IS packets such as Hello packets, CSNPs, and LSPs.
- Adjust the parameters of LSPs.
- Disable the padding of Hello packets on the specified interface.

When configuring the timers of IS-IS packets, note that the smaller the values of the timers, the more quickly the S-switch can detect the changes in the network topology and the greater the

link costs of the network. Properly configure the values of the timers according to the actual conditions of networks, keeping a balance between the speed of network convergence and utilization of bandwidth resources.

Pre-configuration Tasks

Before establishing or maintaining IS-IS neighbor relationships or adjacencies, complete the following tasks:

- Configuring the VLANs to which the physical interfaces belong
- Assigning IP addresses to VLANIF interfaces to ensure that the neighboring nodes are reachable
- [3.2 Configuring Basic IS-IS Functions](#)

Data Preparation

To create or maintain IS-IS neighbor relationships or adjacencies, you need the following data.

No.	Data
1	(Optional) Values of various packet timers
2	Values of LSP parameters

3.3.2 (Optional) Configuring Timers of IS-IS Packets

Configuring the Interval for Sending Hello Packets

Context

On broadcast links, there are Level-1 and Level-2 Hello packets. Different intervals can be set for different packets. If no level is specified, the same interval is configured for sending both Level-1 and Level-2 Hello packets. On point-to-point links, Hello packets are not differentiated on the basis of levels. Thus, the level needs not to be configured.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **isis timer hello hello-interval [level-1 | level-2]** command to set the interval for sending Hello packets on the interface.

By default, Hello packets are sent at intervals of 10 seconds.

----End

Configuring the Number of Invalid Hello Packets

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **isis timer holding-multiplier** *number* [**level-1** | **level-2**] command to set the number of invalid Hello packets.

By default, the number of invalid Hello packets is set to 3. If no level is specified, the same number is set for both Level-1 and Level-2 invalid Hello packets.

----End

Postrequisite

The IS-IS protocol maintains the neighbor relationships between the S-switches by sending and receiving Hello packets. If the local S-switch does not receive Hello packets from its peer over a certain period, that is, it does not receive a specified number of Hello packets continuously within a specified holding time, it deems the peer invalid.

In IS-IS, you can set the number of invalid Hello packets and the interval for sending Hello packets to adjust the holding time.

Configuring the Interval for Sending CSNPs

Context

CSNPs are transmitted by the DIS over the broadcast network to synchronize LSDBs. If no level is specified in the command, the interval for broadcasting the CSNPs of the current level is configured by default.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **isis timer csnp** *csnp-interval* [**level-1** | **level-2**] command to set the interval for sending CSNPs on the interface.

By default, CSNPs are sent at intervals of 10 seconds.

----End

Configuring the Interval for Retransmitting LSPs

Context

On a P2P link, if the local S-switch does not receive a response to a sent LSP within a certain period, it considers that the sent LSP is lost or discarded. To ensure reliable transmission, the local S-switch retransmits the LSP.

The LSPs sent over broadcast links need no response. Thus, do not perform this configuration on broadcast links.

If the type of an interface is changed to non-P2P, this configuration is deleted at the same time.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **isis circuit-type p2p** command to set the network type of the interface to P2P.
- Step 4** Run the **isis timer lsp-retransmit** *retransmit-interval* command to set the interval for retransmitting LSPs over P2P links.

By default, LSPs are retransmitted over P2P links at intervals of 5 seconds.

----End

Configuring the Minimum Interval for Sending LSPs

Context

If LSPs are too large, LSP fragments increase accordingly. In this case, you can configure the S-switch to send LSP fragments in batches. *throttle-interval* specifies the minimum interval between two batches. The optional parameter *count* specifies the number of LSP fragments to be sent at a time.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **isis timer lsp-throttle** *throttle-interval* [**count** *count*] command to set the minimum interval for sending LSPs.

----End

3.3.3 Configuring LSP Parameters

(Optional) Configuring the LSP Refreshment Period

Context

To synchronize all LSPs in the entire area, IS-IS regularly transmits all the current LSPs to neighbors. When configuring the LSP refreshment period, ensure that this period is shorter than the lifetime of LSPs.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
 - Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
 - Step 3** Run the **timer lsp-refresh** *refresh-interval* command to set the LSP refreshment period.
By default, the IS-IS refreshment period is 900 seconds.
- End

(Optional) Configuring LSP Lifetime

Context

When the S-switch generates an LSP, the system sets the lifetime for the LSP. When this LSP is transmitted in the area, its lifetime decreases as time elapses. If the S-switch does not receive an updated LSP all the time and the lifetime of this LSP decreases to 0, the LSP is deleted from the LSDB of the S-switch.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
 - Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
 - Step 3** Run the **timer lsp-max-age** *age-time* command to set the LSP lifetime.
By default, the maximum LSP lifetime is 1200 seconds.
- End

(Optional) Configuring the Intelligent Timer for Generating LSPs

Context

In IS-IS, when the local routing information changes, the S-switch needs to generate new LSPs to advertise the changes. When routing information changes frequently, however, the generation of new LSPs must be delayed. This avoids consuming too many system resources and impairing the system performance.

If the delay is too long, the changes of the local routing information cannot be advertised to the neighbors immediately and thus the network converges slowly.

The intelligent timer addresses these problems to a certain extent by adjusting the delay according to the frequencies of changes on the network. The interval for initially generating an LSP is called *initial-interval*. Then, add an incremental interval to it when each change occurs until the interval is up to the value of *max-interval*. When the interval reaches *max-interval* for three times, it drops to *initial-interval* again.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **timer lsp-generation** *max-interval* [*init-interval* [*incr-interval*]] [**level-1** | **level-2**] command to configure the intelligent timer used to generate LSPs.

----End

(Optional) Ignoring LSP Checksum Errors

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **ignore-lsp-checksum-error** command to configure the IS-IS process to ignore LSP checksum errors.

----End

Postrequisite

When the local IS-IS process receives an LSP, it checks its checksum. If the checksum is different from the calculated checksum, set the aging time and the checksum of the LSP to 0 and advertise this LSP. Thus, the LSP is removed from the LSDBs of other S-switches.

After this configuration, if an LSP has a checksum error, the IS-IS process still processes the LSP as a normal one. Errored LSPs can be corrected through the regular update of LSPs between neighbors. The quantity of LSPs can decrease through the configuration.

(Optional) Configuring the Maximum Size of a Sent LSP and That of a Received LSP

Context

When configuring *max-size*, ensure that the value of *max-size* specified in the **lsp-length originate** command is not more than the value of *max-size* specified in the **lsp-length receive** command.

When enabling IS-IS functions on an interface, ensure that the value of *max-size* specified in the **lsp-length originate** command is not more than the MTU value of the IS-IS interface. Otherwise, the interface is deemed in the MTU down state and the neighbor relationship cannot be set up.

The default MTU size of an IS-IS interface on the S-switch is 1497 bytes. If the S-switch and other products are used in the same network and the S-switch runs IS-IS, ensure that an LSP generated by other ISs contains not more than 1497 bytes. Otherwise, the network cannot operate normally.

Do as follows on each S-switch that needs to run IS-IS.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **lsp-length originate** *max-size* command to set the maximum size of a generated LSP.
- Step 4** (Optional) Run the **lsp-length receive** *max-size* command to set the maximum size of a received LSP.

By default, the maximum size of an LSP to be received or sent is 1497 bytes.

----End

Configuring the Mesh-Group Feature of the Interface

Context

On a network with a higher connectivity, an interface on the S-switch floods a received LSP to other interfaces on the S-switch. This flooding method causes repeated LSP flooding and wastes bandwidth.

To avoid such a problem, you can add certain interfaces to a mesh group. These interfaces do not flood the LSPs received from inside the group to other interfaces of the same group, but floods them outside the group. After **mesh-blocked** is configured on an interface, the interface is blocked and cannot flood LSPs. All the interfaces that join a mesh group ensure the synchronization of the LSDBs in the entire network segment by using the CSNP and Partial Sequence Number Packet (PSNP) mechanisms.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **isis mesh-group** { *mesh-group-number* | **mesh-blocked** } command to add the interface to a mesh group.
- End

Configuring LSP Fragments Extension

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **lsp-fragments-extend** [[**level-1** | **level-2** | **level-1-2**] | [**mode-1** | **mode-2**]] * command to enable the LSP fragments extension of IS-IS processes.
- Step 4** Run the **virtual-system** *virtual-system-id* command to configure a virtual system.
- End

Postrequisite

At least one virtual system ID must be configured so that the S-switch can generate extended LSP fragments. The virtual system IDs must be unique in the entire area and routing domain.

An IS-IS process can be configured with up to 50 virtual system IDs.

NOTE

- If all S-switches in a network support the LSP fragments extension, specify mode-2 in the lsp-fragments-extend command. If certain S-switches in a network do not support the LSP fragments extension, specify mode-1 in the lsp-fragments-extend command.
- The LSP fragments extension takes effect only after the reset isis process-id all command is run. After the IS-IS data structure is reset, all the previous structure information and the neighbor relationships are reestablished.

3.3.4 (Optional) Disable the Padding of Hello Packets on the Specified Interface

Context

The ISs that run the IS-IS protocol establish and maintain neighbor relationships through Hello packets. By default, an interface on the S-switch adds the Type-8 TLV to a Hello packet to be sent to make the Hello packet equal the buffer of the local S-switch in size. Thus, the Hello packet can be used to detect whether the MTU size of a neighbor interface matches the buffer

of the local S-switch. If the MTU size of the neighbor interface is smaller than the depth of the local buffer, the neighbor relationship cannot be set up.

The IS-IS small-hello function can shorten the length of a Hello packet to a great extent so that the S-switches can set up neighbor relationships. This configuration simplifies Hello packets and saves bandwidth on the network.

To set up IS-IS neighbor relationships with other devices, the S-switch should be disabled from padding Hello packets if the MTU size of the neighbor interface is greater than the local MTU size. Otherwise, the IS-IS neighbor relationships cannot be set up.

Do as follows on each S-switch that needs to run IS-IS.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **isis small-hello** command to enable IS-IS small-hello on the specified interface.
- End

3.3.5 Checking the Configuration

Run the following commands to check the configuration.

Action	Command
Check information about the IS-IS interface.	display isis interface [verbose <i>process-id</i>] *
Check the statistics on the IS-IS process.	display isis statistics [level-1 level-2 level-1-2] [<i>process-id</i>]

Set the interval for sending Hello packets to 15 seconds, the number of invalid Hello packets to 10, the interval for sending CSNPs to 123, and the minimum interval for sending LSPs to 159 and then check the configurations. The following is the check result:

<Quidway> **display isis interface verbose**

```

                                Interface information for ISIS(1)
                                -----
Interface      Id      IPV4.State      IPV6.State      MTU      Type      DIS
Vlanif10      001      Up              Down            1497     L1/L2     No/No
Circuit Parameters : small-hello
Description        : HUAWEI, Quidway Series, Vlanif10 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
Retransmit-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
```

3.4 Configuring the IS-IS Attributes in Different Types of Networks

This section describes how to change the network type of an IS-IS interface and configure the parameters of IS-IS in networks of different types.

[3.4.1 Establishing the Configuration Task](#)

[3.4.2 Configuring the Network Type of an IS-IS Interface](#)

[3.4.3 \(Optional\) Configuring the DIS Priority of an Interface](#)

[3.4.4 Checking the Configuration](#)

3.4.1 Establishing the Configuration Task

Applicable Environment

IS-IS attributes vary with the types of networks. This section describes how to configure IS-IS attributes in different types of networks. You can adopt the following configurations to control and optimize various networks, such as to:

- Change the link type of an Ethernet interface to P2P to emulate a P2P interface.
- Control the DIS election.
- Set the negotiation mode in which P2P neighbor relationships can be set up.
- Set IS-IS not to check IP addresses when the neighbor relationship is set up between the P2P interfaces on two nodes. In this manner, the neighbor relationship can be set up between two P2P interfaces that reside at different network segments.

Pre-configuration Tasks

Before configuring the IS-IS attributes in different types of networks, complete the following tasks:

- Configuring the VLANs to which the physical interfaces belong
- Assigning IP addresses to VLANIF interfaces to ensure that the neighboring nodes are reachable
- [3.2 Configuring Basic IS-IS Functions](#)

Data Preparation

To configure the IS-IS attributes in different types of networks, you need the following data.

No.	Data
1	Network type of the interface
2	(Optional) DIS priority of the interface

3.4.2 Configuring the Network Type of an IS-IS Interface

Context

If the network types of two neighboring IS-IS interfaces are different, the local S-switch may not learn the correct routes. In this case, perform this configuration. By default, the network type of an interface depends on the physical interface.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **isis circuit-type p2p** command to set the network type of the interface to P2P.
- End

3.4.3 (Optional) Configuring the DIS Priority of an Interface

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **isis dis-priority** *priority [level-1 | level-2]* command to set the DIS priority. The greater the value, the higher the priority.

By default, the DIS priority of an IS-IS interface is 64.

Level-1 DISs and Level-2 DISs are elected respectively, and you can configure different priorities for them. If no level is specified in the command, the DIS priority is configured for both Level-1 and Level-2.

The DIS is elected according to the DIS priority. The IS where the interface with the highest DIS priority resides is elected as the DIS. In the case of equal priorities, the interface with the highest MAC address is selected. An interface with the DIS priority of 0 still participates in the DIS election, which is different from OSPF.

 **NOTE**

- The DIS priority is valid for only broadcast networks.
- If the network type of an Ethernet interface is changed to P2P through the isis circuit-type command, IS-IS processes the interface as a P2P interface. In this case, the dis-priority command does not take effect.

----End

3.4.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about the IS-IS interface.	display isis interface [verbose <i>process-id</i>] *

Set the network type to P2P and the DIS priority to 100 on the VLANIF 10 interface, and check the configurations. The following is the check result:

<Quidway> **display isis interface verbose**

```

                                Interface information for ISIS(1)
                                -----
Interface      Id      IPV4.State      IPV6.State      MTU   Type   DIS
Vlanif10      002      Up              Down            1497  L1/L2  --
Circuit Parameters : p2p
Description        : HUAWEI, Quidway Series, Vlanif10 Interface
SNPA Address       : 00e0-095b-4201
IP Address         : 123.1.1.1
IPV6 Link Local Address :
IPV6 Global Address(es) :
Csnp Timer Value   : L1    10  L2    10
Hello Timer Value   :      15
DIS Hello Timer Value :
Hello Multiplier Value :      10
Cost               : L1    10  L2    10
Ipv6 Cost          : L1    10  L2    10
Priority           : L1    100  L2    100
Retransmit Timer Value : L12    5
Retransmit-Throttle Timer : L12    50
Bandwidth-Value     : Low 1000000000 High      0
Static Bfd          : NO
Dynamic Bfd         : NO
Fast-Sense Rpr      : NO
Extended-Circuit-Id Value : 0000000001

```

3.5 Configuring the Attributes of IS-IS Routes

This section describes how to adjust the parameters of IS-IS routing entries and configure the link cost and priority of IS-IS.

3.5.1 Establishing the Configuration Task

3.5.2 Configuring the Cost of an IS-IS Interface

3.5.3 Configuring the Priority of IS-IS

3.5.4 Checking the Configuration

3.5.1 Establishing the Configuration Task

Applicable Environment

This section describes how to change the attributes of IS-IS routes, such as the cost value and priority. By setting proper attributes of IS-IS routes, you can modify the routing table and forwarding table. Thus, the optimum routes can be selected during the routing.

Pre-configuration Tasks

Before configuring IS-IS routing attributes, complete the following tasks:

- Configuring the VLANs to which the physical interfaces belong
- Assigning IP addresses to VLANIF interfaces to ensure that the neighboring nodes are reachable
- [3.2 Configuring Basic IS-IS Functions](#)

Data Preparation

Before configuring IS-IS routing attributes, you need the following data.

No.	Data
1	Cost of the IS-IS interface
2	Priority of the IS-IS protocol

3.5.2 Configuring the Cost of an IS-IS Interface

Configuring the IS-IS Cost Type

Context

Do as follows on the S-switch as required.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **isis [process-id]** command to enter the IS-IS view.

Step 3 Run the **cost-style { narrow | wide | wide-compatible | { narrow-compatible | compatible } [relax-spf-limit] }** command to configure the IS-IS cost type.

The cost range of an interface and that of a received route vary with the cost type.

- If the cost type is narrow, the cost of an interface ranges from 1 to 63. The maximum cost of a received route is 1023.

- If the cost type is narrow-compatible or compatible, the cost of an interface ranges from 1 to 63. The cost of a 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 not more than 1023 and the link cost of every interface that the route passes through is less than 63, the route is received and the cost of the route is the actual one.

If the cost of the route is not more than 1023 but the link costs of certain interfaces that the route passes through are more than 63, the S-switch 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 is the actual one. The routes behind the interface are discarded.

If the cost of the route is more than 1023, the S-switch can learn only the routes of the interface whose link cost exceeds 1023 first. The routes of the network segment where the interface resides and routes imported by the interface can be learned by the S-switch. The cost of the route is 1023. The routes behind the interface are discarded.
 - If **relax-spf-limit** is set, there is no limitation to the link costs of interfaces or route costs. The cost of the route is the actual one.
- If the cost type is wide-compatible or wide, the cost of an interface ranges from 1 to 16777215. If the cost is 16777215, the neighbor TLV (with the cost of 16777215) generated on the link cannot be used in the route calculation. Instead, this neighbor TLV can only be used to deliver TE information. The maximum cost of the received routes is 0 x FFFFFFFF.

----End

Configuring the Cost of an IS-IS Interface

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **isis cost cost [level-1 | level-2]** command to configure the cost type of the IS-IS interface.

If no level is specified, the link cost is set for both Level-1 and Level-2.

By default, the link cost of an IS-IS interface is 10.

You can use the command to configure the cost of a certain interface.

----End

Configuring the Global Cost

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **circuit-cost** *cost* [**level-1** | **level-2**] command to configure the global IS-IS cost.
- If no level is specified, the link cost is set for Level-1-2 interfaces.
- You can use the command to change the cost of all interfaces at a time.
- End

Enabling Auto-Cost

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **bandwidth-reference** *value* command to set the reference value of the bandwidth.
- By default, the reference value of the bandwidth is 100 Mbit/s.
- Step 4** Run the **auto-cost enable** command to configure the interface to automatically calculate its cost.
- The **circuit-cost** or **isis cost** command is preferred over this command.
- End

Postrequisite

If the cost type is wide or wide-compatible, the bandwidth reference value configured in [Step 3](#) is valid.

Then, the cost of each interface = (bandwidth-reference/interface bandwidth) x 10. The bandwidth reference values of the ISs in an IS-IS area should be the same.

If the cost type is narrow, narrow-compatible, or compatible, the cost of each interface can be obtained from [Table 3-1](#).

Table 3-1 Relationship between interface costs and the bandwidth

Cost	Interface Bandwidth Range
60	Interface bandwidth ≤ 10M
50	10M < interface bandwidth ≤ 100M
40	100M < interface bandwidth ≤ 155M
30	155M < interface bandwidth ≤ 622M

Cost	Interface Bandwidth Range
20	622M < interface bandwidth ≤ 2.5G
10	2.5G < interface bandwidth

 **NOTE**

To change the cost of the loopback interface, run the **isis cost** command in the interface view.

3.5.3 Configuring the Priority of IS-IS

(Optional) Configuring the Priority of the IS-IS Protocol

Context

Do as follows on the S-switch as required.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **isis [process-id]** command to enter the IS-IS view.

Step 3 Run the **preference preference** command to set the priority of the IS-IS protocol.

This command is used to set the priority of the IS-IS protocol. The smaller the configured value, the higher the priority.

By default, the priority of the IS-IS protocol is 15.

----End

Postrequisite

The S-switch can run multiple routing protocols at the same time. When multiple routing protocols discover routes to the same destination, the route discovered by the protocol with the highest priority is adopted.

Configuring the Preference of Specific IS-IS Routes

Context

Do as follows on the S-switch as required.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **isis [process-id]** command to enter the IS-IS view.

- Step 3** Run the **preference route-policy** *route-policy-name* command to set the preference of specific routes through the configuration of the routing policy.

----End

Postrequisite

You can set the preference of specific routes by using the **preference route-policy** command. If the **apply preference** clause is included in the **preference route-policy** command, the preference of routes is as follows:

- Matched routes: Their preference is set by the **apply** clause.
- Unmatched routes: Their preference is set by the **preference preference** command.

If the **apply preference** clause is not included in the **preference route-policy** command, the preference of all routes is set by the **preference preference** command.

Configuring the Preference of IS-IS Equal-Cost Routes

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **nexthop ip-address weight value** command to set the preference of IS-IS load balancing.

----End

Postrequisite

After IS-IS uses the SPF algorithm to calculate the equal-cost routes, you can run the **nexthop** command to choose the route with the highest preference among the equal-cost routes as the next hop. The smaller the weight, the higher the preference of the route. By default, the value of **weight** is 255. It indicates that the load balancing is carried out among the equal-cost routes without distinguishing their preferences.

3.5.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the IS-IS interface.	display isis interface [verbose <i>process-id</i>] *

Action	Command
Check the IS-IS routing information.	display isis route [<i>process-id</i>] [ipv4] [{ <i>ip-address</i> [<i>mask</i> <i>mask-length</i>] } { level-1 level-2 } verbose] * display isis process-id route [ipv4] [{ <i>ip-address</i> [<i>mask</i> <i>mask-length</i>] } { level-1 level-2 } verbose] *

Set the cost of the VLANIF 10 interface to 20 and check the configuration. The following is the check result:

<Quidway> **display isis interface verbose**

```

                                Interface information for ISIS(1)
                                -----
Interface      Id      IPV4.State      IPV6.State      MTU   Type   DIS
Vlanif10      001      Up              Down            1497  L1/L2  No/No
Circuit Parameters      : small-hello
Description              : HUAWEI, Quidway Series, Vlanif10 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
Retransmit-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
  
```

3.6 Controlling the Advertisement of IS-IS Routing Information

This section describes how to configure IS-IS to generate routes based on specified rules and set the rules for route leaking.

[3.6.1 Establishing the Configuration Task](#)

[3.6.2 Configuring IS-IS Route Aggregation](#)

[3.6.3 Configuring IS-IS to Generate Default Routes](#)

[3.6.4 Configuring IS-IS Route Leaking from Level-2 to Level-1](#)

[3.6.5 Checking the Configuration](#)

3.6.1 Establishing the Configuration Task

Applicable Environment

To maintain the routes reaching all segments, an IS is required to have powerful capabilities in storage and route calculation. To reduce the burden brought by calculation and storage on the S-switch, you can set certain filtering rules on the S-switch and enable route aggregation. Through these configurations, fewer routes are transmitted. The routing entries maintained by the local S-switch and other S-switches in the network decrease accordingly.

This section describes how to control the advertisement of IS-IS routing information, for example, advertise aggregated routes, generate default routes, and configure route leaking.

Pre-configuration Tasks

Before configuring the advertisement of IS-IS routing information, complete the following tasks:

- Configuring the VLANs to which the physical interfaces belong
- Assigning IP addresses to VLANIF interfaces to ensure that the neighboring nodes are reachable
- [3.2 Configuring Basic IS-IS Functions](#)

Data Preparation

To configure the advertisement of IS-IS routing information, you need the following data.

No.	Data
1	Aggregated route
2	Type of route leaking

3.6.2 Configuring IS-IS Route Aggregation

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis [process-id]** command to enter the IS-IS view.
- Step 3** Run the **summary ip-address mask [avoid-feedback | generate_null0_route | tag tag | [level-1 | level-1-2 | level-2]] *** command to configure the IS-IS route aggregation.

You can aggregate the routes with the same next hop into one route, thus reducing the number of IS-IS routing entries in the routing table.

----End

3.6.3 Configuring IS-IS to Generate Default Routes

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **default-route-advertise** [**always** | **match default** | **route-policy** *route-policy-name*] [**cost** *cost*] [**tag** *tag*] [**level-1** | **level-1-2** | **level-2**] [**avoid-learning**] command to configure IS-IS to generate default routes.

The level of the S-switch determines the level of the default routes. After the **default-route-advertise** command is run, the generated default routes are advertised to only other S-switches of the same level. You can use the routing policy to force IS-IS to generate default routes only if a route in the routing table matches the policy.

----End

3.6.4 Configuring IS-IS Route Leaking from Level-2 to Level-1

Context

The command is run on the Level-1-2 S-switch that is connected to the external area. By default, the routing information of the Level-2 S-switch is not advertised to Level-1 areas.

Through IS-IS route leaking, the Level-1-2 S-switch can import the Level-2 routing information into Level-1 and advertise the information through Level-1 LSPs.

Do as follows on the corresponding Level-1-2 S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **import-route isis level-2 into level-1** [**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* }] [**tag** *tag*] command to enable IS-IS route leaking.

The routes in the backbone area and other Level-1 areas can be leaked into the Level-1 area where the local S-switch resides. In this manner, other S-switches in the same area can generate more accurate routing tables.

----End

3.6.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the LSDB.	display isis lsdb [{ level-1 level-2 } { local <i>lsp-id</i> is-name <i>symbolic-name</i> } <i>process-id</i> verbose] *
Check the IS-IS routing information.	display isis route [<i>process-id</i>] [ipv4] [{ <i>ip-address</i> [<i>mask</i> <i>mask-length</i>] } { level-1 level-2 } verbose] * display isis process-id route [ipv4] [{ <i>ip-address</i> [<i>mask</i> <i>mask-length</i>] } { level-1 level-2 } verbose] *

3.7 Controlling the Receiving of IS-IS Routing Information

This section controls the routing information inside and outside the domain.

3.7.1 Establishing the Configuration Task

3.7.2 Configuring IS-IS to Filter the Received Routing Information

3.7.3 Configuring IS-IS to Import External Routes

3.7.4 Checking the Configuration

3.7.1 Establishing the Configuration Task

Applicable Environment

To maintain the routes reaching all segments, the S-switch is required to have powerful capabilities in storage and route calculation. To reduce the burden brought by storage and calculation, you can set certain filtering rules on the S-switch to decrease the received routes so that the local S-switch maintains fewer routing entries.

This section describes how to control the receiving of IS-IS routing information, for example, filter the received routes and import external routes.

Pre-configuration Tasks

Before configuring the receiving of IS-IS routing information, complete the following tasks:

- Configuring the VLANs to which the physical interfaces belong
- Assigning IP addresses to VLANIF interfaces to ensure that the neighboring nodes are reachable
- [3.2 Configuring Basic IS-IS Functions](#)

Data Preparation

To configure the receiving of IS-IS routing information, you need the following data.

No.	Data
1	Filtering list that is needed to filter routing information

No.	Data
2	Protocol name and process ID of the external routes to be imported

3.7.2 Configuring IS-IS to Filter the Received Routing Information

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **import** command to configure IS-IS to filter the received routing information.
- End

3.7.3 Configuring IS-IS to Import External Routes

Context

IS-IS regards the routes discovered by other routing protocols as external routes. When IS-IS imports routes from other protocols, you can specify default costs of the imported routes.

If no level is specified in the **import-route** command, routes are imported to Level-2 routing tables.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** 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 routes from a specified protocol.
- Step 4** Run the **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]] command to filter the imported routes before being advertised.
- End

3.7.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the LSDB.	display isis lsdb [{ level-1 level-2 }] [{ local <i>lsp-id</i> is-name <i>symbolic-name</i> } <i>process-id</i> verbose] *
Check the IS-IS routing information.	display isis route [<i>process-id</i>] [ipv4] [{ <i>ip-address</i> [<i>mask</i> <i>mask-length</i>] } { level-1 level-2 } verbose] * display isis process-id route [ipv4] [{ <i>ip-address</i> [<i>mask</i> <i>mask-length</i>] } { level-1 level-2 } verbose] *

Run the **display isis route** command. If the IS-IS neighbor relationship is correctly established, you can view that the global cost of IS-IS process 1 on the local S-switch changes to 30 and the process imports a static route to 169.1.1.0/24.

<Quidway> **display isis route**

```

                ISIS(1) Level-2 Forwarding Table
                -----
IPv4 Destination      IntCost      ExtCost  ExitInterface  NextHop      Flags
-----
123.1.1.0/24          30            NULL      Vlanif10       Direct       D/-/L/-
20.0.0.0/24           30            NULL      Vlanif20       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

```

3.8 Adjusting and Optimizing IS-IS

This section describes how to configure the status of IS-IS interfaces and adjust LSP parameters.

3.8.1 Establishing the Configuration Task

3.8.2 (Optional) Configuring the Level of an IS-IS Interface

3.8.3 Setting the Status of an IS-IS Interface to Suppressed

3.8.4 Configuring SPF Parameters

3.8.5 Enabling LSP Fast Flooding

3.8.6 Configuring IS-IS Dynamic Hostname Mapping

3.8.7 Configuring the LSP Overload Bit

3.8.8 Configuring Output of the Adjacency Status

3.8.9 Checking the Configuration

3.8.1 Establishing the Configuration Task

Applicable Environment

This section describes how to adjust and optimize an IS-IS network. The details are as follows:

- Configure the level and status of IS-IS interfaces to decrease the flooding of broadcast packets in the network.
- Adjust SPF parameters to avoid the problem of resource consumption caused by frequent changes in the network.
- Configure the LSP fast flooding and overload bit to increase the convergence speed of the network and reduce the packets lost during the convergence.
- Configure IS-IS dynamic hostname mapping to meet users' requirements on easy maintenance.

Pre-configuration Tasks

Before adjusting and optimizing IS-IS, complete the following tasks:

- Configuring the VLANs to which the physical interfaces belong
- Assigning IP addresses to VLANIF interfaces to ensure that the neighboring nodes are reachable
- [3.2 Configuring Basic IS-IS Functions](#)

Data Preparation

To adjust and optimize IS-IS, you need the following data.

No.	Data
1	Level of the interface
2	Parameters of the SPF timer
3	Mapping between the system ID and the hostname

3.8.2 (Optional) Configuring the Level of an IS-IS Interface

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface interface-type interface-number** command to enter the interface view.
- Step 3** Run the **isis circuit-level [level-1 | level-1-2 | level-2]** command to configure the level of the interface.

By default, the level of an interface is Level-1-2.

If the local S-switch is a Level-1-2 S-switch and needs to establish a Level-1 or Level-2 relationship with the peer, this command can be used to restrict the interface to send and receive only the Hello packets at this level. Over P2P links, only one type of Hello packets can be transmitted and received. This mode simplifies the process and saves bandwidth.

 **NOTE**

Changing the level of an IS-IS interface is valid only when the level of the IS-IS process is Level-1-2. If the process is not a Level-1-2 process, the level of the IS-IS process determines the level of an established adjacency.

----End

3.8.3 Setting the Status of an IS-IS Interface to Suppressed

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **isis silent** command to set the status of the IS-IS interface is set to suppressed.

----End

Postrequisite

When an IS-IS network is connected to other routing domains, you need to enable IS-IS on the outbound interface. Thus, the S-switchs inside the domain can learn the outbound routes. The interface, however, sends IS-IS Hello packets to the network segment where it resides, which is unnecessary. In this case, you can run the **isis silent** command to set the IS-IS interface to suppressed.

When an IS-IS interface is suppressed, it does not send or receive any IS-IS packet. But the routes of the network segment where the interface resides can still be advertised to other S-switchs in the domain.

 **NOTE**

If the status of the IS-IS protocol on the interfaces in the domain is Down, the S-switchs within the domain cannot learn the outbound routes.

3.8.4 Configuring SPF Parameters

Configuring the SPF Intelligent Timer

Context

According to the IS-IS protocol, the S-switch needs to recalculate the shortest path when an LSDB changes. Frequent route calculations consume a lot of system resources and affect the

system performance. Delaying SPF calculation improves the efficiency of route calculation to a certain extent and reduces the resource consumption. A long delay, however, slows down the network convergence.

The SPF intelligent timer is a good solution to the problem. It can adjust the delay according to the frequency of changes in an LSDB. The interval for initially calculating the SPF is called *initial interval*. Then, add one *incremental interval* to it when each change occurs until the interval is up to *max-interval*. When the interval reaches *max-interval* for three times, it drops to *initial-interval* again.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
 - Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
 - Step 3** Run the **timer spf** *max-interval* [*init-interval* [*incr-interval*]] command to configure the SPF intelligent timer.
- End

Configuring the Duration for SPF Calculation

Context

When a routing table contains more than 150000 entries, the SPF calculation of IS-IS occupies the CPU resources for a long time. To avoid this, you can slice the SPF calculation. Through this configuration, you can also set the duration for each SPF calculation. If an SPF calculation does not process all the routing information, the calculation continues one second later.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
 - Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
 - Step 3** Run the **spf-slice-size** *duration-time* command to configure the duration for each SPF calculation.
- End

3.8.5 Enabling LSP Fast Flooding

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **flash-flood** [{ **level-1** | **level-2** } | *lsp-count* | **max-timer-interval** *interval*] * command to enable the LSP fast flooding.

You can use the **flash-flood** command to speed up the LSP flooding. You can specify the number of LSPs flooded each time for all the interfaces that run an IS-IS process. If the number of LSPs to be sent is greater than the specified number, the LSPs of the specified number are flooded each time. If you have specified **max-timer-interval**, the LSPs are flooded after the timer expires.

----End

3.8.6 Configuring IS-IS Dynamic Hostname Mapping

Configuring the Hostname for the Local IS

Context

This command is used to configure a symbolic name for the local IS-IS process and also to enable the mapping of the system ID to the hostname. The name configured is added to LSPs and advertised to other neighbors through the LSPs.

You must run the **is-name** command before the dynamic hostname mapping of IS-IS processes is enabled. Otherwise, the **display** command cannot display the mapping between the system ID and the hostname.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **is-name** *symbolic-name* command to configure the hostname for the local IS.

----End

Configuring the Hostname for the Remote IS

Context

This command is used to locally configure a symbolic name for a remote IS-IS S-switch. Each system ID matches only one name.

If the remote S-switch is already configured with a mapping between the hostname and the system ID, that mapping overrides the static mapping configured on the local S-switch.

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **is-name map** *system-id symbolic-name* command to configure the hostname for the remote IS.
- End

3.8.7 Configuring the LSP Overload Bit

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **set-overload** [**on-startup** [*timeout1*] | **start-from-nbr** *system-id* [*nbr-timeout2* [*nbr-timeout1*]]] [**allow** { **interlevel** | **external** } *] command to configure the overload bit.

After LSPs are configured with the overload fields, they are flooded in the network. These LSPs, however, are not used when the routes that pass the overload S-switch are calculated. When the overload bit is set for the S-switch, the other S-switches no longer forward packets to this S-switch. The packets destined to the S-switch, however, are still sent to the S-switch.

If the S-switch in an IS-IS area fails, the calculation of the routes in the entire area may be incorrect. To locate the fault, you can set the overload bit for this S-switch to isolate the S-switch from the IS-IS network temporarily.

----End

3.8.8 Configuring Output of the Adjacency Status

Context

Do as follows on the S-switch as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to enter the IS-IS view.
- Step 3** Run the **log-peer-change** command to enable the output of the adjacency status.

After the local terminal monitor and the output of the adjacency status are enabled, the changes of IS-IS adjacencies are output on the configuration terminal until the output is disabled.

----End

3.8.9 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the table of mappings between the local S-switch names and system IDs.	display isis name-table [<i>process-id</i>]
Check information about the LSDB.	display isis lsdb [{ level-1 level-2 } { local <i>lsp-id</i> is-name <i>symbolic-name</i> } <i>process-id</i> verbose] *
Check information about the IS-IS interface.	display isis interface [verbose <i>process-id</i>] *
Check the SPF log of IS-IS.	display isis spf-log [<i>process-id</i>]
Check the SPF tree of IS-IS.	display isis spf-tree [systemid <i>systemid</i> dname <i>dname</i>] [{ level-1 level-2 } verbose] * [<i>process-id</i>]

Run the **display isis name-table 1** command, and you can view that the hostname of the local S-switch is **abc**.

```
<Quidway> display isis name-table 1
System ID      Hostname      Type
1111.1111.1111  abc          DYNAMIC
```

3.9 Improving the Security of an IS-IS Network

This section describes how to configure the IS-IS authentication mode and password.

3.9.1 Establishing the Configuration Task

3.9.2 Configuring Area Authentication and Routing Domain Authentication

3.9.3 Configuring the Authentication on an Interface

3.9.4 Checking the Configuration

3.9.1 Establishing the Configuration Task

Applicable Environment

In a network that requires high security, you can configure the IS-IS authentication functions. This configuration can improve the security of the network to meet users' requirements on security. The IS-IS authentication functions include area authentication, routing domain authentication, and interface authentication.

Pre-configuration Tasks

Before improving the security of an IS-IS network, complete the following tasks:

- Configuring the VLANs to which the physical interfaces belong
- Assigning IP addresses to VLANIF interfaces to ensure that the neighboring nodes are reachable
- [3.2 Configuring Basic IS-IS Functions](#)

Data Preparation

To improve the security of an IS-IS network, you need the following data.

No.	Data
1	Authentication mode and password

3.9.2 Configuring Area Authentication and Routing Domain Authentication

Context

If area authentication is required, the area authentication password is encapsulated into Level-1 LSPs, CSNPs, and PSNPs in a specified mode. The S-switches in an area must adopt the same area authentication mode and password so that IS-IS packets can be normally flooded.

Similarly, for domain authentication, the password is also encapsulated into Level-2 LSPs, CSNPs, and PSNPs in a specified mode. The S-switches in a domain must adopt the same domain authentication mode and password so that IS-IS packets can be normally flooded.

Whether IS-IS packets pass the area or domain authentication does not affect the establishment of Level-1 or Level-2 neighbor relationships.

Do as follows on the S-switch in a network that has high requirements on security as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis [process-id]** command to enter the IS-IS view.
- Step 3** Run the **area-authentication-mode { simple password | md5 password-key } [ip | osi]** command to configure the mode of area authentication.
- Step 4** Run the **domain-authentication-mode { simple password | md5 password-key } [ip | osi]** command to configure the mode of domain authentication.

----End

3.9.3 Configuring the Authentication on an Interface

Context

Do as follows on the S-switch in a network that has high requirements on security as required.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface** *interface-type interface-number* command to enter the interface view.
- Step 3** Run the **isis authentication-mode** { **simple** *password* | **md5** *password-key* } [**level-1** | **level-2**] [**ip** | **osi**] command to set the IS-IS authentication mode and password on the interface.
- End

Postrequisite

The authentication set on an interface applies to Hello packets to confirm the validity and correctness of the neighbor. Two S-switchs can set up the neighbor relationship only after the Hello packets pass the authentication.



NOTE

level-1 and level-2 are displayed only on Ethernet interfaces. If no level is specified, Level-1 and Level-2 adopts the same authentication mode and password.

3.9.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the IS-IS neighbors.	display isis peer [verbose] [<i>process-id</i>]
Check information about the IS-IS neighbors.	display isis brief [<i>process-id</i>]

3.10 Maintaining IS-IS

This section describes how to reset IS-IS connections or debug IS-IS.

[3.10.1 Resetting the IS-IS Data Structure](#)

[3.10.2 Resetting a Specific IS-IS Neighbor](#)

[3.10.3 Debugging IS-IS](#)

3.10.1 Resetting the IS-IS Data Structure



CAUTION

After you reset the IS-IS data structure, all the previous structure information and neighbor relationships are cleared. Thus, confirm the action before you use the command.

After you confirm the need to reset the IS-IS data structure, run the following **reset** command in the user view.

Action	Command
Reset the IS-IS data structure.	reset isis all [<i>process-id</i>]

3.10.2 Resetting a Specific IS-IS Neighbor



CAUTION

The specified IS-IS neighbor relationships are deleted after you reset a specified IS-IS neighbor with the **reset isis** command. Thus, confirm the action before you use the command.

After modifying the IS-IS routing policy, you need to reset the specified IS-IS neighbor to make the modification take effect. To reset a specified IS-IS neighbor, run the following **reset** command in the user view.

Action	Command
Reset a specific IS-IS neighbor.	reset isis peer system-id [<i>process-id</i>]

3.10.3 Debugging IS-IS



CAUTION

Debugging affects the performance of the system. So, after debugging, run the **undo debugging all** command to disable it immediately.

When an IS-IS fault occurs, run the following **debugging** commands in the user view to debug IS-IS and locate the fault.

Action	Command
Debug IS-IS.	debugging isis all [<i>process-id</i>]
Debug IS-IS adjacencies.	debugging isis adjacency [<i>process-id</i>]
Debug IS-IS authentication errors.	debugging isis authentication-error [<i>process-id</i>]
Debug IS-IS checksum errors.	debugging isis checksum-error [<i>process-id</i>]

Action	Command
Debug the interface-level IS-IS information.	debugging isis circuit-information [<i>process-id</i>]
Debug IS-IS configuration errors.	debugging isis configuration-error [<i>process-id</i>]
Debug the IS-IS data link receiving packets.	debugging isis datalink-receiving-packet [<i>process-id</i>]
Debug the IS-IS data link sending packets.	debugging isis datalink-sending-packet [<i>process-id</i>]
Debug IS-IS events.	debugging isis event [<i>process-id</i>]
Debug IS-IS general errors.	debugging isis general-error [<i>process-id</i>]
Debug IS-IS GR events.	debugging isis graceful-restart [<i>process-id</i>]
Debug IS-IS HA events.	debugging isis ha-events [<i>process-id</i>]
Debug the IS-IS interface information.	debugging isis interface-information [<i>process-id</i>]
Debug the IS-IS memory allocation.	debugging isis memory-allocating [<i>process-id</i>]
Debug IS-IS miscellaneous errors.	debugging isis miscellaneous-errors
Debug the packets received by IS-IS.	debugging isis receiving-packet-content [<i>process-id</i>]
Debug the contents of the packets received by IS-IS (displayed in the format of the packets).	debugging isis receiving-packet-regular-content [<i>process-id</i>]
Debug the local update packets.	debugging isis self-originate-update [<i>process-id</i>]
Debug the packets transmitted by IS-IS.	debugging isis sending-packet-content [<i>process-id</i>]
Debug the contents of the packets sent by IS-IS (displayed in the format of packets).	debugging isis sending-packet-regular-content [<i>process-id</i>]
Debug SNP packets.	debugging isis snp-packet [<i>process-id</i>]
Debug SPF events.	debugging isis spf-event [<i>process-id</i>]
Debug the SPF process used for SPF calculation.	debugging isis spf-prc [<i>process-id</i>]
Debug the SPF summary.	debugging isis spf-summary [<i>process-id</i>]
Debug the SPF timers.	debugging isis spf-timer [<i>process-id</i>]
Debug IS-IS task errors.	debugging isis task-error [<i>process-id</i>]
Debug the IS-IS timers.	debugging isis timer [<i>process-id</i>]

Action	Command
Debug the IS-IS traffic engineering.	debugging isis traffic-eng { advertisement event } [<i>process-id</i>]
Debug the IS-IS update packets.	debugging isis update-packet [<i>process-id</i>]
Debug the IS-IS update processes.	debugging isis update-process [<i>process-id</i> ipv4-acl <i>acl-numbe</i> [<i>process-id</i>]]

3.11 Configuration Examples

This section provides several configuration examples of IS-IS.

[3.11.1 Example for Configuring Basic IS-IS Functions](#)

[3.11.2 Example for Configuring IS-IS Route Aggregation](#)

[3.11.3 Example for Configuring the DIS Election of IS-IS](#)

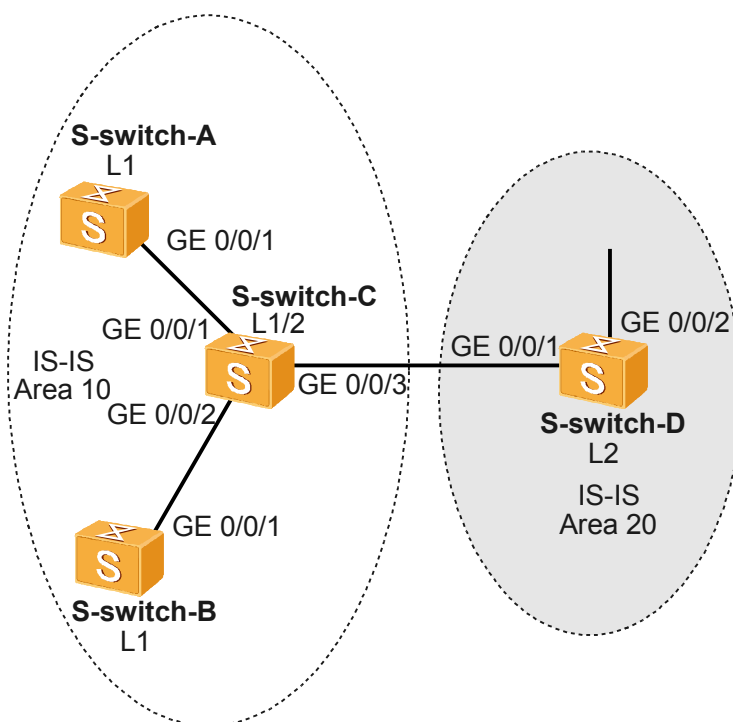
[3.11.4 Example for Configuring IS-IS Load Balancing](#)

3.11.1 Example for Configuring Basic IS-IS Functions

Networking Requirements

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

- S-switch-A, S-switch-B, S-switch-C, and S-switch-D belong to the same domain. The IS-IS routing protocol runs on these four S-switchs to ensure connectivity on an IP network.
- The areas IDs of S-switch-A, S-switch-B, and S-switch-C are all 10, and the area ID of S-switch-D is 20.
- S-switch-A and S-switch-B are Level-1 S-switchs. S-switch-C is the Level-1-2 S-switch. S-switch-D is the Level-2 S-switch.

Figure 3-3 Networking diagram for configuring basic IS-IS functions

S-switch	Interface	VLANIF Interface	IP Address
S-switch-A	GE 0/0/1	VLANIF 10	10.1.1.2/24
S-switch-B	GE 0/0/1	VLANIF 20	10.1.2.2/24
S-switch-C	GE 0/0/1	VLANIF 10	10.1.1.1/24
S-switch-C	GE 0/0/2	VLANIF 20	10.1.2.1/24
S-switch-C	GE 0/0/3	VLANIF 30	192.168.0.1/24
S-switch-D	GE 0/0/1	VLANIF 30	192.168.0.2/24
S-switch-D	GE 0/0/2	VLANIF 40	172.16.1.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the VLANs to which the physical interfaces belong.
2. Assign IP addresses to VLANIF interfaces.
3. Run the IS-IS process on each S-switch, specify the network entity, and configure the level.
4. Check the IS-IS database and routing table of each S-switch.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID of each interface, as shown in [Figure 3-3](#)
- IP address of each VLANIF interface, as shown in [Figure 3-3](#)

- System ID, level, and area ID of each S-switch
 - S-switch-A: The system ID is 0000.0000.0001; the area ID is 10; the level is Level-1.
 - S-switch-B: The system ID is 0000.0000.0002; the area ID is 10; the level is Level-1.
 - S-switch-C: The system ID is 0000.0000.0003; the area ID is 10; the level is Level-1-2.
 - S-switch-D: The system ID is 0000.0000.0004; the area ID is 20; the level is Level-2.

Configuration Procedure

1. Configure the IDs of the VLANs to which the interfaces belong.
The configuration details are not mentioned.
2. Assign IP addresses to VLANIF interfaces.
The configuration details are not mentioned.
3. Run the IS-IS progress on each S-switch, specify the network entity, and configure the level.

Configure S-switch-A.

```
[S-switch-A] isis 1
[S-switch-A-isis-1] is-level level-1
[S-switch-A-isis-1] network-entity 10.0000.0000.0001.00
[S-switch-A-isis-1] quit
```

Configure S-switch-B.

```
[S-switch-B] isis 1
[S-switch-B-isis-1] is-level level-1
[S-switch-B-isis-1] network-entity 10.0000.0000.0002.00
[S-switch-B-isis-1] quit
```

Configure S-switch-C.

```
[S-switch-C] isis 1
[S-switch-C-isis-1] network-entity 10.0000.0000.0003.00
[S-switch-C-isis-1] quit
```

Configure S-switch-D.

```
[S-switch-D] isis 1
[S-switch-D-isis-1] is-level level-2
[S-switch-D-isis-1] network-entity 20.0000.0000.0004.00
[S-switch-D-isis-1] quit
```

4. Enable the IS-IS progress on each interface and enable IS-IS small-hello.

Configure S-switch-A.

```
[S-switch-A] interface vlanif 10
[S-switch-A-Vlanif10] isis enable 1
[S-switch-A-Vlanif10] quit
```

Configure S-switch-B.

```
[S-switch-B] interface vlanif 20
[S-switch-B-Vlanif20] isis enable 1
[S-switch-B-Vlanif20] quit
```

Configure S-switch-C.

```
[S-switch-C] interface vlanif 10
[S-switch-C-Vlanif10] isis enable 1
[S-switch-C-Vlanif10] quit
[S-switch-C] interface vlanif 20
[S-switch-C-Vlanif20] isis enable 1
[S-switch-C-Vlanif20] quit
[S-switch-C] interface vlanif 30
[S-switch-C-Vlanif30] isis enable 1
[S-switch-C-Vlanif30] quit
```

Configure S-switch-D.

```
[S-switch-D] interface vlanif 30
[S-switch-D-Vlanif30] isis enable 1
[S-switch-D-Vlanif30] quit
[S-switch-D] interface vlanif 40
[S-switch-D-Vlanif40] isis enable 1
[S-switch-D-Vlanif40] quit
```

5. Verify the configuration.

Display the IS-IS LSDB of each S-switch.

```
[S-switch-A] display isis lsdb
```

```
Database information for ISIS(1)
-----

Level-1 Link State Database
```

LSPID OL	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
0000.0000.0003.01-00	0x00000004	0xa7dd	582	55	0/0/0
0000.0000.0003.02-00	0x00000002	0xc0c4	524	55	0/0/0

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
ATT-Attached, P-Partition, OL-Overload

```
[S-switch-B] display isis lsdb
```

```
Database information for ISIS(1)
-----

Level-1 Link State Database
```

LSPID OL	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

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
ATT-Attached, P-Partition, OL-Overload

```
[S-switch-C] display isis lsdb
```

```
Database information for ISIS(1)
-----

Level-1 Link State Database
```

LSPID OL	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
0000.0000.0003.01-00*	0x00000005	0xa5de	569	55	0/0/0
0000.0000.0003.02-00*	0x00000003	0xbec5	569	55	0/0/0

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
ATT-Attached, P-Partition, OL-Overload

```
Level-2 Link State Database
```

LSPID OL	Seq Num	Checksum	Holdtime	Length	ATT/P/ OL
0000.0000.0003.00-00*	0x00000008	0x55bb	650	100	0/0/0
0000.0000.0003.03-00*	0x00000003	0xef91	650	55	0/0/0

```
0000.0000.0004.00-00    0x00000005    0x651          629          84          0/0/0
```

*(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
ATT-Attached, P-Partition, OL-Overload

[S-switch-D] **display isis lsdb**

```
Database information for ISIS(1)
-----
```

Level-2 Link State Database

LSPID OL	Seq Num	Checksum	Holdtime	Length	ATT/P/ OL
0000.0000.0003.00-00	0x00000008	0x55bb	644	100	0/0/0
0000.0000.0003.03-00	0x00000003	0xef91	644	55	0/0/0
0000.0000.0004.00-00*	0x00000005	0x651	624	84	0/0/0

*(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 S-switch. A default route must be available in the routing table of the Level-1 S-switch and the next hop is a Level-1-2 S-switch. The routing table of the Level-2 S-switch must contain all Level-1 and Level-2 routes.

[S-switch-A] **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	Vlanif10	10.1.1.1	
A/-/-/-					
10.1.1.0/24	10	NULL	Vlanif10	Direct	D/-/
L/-					
10.1.2.0/24	20	NULL	Vlanif10	10.1.1.1	
A/-/-/-					
192.168.0.0/24	20	NULL	Vlanif10	10.1.1.1	
A/-/-/-					

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
U-Up/Down Bit Set

[S-switch-C] **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	Vlanif10	Direct	D/-/
L/-					
10.1.2.0/24	10	NULL	Vlanif20	Direct	D/-/
L/-					
192.168.0.0/24	10	NULL	Vlanif30	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	Vlanif10	Direct	D/-/
L/-					
10.1.2.0/24	10	NULL	Vlanif20	Direct	D/-/
L/-					
192.168.0.0/24	10	NULL	Vlanif30	Direct	D/-/
L/-					
172.16.0.0/16	20	NULL	Vlanif40	192.168.0.2	
A/-/-/-					

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
U-Up/Down Bit Set

[S-switch-D] **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	Vlanif30	Direct	D/-/
L/-					
10.1.1.0/24	20	NULL	Vlanif30	192.168.0.1	
A/-/-/-					
10.1.2.0/24	20	NULL	Vlanif30	192.168.0.1	
A/-/-/-					
172.16.0.0/16	10	NULL	Vlanif40	Direct	
A/-/-/-					

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
U-Up/Down Bit Set

Configuration Files

- Configuration file of S-switch-A

```
#
 sysname S-switch-A
#
 vlan batch 10
#
 isis 1
  is-level level-1
 network-entity 10.0000.0000.0001.00
#
 interface Vlanif10
  ip address 10.1.1.2 255.255.255.0
  isis enable 1
#
 interface GigabitEthernet0/0/1
  port trunk allow-pass vlan 10
#
return
```

- Configuration file of S-switch-B

```
#
 sysname S-switch-B
#
 vlan batch 20
#
 isis 1
  is-level level-1
 network-entity 10.0000.0000.0002.00
#
 interface Vlanif20
  ip address 10.1.2.2 255.255.255.0
```

```
isis enable 1
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 20
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
vlan batch 10 20 30
#
isis 1
network-entity 10.0000.0000.0003.00
#
interface Vlanif10
ip address 10.1.1.1 255.255.255.0
isis enable 1
#
interface Vlanif20
ip address 10.1.2.1 255.255.255.0
isis enable 1
#
interface Vlanif30
ip address 192.168.0.1 255.255.255.0
isis enable 1
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 30
#
return
```

- Configuration file of S-switch-D

```
#
sysname S-switch-D
#
vlan batch 30 40
#
isis 1
is-level level-2
network-entity 20.0000.0000.0004.00
#
interface Vlanif30
ip address 192.168.0.2 255.255.255.0
isis enable 1
#
interface Vlanif40
ip address 172.16.1.1 255.255.0.0
isis enable 1
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 40
#
Return
```

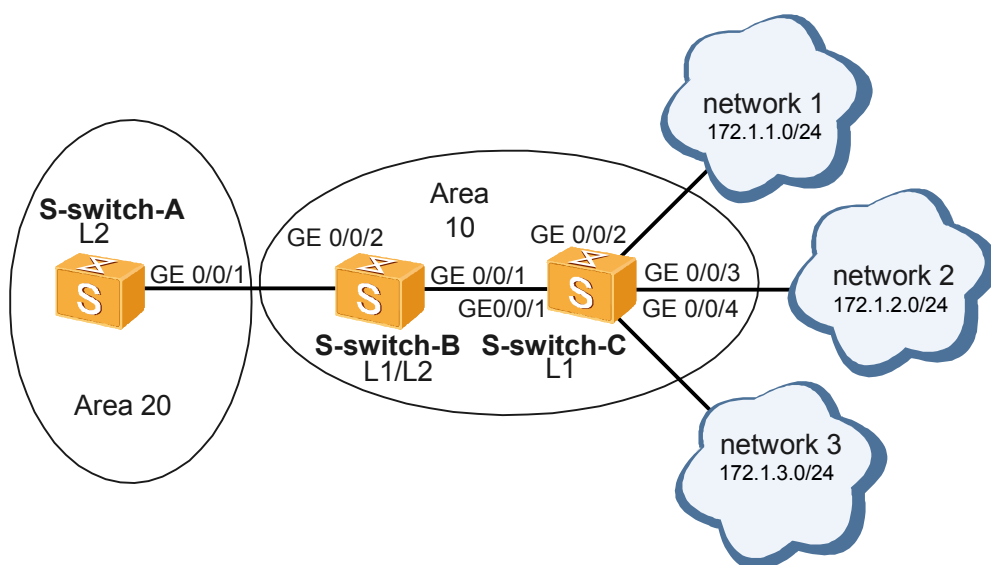
3.11.2 Example for Configuring IS-IS Route Aggregation

Networking Requirements

As shown in **Figure 3-4**:

- S-switch-A, S-switch-B, and S-switch-C are interconnected by running the IS-IS protocol.
- S-switch-A belongs to Area 20. S-switch-B and S-switch-C belong to Area 10.
- S-switch-A is a Level-2 S-switch. S-switch-B is a Level-1-2 S-switch. S-switch-C is a Level-1 S-switch.
- The addresses in Area 10 can be aggregated as 172.1.0.0/16.

Figure 3-4 Networking diagram for configuring IS-IS route convergence



S-switch	Interface	VLANIF Interface	IP Address
S-switch-A	GE 0/0/1	VLANIF 50	172.2.1.1/24
S-switch-B	GE 0/0/1	VLANIF 10	172.1.4.2/24
S-switch-B	GE 0/0/2	VLANIF 50	172.2.1.2/24
S-switch-C	GE 0/0/1	VLANIF 10	172.1.4.1/24
S-switch-C	GE 0/0/2	VLANIF 20	172.1.1.1/24
S-switch-C	GE 0/0/3	VLANIF 30	172.1.2.1/24
S-switch-C	GE 1/0/4	VLANIF 40	172.1.3.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic IS-IS functions on each S-switch so that the S-switches can be interconnected.
2. Check the IS-IS routing table of S-switch-A.
3. Configure route convergence on S-switch-B.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID of each interface, as shown in [Figure 3-4](#)
- IP address of each VLANIF interface, as shown in [Figure 3-4](#)
- System ID, level, and area ID of each S-switch
 - S-switch-A: The system ID is 0000.0000.0001; the area ID is 20; the level is Level-2.
 - S-switch-B: The system ID is 0000.0000.0002; the area ID is 10; the level is Level-1-2.
 - S-switch-C: The system ID is 0000.0000.0003; the area ID is 10; the level is Level-1.

Configuration Procedure

1. Configure the VLAN ID of each physical interface.
The configuration details are not mentioned here.
2. Assign IP addresses to VLANIF interfaces.
The configuration details are not mentioned here.
3. Configure basic IS-IS functions.

Configure S-switch-A.

```
[S-switch-A] isis 1
[S-switch-A-isis-1] is-level level-2
[S-switch-A-isis-1] network-entity 20.0000.0000.0001.00
[S-switch-A-isis-1] quit
[S-switch-A] interface vlanif 50
[S-switch-A-Vlanif50] isis enable 1
[S-switch-A-Vlanif50] quit
```

Configure S-switch-B.

```
[S-switch-B] isis 1
[S-switch-B-isis-1] network-entity 10.0000.0000.0002.00
[S-switch-B-isis-1] quit
[S-switch-B] interface vlanif 10
[S-switch-B-Vlanif10] isis enable 1
[S-switch-B-Vlanif10] quit
[S-switch-B] interface vlanif 50
[S-switch-B-Vlanif50] isis enable 1
[S-switch-B-Vlanif50] quit
```

Configure S-switch-C.

```
[S-switch-C] isis 1
[S-switch-C-isis-1] is-level level-1
[S-switch-C-isis-1] network-entity 10.0000.0000.0003.00
[S-switch-C-isis-1] quit
[S-switch-C] interface vlanif 10
[S-switch-C-Vlanif10] isis enable 1
[S-switch-C-Vlanif10] quit
```

The configurations of the VLANIF 20, VLANIF30, and VLANIF 40 interfaces are the same as the configuration of the VLANIF 10 interface.

4. Check the IS-IS routing table of S-switch-A.

```
[S-switch-A] 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	20	NULL	Vlanif50	172.2.1.2	
A/-/-/-					

```

172.1.2.0/24      20      NULL      Vlanif50      172.2.1.2
A/-/-/-
172.1.3.0/24      20      NULL      Vlanif50      172.2.1.2
A/-/-/-
172.1.4.0/24      20      NULL      Vlanif50      172.2.1.2
A/-/-/-
172.2.1.0/24      10      NULL      Vlanif50      Direct      D/-/
L/-

```

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
U-Up/Down Bit Set

5. Configure route convergence on S-switch-B.

Aggregate 172.1.1.0/24, 172.1.2.0/24, 172.1.3.0/24, and 172.1.4.0/24 as 172.1.0.0/16 on S-switch-B.

```

[S-switch-B] isis 1
[S-switch-B-isis-1] summary 172.1.0.0 255.255.0.0 level-1-2
[S-switch-B-isis-1] quit

```

6. Verify the configuration.

Display the routing table of S-switch-A, and you can find that 172.1.1.0/24, 172.1.2.0/24, 172.1.3.0/24, and 172.1.4.0/24 are aggregated as 172.1.0.0/16.

```

[S-switch-A] 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	Vlanif50	172.2.1.2	
A/-/-/-					
172.2.1.0/24	10	NULL	Vlanif50	Direct	D/-/
L/-					

Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
U-Up/Down Bit Set

Configuration Files

- Configuration file of S-switch-A

```

#
sysname S-switch-A
#
vlan batch 50
#
isis 1
is-level level-2
network-entity 20.0000.0000.0001.00
#
interface Vlanif50
ip address 172.2.1.1 255.255.255.0
isis enable 1
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 50
#
return

```

- Configuration file of S-switch-B

```

#
sysname S-switch-B
#
vlan batch 10 50
#

```

```
isis 1
network-entity 10.0000.0000.0002.00
summary 172.1.0.0 255.255.0.0 level-1-2
#
interface Vlanif10
ip address 172.1.4.2 255.255.255.0
isis enable 1
#
interface Vlanif50
ip address 172.2.1.2 255.255.255.0
isis enable 1
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 50
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
vlan batch 10 20 30 40
#
isis 1
is-level level-1
network-entity 10.0000.0000.0003.00
#
interface Vlanif10
ip address 172.1.4.1 255.255.255.0
isis enable 1
#
interface Vlanif20
ip address 172.1.1.1 255.255.255.0
isis enable 1
#
interface Vlanif30
ip address 172.1.2.1 255.255.255.0
isis enable 1
#
interface Vlanif40
ip address 172.1.3.1 255.255.255.0
isis enable 1
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 30
#
interface GigabitEthernet1/0/4
port trunk allow-pass vlan 40
#
return
```

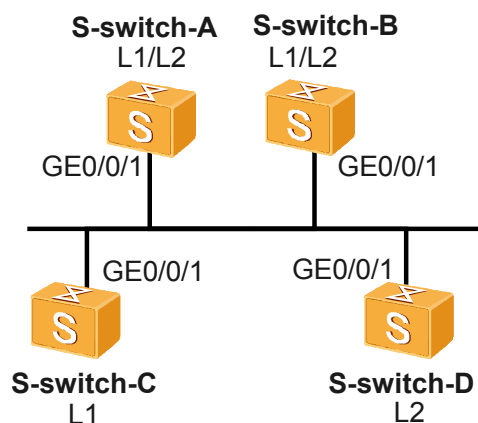
3.11.3 Example for Configuring the DIS Election of IS-IS

Networking Requirements

As shown in [Figure 3-5](#):

- S-switch-A, S-switch-B, S-switch-C, and S-switch-D are interconnected by running the IS-IS protocol.
- S-switch-A, S-switch-B, S-switch-C, and S-switch-D belong to Area 10.
- S-switch-A and S-switch-B are Level-1-2 S-switchs. S-switch-C is the Level-1 S-switch. S-switch-D is the Level-2 S-switch.
- It is required to change the DIS priority of the interface to configure S-switch-A to a Level-1-2 DIS.

Figure 3-5 Networking diagram for configuring the DIS election of IS-IS



S-switch	Interface	VLANIF Interface	IP Address
S-switch-A	GE 0/0/1	VLANIF 10	10.1.1.1/24
S-switch-B	GE 0/0/1	VLANIF 10	10.1.1.2/24
S-switch-C	GE 0/0/1	VLANIF 10	10.1.1.3/24
S-switch-D	GE 0/0/1	VLANIF 10	10.1.1.4/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic IS-IS functions on each S-switch so that the S-switchs can be interconnected.
2. Check information about the IS-IS interface on each S-switch with the default priority.
3. Configure the DIS priority on the S-switch.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID of each interface, as shown in [Figure 3-5](#)
- IP address of each VLANIF interface, as shown in [Figure 3-5](#)
- System ID, level, and area ID of each S-switch
 - S-switch-A: The system ID is 0000.0000.0001; the area ID is 10; the DIS priority is 100; the level is Level-1.
 - S-switch-B: The system ID is 0000.0000.0002; the area ID is 10; the level is Level-1-2.

- S-switch-C: The system ID is 0000.0000.0003; the area ID is 10; the level is Level-1.
- S-switch-D: The system ID is 0000.0000.0004; the area ID is 10; the level is Level-2.

Configuration Procedure

1. Configure the IDs of the VLANs to which the interfaces belong.

The configuration details are not mentioned here.

2. Assign IP addresses to VLANIF interfaces.

The configuration details are not mentioned here.

3. Display the MAC address of the VLANIF 10 interface on each S-switch.

Display the MAC address of the VLANIF 10 interface on S-switch-A.

```
[S-switch-A] display arp interface vlanif 10
```

IP ADDRESS	MAC ADDRESS	EXPIRE (M)	TYPE	INTERFACE VLAN/CEVLAN PVC	VPN-INSTANCE
10.1.1.1	00e0-fc10-afec		I -	Vlanif10	
Total:1	Dynamic:0	Static:0	Interface:1		

Display the MAC address of the VLANIF 10 interface on S-switch-B.

```
[S-switch-B] display arp interface vlanif 10
```

IP ADDRESS	MAC ADDRESS	EXPIRE (M)	TYPE	INTERFACE VLAN/CEVLAN PVC	VPN-INSTANCE
10.1.1.2	00e0-fccd-acdf		I -	Vlanif10	
Total:1	Dynamic:0	Static:0	Interface:1		

Display the MAC address of the VLANIF 10 interface on S-switch-C.

```
[S-switch-C] display arp interface vlanif 10
```

IP ADDRESS	MAC ADDRESS	EXPIRE (M)	TYPE	INTERFACE VLAN/CEVLAN PVC	VPN-INSTANCE
10.1.1.3	00e0-fc50-25fe		I -	Vlanif10	
Total:1	Dynamic:0	Static:0	Interface:1		

Display the MAC address of the VLANIF 10 interface on S-switch-D.

```
[S-switch-D] display arp interface vlanif 10
```

IP ADDRESS	MAC ADDRESS	EXPIRE (M)	TYPE	INTERFACE VLAN/CEVLAN PVC	VPN-INSTANCE
10.1.1.4	00e0-fcfd-305c		I -	Vlanif10	
Total:1	Dynamic:0	Static:0	Interface:1		

4. Configure basic IS-IS functions.

Configure S-switch-A.

```
[S-switch-A] isis 1
[S-switch-A-isis-1] network-entity 10.0000.0000.0001.00
[S-switch-A-isis-1] quit
[S-switch-A] interface vlanif 10
[S-switch-A-Vlanif10] isis enable 1
[S-switch-A-Vlanif10] quit
```

Configure S-switch-B.

```
[S-switch-B] isis 1
[S-switch-B-isis-1] network-entity 10.0000.0000.0002.00
[S-switch-B-isis-1] quit
[S-switch-B] interface vlanif 10
[S-switch-B-Vlanif10] isis enable 1
[S-switch-B-Vlanif10] quit
```

Configure S-switch-C.

```
[S-switch-C] isis 1
[S-switch-C-isis-1] network-entity 10.0000.0000.0003.00
[S-switch-C-isis-1] is-level level-1
[S-switch-C-isis-1] quit
[S-switch-C] interface vlanif 10
[S-switch-C-Vlanif10] isis enable 1
[S-switch-C-Vlanif10] quit
```

Configure S-switch-D.

```
[S-switch-D] isis 1
[S-switch-D-isis-1] network-entity 10.0000.0000.0004.00
[S-switch-D-isis-1] is-level level-2
[S-switch-D-isis-1] quit
[S-switch-D] interface vlanif 10
[S-switch-D-Vlanif10] isis enable 1
[S-switch-D-Vlanif10] quit
```

Display information about the IS-IS neighbors of S-switch-A.

```
[S-switch-A] display isis peer
```

```
Peer information for ISIS(1)
-----
```

System Id	Interface	Circuit Id	State	HoldTime	Type
PRI 0000.0000.0002 (L1L2) 64	Vlanif10	0000.0000.0002.01	Up	9s	L1
0000.0000.0003 64	Vlanif10	0000.0000.0002.01	Up	27s	L1
0000.0000.0002 64	Vlanif10	0000.0000.0004.01	Up	28s	L2 (L1L2)
0000.0000.0004 64	Vlanif10	0000.0000.0004.01	Up	8s	L2

Display information about the IS-IS interfaces on S-switch-A.

```
[S-switch-A] display isis interface
```

```
Interface information for ISIS(1)
-----
```

Interface	Id	IPV4.State	IPV6.State	MTU	Type	DR
Vlanif10	001	Up	Down	1497	L1/L2	No/

No

Display information about the IS-IS interfaces on S-switch-B.

```
[S-switch-B] display isis interface
```

```
Interface information for ISIS(1)
-----
```

Interface	Id	IPV4.State	IPV6.State	MTU	Type	DR
Vlanif10	001	Up	Down	1497	L1/L2	Yes/

No

Display information about the IS-IS interfaces on S-switch-D.

```
[S-switch-D] display isis interface
```

```
Interface information for ISIS(1)
-----
```

Interface	Id	IPV4.State	IPV6.State	MTU	Type	DR
Vlanif10	001	Up	Down	1497	L1/L2	No/

Yes

 **NOTE**

When the default DIS priority is used,

- The MAC address of the interface on S-switch-B is the largest one among that of the interfaces on the Level-1 S-switchs. Thus, S-switch-B is elected as the Level-1 DIS.
- The MAC address of the interface on S-switch-D is the largest one among that of the interfaces on the Level-2 S-switchs. Thus, S-switch-D is elected as the Level-2 DIS.

The Level-1 pseudonode is 0000.0000.0002.01. The Level-2 pseudonode is 0000.0000.0004.01.

5. Configure the DIS priority of S-switch-A.

```
[S-switch-A] interface vlanif 10
[S-switch-A-Vlanif10] isis dis-priority 100
[S-switch-A-Vlanif10] quit
```

Display information about the IS-IS neighbors of S-switch-A.

```
[S-switch-A] display isis peer
```

```

Peer information for ISIS(1)
-----
System Id      Interface      Circuit Id      State HoldTime Type
PRI
0000.0000.0002 Vlanif10      0000.0000.0001.01 Up    21s    L1
(L1L2) 64
0000.0000.0003 Vlanif10      0000.0000.0001.01 Up    27s    L1
64
0000.0000.0002 Vlanif10      0000.0000.0001.01 Up    28s    L2
(L1L2) 64
0000.0000.0004 Vlanif10      0000.0000.0001.01 Up    30s    L2
64
```

6. Verify the configuration.

Display information about the IS-IS interfaces on S-switch-A.

```
[S-switch-A] display isis interface
```

```

Interface information for ISIS(1)
-----
Interface      Id      IPV4.State      IPV6.State      MTU   Type   DR
Vlanif10      001      Up              Down            1497  L1/L2  Yes/
Yes
```

As displayed above, after the DIS priority of the IS-IS interface is changed, S-switch-A immediately becomes a Level-1-2 DIS and its pseudonode is 0000.0000.0001.01.

Display information about the IS-IS neighbors and IS-IS interfaces on S-switch-B.

```
[S-switch-B] display isis peer
```

```

Peer information for ISIS(1)
-----
System Id      Interface      Circuit Id      State HoldTime   Type
PRI
0000.0000.0001 Vlanif10      0000.0000.0001.01 Up    7s          L1
(L1L2) 100
0000.0000.0003 Vlanif10      0000.0000.0001.01 Up    25s
L1      64
0000.0000.0001 Vlanif10      0000.0000.0001.01 Up    7s          L2
(L1L2) 100
0000.0000.0004 Vlanif10      0000.0000.0001.01 Up    25s
L2      64
```

```
[S-switch-B] display isis interface
```

```

Interface information for ISIS(1)
-----
Interface      Id      IPV4.State      IPV6.State      MTU   Type   DR
Vlanif10      001      Up              Down            1497  L1/L2  No/No
```

Display information about the IS-IS neighbors and IS-IS interfaces on S-switch-D.

```
[S-switch-D] display isis peer
```

Peer information for ISIS(1)						
System Id	Interface	Circuit Id	State	HoldTime	Type	
PRI 0000.0000.0001 100	Vlanif10	0000.0000.0001.01	Up	9s	L2	
0000.0000.0002 L2 64	Vlanif10	0000.0000.0001.01	Up	28s		
[S-switch-D] display isis interface						
Interface information for ISIS(1)						
Interface	Id	IPV4.State	IPV6.State	MTU	Type	DR
Vlanif10	001	Up	Down	1497	L1/L2	No/No

Configuration Files

- Configuration file of S-switch-A


```
#
sysname S-switch-A
#
vlan batch 10
#
isis 1
network-entity 10.0000.0000.0001.00
#
interface Vlanif10
ip address 10.1.1.1 255.255.255.0
isis enable 1
isis dis-priority 100
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
return
```
- Configuration file of S-switch-B


```
#
sysname S-switch-B
#
vlan batch 10
#
isis 1
network-entity 10.0000.0000.0002.00
#
interface Vlanif10
ip address 10.1.1.2 255.255.255.0
isis enable 1
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
return
```
- Configuration file of S-switch-C


```
#
sysname S-switch-C
#
vlan batch 10
#
isis 1
is-level level-1
network-entity 10.0000.0000.0003.00
#
interface Vlanif10
ip address 10.1.1.3 255.255.255.0
isis enable 1
#
interface GigabitEthernet0/0/1
```

```
port trunk allow-pass vlan 10
#
return

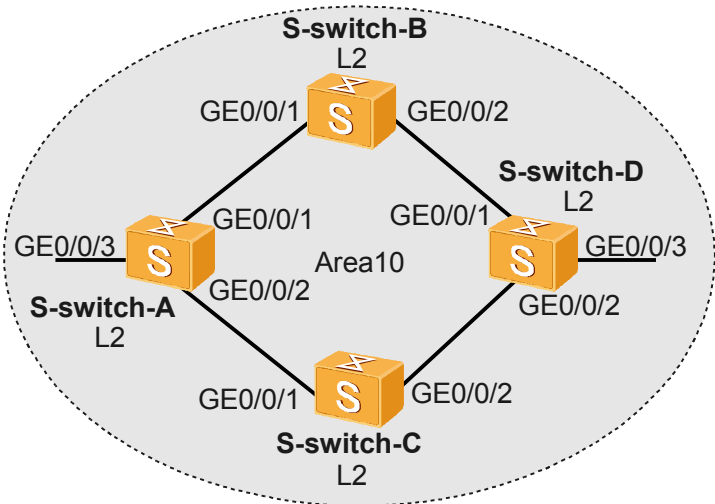
● Configuration file of S-switch-D
#
sysname S-switch-D
#
vlan batch 10
#
isis 1
 is-level level-2
network-entity 10.0000.0000.0004.00
#
interface Vlanif10
 ip address 10.1.1.4 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
return
```

3.11.4 Example for Configuring IS-IS Load Balancing

Networking Requirements

- As shown in [Figure 3-6](#):
- S-switch-A, S-switch-B, S-switch-C, and S-switch-D are interconnected in an IP network by running the IS-IS protocol.
 - S-switch-A, S-switch-B, S-switch-C, and S-switch-D are Level-2 S-switchs in Area 10.
 - Load balancing is required for the transmission of the traffic from S-switch-A to S-switch-D through S-switch-B and S-switch-C respectively.

Figure 3-6 Networking diagram for configuring IS-IS load balancing



S-switch	Interface	VLANIF Interface	IP Address
S-switch-A	GE 0/0/1	VLANIF 10	10.1.1.1/24
S-switch-A	GE 0/0/2	VLANIF 20	10.1.2.1/24

S-switch-A	GE 0/0/3	VLANIF 50	172.16.1.1/24
S-switch-B	GE 0/0/1	VLANIF 10	10.1.1.2/24
S-switch-B	GE 0/0/2	VLANIF 30	192.168.0.1/24
S-switch-C	GE 0/0/1	VLANIF 20	10.1.2.2/24
S-switch-C	GE 0/0/2	VLANIF 40	192.168.1.1/24
S-switch-D	GE 0/0/1	VLANIF 30	192.168.0.2/24
S-switch-D	GE 0/0/2	VLANIF 40	192.168.1.2/24
S-switch-D	GE 0/0/3	VLANIF 60	172.17.1.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable basic IS-IS functions on each S-switch so that the S-switches can be interconnected.
2. Set the number of equal-cost routes to 1 to carry out load balancing, and check information about the routing table.
3. Configure load balancing on S-switch-A and check information about the routing table.
4. (Optional) Configure the preference for equal-cost routes on S-switch-A.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID of each interface, as shown in [Figure 3-6](#)
- IP address of each VLANIF interface, as shown in [Figure 3-6](#)
- System ID, level, and area ID of each S-switch
 - S-switch-A: The system ID is 0000.0000.0001; the area ID is 10; the level is Level-2.
 - S-switch-B: The system ID is 0000.0000.0002; the area ID is 10; the level is Level-2.
 - S-switch-C: The system ID is 0000.0000.0003; the area ID is 10; the level is Level-2.
 - S-switch-D: The system ID is 0000.0000.0004; the area ID is 10; the level is Level-2.
- Number of equal-cost routes for load balancing on S-switch-A: 1
- Load balancing mode on S-switch-A
- Weight for the preference of the equal-cost routes on S-switch-C: 1

Configuration Procedure

1. Configure the IDs of the VLANs to which the interfaces belong.
The configuration details are not mentioned here.
2. Assign IP addresses to VLANIF interfaces.
The configuration details are not mentioned here.
3. Configure basic IS-IS functions.
The configuration details are not mentioned here.
4. Set the number of equal-cost routes for load balancing to 1 on S-switch-A.
[S-switch-A] **isis 1**

```
[S-switch-A-isis-1] maximum load-balancing 1
[S-switch-A-isis-1] quit
```

Display the routing table of S-switch-A.

```
[S-switch-A] 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    Vlanif20       10.1.2.2
  A/-/-/-
  10.1.1.0/24           10      NULL    Vlanif10       Direct         D/-/
  L/-
  172.16.1.0/24         10      NULL    Vlanif50       Direct         D/-/
  L/-
  172.17.1.0/24         30      NULL    Vlanif10       10.1.1.2
  A/-/-/-
  10.1.2.0/24           10      NULL    Vlanif20       Direct         D/-/
  L/-
  192.168.0.0/24        20      NULL    Vlanif10       10.1.1.2
  A/-/-/-

```

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, 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, IS-IS chooses the next hop 10.1.1.2 (S-switch-B) as the only best route to the destination network 172.17.1.0. This is because S-switch-B has a smaller system ID.

5. Restore the default number of equal-cost routes for load balancing on S-switch-A.

```
[S-switch-A] isis 1
[S-switch-A-isis-1] undo maximum load-balancing
[S-switch-A-isis-1] quit
```

Display the routing table of S-switch-A.

```
[S-switch-A] 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    Vlanif20       10.1.2.2
  A/-/-/-
  10.1.1.0/24           10      NULL    Vlanif10       Direct         D/-/
  L/-
  172.16.1.0/24         10      NULL    Vlanif50       Direct         D/-/
  L/-
  172.17.1.0/24         30      NULL    Vlanif10       10.1.1.2
  A/-/-/-
  10.1.2.0/24           10      NULL    Vlanif20       10.1.2.2
  L/-
  192.168.0.0/24        20      NULL    Vlanif10       10.1.1.2
  A/-/-/-

```

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

As shown in the routing table, the number of equal-cost routes for load balancing is restored to the default value of 6. Both the next hops of S-switch-A, 10.1.1.2 (that is, S-switch-B) and 10.1.2.2 (that is, S-switch-C) now become valid.

6. (Optional) Configure the preference for equal-cost routes on S-switch-A.

If you do not perform load balancing through S-switch-B and S-switch-C, configure the preference of the equal-cost routes and specify the next hop.

```
[S-switch-A] isis
[S-switch-A-isis-1] nexthop 10.1.2.2 weight 1
[S-switch-A-isis-1] quit
```

7. Verify the configuration.

Display the routing table of S-switch-A.

```
[S-switch-A] display isis route
```

Route information for ISIS(1)

ISIS(1) Level-2 Forwarding Table

IPv4 Destination Flags	IntCost	ExtCost	ExitInterface	NextHop
192.168.1.0/24 A/-/-/-	20	NULL	Vlanif20	10.1.2.2
10.1.1.0/24 L/-	10	NULL	Vlanif10	Direct D/-/
172.16.1.0/24 L/-	10	NULL	Vlanif50	Direct D/-/
172.17.1.0/24 A/-/-/-	30	NULL	Vlanif20	10.1.2.2
10.1.2.0/24 L/-	10	NULL	Vlanif20	Direct D/-/
192.168.0.0/24 A/-/-/-	20	NULL	Vlanif10	10.1.1.2

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

As shown in the routing table, the preference (with the weight of 1) of the next hop 10.1.2.2, the S-switch-C, is higher than that of 10.1.1.2, the S-switch-B, after the preference is configured for equal-cost routes. Thus, IS-IS chooses the next hop 10.1.2.2 as the best route.

Configuration Files

- Configuration file of S-switch-A

```
#
 sysname S-switch-A
#
 vlan batch 10 20 50
#
 isis 1
 is-level level-2
 network-entity 10.0000.0000.0001.00
 nexthop 10.1.2.2 weight
#
 interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
#
 interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
 isis enable 1
#
 interface Vlanif50
 ip address 172.16.1.1 255.255.255.0
```

```
isis enable 1
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 50
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
vlan batch 10 30
#
isis 1
is-level level-2
network-entity 10.0000.0000.0002.00
#
interface Vlanif10
ip address 10.1.1.2 255.255.255.0
isis enable 1
#
interface Vlanif30
ip address 192.168.0.1 255.255.255.0
isis enable 1
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 30
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
vlan batch 20 40
#
isis 1
is-level level-2
network-entity 10.0000.0000.0003.00
#
interface Vlanif20
ip address 10.1.2.2 255.255.255.0
isis enable 1
#
interface Vlanif40
ip address 192.168.1.1 255.255.255.0
isis enable 1
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 40
#
return
```

- Configuration file of S-switch-D

```
#
sysname S-switch-D
#
vlan batch 30 40 60
#
```

```
isis 1
 is-level level-2
 network-entity 10.0000.0000.0004.00
#
interface Vlanif30
 ip address 192.168.0.2 255.255.255.0
 isis enable 1
#
interface Vlanif40
 ip address 192.168.1.2 255.255.255.0
 isis enable 1
#
interface Vlanif60
 ip address 172.17.1.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 40
#
interface GigabitEthernet0/0/3
 port trunk allow-pass vlan 60
#
return
```

4 RIP Configuration

About This Chapter

This chapter describes the RIP fundamentals and configuration steps for basic RIP Functions, RIP routing information and adjusting and optimizing RIP networks, along with typical examples.

[4.1 Introduction](#)

This section describes basic concepts and the principle of RIP.

[4.2 Configuring Basic RIP Functions](#)

This section describes how to configure basic RIP functions.

[4.3 Configuring RIP Route Attributes](#)

This section describes how to change route selection by configuring RIP route attributes.

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

This section describes how to control the advertising of RIP routing information in the complicated networking environment.

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

This section describes how to control the receiving of RIP routing information in the complicated networking environment.

[4.6 Configuring RIP-2 Features](#)

This section describes how to configure RIP-2 route aggregation and RIP-2 authentication.

[4.7 Optimizing a RIP Network](#)

This section describes how to adjust and optimize RIP networks.

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

This section describes how to bind MIB and RIP.

[4.9 Maintaining RIP](#)

This section describes how to maintain RIP.

[4.10 Configuration Examples](#)

This section provides several configuration examples of RIP.

4.1 Introduction

This section describes basic concepts and the principle of RIP.

[4.1.1 Overview of RIP](#)

[4.1.2 RIP Features Supported by S-switch](#)

4.1.1 Overview of RIP

The Routing Information Protocol (RIP) is a simple Interior Gateway Protocol (IGP). It is mainly used in small-scale and simply-structured networks such as campus networks and regional networks. RIP is not suitable for complex environments or large-scale networks.

RIP is a protocol based on the Distance-Vector algorithm. It exchanges the routing information through User Datagram Protocol (UDP) packets. The number of the port used by RIP is 520.

RIP employs hop count to measure the distance to the destination. The distance is called the metric value. In RIP, the hop count from a S-switch to its directly connected network is 0, and that to a network, which can be reached through another S-switch, is 1, and so on. To speed up the convergence, RIP regulates 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, that is, the destination network or the host is unreachable. RIP, therefore, is not applied to large-scale networks.

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

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

RIP has two versions:

- RIP-1
- RIP-2

RIP-1 is a classful routing protocol.

4.1.2 RIP Features Supported by S-switch

The S-switch supports the following RIP features:

- RIP-1 and RIP-2
- RIP multi-instance

4.2 Configuring Basic RIP Functions

This section describes how to configure basic RIP functions.

[4.2.1 Establishing the Configuration Task](#)

[4.2.2 Enabling RIP](#)

[4.2.3 Enabling RIP on the Specified Network Segment](#)

[4.2.4 Configuring RIP Version Number](#)

[4.2.5 Checking the Configuration](#)

4.2.1 Establishing the Configuration Task

Applicable Environment

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

Pre-configuration Tasks

Before configuring basic RIP functions, complete the following tasks:

- Configuring the VLANs to which the physical interfaces belong
- Assigning IP addresses to VLANIF interfaces to ensure that the neighboring nodes are reachable

Data Preparation

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

No.	Data
1	RIP process number
3	RIP version number

4.2.2 Enabling RIP

Context

Do as follows on the S-switch 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.

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

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

----End

4.2.3 Enabling RIP on the Specified Network Segment

Context

Do as follows on the S-switch 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.

----End

4.2.4 Configuring RIP Version Number

Procedure

- Configuring the Global RIP Version Number

Do as follows on the RIP S-switch:

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 the VLANIF Interface

Do as follows on the RIP S-switch:

1. Run:

system-view

The system view is displayed.

2. Run:

interface *interface-type interface-number*

The VLANIF 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.

By default, an interface receives RIP-1 and RIP-2 packets and only sends RIP-1 packets. When you configure RIP-2 for an interface, you can configure it to send packets in broadcast or multicast mode simultaneously. If the RIP version number of the interface is not set, the global version number is used as the standard version number.

----End

4.2.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the running status and configuration of RIP.	display rip [<i>process-id</i> vpn-instance <i>vpn-instance-name</i>]
Check the activated and inactivated RIP routes.	display rip <i>process-id</i> route

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 display shows that two VPN instances are running. The first one is a public network instance; the second one is named **VPN-Instance-1**.

```
<Quidway> 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 : 3
  Update time : 30 sec Age time : 180 sec
  Suppress time : 0 sec Garbage-collect time : 120 sec
  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
    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 : 3
        Update time : 30 sec Age time : 180 sec
        Suppress time : 0 sec Garbage-collect time : 120 sec
        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
    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

```

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

<Quidway> **display rip 1 route**

Route Flags: R - RIP

A - Aging, S - Suppressed, G - Garbage-collect

Peer 192.4.5.1 on vlanif/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

4.3 Configuring RIP Route Attributes

This section describes how to change route selection by configuring RIP route attributes.

4.3.1 Establishing the Configuration Task

4.3.2 Configuring Additional Metrics of an Interface

4.3.3 Configuring RIP Preference

4.3.4 Setting the Maximum Number of Equal-Cost Routes

4.3.5 Checking the Configuration

4.3.1 Establishing the Configuration Task

Applicable Environment

In actual applications, to meet the requirements of a complicated networking environment, you can change RIP routing policies by configuring RIP route attributes. The related actions are as follows

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

Pre-configuration Tasks

Before configuring RIP route attributes, complete the following tasks:

- Configuring the IP addresses of VLANIF interfaces to make the network layers accessible
- [4.2 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

4.3.2 Configuring Additional Metrics of an Interface

Context

Do as follows on the RIP S-switch:

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
```

The metric added to a sent route is set.

Using the **rip metricin** command, you can add an additional metric to a received route, and add the route to the routing table. As a result, the metric in the routing table changes. The **rip metricout** command is used for route advertisement. When a route is advertised, an additional metric is added, but the metric in the routing table does not change.

----End

4.3.3 Configuring RIP Preference

Context

Do as follows on the RIP S-switch:

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.

----End

4.3.4 Setting the Maximum Number of Equal-Cost Routes

Context

Do as follows on the RIP S-switch:

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.

----End

4.3.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the running status and configuration of RIP.	display rip [<i>process-id</i> vpn-instance <i>vpn-instance-name</i>]
Check all activated routes in the RIP database.	display rip process-id database
Check all activated and inactivated RIP routes.	display rip process-id route

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

```
<Quidway> display rip 100 database
10.0.0.0/8, cost 1, ClassfulSumm
10.0.0.0/24, cost 1, nexthop 10.0.0.1, Rip-interface
11.0.0.0/8, cost 1, ClassfulSumm
11.0.0.0/24, cost 1, nexthop 10.0.0.1, Imported
```

4.4 Controlling the Advertising of RIP Routing Information

This section describes how to control the advertising of RIP routing information in the complicated networking environment.

4.4.1 Establishing the Configuration Task

4.4.2 Configuring RIP to Advertise Default Routes

4.4.3 Disabling an Interface from Sending Update Packets

4.4.4 Configuring RIP to Import External Routes

4.4.5 Checking the Configuration

4.4.1 Establishing the Configuration Task

Applicable Environment

In actual applications, to meet the requirements of a complicated networking environment, it is required to control the advertising of RIP routing information accurately. Through the configuration procedures in this section, the following can be implemented:

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

Pre-configuration Tasks

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

- Configuring the IP addresses of VLANIF interfaces to make the network layers accessible
- [4.2 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	Protocol name and process ID of the external route to be imported

4.4.2 Configuring RIP to Advertise Default Routes

Context

Do as follows on the RIP S-switch:

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 [ cost cost ]
```

RIP is enabled to advertise a default route.

You can configure a S-switch to advertise a default route with the specified metric to its RIP neighbors.

----End

4.4.3 Disabling an Interface from Sending Update Packets

Procedure

- Configuration in a RIP Process (with Higher Priority)

Do as follows on the RIP S-switch:

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. Set the interface status to be silent according to the requirements.

Run:

```
silent-interface all
```

All interfaces are set to be silent.

Or

Run:

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

An interface is disabled from sending Update packets.

You can set an interface to be silent. Thus, the interface receives packets to update its routing table only, but it sends no RIP packets. The priority of **silent-interface** is higher than that of **rip input/rip output** configured on the interface.

By default, an interface does not work in the silent state.

- Configuration in the Interface View (with Lower Priority)

Do as follows on the RIP router:

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.

With this command, you can specify whether to send RIP Update packets for an interface. Its priority is lower than that of the **silent-interface** command. By default, an interface is allowed to send RIP Update packets.

----End

4.4.4 Configuring RIP to Import External Routes

Context

Do as follows on the RIP S-switch:

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 for imported routes is set.

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

Step 4 Run:

```
import-route protocol [ process-id ] [ cost cost ] [ route-policy route-policy-name ]
```

The external routes are imported.

Step 5 (Optional) Run:

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

The imported routes are filtered when they are advertised.

If RIP has to advertise the routing information of other protocols, you can specify *protocol* to filter the specific routing information. If *protocol* is not specified, all the routing information to be advertised is filtered, including the imported routes and the local RIP routes (equivalent to the directly connected routes).

 **NOTE**

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

----End

4.4.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the running status and configuration of RIP.	display rip [<i>process-id</i> vpn-instance <i>vpn-instance-name</i>]
Check all activated routes in the RIP database.	display rip process-id database
Check all activated and inactivated RIP routes.	display rip process-id route

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

```
<Quidway> display rip 100 database
 172.4.0.0/16, cost 1, ClassfulSumm
 172.4.0.0/16, cost 1, nexthop 192.13.14.1
 192.4.5.0/24, cost 2, ClassfulSumm
 192.4.5.0/24, cost 2, nexthop 192.13.14.1
 192.13.14.0/24, cost 0, ClassfulSumm
 192.13.14.0/24, cost 0, Rip-interface
```

4.5 Controlling the Receiving of RIP Routing Information

This section describes how to control the receiving of RIP routing information in the complicated networking environment.

4.5.1 Establishing the Configuration Task

4.5.2 Disabling an Interface from Receiving RIP Update Packets

4.5.3 Disabling RIP from Receiving Host Routes

4.5.4 Configuring RIP to Filter the Received Routes

4.5.5 Checking the Configuration

4.5.1 Establishing the Configuration Task

Applicable Environment

In actual applications, to meet the requirements of a complicated networking environment, it is required to control the receiving of RIP routing information accurately. Through the configuration procedures in this section, the following can be implemented:

- 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 the IP addresses of VLANIF interfaces to make the network layers accessible
- [4.2 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

4.5.2 Disabling an Interface from Receiving RIP Update Packets

Context

Do as follows on the RIP S-switch:

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.

With this command, you can specify whether to receive RIP Update packets for an interface. Its priority is lower than that of the **silent-interface** command. By default, an interface is allowed to receive RIP Update packets.

----End

4.5.3 Disabling RIP from Receiving Host Routes

Context

Do as follows on the RIP S-switch:

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 accepting host routes.

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

----End

4.5.4 Configuring RIP to Filter the Received Routes

Context

The S-switch can filter the routing information. To filter the imported and advertised routes, you can configure the inbound and outbound filtering policy by specifying the ACL and IP-prefix list.

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

Do as follows on the RIP S-switch:

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 Configure RIP to filter the imported routes according to the requirements:

- Run:

```
filter-policy acl-number import
```

The learnt routing information is filtered based on an ACL.

- Run:

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

The routing information advertised by neighbors is filtered on the basis of the destination address prefix.

- 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 on the basis of the destination address prefix and the neighbors.

----End

4.5.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the running status and configuration of RIP.	display rip [<i>process-id</i> vpn-instance <i>vpn-instance-name</i>]
Check all activated RIP routes in the database.	display rip <i>process-id</i> database [verbose]
Check information about RIP interfaces.	display rip <i>process-id</i> interface [<i>interface-type</i> <i>interface-number</i>] [verbose]
Check information about RIP neighbors.	display rip <i>process-id</i> neighbor [verbose]
Check all activated and inactivated RIP routes.	display rip <i>process-id</i> route

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

```
<Quidway> display rip 100 database
172.4.0.0/16, cost 1, ClassfulSumm
172.4.0.0/16, cost 1, nexthop 192.13.14.1
192.4.5.0/24, cost 2, ClassfulSumm
192.4.5.0/24, cost 2, nexthop 192.13.14.1
192.13.14.0/24, cost 0, ClassfulSumm
192.13.14.0/24, cost 0, Rip-interface
```

4.6 Configuring RIP-2 Features

This section describes how to configure RIP-2 route aggregation and RIP-2 authentication.

[4.6.1 Establishing the Configuration Task](#)

[4.6.2 Configuring RIP-2 Route Aggregation](#)

[4.6.3 Configuring Packet Authentication of RIP-2](#)

[4.6.4 Checking the Configuration](#)

4.6.1 Establishing the Configuration Task

Applicable Environment

RIP-2 features include:

- RIP-2 route aggregation
- RIP-2 authentication mode

Pre-configuration Tasks

Before configuring basic RIP-2 functions, complete the following tasks:

- Configuring the link layer protocol
- Configuring the IP addresses of interfaces to make the network layers accessible

Data Preparation

To configure basic RIP-2 functions, you need the following data.

No.	Data
1	RIP-2 process ID
2	Network segment where the RIP-2 interface resides

4.6.2 Configuring RIP-2 Route Aggregation

Procedure

- Enabling RIP-2 Automatic Route Aggregation

Do as follows on the RIP S-switch:

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:

```
summary
```

RIP-2 automatic route aggregation is enabled.

Route aggregation indicates that you can aggregate different subnet routes in the same natural network segment into one natural mask route when they are transmitted to other network segments. Thus the network traffic and the size of the routing table is reduced.

Route aggregation does not take effect on RIP-1. RIP-2 supports the Variable Length Subnet Mask (VLSM) and Classless Inter-Domain Routing (CIDR). To broadcast all subnet routes, you can disable the automatic route aggregation of RIP-2.

- Configuring RIP-2 to Advertise the Aggregation Address

Do as follows on the RIP router:

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 aggregation IP address for RIP-2 is advertised.

----End

4.6.3 Configuring Packet Authentication of RIP-2

Context

Do as follows on the RIP S-switch:

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 Perform the following 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-key key-id | usual password-key }
```

MD5 authentication in the cipher text is configured for RIP-2 packets.

RIP-2 supports the following authentication modes:

- Simple authentication
- MD5 authentication

Simple authentication does not guarantee security. The authentication key, which is not encrypted, is sent along with a packet. Hence, the authentication in the plain text cannot meet the high requirements for security.

The MD5 type must be specified along with the MD5 authentication. The **usual** type supports IETF standard authentication packets, and the **nonstandard** type supports nonstandard authentication packets.

----End

4.6.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the running status and configuration of RIP.	display rip [<i>process-id</i> vpn-instance <i>vpn-instance-name</i>]
Check all activated RIP routes in the database.	display rip <i>process-id</i> database [verbose]
Check all activated and inactivated RIP routes.	display rip <i>process-id</i> route

4.7 Optimizing a RIP Network

This section describes how to adjust and optimize RIP networks.

4.7.1 Establishing the Configuration Task

4.7.2 Configuring RIP Timers

4.7.3 Setting the Interval for Sending Packets and the Number of the Sent Packets

4.7.4 Configuring Split Horizon and Poison Reverse

4.7.5 Configuring RIP to Check the Validity of the Update Packets

4.7.6 Configuring RIP Neighbors

4.7.7 Checking the Configuration

4.7.1 Establishing the Configuration Task

Applicable Environment

In particular networking environments, you need to configure RIP features and optimize the performance of a RIP network. Through the configuration procedures in this section, the following can be implemented:

- Change the convergence speed of the RIP network by adjusting RIP timers.

- Improve the performance of the RIP network by adjusting the number of Update packets that an interface can send and the interval between Update packets.
- Configure split horizon and poison reverse to avoid routing loops.
- Check the validity of packets and authenticate packets in the networking environment demanding high security.
- Configure RIP features on the interface or link as required.

Pre-configuration Tasks

Before optimizing a RIP network, complete the following tasks:

- Configuring the IP addresses of VLANIF interfaces to make the network layers accessible
- [4.2 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 the interface sends each time and the interval between Update packets
3	Maximum number of equal-cost routes
4	Packet authentication mode and password
5	IP addresses of RIP neighbors

4.7.2 Configuring RIP Timers

Context

Do as follows on the RIP S-switch:

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 suppress garbage-collect
```

The RIP timers are configured.

RIP has the following timers:

- Update timer
- Age timer
- Suppress timer
- Garbage-collect timer

Changing the values of the preceding timers affects the RIP convergence speed.

The RIP timers take effect instantly after being changed.

Any improper configuration of these four timers causes the instability of routes. The values of these timers should follow the rule of *update < age* and *suppress < garbage-collect*. For example, when the update time is longer than the aging time, the router cannot inform its neighbors of the change on time if a RIP route changes during the update time.

By default, the Update timer is 30s; the Age timer is 180s; the Suppress timer is 0s; the Garbage-collect timer is four times the Update timer, namely, 120s.

In actual situations, the Garbage-collect timer is not fixed. When the Update timer is set to 30s, the Garbage-collect timer may range from 90s to 120s.

Before RIP permanently deletes the unreachable routes from the routing table, it advertises this route (the weight is set to 16) by periodically sending Update packets four times. Thus, all the neighbors know that this route is unreachable. As the route is accessible at the beginning of an Update period, the Garbage-collect timer is actually three or four times the Update timer.

----End

4.7.3 Setting the Interval for Sending Packets and the Number of the Sent Packets

Context

Do as follows on the RIP S-switch:

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 between Update packets and the maximum number of packets sent each time are set on the interface.

----End

4.7.4 Configuring Split Horizon and Poison Reverse

Context

Do as follows on the RIP S-switch:

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 split-horizon
```

Split horizon is enabled.

Step 4 Run:

```
rip poison-reverse
```

Poison reverse is enabled.

If both split horizon and poison reverse are configured, only poison reverse takes effect.

----End

4.7.5 Configuring RIP to Check the Validity of the Update Packets

Procedure

- Configuring the Zero Field Check for RIP-1 Packets

Do as follows on the RIP S-switch:

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 RIP-1 packets.

Certain fields in a RIP-1 packet must be 0s, and they are called zero fields. RIP-1 checks the zero fields on receiving a packet. If the value of any zero field is not 0, the packet is not processed.

As a RIP-2 packet contains no zero fields, this configuration is invalid to RIP-2.

- **Configuring the Source Address Check for RIP Update Packets**

Do as follows on the RIP router:

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 to pass the check, it is not processed.

By default, the source address check is enabled.

----End

4.7.6 Configuring RIP Neighbors

Context

RIP sends packets in broadcast or multicast mode. If RIP runs on the links that do not support the forwarding of broadcast or multicast packets, you must specify RIP neighbors manually.

Do as follows on the RIP S-switch:

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
```

RIP neighbors are configured.

----End

4.7.7 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the running status and configuration of RIP.	display rip [<i>process-id</i> vpn-instance <i>vpn-instance-name</i>]
Check all activated RIP routes in the database.	display rip <i>process-id</i> database [verbose]
Check information about RIP interfaces.	display rip <i>process-id</i> interface [<i>interface-type</i> <i>interface-number</i>] [verbose]
Check information about RIP neighbors.	display rip <i>process-id</i> neighbor [verbose]
Check all activated and inactivated RIP routes.	display rip <i>process-id</i> route

Run the **display rip** *process-id* **interface** [*interface-type* *interface-number*] [**verbose**] command, and you can view RIP information about the specified interface and the interface status as Up.

```
<Quidway> display rip 1 interface vlanif 1
-----
Interface      IP Address      State    Protocol      MTU
-----
Vlanif 1       1.1.1.2         UP       RIPv1 Compatible  500
```

4.8 Configuring the Network Management Function in RIP

This section describes how to bind MIB and RIP.

4.8.1 Establishing the Configuration Task

4.8.2 Configuring RIP and MIB Binding

4.8.3 Checking the Configuration

4.8.1 Establishing the Configuration Task

Applicable Environment

Through the procedures in this section, you can bind RIP to a MIB.

Pre-configuration Tasks

Before configuring the network management function of RIP, complete the following tasks:

- Configuring the IP addresses of VLANIF interfaces to make the network layers accessible

- [4.2 Configuring Basic RIP Functions](#)

Data Preparation

None.

4.8.2 Configuring RIP and MIB Binding

Context

Do as follows on the RIP S-switch:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rip mib-binding process-id
```

RIP is bound to a MIB.

This command binds a MIB to a RIP process ID and specifies the ID of the RIP process that accepts SNMP requests.

----End

4.8.3 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the configuration parameters that are valid on the S-switch.	display current-configuration

4.9 Maintaining RIP

This section describes how to maintain RIP.



CAUTION

Debugging affects the performance of the system. So, after debugging, run the **undo debugging all** command to disable it immediately.

When a RIP fault occurs, run the following **debugging** command in the user view to debug RIP and locate the fault.

Action	Command
Debug RIP packets.	debugging rip <i>process-id</i> [brief error event job packet receive route-processing send timer]

4.10 Configuration Examples

This section provides several configuration examples of RIP.

4.10.1 Example for Configuring RIP Version

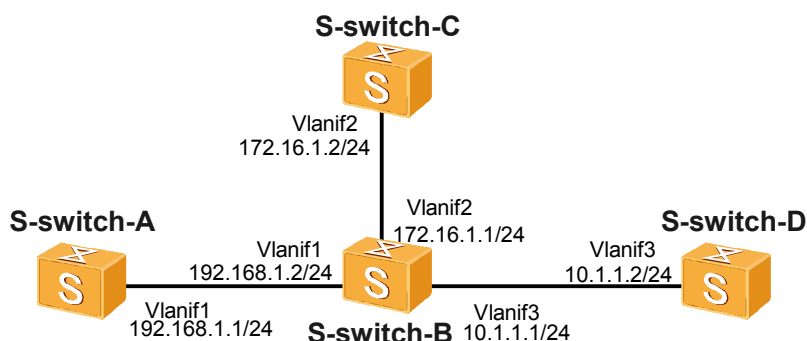
4.10.2 Example for Configuring RIP to Import External Routes

4.10.1 Example for Configuring RIP Version

Networking Requirements

As shown in [Figure 4-1](#), it is required that RIP be enabled on all interfaces of S-switch-A, S-switch-B, S-switch-C, and S-switch-D and the S-switchs interconnect with each other through RIP-2.

Figure 4-1 Networking diagram of configuring the RIP version number



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the IP address of each VLANIF interface to make the network layers accessible.
2. Enable RIP on each S-switch and configure basic RIP functions.
3. Configure RIP-2 on each S-switch and check the subnet masks.

Data Preparation

To complete the configuration, you need the following data:

- RIP network segment 192.168.1.0 on S-switch-A
- RIP network segment 192.168.1.0, 172.16.0.0, and 10.0.0.0 on S-switch-B

- RIP network segment 172.16.0.0 on S-switch-C
- RIP network segment 10.0.0.0 on S-switch-D
- RIP-2 on S-switch-A, S-switch-B, S-switch-C, and S-switch-D

Configuration Procedure

1. Configure the IP address of each interface

The details are not mentioned here.

2. Configure basic RIP functions.

Configure S-switch-A.

```
[S-switch-A] rip
[S-switch-A-rip-1] network 192.168.1.0
[S-switch-A-rip-1] quit
```

Configure S-switch-B.

```
[S-switch-B] rip
[S-switch-B-rip-1] network 192.168.1.0
[S-switch-B-rip-1] network 172.16.0.0
[S-switch-B-rip-1] network 10.0.0.0
[S-switch-B-rip-1] quit
```

Configure S-switch-C.

```
[S-switch-C] rip
[S-switch-C-rip-1] network 172.16.0.0
[S-switch-C-rip-1] quit
```

Configure S-switch-D.

```
[S-switch-D] rip
[S-switch-D-rip-1] network 10.0.0.0
[S-switch-D-rip-1] quit
```

Check the RIP routing table of S-switch-A.

```
[S-switch-A] display rip 1 route
Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
-----
Peer 192.168.1.2 on vlanif1
  Destination/Mask      Nexthop      Cost    Tag    Flags    Sec
  10.0.0.0/8            192.168.1.2    1      0      RA       14
  172.16.0.0/16         192.168.1.2    1      0      RA       14
  192.168.1.0/24        192.168.1.2    1      0      RA       14
```

From the routing table, you can view that the routes advertised by RIP-1 use natural masks.

3. Configure the RIP version number.

Configure RIP-2 on S-switch-A.

```
[S-switch-A] rip
[S-switch-A-rip-1] version 2
[S-switch-A-rip-1] quit
```

Configure RIP-2 on S-switch-B.

```
[S-switch-B] rip
[S-switch-B-rip-1] version 2
[S-switch-B-rip-1] quit
```

Configure RIP-2 on S-switch-C.

```
[S-switch-C] rip
[S-switch-C-rip-1] version 2
[S-switch-C-rip-1] quit
```

Configure RIP-2 on S-switch-D.

```
[S-switch-D] rip
[S-switch-D-rip-1] version 2
```

```
[S-switch-D-rip-1] quit
```

4. Verify the configuration.

Check the RIP routing table of S-switch-A.

```
[S-switch-A] display rip 1 route
```

```
Route Flags: R - RIP
```

```
A - Aging, S - Suppressed, G - Garbage-collect
```

```
-----
Peer 192.168.1.2 on Vlanif1
Destination/Mask    Nexthop    Cost    Tag    Flags    Sec
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
192.168.1.0/24      192.168.1.2    1      0      RA       14
```

From the routing table, you can view that the routes advertised by RIP-2 contain accurate subnet masks.



NOTE

The aging time of a RIP route is long. Therefore, a RIP-1 route may still exist in the routing table after you configure RIP-2.

Configuration Files

- Configuration file of S-switch-A

```
#
 sysname S-switch-A
#
interface Vlanif1
 ip address 192.168.1.1 255.255.255.0
#
rip 1
 version 2
 network 192.168.1.0
#
return
```

- Configuration file of S-switch-B

```
#
 sysname S-switch-B
#
interface Vlanif1
 ip address 192.168.1.2 255.255.255.0
#
interface Vlanif2
 undo shutdown
 ip address 172.16.1.1 255.255.255.0
#
interface Vlanif3
 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 S-switch-C

```
#
 sysname S-switch-C
#
interface Vlanif2
 ip address 172.16.1.2 255.255.255.0
#
rip 1
 version 2
```

```

network 172.16.0.0
#
return

```

- Configuration file of S-switch-D

```

#
sysname S-switch-D
#
interface Vlanif3
ip address 10.1.1.2 255.255.255.0
#
rip 1
version 2
network 10.0.0.0
#
return

```

4.10.2 Example for Configuring RIP to Import External Routes

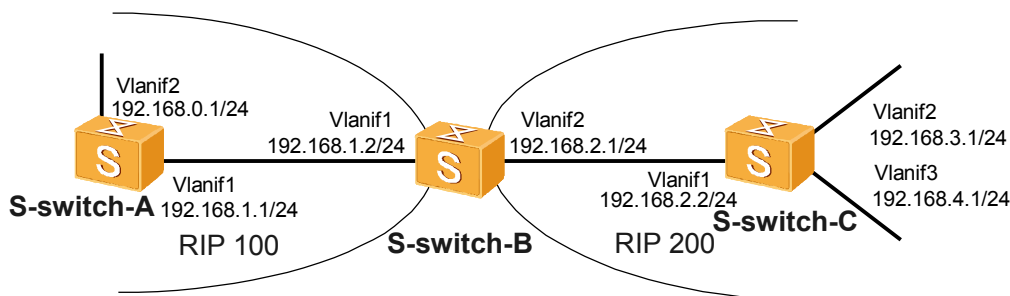
Networking Requirements

As shown in [Figure 4-2](#), two RIP processes, RIP 100 and RIP 200, run on S-switch-B. S-switch-B exchanges routing information with S-switch-A through RIP 100. S-switch-B exchanges routing information with S-switch-C through RIP 200.

It is required that the two processes of S-switch-B import the RIP routes from each other. The cost of the imported RIP 200 routes defaults to 3.

It is required that a filtering policy be configured on S-switch-B to filter out the imported RIP 200 route 192.168.4.0/24 and prevent it from being advertised to S-switch-A.

Figure 4-2 Networking diagram of configuring RIP to import external routes



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable RIP 100 and RIP 200 on each S-switch and specify the network segments.
2. Configure the two processes on S-switch-B to import the routes from each other and set the default cost of the imported RIP 200 routes to 3.
3. Configure an ACL on S-switch-B to filter the routes imported from RIP 200.

Data Preparation

To complete the configuration, you need the following data:

- RIP 100 on S-switch-A and the network segment 192.168.1.0 and 192.168.0.0
- RIP 100 and RIP 200 on S-switch-B and the network segment 192.168.1.0 and 192.168.2.0
- RIP 200 on S-switch-C and the network segment 192.168.2.0, 192.168.3.0, and 192.168.4.0
- Default cost of the imported RIP 200 routes as 3; ACL 2000 to deny the route with the source network segment of 192.168.4.0 and import RIP100 routes to RIP 200

Configuration Procedure

1. Configure the IP address of each interface.

The details are not mentioned here.

2. Configure basic RIP functions.

Enable RIP process 100 on S-switch-A.

```
[S-switch-A] rip 100
[S-switch-A-rip-100] network 192.168.0.0
[S-switch-A-rip-100] network 192.168.1.0
[S-switch-A-rip-1] quit
```

Enable the two RIP processes, process 100 and process 200, on S-switch-B.

```
[S-switch-B] rip 100
[S-switch-B-rip-100] network 192.168.1.0
[S-switch-B-rip-100] quit
[S-switch-B] rip 200
[S-switch-B-rip-200] network 192.168.2.0
[S-switch-B-rip-200] quit
```

Enable RIP process 200 on S-switch-C.

```
[S-switch-C] rip 200
[S-switch-C-rip-200] network 192.168.2.0
[S-switch-C-rip-200] network 192.168.3.0
[S-switch-C-rip-200] network 192.168.4.0
[S-switch-C-rip-1] quit
```

Check the routing table of S-switch-A.

```
[S-switch-A] 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	vlanif2	
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	vlanif1	
192.168.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0	
192.168.1.2/32	Direct	0	0	D	192.168.1.2	vlanif1	

3. Configure RIP to import external routes.

Set the default route cost to 3 on S-switch-B and import the routes of the two RIP processes into the routing table of each other.

```
[S-switch-B] rip 100
[S-switch-B-rip-100] default-cost 3
[S-switch-B-rip-100] import-route rip 200
[S-switch-B-rip-100] quit
[S-switch-B] rip 200
[S-switch-B-rip-200] import-route rip 100
[S-switch-B-rip-200] quit
[S-switch-B-rip-1] quit
```

Check the routing table of S-switch-A after the routes are imported.

```
[S-switch-A] 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	vlanif2	
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	vlanif1	
192.168.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0	
192.168.1.2/32	Direct	0	0	D	192.168.1.2	vlanif1	
192.168.2.0/24	RIP	100	4	D	192.168.1.2	vlanif1	
192.168.3.0/24	RIP	100	4	D	192.168.1.2	vlanif1	
192.168.4.0/24	RIP	100	4	D	192.168.1.2	vlanif1	

4. Configure RIP to filter the imported routes.

Configure an ACL on S-switch-B and set a rule to deny the packets with the source address of 192.168.4.0/24.

```
[S-switch-B] acl 2000
[S-switch-B-acl-basic-2000] rule deny source 192.168.4.0 0.0.0.255
[S-switch-B-acl-basic-2000] rule permit
[S-switch-B-acl-basic-2000] quit
```

Filter out the imported route 192.168.4.0/24 of RIP 200 on S-switch-B according to the ACL rule.

```
[S-switch-B] rip 100
[S-switch-B-rip-100] filter-policy 2000 export
```

5. Verify the configuration.

Check the routing table of S-switch-A after the filtering.

```
[S-switch-A] 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	vlanif2	
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	vlanif1	
192.168.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0	
192.168.1.2/32	Direct	0	0	D	192.168.1.2	vlanif1	
192.168.2.0/24	RIP	100	4	D	192.168.1.2	vlanif1	
192.168.3.0/24	RIP	100	4	D	192.168.1.2	vlanif1	

Configuration Files

- Configuration file of S-switch-A

```
#
 sysname S-switch-A
#
interface vlanif2
 ip address 192.168.0.1 255.255.255.0
#
interface vlanif1
 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 S-switch-B

```
#
 sysname S-switch-B
#
acl number 2000
 rule 5 deny source 192.168.4.0 0.0.0.255
 rule 10 permit
#
interface vlanif1
 ip address 192.168.1.2 255.255.255.0
#
interface vlanif2
 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 S-switch-C

```
#
 sysname S-switch-C
#
interface vlanif2
 ip address 192.168.3.1 255.255.255.0
#
interface vlanif3
 ip address 192.168.4.1 255.255.255.0
#
interface vlanif1
 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
```

5 BGP Configuration

About This Chapter

This chapter describes the BGP fundamentals and configuration steps for basic BGP functions, controlling BGP routing information, adjusting and optimizing BGP, along with typical examples.

[5.1 Introduction](#)

This section describes the principle and concepts of BGP.

[5.2 Configuring Basic BGP Functions](#)

This section describes how to start a BGP process, and configure a BGP peer.

[5.3 Configuring BGP Route Attributes](#)

This section describes how to configure BGP route attributes to change BGP route selection principles.

[5.4 Configuring BGP Filters](#)

This section describes how to configure BGP filters.

[5.5 Controlling the Route Advertisement](#)

This section describes how to configure BGP to advertise routes.

[5.6 Controlling BGP to Import Routes](#)

This section describes how to configure BGP to import external routes.

[5.7 Configuring Parameters for a BGP Connection](#)

This section describes how to configure parameters of a BGP connection to adjust and optimize the performance of a BGP network.

[5.8 Configuring BFD for BGP](#)

This section describes how to configure BFD for BGP to speed up the network convergence.

[5.9 Configuring BGP Load Balancing](#)

This section describes how to configure attributes to implement BGP load balancing.

[5.10 Configuring BGP Security](#)

This section describes how to enhance BGP security.

[5.11 Maintaining BGP](#)

This section describes how to maintain BGP.

5.12 Configuration Examples

This section provides several configuration examples of BGP.

5.1 Introduction

This section describes the principle and concepts of BGP.

5.1.1 BGP Overview

5.1.2 BGP Features Supported by the S-switch

5.1.3 Update History

5.1.1 BGP Overview

The Border Gateway Protocol (BGP) is a dynamic routing protocol used between Autonomous Systems (ASs). BGP has three early versions, BGP-1 (defined in RFC 1105), BGP-2 (defined in RFC 1163), and BGP-3 (defined in RFC 1267). The present version of BGP is BGP-4 (defined in RFC 1771).

BGP-4 as an exterior routing protocol on the Internet is widely used among Internet Service Providers (ISPs).

NOTE

BGP stated in this manual refers to BGP-4, unless otherwise stated.

The characteristics of BGP are as follows:

- BGP is an Exterior Gateway Protocol (EGP), and is used to control the route advertisement and select the optimal route rather than discover and 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 the Classless Inter-Domain Routing (CIDR).
- BGP transmits only the updated routes. This reduces the bandwidth occupied by BGP to transmit routes. BGP is applied to the Internet where a large amount of routes are transmitted.
- BGP eliminates route loops by adding the AS_Path to BGP routes.
- BGP provides rich routing policies to select and filter routes flexibly.
- BGP can expand easily to adapt to the new development of networks.

BGP runs on a S-switch in either of the following modes:

- IBGP
- EBGP

BGP is called Internal BGP (IBGP) when it runs within an AS; it is called External BGP (EBGP) when it runs among ASs.

5.1.2 BGP Features Supported by the S-switch

Interfaces That Support BGP

The creation of BGP routing tables and configurations of BGP functions must be performed on Layer 3 interfaces. Except the MEth interface, the physical interfaces on the S-switch, however, are Layer 2 interfaces. To facilitate the configurations, do as follows on the S-switch:

- Create a VLAN to which a Layer 2 interface belongs, assign an IP address to a VLANIF interface, and enable BGP functions on the VLANIF interface.
- Assign an IP address to a loopback interface and enable BGP functions on the loopback interface.



NOTE

For the following configuration tasks, the configurations in the interface view are performed on the preceding interfaces, unless otherwise stated.

Main Route Attributes

The S-switch enabled with BGP supports the following attributes:

- Origin
- AS_Path
- Next_Hop
- Multi-Exit-Discriminator (MED)
- Local_Pref

Route Selection Principles of BGP

On a S-switch, when multiple routes are available to the same destination, BGP selects routes according to the following principles:

1. Selecting a locally generated route with a lower preference. The preference is the preference value of various protocol routes including direct routes and static routes in the IP routing table. You can run the **display ip routing-table** command to view the preference value. The smaller the preference value is, the higher the preference is. The route whose preference value is the smallest has the highest preference.



NOTE

The locally generated routes refer to the routes imported by BGP through the commands of **import** and **network** or the routes aggregated through the commands of **aggregate** and **summary automatic**. Compared with the routes received from BGP peers, the locally routes are defined.

2. Selecting a protocol route in the following order: the Open Shortest Path First (OSPF), the Intermediate System-to-Intermediate System (IS-IS) Level-1, IS-IS Level-2, EBGp (including aggregated BGP routes), static, the Routing Information Protocol (RIP), OSPF_ASE, and IBGP, if different protocol routes have the same preference value.



NOTE

BGP prefers direct routes when there are direct routes among locally generated routes, because the minimum preference value of direct routes is 0.

3. Discarding the routes with the unreachable Next_Hop.
4. Preferring the labeled IPv4 routes unconditionally.
5. Preferring the route with the largest PreVal.
6. Preferring the route with the highest Local_Pref.

7. Preferring the aggregated route. The preference of an aggregated route is higher than that of a non-aggregated route.
8. Preferring the route with the shortest AS_Path.
9. Comparing the Origins and selecting the routes whose Origins are IGP, EGP, and Incomplete.
10. Preferring the route with the smallest MED.
11. Preferring the routes learned from EBGP. The preference of an EBGP route is higher than that of an IBPG route.
12. Preferring the route of an IGP with the smallest metric in an AS. Multiple routes are selected to perform load balancing according to the number of configured routes, if load balancing is configured and there are multiple external routes with the same AS_Path.
13. Preferring the route with the shortest Cluster_List.
14. Preferring the route with the smallest Originator_ID.
15. Preferring the route advertised by the S-switch with the smallest router ID.
16. Comparing IP addresses of the peers and Preferring the route that is learnt from the peer with a smaller IP address.

Route Selection Principles During Applications of BGP Load Balancing

In the BGP routing table, the next hop address of a route may not be the address of the peer directly connected to the local S-switch. This is because BGP does not change the next hop of a route when a BGP speaker advertises routes learned from an EBGP peer to an IBGP peer. In this case, to ensure that a packet is correctly forwarded, the S-switch must find a reachable address, and then forwards the packet to the next hop according to the routing table. In this process, the route to the reachable address is called a dependent route. BGP forwards packets according to dependent routes. The process of finding a dependent route according to the next hop address is called route iteration.

The S-switch supports BGP load balancing based on route iteration. That is, if a dependent route is configured for load balancing (suppose there are three next hop addresses), BGP generates the same number of next hop addresses to forward packets. BGP load balancing based on iteration need not be configured through commands. This feature is always enabled on the S-switch.

BGP load balancing is different from that of an Interior Gateway Protocol (IGP) in the following implementation methods:

- For different routes to a same destination address, an IGP calculates the metrics of routes according to its routing algorithm. Load balancing is performed among the routes with the same metric.
- BGP does not have a routing algorithm, so it cannot determine whether to perform load balancing among routes according to the metrics. BGP, however, has many route attributes with different priorities in route selection principles. BGP performs load balancing according to route selection principles. That is, load balancing is performed according to the maximum number of equal-cost routes only when all the routes have the same high preference.

NOTE

- BGP load balancing is performed only among the routes with the same AS_Path.
- BGP load balancing is also applied to the ASs in a confederation.

Principles for BGP Route Advertisement

On a S-switch, BGP advertises routes according to the following principles:

- The BGP speaker advertises only the optimal route to its peer when multiple valid routes are available.
- The BGP speaker sends only the routes in use to its peer.
- The BGP speaker advertises the routes learned from EBGp to all BGP peers (including EBGp peers and IBGP peers) instead of the peers that advertise the routes.
- The BGP speaker does not advertise the routes learned from IBGP to its IBGP peers.
- The BGP speaker advertises the routes learned from IBGP to its EBGp peers when the synchronization function between BGP and an IGP is disabled.
- The BGP speaker advertises all BGP routes to the new peers when the relationships are set up.

Route Aggregation

In a large-scale network, the BGP routing table is large. You can configure route aggregation to reduce the size of the routing table.

Route aggregation refers to the process of aggregating multiple routes. BGP advertises only the aggregated route rather than all the specific routes to their peers.

The S-switch supports automatic aggregation and manual aggregation. Manual aggregation can be used to control the attributes of the aggregated route and determine whether to advertise the specific routes.

Synchronizing IBGP and an IGP

IBGP and an IGP are synchronized so that unreachable routes are not advertised to nodes of external ASs.

If the synchronization function is configured, the S-switch checks the IGP routing table before adding an IBGP route to the routing table and advertising it to EBGp peers. The IBGP route is added to the routing table and advertised to the EBGp peers only when the IGP also learns this IBGP route.

The synchronization function can be disabled in the following situations:

- The local AS is not a transit AS.
- All BGP speakers in the local AS establish IBGP peer relationships and the network is fully meshed.

BFD for BGP

The S-switch supports Bidirectional Forwarding Detection (BFD) in IPv4 to provide fast detection of faults on the links for BGP.

BFD can fast detect faults on the links between BGP peers and report the faults to BGP. Fast convergence of BGP routes is thus implemented.

5.1.3 Update History

Version	Revision
V100R002C01B050	This is the first release.

5.2 Configuring Basic BGP Functions

This section describes how to start a BGP process, and configure a BGP peer.

[5.2.1 Establishing the Configuration Task](#)

[5.2.2 Starting a BGP Process](#)

[5.2.3 Configuring a BGP Peer](#)

[5.2.4 \(Optional\) Configuring a Local Interface for a BGP Connection](#)

[5.2.5 Checking the Configuration](#)

5.2.1 Establishing the Configuration Task

Applicable Environment

This section describes the configuration of a BGP network.

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 node, but the BGP connection can be created through logical links. To enhance the stability of BGP connections, the loopback interface addresses are used to set up the peer relationships.

To configure BGP to advertise and import routes, see [5.5.2 Configuring BGP to Advertise Local Routes](#) and [5.6.2 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 used in the extended address family view, however, are valid only in related applications.

NOTE

The commands in the BGP-IPv4 unicast address family view can be run in the BGP view. These commands, however, are described in the BGP-IPv4 unicast address family view in configuration files.

Pre-configuration Tasks

Before configuring basic BGP functions, complete the following tasks:

- Configuring the link layer protocol
- Creating a VLAN to which each interface belongs and assigning an IP address to each VLANIF interface

Data Preparation

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

No.	Data
1	Local AS number and router ID
2	IPv4 address of the peer and AS number
3	(Optional) Source address of the Update packet

5.2.2 Starting a BGP Process

Context

Do as follows on the S-switchs on which BGP connections need to be set up.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enable a BGP process (the local AS number is specified) and enter the BGP view.
- Step 3** Run the **router-id router-id** command to set the router ID of BGP.

Configuring or changing the router ID of BGP results in the resetting of the BGP connection.

 **TIP**

The command is optional. To enhance the reliability of a network, you can configure the address of the loopback interface as the router ID manually. If the router ID is not set, BGP automatically selects the router ID in the system view as the router ID of BGP.

----End

5.2.3 Configuring a BGP Peer

Configuring an IBGP Peer

Context

Do as follows on the S-switchs on which IBGP peer relationships need to be set up.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** Run the **peer ipv4-address as-number as-number** command to specify the IP address and the number of the AS where a BGP peer resides.

The number of the AS where the specified peer resides should be the same as that of the local AS.

The IP address of the specified peer can be one of the following types:

- IP address of a VLANIF interface on a directly connected peer
- IP address of a loopback interface on a reachable peer

If the IP address of a specified peer is a loopback address, or an IP address of another non-directly-connected network, you need to perform [5.2.4 \(Optional\) Configuring a Local Interface for a BGP Connection](#) to ensure the correct establishment of the peer.

Step 4 (Optional) Run the **peer *ipv4-address* *description* *description-text*** command to configure the description of a peer.

You can manage the network easily by configuring the descriptions.

----End

Configuring an IBGP Peer

Context

Do as follows on the S-switches on which EBGP peer relationships need to be set up.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp *as-number*** command to enter the BGP view.

Step 3 Run the **peer *ipv4-address* *as-number* *as-number*** command to specify the IP address and the number of the AS where a BGP peer resides.

The IP address and the number of the AS where a peer resides are specified.

The number of the AS where the specified peer resides must be different from that of the local AS.

The IP address of the specified peer can be one of the following types:

- IP address of a VLANIF interface on a directly connected peer
- IP address of a loopback interface on a reachable peer

If the IP address of a specified peer is a loopback address, or an IP address of another non-directly-connected network, you need to perform [5.2.4 \(Optional\) Configuring a Local Interface for a BGP Connection](#) to ensure the correct establishment of the peer.

Step 4 Run the **peer *ipv4-address* *ebgp-max-hop* [*number*]** command to set the maximum number of hops for EBGP peer relationships.

A directly connected physical link must be available between EBGP peers. If the requirement is not met, you must use the **peer *ebgp-max-hop*** command to configure EBGP peers to establish TCP connections through multiple hops.

Step 5 (Optional) Run the **peer *ipv4-address* *description* *description-text*** command to set the description of a peer.

You can manage the network easily by configuring the descriptions.

----End

5.2.4 (Optional) Configuring a Local Interface for a BGP Connection

Context

When IP addresses of the specified peers belong to a non-directly-connected network, do as follows on the S-switchs.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** Run the **peer ipv4-address connect-interface interface-type interface-number** command to configure a local interface used for a BGP connection.

To improve the reliability and stability of BGP connections, you can configure the local interface as the loopback interface to set up BGP connections. In this manner, when redundant links are available in the network, the BGP connections are not torn down, if an interface or a link fails.

NOTE

When establishing multiple peers between two S-switchs through various networks, you should run the **peer connect-interface** command to specify the interface through which a BGP connection is set up

----End

5.2.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the TCP connection.	display tcp status
Check information about BGP peers.	display bgp peer [verbose] display bgp peer ip-address { log-info verbose } display bgp vpnv4 vpn-instance vpn-instance-name peer [ipv4-address { log-info verbose } [verbose]]

5.3 Configuring BGP Route Attributes

This section describes how to configure BGP route attributes to change BGP route selection principles.

[5.3.1 Establishing the Configuration Task](#)

[5.3.2 Setting the BGP Preference](#)

[5.3.3 Setting the PrefVal for a BGP Peer](#)

[5.3.4 Setting the Default Local_Pref for the Local Device](#)

[5.3.5 Setting the MED](#)

[5.3.6 Configuring the Next_Hop](#)

[5.3.7 Setting the AS_Path](#)

[5.3.8 Checking the Configuration](#)

5.3.1 Establishing the Configuration Task

Applicable Environment

BGP has many route attributes. You can change route selection principles by configuring the following attributes:

- BGP preference
After the BGP preference is set, Routing Management (RM) is affected when selecting routes between BGP and other routing protocols.
- PrefVals of BGP routes
After the PrefVals of BGP routes is set, the route with the largest PrefVal is preferred when multiple routes to the same destination exist in the BGP routing table.
- Local_Pref
When the S-switch obtains multiple routes with the same destination address and different next hop addresses through IBGP peers, it determines the optimal route when traffic goes out of the AS by setting the Local_Pref.
- MED
After the MED is set, BGP can notify other ASs of selecting the route with the smallest MED when traffic comes in the AS.
- Next_Hop
- AS_Path

Pre-configuration Tasks

Before configuring BGP route attributes, complete the following tasks:

- Configuring the link layer protocol
- Creating a VLAN to which each interface belongs and assigning an IP address to each VLANIF interface
- [5.2 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

No.	Data
4	MED

5.3.2 Setting the BGP Preference

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **preference { external internal local | route-policy route-policy-name }** command to set the BGP preference.

BGP has the following types of routes:

- Routes learned from external peers (EBGP)
- Routes learned from internal peers (IBGP)
- Routes originated locally (Local Originated)

You can set different preferences for these three types of routes.

You can also apply routing policies to set the preferences for the specified routes that meet the requirements. You can set the default preferences for the routes that do not meet the requirements.

NOTE

You cannot use the **peer route-policy** command to apply routing policies to set the preference for BGP.

----End

5.3.3 Setting the PrefVal for a BGP Peer

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** Run the **peer ipv4-address preferred-value value** command to set the PrefVal is set for a peer.

By default, the original PrefVal of a route learned from a peer is 0.

----End

5.3.4 Setting the Default Local_Pref for the Local Device

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **default local-preference preference** command to set the default Local_Pref for the local device.

By default, the Local_Pref of BGP is 100.

----End

5.3.5 Setting the MED

Setting the MED for the Local Device

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **default med med** command to set the default MED.

----End

Comparing the MEDs of Routes from Different ASs

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **compare-different-as-med** command to compare the MEDs of routes from different ASs.

The S-switch compares only the MEDs of the routes from the same AS (different peers). After this command is run, BGP can compare the MEDs of routes from different ASs.

----End

(Optional) Configuring the Processing Method When the MED Is not Set

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **bestroute med-none-as-maximum** command to set the MED as the maximum value 4294967295 if it is not set.

By default, the MED is 0 if it is not set.

----End

5.3.6 Configuring the Next_Hop

Modifying the Next Hop When Advertising a Route to an IBGP Peer

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.

- Step 4** Run the **peer *ipv4-address* next-hop-local** command to configure the address of a S-switch as the next hop for route advertisement.

In certain networks, to ensure that an IBGP peer can find the correct next hop, you can configure the local S-switch to modify the next hop of a route as its address when the local S-switch advertises the route to its IBGP peer. By default, the S-switch does not modify the next hop address when advertising a route to its IBGP peer.

 **NOTE**

If BGP load balancing is configured, the local S-switch modifies the next hop address as its address when advertising routes to IBGP peer, regardless of whether the **peer next-hop-local** command is used or not.

----End

Not Modifying the Next Hop Address When Advertising a Route to an IBGP Peer

Context

Do as follows on the S-switchs that import IGP routes.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp *as-number*** command to enter the BGP view.
- Step 3** Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **peer *ipv4-address* next-hop-invariable** command to configure the S-switch not to modify the next hop address of an IGP route when advertising the imported IGP route.

By default, when a peer advertises an imported IGP route, the peer changes the next hop address to the address of the interface connecting the local S-switch and the remote peer.

----End

5.3.7 Setting the AS_Path

Allowing the Local AS Number Repeated

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp *as-number*** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **peer *ipv4-address* allow-as-loop [*number*]** command to set the local AS number to be repeated.

Generally, BGP checks the AS_Path of a route sent from the peer. If the local AS number already exists, BGP ignores this route to avoid route loops.

In some special applications, you can use the command to allow the AS_Path of a route sent from a peer to contain the local AS number. You can also set the number of times when the local AS number is repeated.

----End

Configuring the AS_Path Not as One of the Route Selection Rules

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **bestroute as-path-neglect** command to configure the AS_Path not as one of the route selection rules.

After this command is used, BGP does not compare the lengths of AS paths.

By default, the AS path with the smallest length is preferred.

----End

Configuring a Fake AS Number

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** Run the **peer ipv4-address fake-as fake-as-number** command to set a fake AS number.

The actual AS number cannot be displayed after the command is run. EBGP peers in other ASs can only learn this fake AS number. That is, when the peers in other ASs specify the local peers, you can set the AS number as the fake one.

This command is applicable to only EBGP peers.

----End

Configuring the AS_Path to Carry Only the Public AS Number

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **peer ipv4-address public-as-only** command to configure the AS_Path to carry only the public AS number.

The AS number ranges from 1 to 65535. The public AS number ranges from 1 to 64511 and the private AS number ranges from 64512 to 65534. 65535 is used as the reserved AS number in certain applications.

The public AS number can be used on the Internet, because Internet addresses 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 the internal routing domain.

BGP carries an AS number (either public or private) when advertising routes. In some situations, the private AS number does not need to be transmitted. You can then use the command to configure the AS_Path to carry only the public AS number.

This command is applicable to only EBGP peers.

----End

5.3.8 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the AS_Path.	display bgp paths [<i>as-regular-expression</i>] display bgp vpnv4 vpn-instance <i>vpn-instance-name</i> paths [<i>as-regular-expression</i>]
Check the BGP routing table.	display bgp routing-table [<i>network</i>] [<i>mask</i> <i>mask-length</i>] [longer-prefixes]
Check routing information about the specified BGP community.	display bgp routing-table community [<i>community-number</i> <i>aa:nn</i>] &<1-13> [internet no-advertise no-export no-export-subconfed] * [whole-match]
Check the routes matching the specified BGP community filter.	display bgp routing-table community-filter <i>community-filter-number</i> [whole-match]

5.4 Configuring BGP Filters

This section describes how to configure BGP filters.

[5.4.1 Establishing the Configuration Task](#)

[5.4.2 Configuring a Routing Policy for Advertising BGP Routes](#)

[5.4.3 Configuring a Routing Policy for Receiving BGP Routes](#)

[5.4.4 Configuring BGP Soft Resetting](#)

[5.4.5 Checking the Configuration](#)

5.4.1 Establishing the Configuration Task

Applicable Environment

Through powerful functions of filters, BGP can flexibly send and receive specific routes.

- Applying a Route-Policy

A Route-Policy is used to match the routes or certain attributes of the routes, and to change the attributes if the routes meet matching rules. The matching rules can be the following clauses.

The Route-Policy comprises multiple nodes and each node contains the following clauses:

- **if-match** clauses: define the matching rules that the routes meet. The matching objects are some attributes of the route.
- **apply** clauses: specify actions, that is, configuration commands are run after a route satisfies the matching rules specified by the **if-match** clauses. The **apply** clauses can change some attributes of the route.

- Controlling the received routes

BGP can use the routing policy on or filter the globally received routes and only the routes received from a certain peer.

When BGP receives routes from peers, BGP may be prone to service attacks and receive a large number of attack routes. The resources of the S-switch are thus consumed. In the case of too many BGP routes caused by malicious attacks or incorrect configurations, the administrator must limit the resources consumed by the network and S-switch according to the network planning and performance of the S-switch. BGP can control peers to limit the number of routes sent by peers.

- Resetting BGP connections

After changing BGP route selection principles, you must reset the BGP connection to validate the new configuration. The BGP connection is thus interrupted. BGP supports the Route-Refresh capability on the S-switch. When the principles are changed, the system refreshes the BGP routing table dynamically. So, the BGP connection is not interrupted.

If the peer supports the Route-Refresh capability, you can run the **refresh bgp** command to manually perform soft resetting for the BGP connection. The routing table is thus refreshed.

If the peer does not support the Route-Refresh capability, you can run the **peer keep-all-routes** command. In this manner, the BGP routing table can be refreshed.

Pre-configuration Tasks

Before configuring BGP filters, complete the following task:

- [5.2 Configuring Basic BGP Functions](#)

Data Preparation

To configure BGP filters, you need the following data.

No.	Data
1	Inbound interface and outbound interface, and name of the routing policy

5.4.2 Configuring a Routing Policy for Advertising BGP Routes

Configuring BGP to Filter the Globally Imported Routes

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **filter-policy { acl-number | ip-prefix ip-prefix-name } export [protocol [process-id]]** command to filter the imported routes.

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 through the **network** command.

----End

Applying a Routing Policy to the Routes Advertised by Specified BGP Peers

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.

Step 2 Run the **bgp as-number** command to enter the BGP view.

Step 3 (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.

Step 4 Run the **peer ipv4-address route-policy route-policy-name export** command to apply a routing policy to the advertised routes.

 **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.

----End

Applying a Filter to the Routes Advertised by Specified BGP Peers

Context

Do as follows on the S-switchs that run BGP.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp as-number** command to enter the BGP view.

Step 3 (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.

Step 4 Run the following command as required.

- Run the **peer ipv4-address filter-policy acl-number export** command to configure BGP to filter routes according to an ACL.
- Run the **peer ipv4-address as-path-filter as-path-filter-number export** command to configure BGP to filter routes according to the AS_Path filter.
- Run the **peer ipv4-address ip-prefix ip-prefix-name export** command to configure BGP to filter routes according to the prefix list.

----End

5.4.3 Configuring a Routing Policy for Receiving BGP Routes

Configuring BGP to Filter the Globally Received Routes

Context

Do as follows on the S-switchs that run BGP.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp as-number** command to enter the BGP view.

Step 3 (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.

Step 4 Run the **filter-policy { acl-number | ip-prefix ip-prefix-name } import** command to filter all the received BGP routes.

The routes received by BGP are filtered. Only those routes that meet the matching rules are received by BGP and are added to the routing table.

----End

Applying a Routing Policy to the Routes Received by Specified BGP Peers

Context

Do as follows on the S-switchs that run BGP.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp as-number** command to enter the BGP view.

Step 3 (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.

Step 4 Run the **peer ipv4-address route-policy route-policy-name import** command to apply a routing policy 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.

----End

Applying a Filter to the Routes Received by Specified BGP Peers

Context

Do as follows on the S-switchs that run BGP.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp as-number** command to enter the BGP view.

Step 3 (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.

Step 4 Run the following command as required.

- Run the **peer ipv4-address filter-policy acl-number import** command to configure BGP to filter routes according to an ACL.
- Run the **peer ipv4-address as-path-filter as-path-filter-number import** command to configure BGP to filter routes according to the AS_Path filter.

- Run the **peer *ipv4-address* ip-prefix *ip-prefix-name* import** command to configure BGP to filter routes according to the prefix list.

----End

Limiting the Number of Routes Received from a Peer

Context

Do as follows on the S-switchs that run BGP.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp *as-number*** command to enter the BGP view.

Step 3 Run the **peer *ipv4-address* route-limit *limit* [*percentage*] [**alert-only** | **idle-forever** | **idle-timeout** *times*]** command to set the number of routes received from a peer.

The command can be used to control the peer to receive routes. 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 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 disconnected. The S-switch does not retry setting up a connection. An alarm is generated and recorded in the log. Run the **display bgp peer** command or 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 disconnected. The S-switch retries setting up a connection after the timer expires. An alarm is generated and recorded in the log. Run the **display bgp peer** command or 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 preceding parameters are not set, the peer relationship is disconnected. The S-switch retries setting up a connection after 30 seconds. An alarm is generated and recorded in the log.

----End

5.4.4 Configuring BGP Soft Resetting

Enabling the Route-Refresh Capability

Context

Do as follows on the S-switchs that run BGP.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp as-number** command to enter the BGP view.

Step 3 Run the **peer ipv4-address capability-advertise { route-refresh | conventional }** command to enable the Route-Refresh capability.

When all BGP speakers are enabled with the Route-Refresh capabilities, the local S-switch sends Route-Refresh messages to peers, if the routing policy of BGP changes. After receiving the messages, the peers send the messages to the local S-switch. In this case, the BGP routing table is dynamically refreshed and the new routing policy is applied without interrupting BGP connections.

----End

Keeping All the Routing Updates of the Peers

Context

Do as follows on the S-switchs that run BGP.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp as-number** command to enter the BGP view.

Step 3 (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.

Step 4 Run the **peer ipv4-address keep-all-routes** command to keep all the routing updates of the peers.

After this command is used, all the routing updates sent by the specified peer are kept regardless of whether the filtering policy is used or not. When the local routing policy changes, the routing update information can be used to generate BGP routes again.

----End

Soft Resetting for BGP Connections

Context

Run the **refresh bgp** command in the user view.

Do as follows on the S-switchs that run BGP.

Procedure

Run the **refresh bgp { all | ipv4-address | external | internal } { export | import }** command to soft reset BGP connections.

Run the refresh bgp command in the user view

----End

5.4.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the routes advertised by BGP.	display bgp network
Check the routes matching the specified AS_Path filter.	display bgp routing-table as-path-filter <i>as-path-filter-number</i>
Check the routes matching the specified BGP community filter.	display bgp routing-table community-filter <i>community-filter-number</i> [whole-match]
Check the routes advertised or received by BGP peers.	display bgp routing-table peer <i>ipv4-address</i> { advertised-routes received-routes } [statistics]

5.5 Controlling the Route Advertisement

This section describes how to configure BGP to advertise routes.

5.5.1 Establishing the Configuration Task

5.5.2 Configuring BGP to Advertise Local Routes

5.5.3 Configuring BGP Route Aggregation

5.5.4 Configuring BGP to Advertise Default Routes to the Peers

5.5.5 Configuring Split Horizon Between EBGPeers

5.5.6 Checking the Configuration

5.5.1 Establishing the Configuration Task

Applicable Environment

- BGP route aggregation
In medium or large-scale BGP networks, route aggregation needs to be configured when the routes are advertised to the peers. This reduces the size of the routing table of the peers. BGP supports automatic aggregation and manual aggregation.
- EBGPe split horizon
If multiple EBGPe peers are set up between two ASs, the routes received from the peers of an AS are advertised to peers of the AS through other EBGPe peers. When the routes reach an EBGPe peer, the EBGPe peer discards the route according to the AS_Path, if the EBGPe peer is not configured to permit AS loops. This wastes resources.
You can run the **as-split-horizon** command to prohibit the route received from the peers of an AS from being forwarded to the peers of the AS. This can reduce unnecessary route advertisement.
- Controlling the advertised routes
BGP can filter or perform routing policies for the routes advertised by a certain peer.

Pre-configuration Tasks

Before controlling the route advertisement, complete the following task:

- [5.2 Configuring Basic BGP Functions](#)

Data Preparation

To control the route advertisement, you need the following data.

No.	Data
1	Aggregation mode and route aggregated

5.5.2 Configuring BGP to Advertise Local Routes

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **network ipv4-address [mask | mask-length] [route-policy route-policy-name]** command to configure BGP to advertise local routes.

The local routes to be advertised must exist in the local routing table. Using routing policies can control the routes to be advertised more flexibly.

----End

5.5.3 Configuring BGP Route Aggregation

Context

BGP supports route aggregation in the following modes:

- Automatic aggregation
Aggregates the subnet routes imported by BGP. After automatic aggregation is configured, BGP aggregates routes according to the natural network segment and sends the aggregated route to only the peers. For example, 10.1.1.1/24 and 10.2.1.1/24 are aggregated to 10.0.0.0/8, which is a Class A address.
- Manual aggregation
Aggregates routes in the local BGP routing table. Generally, manual aggregation takes precedence over automatic aggregation.

Configuring Automatic Aggregation

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **summary automatic** command to configure BGP to aggregate subnet routes automatically.

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 through the **network** command.

----End

Configuring Manual Aggregation

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **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] *** command to configure manual aggregation.

Manual aggregation is valid for the routing 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 various routing policies and set the route attributes when using manual aggregation.

----End

5.5.4 Configuring BGP to Advertise Default Routes to the Peers

Context

Do as follows on the S-switches that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **peer 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>]** command to configure BGP to advertise default routes to the peers.

NOTE

After the peer default-route-advertise command is used, BGP sends a default route with the local address as the next hop address to the specified peer, regardless of whether there are default routes in the routing table.

----End

5.5.5 Configuring Split Horizon Between EBGPeers

Context

Do as follows on the S-switches on which EBGPeer relationships are set up.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** Run the **as-split-horizon** command to configure split horizon between EBGPeers.

When multiple EBGPeers are set up between two ASs, the command is applied.

After the command is used, the route received from the peers of an AS is not forwarded to the peers of the AS. This reduces unnecessary route advertisement.

----End

5.5.6 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the routes advertised by BGP.	display bgp network
Check the routes of CIDR.	display bgp routing-table cidr

Action	Command
Check the routes advertised or received by BGP peers.	display bgp routing-table peer <i>ipv4-address</i> { advertised-routes received-routes } [statistics]

5.6 Controlling BGP to Import Routes

This section describes how to configure BGP to import external routes.

[5.6.1 Establishing the Configuration Task](#)

[5.6.2 Configuring BGP to Import Default Routes](#)

[5.6.3 Configuring BGP to Import Routes](#)

[5.6.4 Checking the Configuration](#)

5.6.1 Establishing the Configuration Task

Applicable Environment

The external routes are imported. BGP can send the routes of the local AS to its neighboring ASs, but it does not discover routes within the AS. Instead, BGP imports IGP routes to the BGP routing table and advertises them to the peers. When importing IGP routes, BGP filters routes according to different routing protocols.

Pre-configuration Tasks

Before controlling BGP to import routes, complete the following task:

- [5.2 Configuring Basic BGP Functions](#)

Data Preparation

None

5.6.2 Configuring BGP to Import Default Routes

Context

Do as follows on the S-switches that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.

Step 4 Run the **default-route imported** command to configure BGP to import default routes.

----End

5.6.3 Configuring BGP to Import Routes

Context

Do as follows on the S-switchs that run BGP.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp as-number** command to enter the BGP view.

Step 3 (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.

Step 4 Run the **import-route protocol [process-id] [med med | route-policy route-policy-name] *** command to configure BGP to import routes discovered by other routing protocols.

NOTE

When dynamic routing protocols are imported, you need specify the protocol number.

If the default-route imported command is not used, BGP cannot import default routes, when you run the import-route command to import routes of other protocols.

----End

5.6.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the routes matching the specified AS_Path filter.	display bgp routing-table as-path-filter as-path-filter-number
Check the routes of CIDR.	display bgp routing-table cidr
Check the routes matching the specified BGP community filter.	display bgp routing-table community-filter community-filter-number [whole-match]

5.7 Configuring Parameters for a BGP Connection

This section describes how to configure parameters of a BGP connection to adjust and optimize the performance of a BGP network.

[5.7.1 Establishing the Configuration Task](#)

[5.7.2 Configuring BGP Timers](#)

[5.7.3 Setting the Interval for Sending Update Messages](#)

[5.7.4 Enabling Fast Resetting for EBGPeer Relationships](#)[5.7.5 Checking the Configuration](#)

5.7.1 Establishing the Configuration Task

Applicable Environment

By configuring BGP timers, you can adjust the convergence speed of the network and change the network bandwidth occupied by BGP packets.

After a BGP connection is set up between peers, the peers periodically send Keepalive messages to each other. In this case, the BGP connection is not regarded as interrupted by the peers. If the S-switch does not receive any Keepalive message or any other types of messages from the peer within the hold time, the BGP connection is regarded as interrupted. The BGP connection is thus disconnected.

When a S-switch sets up a BGP connection, it compares the hold time. The smaller hold time is taken as the negotiated hold time. If the negotiation result is 0, no Keepalive message is transmitted and the hold time is not detected.

If the timer value changes, the BGP connection may be interrupted for a short time. This is because the peers need to negotiate again.

Pre-configuration Tasks

Before configuring parameters for a BGP connection, complete the following task:

- [5.2 Configuring Basic BGP Functions](#)

Data Preparation

To configure parameters for a BGP connection, you need the following data.

No.	Data
1	Values of BGP timers
2	Interval for sending Update packets

5.7.2 Configuring BGP Timers

Context



CAUTION

If the values of the timers change after the timer command or the peer timer command is run, the BGP connection set up between the nodes is interrupted. So, confirm the action before you use the command.

Configuring the Global Timer

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** Run the **timer keepalive keepalive-time hold hold-time** command to configure the global timer.

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 3 seconds at least. By default, the lifetime is 60 seconds and the hold time is 180 seconds.

When setting the values of *keepalive-time* and *hold-time*, note the following:

- The lifetime and hold time cannot be 0 at the same time. Otherwise, the BGP timer becomes invalid. That is, BGP does not detect link faults according to the timer.
- The hold time is much greater than the lifetime, such as, **timer keepalive 1 hold 65535**. If the hold time is too long, BGP cannot detect link faults timely.

After peer relationships are set up, the lifetime and hold time are negotiated by both peers. The smaller value of *hold-time* contained in Open messages of both peers is taken as the hold time. The smaller value of one third of *hold-time* and *keepalive-time* is taken as the lifetime.

----End

Configuring a Timer for a Peer

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** Run the **peer ipv4-address timer keepalive keepalive-time hold hold-time** command to set the lifetime and the hold time for a peer.

For the relationship between *keepalive-time* and *hold-time*, refer to the section "Configuring the Global Timer."

The peer timer takes precedence over the global timer.

----End

5.7.3 Setting the Interval for Sending Update Messages

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** Run the **peer ipv4-address route-update-interval interval** command to set the interval for sending Update messages.
- End

5.7.4 Enabling Fast Resetting for EBGP Peer Relationships

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** Run the **ebgp-interface-sensitive** command to enable fast resetting for EBGP peer relationships.
- After this function is enabled, BGP detects the failure on an EBGP link rapidly and then resets BGP connections on the interface immediately.
 - After this function is disabled, the repeated setup and deletion of BGP connections caused by route flapping are avoided. This saves the network bandwidth.
- End

5.7.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about BGP peers.	display bgp peer [verbose]

5.8 Configuring BFD for BGP

This section describes how to configure BFD for BGP to speed up the network convergence.

[5.8.1 Establishing the Configuration Task](#)

[5.8.2 Configuring BFD for BGP in the Public Network Instance](#)

[5.8.3 Configuring BFD for BGP in a Private Network](#)

5.8.4 Checking the Configuration

5.8.1 Establishing the Configuration Task

Applicable Environment

BGP periodically sends Keepalive messages to the peer to detect faults on the peer. 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 BGP. 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 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
- [5.2 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 intervals for sending and receiving BFD control packets and the local detection multiplier

5.8.2 Configuring BFD for BGP in the Public Network Instance

Context

Do as follows on S-switches at the two ends of a link on which a BFD session needs to be set up.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bfd** command to enable global BFD on the local node.
- Step 3** Run the **bgp as-number** command to enter the BGP view.
- Step 4** Run the **peer ipv4-address bfd enable** command to configure BFD on a peer.

Default values are used to set up the BFD session between the local node and the peer.

Step 5 Run the **peer ipv4-address bfd { min-tx-interval min-tx-interval | min-rx-interval min-rx-interval | detect-multiplier multiplier } *** command to set the parameters used to set up a BFD session.

 **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.

----End

5.8.3 Configuring BFD for BGP in a Private Network

Context

Do as follows on the S-switches at both ends of the link that needs to set up a BFD session.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bfd** command to enable global BFD on the local node.

Step 3 Run the **bgp as-number** command to enter the BGP view.

Step 4 (Optional) Run the **ipv4-family vpn-instance vpn-instance-name** command to enter the BGP-VPN instance view.

Step 5 Run the **peer ipv4-address bfd enable** command to configure BFD on a peer.

Default values are used to set up the BFD session between the local node and the peer.

Step 6 Run the **peer ipv4-address bfd { min-tx-interval min-tx-interval | min-rx-interval min-rx-interval | detect-multiplier multiplier } *** command to set the parameters used to set up a BFD session.

----End

5.8.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the BFD sessions established by BGP peers.	display bgp bfd session { [vpnv4 vpn-instance vpn-instance-name] peer ipv4-address all }
Check BGP peers.	display bgp [vpnv4 vpn-instance vpn-instance-name] peer [ipv4-address] [verbose]

5.9 Configuring BGP Load Balancing

This section describes how to configure attributes to implement BGP load balancing.

5.9.1 Establishing the Configuration Task

5.9.2 Setting the Number of Routes for Load Balancing

5.9.3 Checking the Configuration

5.9.1 Establishing the Configuration Task

Applicable Environment

When BGP selects routes, the BGP routes can be equal-cost ones for load balancing only when the first ten attributes described in [Route Selection Principles of BGP](#) are the same and they have the same AS_Path.

Pre-configuration Tasks

Before configuring BGP load balancing, complete the following task:

- [5.2 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

5.9.2 Setting the Number of Routes for Load Balancing

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **maximum load-balancing number** command to set the number of routes for load balancing.

By default, the number of routes for load balancing is 1.

----End

5.9.3 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the BGP routing table.	display bgp routing-table [<i>network</i>] [<i>mask</i> <i>mask-length</i>] [longer-prefixes]
Check the routing table.	display ip routing-table [verbose]

5.10 Configuring BGP Security

This section describes how to enhance BGP security.

[5.10.1 Establishing the Configuration Task](#)

[5.10.2 Configuring the MD5 Authentication](#)

[5.10.3 Checking the Configuration](#)

5.10.1 Establishing the Configuration Task

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 a TCP connection is set up. The MD5 authentication, however, does not authenticate BGP packets. Instead, it sets the MD5 authentication password for the TCP connection, and the authentication is then complete by TCP. If the authentication fails, the TCP connection cannot be established.

Pre-configuration Tasks

Before configuring BGP security, complete the following task:

- [5.2 Configuring Basic BGP Functions](#)

Data Preparation

To configure BGP security, you need the following data.

No.	Data
1	MD5 authentication password
2	Process ID of the routing protocol run on each S-switch
3	IP addresses of BGP peers for the S-switches

5.10.2 Configuring the MD5 Authentication

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** Run the **peer ipv4-address password { cipher cipher-password | simple simple-password }** command to configure an MD5 authentication password.

----End

5.10.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about BGP peers.	display bgp peer [<i>ipv4-address</i>] verbose

5.11 Maintaining BGP

This section describes how to maintain BGP.

[5.11.1 Resetting BGP Connections](#)

[5.11.2 Debugging BGP](#)

5.11.1 Resetting BGP Connections



CAUTION

The BGP connection 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 or the configuration changes, you needs to reset BGP connections to validate the configuration. To reset BGP connections, run the following **reset** commands in the user view.

Action	Command
Reset all BGP connections.	reset bgp all
Reset the BGP connection between the specified AS.	reset bgp as-number

Action	Command
Reset the BGP connection between the specified peers.	reset bgp <i>ipv4-address</i>
Reset all EBGP connections.	reset bgp external
Reset all IBGP connections.	reset bgp internal
Resets the BGP peer relationship of the specified VPN instance.	reset bgp vpn-instance <i>vpn-instance-name</i> { <i>as-number</i> <i>ipv4-address</i> all external internal }
Resets all BGP peer relationships of IPv4.	reset bgp ipv4 all

5.11.2 Debugging BGP



CAUTION

Debugging affects the performance of the system. So, after debugging, run the **undo debugging all** command to disable it immediately.

When a BGP fault occurs, run the following **debugging** commands in the user view to locate the fault.

Action	Command
Enable all the debugging of BGP.	debugging bgp all
Enable the debugging of BGP events.	debugging bgp event
Enable the debugging of BGP packets.	debugging bgp { keepalive open packet route-refresh } [receive send] [verbose]
Enable the debugging of BGP Update packets.	debugging bgp update [acl <i>acl-number</i> ipv4] [peer <i>ipv4-address</i> ip-prefix <i>ip-prefix-name</i>] [receive send] [verbose]

5.12 Configuration Examples

This section provides several configuration examples of BGP.

[5.12.1 Example for Configuring Basic BGP Functions](#)

[5.12.2 Example for Configuring BGP to Interact with an IGP](#)

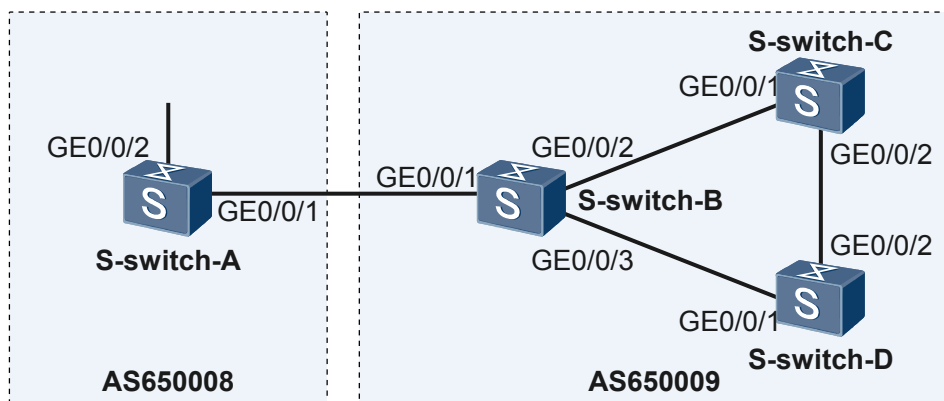
[5.12.3 Example for Configuring BGP Load Balancing and the MED](#)

5.12.1 Example for Configuring Basic BGP Functions

Networking Requirements

As shown in [Figure 5-1](#), all S-switchs run BGP. An EBGP peer relationship is set up between S-switch-A and S-switch-B. IBGP peer relationships are set up between S-switch-B, S-switch-C, and S-switch-D.

Figure 5-1 Networking diagram of configuring basic BGP functions



S-switch	Interface	VLANIF Interface	IP Address
S-switch-A	GigabitEthernet 0/0/1	VLANIF 10	200.1.1.2/24
S-switch-A	GigabitEthernet 0/0/2	VLANIF 50	8.1.1.1/8
S-switch-B	GigabitEthernet 0/0/1	VLANIF 10	200.1.1.1/24
S-switch-B	GigabitEthernet 0/0/2	VLANIF 20	9.1.3.1/24
S-switch-B	GigabitEthernet 0/0/3	VLANIF 30	9.1.1.1/24
S-switch-C	GigabitEthernet 0/0/1	VLANIF 20	9.1.3.2/24
S-switch-C	GigabitEthernet 0/0/2	VLANIF 40	9.1.2.1/24
S-switch-D	GigabitEthernet 0/0/1	VLANIF 30	9.1.1.2/24
S-switch-D	GigabitEthernet 0/0/2	VLANIF 40	9.1.2.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Set up IBGP peer relationships between S-switch-B, S-switch-C and S-switch-D.
2. Create an EBGP peer relationship between S-switch-A and S-switch-B.
3. Advertise routes through the **network** command on S-switch-A and check the routing tables of S-switch-A, S-switch-B, and S-switch-C.
4. Configure BGP on S-switch-B to import direct routes, and check the routing tables of S-switch-A and S-switch-C.

Data Preparation

To complete the configuration, you need the following data:

- The VLAN ID of each interface is shown in [Figure 5-1](#).
- The IP address of each VLANIF interface is shown in [Figure 5-1](#).
- The router ID of S-switch-A is 1.1.1.1 and the number of the AS where it resides is 65008.
- The router IDs of S-switch-B, S-switch-C, and S-switch-D are 2.2.2.2, 3.3.3.3, and 4.4.4.4, and the number of the AS where they reside is 65009.

Configuration Procedure

1. Create a VLAN to which each interface belongs.
The configuration details are not mentioned here.
2. Assign an IP address to each VLANIF interface.
The configuration details are not mentioned here.
3. Create IBGP peer relationships.

Configure S-switch-B.

```
[S-switch-B] bgp 65009
[S-switch-B-bgp] router-id 2.2.2.2
[S-switch-B-bgp] peer 9.1.1.2 as-number 65009
[S-switch-B-bgp] peer 9.1.3.2 as-number 65009
```

Configure S-switch-C.

```
[S-switch-C] bgp 65009
[S-switch-C-bgp] router-id 3.3.3.3
[S-switch-C-bgp] peer 9.1.3.1 as-number 65009
[S-switch-C-bgp] peer 9.1.2.2 as-number 65009
[S-switch-C-bgp] quit
```

Configure S-switch-D

```
[S-switch-D] bgp 65009
[S-switch-D-bgp] router-id 4.4.4.4
[S-switch-D-bgp] peer 9.1.1.1 as-number 65009
[S-switch-D-bgp] peer 9.1.2.1 as-number 65009
[S-switch-D-bgp] quit
```

4. Create an EBGP peer relationship.

Configure S-switch-A

```
[S-switch-A] bgp 65008
[S-switch-A-bgp] router-id 1.1.1.1
[S-switch-A-bgp] peer 200.1.1.1 as-number 65009
```

Configure S-switch-B.

```
[S-switch-B-bgp] peer 200.1.1.2 as-number 65008
[S-switch-B-bgp] quit
```

Check the status of BGP connections.

```
[S-switch-B] 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 the BGP connections between S-switch-B and all the other S-switches are set up.

5. Configure S-switch-A to advertise the route 8.0.0.0/8.

Configure S-switch-A to advertise routes.

```
[S-switch-A-bgp] ipv4-family unicast
[S-switch-A-bgp-af-ipv4] network 8.0.0.0 255.0.0.0
[S-switch-A-bgp-af-ipv4] quit
[S-switch-A-bgp] quit
```

Check the routing table of S-switch-A.

```
[S-switch-A] display bgp routing-table
```

Total Number of Routes: 1

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

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 8.0.0.0/8	0.0.0.0	0		0	i

Check the routing table of S-switch-B.

```
[S-switch-B] display bgp routing-table
```

Total Number of Routes: 1

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

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 8.0.0.0/8	200.1.1.2	0		0	65008i

Check the routing table of S-switch-C.

```
[S-switch-C] display bgp routing-table
```

Total Number of Routes: 1

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

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
i 8.0.0.0/8	200.1.1.2	0	100	0	65008i

From the routing table, you can view that S-switch-C has learned the route to the destination 8.0.0.0 in AS 65008, but the next hop 200.1.1.2 is unreachable. Therefore, this route is invalid.

6. Configure BGP to import direct routes

Configure S-switch-B.

```
[S-switch-B] vlan 65009
[S-switch-B-bgp] ipv4-family unicast
[S-switch-B-bgp-af-ipv4] import-route direct
[S-switch-B-bgp-af-ipv4] quit
[S-switch-B-bgp] quit
```

Check the BGP routing table of S-switch-A.

```
[S-switch-A] display bgp routing-table
```

Total Number of Routes: 4

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

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
---------	---------	-----	--------	---------	----------

```
*> 8.0.0.0/8          0.0.0.0          0          0          i
*> 9.1.1.0/24         200.1.1.1        0          0          65009?
*> 9.1.3.0/24         200.1.1.1        0          0          65009?
* 200.1.1.0/24        200.1.1.1        0          0          65009?
```

Check the BGP routing table of S-switch-C.

```
[S-switch-C] display bgp routing-table
Total Number of Routes: 4
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

      Network          NextHop      MED      LocPrf    PrefVal Path/Ogn
-----
* i  8.0.0.0/8         200.1.1.2      0         100        0       65008i
*> i  9.1.1.0/24        9.1.3.1        0         100        0       ?
   i  9.1.3.0/24        9.1.3.1        0         100        0       ?
*> i  200.1.1.0/24      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 S-switch-A.

Perform the ping operation to verify the configuration.

```
[S-switch-C] ping 8.1.1.1
PING 8.1.1.1: 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
```

Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
vlan batch 10 50
#
interface Vlanif10
 ip address 200.1.1.2 255.255.255.0
#
interface Vlanif50
 ip address 8.1.1.1 255.0.0.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 50
#
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 S-switch-B

```
#
 sysname S-switch-B
#
 vlan batch 10 20 30
#
 interface Vlanif10
  ip address 200.1.1.1 255.255.255.0
#
 interface Vlanif20
  ip address 9.1.3.1 255.255.255.0
#
 interface Vlanif30
  ip address 9.1.1.1 255.255.255.0
#
 interface GigabitEthernet0/0/1
  port trunk allow-pass vlan 10
#
 interface GigabitEthernet0/0/2
  port trunk allow-pass vlan 20
#
 interface GigabitEthernet0/0/3
  port trunk allow-pass vlan 30
#
 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 S-switch-C

```
#
 sysname S-switch-C
#
 vlan batch 20 40
#
 interface Vlanif20
  ip address 9.1.3.2 255.255.255.0
#
 interface Vlanif40
  ip address 9.1.2.1 255.255.255.0
#
 interface GigabitEthernet0/0/1
  port trunk allow-pass vlan 20
#
 interface GigabitEthernet0/0/2
  port trunk allow-pass vlan 40
#
 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 S-switch-D

```

#
 sysname S-switch-D
#
 vlan batch 30 40
#
 interface Vlanif30
  ip address 9.1.1.2 255.255.255.0
#
 interface Vlanif40
  ip address 9.1.2.2 255.255.255.0
#
 interface GigabitEthernet0/0/1
  port trunk allow-pass vlan 30
#
 interface GigabitEthernet0/0/2
  port trunk allow-pass vlan 40
#
 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

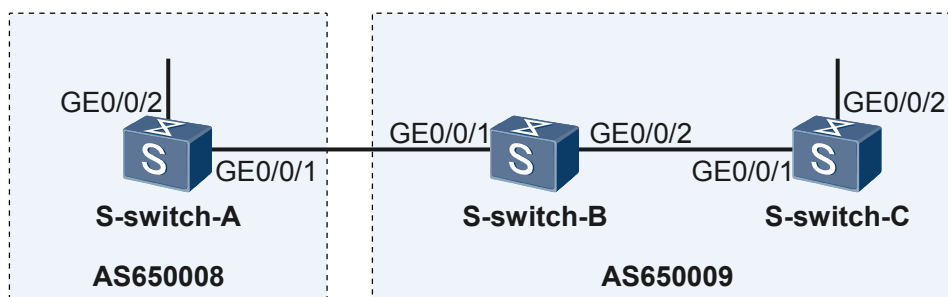
```

5.12.2 Example for Configuring BGP to Interact with an IGP

Networking Requirements

As shown in [Figure 5-2](#), OSPF is used inside AS 65009. An EBGP peer relationship is set up between S-switch-A and S-switch-B. S-switch-C runs OSPF instead of BGP.

Figure 5-2 Networking diagram of configuring BGP to interact with an IGP



S-switch	Interface	VLANIF Interface	IP Address
S-switch-A	GigabitEthernet 0/0/1	VLANIF 10	3.1.1.2/24
S-switch-A	GigabitEthernet 0/0/2	VLANIF 30	8.1.1.1/24
S-switch-B	GigabitEthernet 0/0/1	VLANIF 10	3.1.1.1/24
S-switch-B	GigabitEthernet 0/0/2	VLANIF 20	9.1.1.1/24
S-switch-C	GigabitEthernet 0/0/1	VLANIF 20	9.1.1.2/24
S-switch-C	GigabitEthernet 0/0/2	VLANIF 40	9.1.2.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure OSPF on S-switch-B and S-switch-C.
2. Create an EBGP peer relationship on S-switch-A and S-switch-B.
3. Configure BGP to interact with OSPF on S-switch-B and check the routes.
4. Configure BGP route aggregation on S-switch-B to simplify the BGP routing table.

Data Preparation

To complete the configuration, you need the following data:

- The VLAN ID of each interface is shown in [Figure 5-2](#).
- The IP address of each VLANIF interface is shown in [Figure 5-2](#).
- The router ID of S-switch-A is 1.1.1.1 and the number of the AS where it resides is 65008.
- The router IDs of S-switch-B and S-switch-C are 2.2.2.2 and 3.3.3.3, and the number of the AS where they reside is 65009.

Configuration Procedure

1. Create a VLAN to which each interface belongs.
The configuration details are not mentioned here.
2. Assign an IP address to each VLANIF interface.
The configuration details are not mentioned here.
3. Configure OSPF.

Configure S-switch-B.

```
[S-switch-B] ospf 1
[S-switch-B-ospf-1] area 0
[S-switch-B-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[S-switch-B-ospf-1-area-0.0.0.0] quit
[S-switch-B-ospf-1] quit
```

Configure S-switch-C.

```
[S-switch-C] ospf 1
[S-switch-C-ospf-1] area 0
[S-switch-C-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[S-switch-C-ospf-1-area-0.0.0.0] network 9.1.2.0 0.0.0.255
[S-switch-C-ospf-1-area-0.0.0.0] quit
[S-switch-C-ospf-1] quit
```

4. Create an EBGP peer relationship.

Configure S-switch-A.

```
[S-switch-A] bgp 65008
[S-switch-A-bgp] router-id 1.1.1.1
[S-switch-A-bgp] peer 3.1.1.1 as-number 65009
[S-switch-A-bgp] ipv4-family unicast
[S-switch-A-bgp-af-ipv4] network 8.1.1.0 255.255.255.0
[S-switch-A-bgp-af-ipv4] quit
[S-switch-A-bgp] quit
```

Configure S-switch-B.

```
[S-switch-B] bgp 65009
[S-switch-B-bgp] router-id 2.2.2.2
[S-switch-B-bgp] peer 3.1.1.2 as-number 65008
```

5. Configure BGP to interact with an IGP

On S-switch-B, configure BGP to import OSPF routes.

```
[S-switch-B-bgp] ipv4-family unicast
[S-switch-B-bgp-af-ipv4] import-route ospf 1
[S-switch-B-bgp-af-ipv4] quit
[S-switch-B-bgp] quit
```

Check the routing table of S-switch-A.

```
[S-switch-A] display bgp routing-table
```

Total Number of Routes: 3

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

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	8.1.1.0/24	0.0.0.0	0		0	i
*>	9.1.1.0/24	3.1.1.1	0		0	65009?
*>	9.1.2.0/24	3.1.1.1	2		0	65009?

On S-switch-B, configure BGP to import BGP routes.

```
[S-switch-B] ospf
[S-switch-B-ospf-1] import-route bgp
[S-switch-B-ospf-1] quit
```

Check the routing table of S-switch-C.

```
[S-switch-C] 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	Vlanif20
9.1.1.0/24	Direct	0	0	D	9.1.1.2	Vlanif20
9.1.1.2/32	Direct	0	0	D	127.0.0.1	InLoopBack0
9.1.2.0/24	Direct	0	0	D	9.1.2.1	Vlanif40
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

6. Configure automatic aggregation.

Configure S-switch-B.

```
[S-switch-B] bgp 65009
[S-switch-B-bgp] ipv4-family unicast
[S-switch-B-bgp-af-ipv4] summary automatic
[S-switch-B-bgp-af-ipv4] quit
[S-switch-B-bgp] quit
```

Check the BGP routing table of S-switch-A.

```
[S-switch-A] display bgp routing-table
```

Total Number of Routes: 2

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

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	8.1.1.0/24	0.0.0.0	0		0	i
*>	9.0.0.0	3.1.1.1			0	65009?

Perform the ping operation to verify the configuration.

```
[S-switch-A] 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
```

Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
vlan batch 10 30
#
interface Vlanif10
ip address 3.1.1.2 255.255.255.0
#
interface Vlanif30
ip address 8.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 30
#
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 S-switch-B

```
#
sysname S-switch-B
#
vlan batch 10 20
#
interface Vlanif10
ip address 3.1.1.1 255.255.255.0
#
interface Vlanif20
ip address 9.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 20
#
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 S-switch-C

```

#
sysname S-switch-C
#
vlan batch 20 40
#
interface Vlanif20
ip address 9.1.1.2 255.255.255.0
#
interface Vlanif40
ip address 9.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 40
#
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

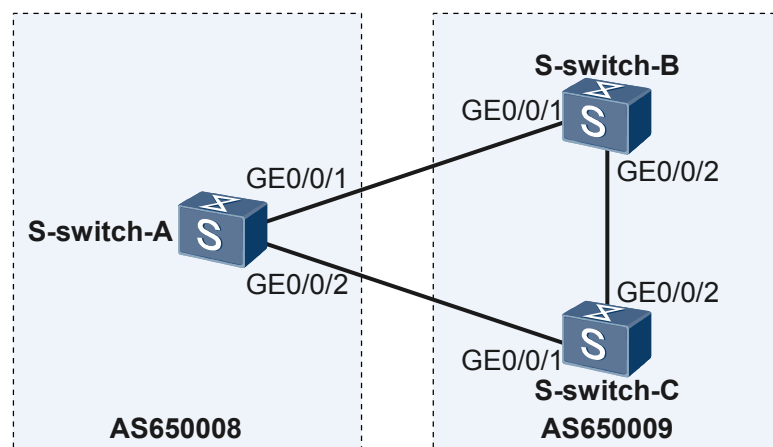
```

5.12.3 Example for Configuring BGP Load Balancing and the MED

Networking Requirements

As shown in [Figure 5-3](#), all S-switchs run BGP. S-switch-A resides in AS 65008. Both S-switch-B and S-switch-C reside in AS 65009. EBGp runs among S-switch-A, S-switch-B, and S-switch-C. IBGP runs between S-switch-B and S-switch-C.

Figure 5-3 Networking diagram of BGP route selection



S-switch	Interface	VLANIF Interface	IP Address
S-switch-A	GigabitEthernet 0/0/1	VLANIF 10	200.1.1.2/24

S-switch-A	GigabitEthernet 0/0/2	VLANIF 20	200.1.2.2/24
S-switch-B	GigabitEthernet 0/0/1	VLANIF 10	200.1.1.1/24
S-switch-B	GigabitEthernet 0/0/2	VLANIF 30	9.1.1.1/24
S-switch-C	GigabitEthernet 0/0/1	VLANIF 20	200.1.2.1/24
S-switch-C	GigabitEthernet 0/0/2	VLANIF 30	9.1.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Set up EBGp peer relationships between S-switch-A and S-switch-B, and between S-switch-A and S-switch-C. Create an IBGP peer relationship between S-switch-B and S-switch-C.
2. Configure load balancing and the MED on S-switch-A and check the routing table.

Data Preparation

To complete the configuration, you need the following data:

- The VLAN ID of each interface is shown in [Figure 5-3](#).
- The IP address of each VLANIF interface is shown in [Figure 5-3](#).
- The router IDs of S-switch-A is 1.1.1.1, the number of the AS where it resides is 65008, and the number of routes for load balancing is 2.
- The router IDs of S-switch-B and S-switch-C are 2.2.2.2 and 3.3.3.3, the number of the AS where they reside is 65008, the default MED of S-switch-B is 100.

Configuration Procedure

1. Create a VLAN to which each interface belongs.
The configuration details are not mentioned here.
2. Assign an IP address to each VLANIF interface.
The configuration details are not mentioned here.
3. Create EBGp peer relationships.

Configure S-switch-A.

```
[S-switch-A] bgp 65008
[S-switch-A-bgp] router-id 1.1.1.1
[S-switch-A-bgp] peer 200.1.1.1 as-number 65009
[S-switch-A-bgp] peer 200.1.2.1 as-number 65009
[S-switch-A-bgp] quit
```

Configure S-switch-B.

```
[S-switch-B] bgp 65009
[S-switch-B-bgp] router-id 2.2.2.2
[S-switch-B-bgp] peer 200.1.1.2 as-number 65008
[S-switch-B-bgp] peer 9.1.1.2 as-number 65009
[S-switch-B-bgp] ipv4-family unicast
[S-switch-B-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
[S-switch-B-bgp-af-ipv4] quit
[S-switch-B-bgp] quit
```

Configure S-switch-C.

```
[S-switch-C] bgp 65009
```

```
[S-switch-C-bgp] router-id 3.3.3.3
[S-switch-C-bgp] peer 200.1.2.2 as-number 65008
[S-switch-C-bgp] peer 9.1.1.1 as-number 65009
[S-switch-C-bgp] ipv4-family unicast
[S-switch-C-bgp-af-ipv4] network 9.1.1.0 255.255.255.0
[S-switch-C-bgp-af-ipv4] quit
[S-switch-C-bgp] quit
```

Check the routing table of S-switch-A.

```
[S-switch-A] display bgp routing-table
```

Total Number of Routes: 2

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

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	9.1.1.0/24	200.1.1.1	0		0	65009i
*		200.1.2.1	0		0	65009i

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 because the router ID of S-switch-B is smaller.

4. Configure load balancing.

Configure S-switch-A.

```
[S-switch-A] bgp 65008
[S-switch-A-bgp] ipv4-family unicast
[S-switch-A-bgp-af-ipv4] maximum load-balancing 2
[S-switch-A-bgp-af-ipv4] quit
[S-switch-A-bgp] quit
```

Check the routing table of S-switch-A.

```
[S-switch-A] display bgp routing-table
```

Total Number of Routes: 2

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

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	9.1.1.0/24	200.1.1.1	0		0	65009i
*>		200.1.2.1	0		0	65009i

You can view that the BGP route 9.1.1.0/24 has two next hops that are 200.1.1.1 and 200.1.2.1. Both of them are optimal routes.

5. Set the MED.

Set the MED sent by S-switch-B to S-switch-A through the policy.

```
[S-switch-B] route-policy 10 permit node 10
[S-switch-B-route-policy] apply cost 100
[S-switch-B-route-policy] quit
[S-switch-B] bgp 65009
[S-switch-B-bgp] peer 200.1.1.2 route-policy 10 export
```

Check the routing table of S-switch-A.

```
[S-switch-A] display bgp routing-table
```

Total Number of Routes: 2

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

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
--	---------	---------	-----	--------	---------	----------

```
*> 9.1.1.0/24      200.1.2.1      0      0      65009i
*      200.1.1.1    100      0      65009i
```

You can view that the MED of route with the next hop as 200.1.1.1 (S-switch-B) is 100, and the MED of the route with the next hop as 200.1.2.1 is 0. Therefore, the route with the smaller MED is selected.

Configuration Files

- Configuration file of S-switch-A

```
#
 sysname S-switch-A
#
 vlan batch 10 20
#
 interface Vlanif10
 ip address 200.1.1.2 255.255.255.0
#
 interface Vlanif20
 ip address 200.1.2.2 255.255.255.0
#
 interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
 interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 20
#
 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 S-switch-B

```
#
 sysname S-switch-B
#
 vlan batch 10 30
#
 interface Vlanif10
 ip address 200.1.1.1 255.255.255.0
#
 interface Vlanif30
 ip address 9.1.1.1 255.255.255.0
#
 interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 10
#
 interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 30
#
 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
 default med 100
 network 9.1.1.0 255.255.255.0
 peer 9.1.1.2 enable
```

```
peer 200.1.1.2 enable
peer 200.1.1.2 route-policy 10 export
#
route-policy 10 permit node 10
  apply cost 100
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
vlan batch 20 30
#
interface Vlanif10
  ip address 200.1.2.1 255.255.255.0
#
interface Vlanif30
  ip address 9.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
  port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/2
  port trunk allow-pass vlan 30
#
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
```

6 Routing Policy Configuration

About This Chapter

This chapter describes the fundamentals of the routing policy and configuration steps for filtering lists, the routing policy, along with typical examples.

[6.1 Introduction](#)

This section describes the principle and concepts of the routing policy.

[6.2 Configuring an IP Prefix List](#)

This section describes how to configure an IP prefix list.

[6.3 Configuring a Route-Policy](#)

This section describes how to configure a Route-Policy, define a group of matching rules, and change the route attributes.

[6.4 Applying Filters to Received Routes](#)

This section describes how to filter received routes.

[6.5 Applying Filters to Advertised Routes](#)

This section describes how to filter advertised routes.

[6.6 Applying Filters to Imported Routes](#)

This section describes how to filter imported routes.

[6.7 Controlling the Valid Time of a Routing Policy](#)

This section describes how to adjust the valid time of the Route-Policy.

[6.8 Configuration Examples](#)

This section provides several configuration examples for the routing policy.

6.1 Introduction

This section describes the principle and concepts of the routing policy.

6.1.1 Overview of the Routing Policy

6.1.2 Routing Policy Features Supported by the S-switch

6.1.3 Logical Relationships Between Configuration Tasks

6.1.4 Update History

6.1.1 Overview of the Routing Policy

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 S-switch advertises or receives routes, the S-switch may use policies to filter routes. The policies are used in the following situations:

- Receive or advertise routes that meet the matching rules only.
- A routing protocol may import routes discovered by other routing protocols to enrich routing information. When importing routes from other routing protocols, the S-switch may import some routes that meet the matching rules, and set attributes of the routes imported to meet the requirements.

To implement a routing policy, you must:

- Define the route attributes, that is, a group of matching rules. You can use the route attributes as matching rules, such as the destination address and the address of the host advertising routes.
- Apply the matching rules for advertised, received, and imported routes.

Routing Policy and Policy-based Routing

Policy-based routing (PBR) is used to search the previous packet forwarding procedure, whereas a packet is often forwarded according to the destination address of the packet in the routing table. PBR supports information based on the source address and the length of packets. PBR selects routes according to the set policy. PBR is applicable to security and load balancing.

Differences between the routing policy and PBR are as [Table 6-1](#).

Table 6-1 Differences between the routing policy and PBR

Routing Policy	PBR
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.

Routing Policy	PBR
Based on the control plane and serves for the routing protocol and routing table.	Based on the forwarding plane and serves for the forwarding policy.
Combines with the routing protocol to complete the policy.	Needs to be manually configured hop by hop to ensure that the packet is forwarded through the policy.
The route-policy command is used.	The policy-based-route command is used.

6.1.2 Routing Policy Features Supported by the S-switch

Filters

The S-switch provides several types of filters for routing protocols, such as ACLs, IP prefix lists, and Route-Policies.

ACL

The S-switch provides Access Control Lists (ACLs) for IPv4 routes. 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.

ip-prefix list

The S-switch provides IPv4 prefix lists.

An IP prefix list is identified by its prefix list name. Each prefix list contains multiple entries. Each entry can specify the matching range in the form of the network prefix. The matching range is identified by an index number that designates the matching sequence.

During the matching, the S-switch checks entries identified by the index number in an ascending order. If a route matches an entry, the route does not match the next entry.

Route-Policy

Route-Policy is a complex filter. A Route-Policy is used to match the route attributes, and to change the route attributes when matching rules are met. The Route-Policy uses the preceding filters to define the matching rules.

A Route-Policy consists of multiple nodes. The relationship between the nodes is "OR". The system checks the nodes according to the index number. When a route matches a node in the Route-Policy, the route does not match the next node.

Each node comprises a set of **if-match** and **apply** clauses. The **if-match** clauses define the matching rules. The matching objects are the route attributes. The relationship between the **if-match** clauses in a node is "AND". A matching succeeds only when all the matching rules specified by the **if-match** clauses are matched. The **apply** clauses specify actions. When a route matches a rule, the apply clauses set some attributes for the route.

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 details of the routing policy configuration, see the related routing protocol configurations.

6.1.3 Logical Relationships Between Configuration Tasks

This chapter is classified into six configuration tasks according to the configuration of the routing policy:

- [4.2.5 Checking the Configuration](#)
- [4.3.3 Configuring RIP Preference](#)
- [4.4.3 Disabling an Interface from Sending Update Packets](#)
- [4.5.3 Disabling RIP from Receiving Host Routes](#)
- [4.6.3 Configuring Packet Authentication of RIP-2](#)
- [4.7.4 Configuring Split Horizon and Poison Reverse](#)

[4.2.5 Checking the Configuration](#) is used to configure matching rules of a specified routing policy and can be configured as required. [4.3.3 Configuring RIP Preference](#) is the basis for configuring the routing policy. After performing this task, you can perform the following four tasks.

6.1.4 Update History

Version	Revision
V100R002C01B050	This is the first release.

6.2 Configuring an IP Prefix List

This section describes how to configure an IP prefix list.

[6.2.1 Establishing the Configuration Task](#)

[6.2.2 Configuring an IPv4 Prefix List](#)

[6.2.3 Checking the Configuration](#)

6.2.1 Establishing the Configuration Task

Applicable Environment

Before applying a routing policy, you should configure 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 the IP prefix list
2	Matched address range

6.2.2 Configuring an IPv4 Prefix List

Context

An IPv4 prefix list is identified by its list name. Each prefix list contains multiple entries. Each entry can specify the matching range in the form of a network prefix and is identified by 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, the route does not match the next entry.

Do as follows on the S-switches to which the IP prefix list is applied.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **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*] command to set an IPv4 prefix list.

The range of the mask length can be specified as *mask-length* <= *greater-equal-value* <= *less-equal-value* <= 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*].

On the S-switch, all unmatched routes are filtered. If all entries are in **deny** mode, all routes are filtered. In this case, you should define **permit 0.0.0.0 0 less-equal 32** so that all the other IPv4 routes can match the entries.

NOTE

If more than one IP prefix entry is defined, at least one entry should be in **permit** mode.

----End

6.2.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about the IPv4 prefix list.	display ip ip-prefix [<i>ip-prefix-name</i>]

Run the **display ip ip-prefix p1** command. You can view information about the prefix list named p1.

```
<Quidway> display ip ip-prefix p1
Prefix-list p1
Permitted 5
Denied 2
index: 10          permit 192.168.0.0/16          ge 17 le 18
```

6.3 Configuring a Route-Policy

This section describes how to configure a Route-Policy, define a group of matching rules, and change the route attributes.

[6.3.1 Establishing the Configuration Task](#)

[6.3.2 Creating a Route-Policy](#)

[6.3.3 \(Optional\) Setting an if-match Clause](#)

[6.3.4 \(Optional\) Setting an apply Clause](#)

[6.3.5 Checking the Configuration](#)

6.3.1 Establishing the Configuration Task

Applicable Environment

A Route-Policy is used to match routes or attributes of routes, and to change the attributes when the matching rules are met. The preceding filters can be used.

A Route-Policy consists of multiple nodes. Each node is classified into the following clauses:

- **If-match** clauses: define matching rules. The matching rules are used by the routes that match the Route-Policy. The matching objects refer to the attributes of the route.
- **Apply** clauses: specify actions, that is, configuration commands used to modify some attributes.

Pre-configuration Tasks

Before configuring a Route-Policy, complete the following tasks:

- [4.2.5 Checking the Configuration](#)
- 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

6.3.2 Creating a Route-Policy

Context

Do as follows on the S-switchs to which the Route-Policy is applied.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **route-policy route-policy-name { permit | deny } node node** command to create a node of the Route-Policy is created and enter the Route-Policy view.

The parameter **permit** specifies a node in a Route-Policy in **permit** mode. If a route matches the node, the S-switch performs the **apply** clauses and the matching is complete.

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.

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, the Route-Policy is denied.
- If all the nodes in the routing policy are in deny mode, all routes fail to match the Route-Policy.

----End

6.3.3 (Optional) Setting an if-match Clause

Context

Do as follows on the S-switchs to which the Route-Policy is applied.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **route-policy** *route-policy-name* { **permit** | **deny** } **node** *node* command to enter the Route-Policy view.

Step 3 Run the following command as required:

- Run the **if-match** **acl** *acl-number* command to match the ACL.
- Run the **if-match** **cost** *cost* command to match the cost of the route.
- Run the **if-match** **interface** *interface-type* *interface-number* command to match the outbound interface of the route.
- Run the **if-match** **ip** { **next-hop** | **route-source** } { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* } command to match the IPv4 route (the next hop or address).
- Run the **if-match** **ip-prefix** *ip-prefix-name* command to match the IP prefix list.

 **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 that latest configuration overrides the previous one.

- Match the type of the route:
 - Run the **if-match** **route-type** { **external-type1** | **external-type1or2** | **external-type2** | **internal** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2** } command to match the Open Shortest Path First (OSPF) routes.
 - Run the **if-match** **route-type** { **is-is-level-1** | **is-is-level-2** } command to match the Intermediate System-to-Intermediate System (IS-IS) routes.
- Run the **if-match** **tag** *tag* command to match the tag of the route.

A node can have multiple or no **if-match** clauses.

 **NOTE**

- For the same node in a Route-Policy, the relationship between the **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 the **if-match** clauses is "AND."
- If no **if-match** clause is specified, all the routes are matched.

----End

6.3.4 (Optional) Setting an apply Clause

Context

Do as follows on the S-switches to which the Route-Policy is applied.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **route-policy** *route-policy-name* { **permit** | **deny** } **node** *node* command to enter the Route-Policy view.

Step 3 Run the following command as required.

- Run the **apply** **cost** [+ | -] *cost* command to set the cost of the route.
- Run the following command as required.

- 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 the **apply ip-address next-hop ipv4-address** command to set the next hop address of the IPv4 route.
- Run the **apply preference preference** command to set the preference of a route.
- Run the **apply tag tag** command to set the tag of a route.

----End

6.3.5 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the Route-Policy.	display route-policy [<i>route-policy-name</i>]

Run the **display route-policy** command. You can view information about the route-policy named *expl*.

```
<Quidway> display route-policy
Route-policy : expl
permit : 10
```

6.4 Applying Filters to Received Routes

This section describes how to filter received routes.

[6.4.1 Establishing the Configuration Task](#)

[6.4.2 Filtering Routes Received by OSPF](#)

[6.4.3 Filtering Routes Received by IS-IS](#)

[6.4.4 Filtering Routes Received by BGP](#)

[6.4.5 Checking the Configuration](#)

6.4.1 Establishing the Configuration Task

Applicable Environment

After defining filters including the IP prefix list, ACL, and Route-Policy related to a routing policy, you need to import the filters to the protocols.

Use the **filter-policy** command in the protocol view and apply an ACL and an IP prefix list to filter received routes. Only the routes that meet the matching rules are received.

The **filter-policy import** command is used to filter 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 routes received from the neighbor and routes sent to the neighbor.

- Link state protocol

A link state protocol generates routes based on Link State Databases (LSDBs). The **filter-policy** command does not affect the Link State Advertisements (LSAs) or LSDBs.

The commands of **filter-policy import** and **filter-policy export** are different.

When a route is received, the **filter-policy import** command identifies the route that is added to a local routing table from a protocol routing table only. The command takes effect on the local core routing table without affecting the protocol routing table.

**NOTE**

You can run the **filter-policy** command and the **import-route** command with different parameters for OSPF, IS-IS, and BGP. For details, refer to related configurations.

Pre-configuration Tasks

Before applying filters to received routes, complete the following tasks:

- [4.2.5 Checking the Configuration](#)
- Configuring an ACL
- [4.3.3 Configuring RIP Preference](#)

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

6.4.2 Filtering Routes Received by OSPF

Context

Do as follows on the S-switches that run OSPF.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf [process-id]** command to start an OSPF process and enter the OSPF view.

Step 3 Run the **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **import** command to filter the received routes.

----End

6.4.3 Filtering Routes Received by IS-IS

Context

Do as follows on the S-switchs that run IS-IS.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **isis** [*process-id*] to start an IS-IS process and enter the IS-IS view.

Step 3 Run the **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **import** command to filter the received routes.

----End

6.4.4 Filtering Routes Received by BGP

Filtering Globally Received Routes

Context

Do as follows on the S-switchs that run BGP.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp** [*process-id*] command to start a BGP process and enter the BGP view.

Step 3 Run the **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **import** command to filter the routes received by BGP.

----End

Filtering Routes Received from the Peers

Context

Do as follows on the S-switchs that run BGP.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp** [*process-id*] command to start a BGP process and enter the BGP view.

- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **peer { group-name | ipv4-address } filter-policy acl-number import** command to filter the routes received from the peers.
- End

6.4.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the protocol routing table.	display ospf [process-id] routing display isis [process-id] route display bgp routing-table
Check information about the IP routing table.	display ip routing-table

Run the **display ip routing-table** command on the local S-switch. You can view that the routes that meet the matching rules are filtered or the actions defined by the **apply** clauses are performed.

6.5 Applying Filters to Advertised Routes

This section describes how to filter advertised routes.

[6.5.1 Establishing the Configuration Task](#)

[6.5.2 Filtering Routes Advertised by OSPF](#)

[6.5.3 Filtering Routes Advertised by IS-IS](#)

[6.5.4 Filtering Routes Advertised by BGP](#)

[6.5.5 Checking the Configuration](#)

6.5.1 Establishing the Configuration Task

Applicable Environment

After defining filters including the IP prefix list, ACL, and Route-Policy related to a routing policy, you need to import the filters to the protocols.

Use the **filter-policy** command in the protocol view and import an ACL and an IP prefix list to filter 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 routes received from the neighbor and routes sent to the neighbor.
- Link state protocol
A link state protocol generates routes based on LSDBs. The **filter-policy** command does not affect LSAs or 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 static routes. Only the LSAs or Link Switched Paths (LSPs) that are imported through the **filter-policy import** command are added to the LSDB. This does not affect LSAs advertised by other nodes.



NOTE

You can run the **filter-policy** command and the **import-route** command with different parameters for OSPF, IS-IS, and BGP. For details, refer to related configurations.

Pre-configuration Tasks

Before applying filters to advertised routes, complete the following tasks:

- [4.2.5 Checking the Configuration](#)
- Configuring an ACL
- [4.3.3 Configuring RIP Preference](#)

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

6.5.2 Filtering Routes Advertised by OSPF

Context

Do as follows on the S-switches that run OSPF.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf [process-id]** command to start an OSPF process and enter the OSPF view.

Step 3 Run the **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]] command to filter the advertised routes.

----End

6.5.3 Filtering Routes Advertised by IS-IS

Context

Do as follows on the S-switchs that run IS-IS.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **isis** [*process-id*] command to start an IS-IS process and enter the IS-IS view.

Step 3 Run the **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** command to filter the received routes.

----End

6.5.4 Filtering Routes Advertised by BGP

Filtering Globally Advertised Routes

Context

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.

Do as follows on the S-switchs that run BGP.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp as-number** command to enter the BGP view.

Step 3 (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.

Step 4 Run the **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]] command to filter the advertised routes.

- If *protocol* is specified, only the routes of the specified protocol are filtered.
- If *protocol* 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 is different in different protocol views:

- For the link state protocol, only the imported routes are filtered.
- For the DV protocol, the imported routes and routes discovered by the protocol are filtered.

----End

Filtering Routes Advertised to the Peers

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp as-number** command to enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **peer { group-name | ipv4-address } filter-policy acl-number export** command to filter the routes advertised to the peers.

----End

6.5.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the protocol routing table.	display ospf [process-id] routing display isis [process-id] route display bgp routing-table
Check information about the IP routing table.	display ip routing-table

Run the **display ip routing-table** command on the neighboring device. You can view that the routes that meet the matching rules set on the neighboring node are filtered or the actions defined by the **apply** clauses are performed.

6.6 Applying Filters to Imported Routes

This section describes how to filter imported routes.

[6.6.1 Establishing the Configuration Task](#)

[6.6.2 Applying a Route-Policy to Routes Imported by OSPF](#)

[6.6.3 Applying a Route-Policy to Routes Imported by IS-IS](#)

[6.6.4 Apply a Route-Policy to Routes Imported by BGP](#)

[6.6.5 Checking the Configuration](#)

6.6.1 Establishing the Configuration Task

Applicable Environment

After defining filters including the IP prefix list, ACL, and Route-Policy related to a routing policy, you need to import the filters to the protocols.

- 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** command to filter the routes. Only the routes that meet the matching rules are advertised.

NOTE

You can run the **filter-policy** command and the **import-route** command with different parameters for OSPF, IS-IS, and BGP. For details, refer to related configurations.

Pre-configuration Tasks

Before applying filters to imported routes, complete the following tasks:

- [4.2.5 Checking the Configuration](#)
- Configuring an ACL
- [4.3.3 Configuring RIP Preference](#)

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

6.6.2 Applying a Route-Policy to Routes Imported by OSPF

Prerequisite

Context

Do as follows on the S-switchs that run OSPF.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf [process-id]** command to start an OSPF process and enter the OSPF view.

- Step 3** Run the **import-route** *protocol* [*process-id*] [**cost** *cost*] [**route-policy** *route-policy-name*] command to import the external routes.
- End

6.6.3 Applying a Route-Policy to Routes Imported by IS-IS

Context

Do as follows on the S-switchs that run IS-IS.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] command to start an IS-IS process and enter the IS-IS view.
- Step 3** Run the **import-route** *protocol* [*process-id*] [**cost** *cost*] [**route-policy** *route-policy-name*] command to import the external routes.
- End

6.6.4 Apply a Route-Policy to Routes Imported by BGP

Context

Do as follows on the S-switchs that run BGP.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp** [*process-id*] command to start a BGP process and enter the BGP view.
- Step 3** (Optional) Run the **ipv4-family unicast** command to enter the BGP-IPv4 unicast address family view.
- Step 4** Run the **import-route** *protocol* [*process-id*] [**route-policy** *route-policy-name*] command to apply a Route-Policy to routes imported by BGP.
- End

6.6.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the protocol routing table.	display ospf [<i>process-id</i>] routing display isis [<i>process-id</i>] route display bgp routing-table

Action	Command
Check information about the IP routing table.	display ip routing-table

Run the **display ip routing-table** command on the local S-switch. You can view that the routes that meet the matching rules are filtered or the actions defined by the **apply** clauses are performed.

6.7 Controlling the Valid Time of a Routing Policy

This section describes how to adjust the valid time of the Route-Policy.

6.7.1 Establishing the Configuration Task

6.7.2 Setting the Delay for Applying the Routing Policy

6.7.3 Checking the Configuration

6.7.1 Establishing the Configuration Task

Applicable Environment

When the configurations of multiple matched routing policies change, the Routing Management (RM) immediately notifies various protocols of re-applying routing policies, if the configuration of a routing policy is complete. The incomplete routing policy may cause route flapping.

The S-switch provides the following rules for processing changes of a routing policy:

- If the valid time of the routing policy is set, RM does not notify various protocols of processing the changes immediately, when the commands used to configure the routing policy change. Instead, RM waits for a period (by default, the period is 0), and then notifies various protocols of applying the changed routing policy.
- If the routing policy changes again during the waiting time, RM resets the timer.

You can run the related commands to set the waiting time as required.

Pre-configuration Tasks

None.

Data Preparation

To set the valid time of a routing policy, you need the following data.

No.	Data
1	Delay for applying the routing policy

6.7.2 Setting the Delay for Applying the Routing Policy

Context

Do as follows on the S-switchs on which the delay for applying the routing policy needs to be changed.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **route-policy-change notify-delay *delay-time*** command to set the delay for applying the routing policy.

The value ranges from 0 to 180, in seconds. By default, it is 0 seconds. That is, RM notifies the protocol of applying a new routing policy after the routing policy changes.

The polices affected by the timer are ACL, IP prefix list, and Route-Policy.

Step 3 (Optional) Run the **refresh bgp all** command to configure BGP to apply the new routing policy.

If you want to know the effect of the policy filtering, you can run the command to configure BGP to apply new policies immediately.

----End

6.7.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the delay for applying the routing policy.	display current-configuration include notify-delay

Run the **display current-configuration** command. You can view the delay for applying the routing policy.

```
<Quidway> display current-configuration | include notify-delay
route-policy-change notify-delay 10
```

6.8 Configuration Examples

This section provides several configuration examples for the routing policy.

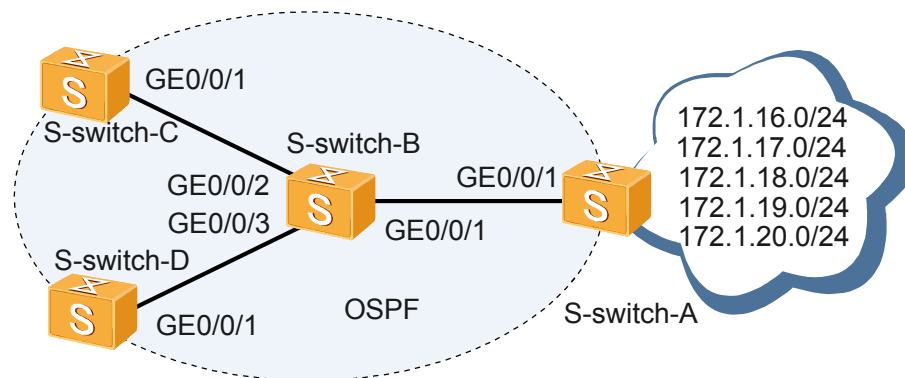
6.8.1 Example for Filtering Received and Advertised Routes

6.8.1 Example for Filtering Received and Advertised Routes

Networking Requirements

As shown in **Figure 6-1**, in a network that runs OSPF, S-switch-A receives routes from the Internet and provides some of these routes for S-switch-B. S-switch-A is required to provide 172.1.17.0/24, 172.1.18.0/24, and 172.1.19.0/24 to S-switch-B. S-switch-C receives only 172.1.18.0/24 and S-switch-D receives all routes provided by S-switch-B.

Figure 6-1 Networking diagram for filtering received and advertised routes



S-switch	Interface	VLANIF Interface	IP Address
S-switch-A	GigabitEthernet 0/0/1	VLANIF 10	192.168.1.1/24
S-switch-B	GigabitEthernet 0/0/1	VLANIF 10	192.168.1.2/24
S-switch-B	GigabitEthernet 0/0/2	VLANIF 20	192.168.2.1/24
S-switch-B	GigabitEthernet 0/0/3	VLANIF 30	192.168.3.1/24
S-switch-C	GigabitEthernet 0/0/1	VLANIF 20	192.168.2.2/24
S-switch-D	GigabitEthernet 0/0/1	VLANIF 30	192.168.3.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create the ID of the VLAN to which each interface belongs.
2. Assign an IP address to each VLANIF interface.
3. Configure basic OSPF functions on S-switch-A, S-switch-B, S-switch-C, and S-switch-D.
4. Configure static routes on S-switch-A and import these routes into OSPF.
5. Configure the policy for advertising routes on S-switch-A and check the filtering result on S-switch-B.
6. Configure the policy for receiving routes on S-switch-C and check the filtering result on S-switch-C.

Data Preparation

To complete the configuration, you need the following data:

- Five static routes imported by S-switch-A
- S-switch-A, S-switch-B, S-switch-C, and S-switch-D located in Area 0, that is, the backbone area

- Names of the IP prefix list and route to be filtered

Configuration Procedure

- Create a VLAN to which each interface belongs.
The configuration details are not mentioned here.
- Assign an IP address to each VLANIF interface.
The configuration details are not mentioned here.
- Configure basic OSPF functions.

Configure S-switch-A.

```
[S-switch-A] ospf
[S-switch-A-ospf-1] area 0
[S-switch-A-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[S-switch-A-ospf-1-area-0.0.0.0] quit
[S-switch-A-ospf-1] quit
```

Configure S-switch-B.

```
[S-switch-B] ospf
[S-switch-B-ospf-1] area 0
[S-switch-B-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[S-switch-B-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[S-switch-B-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[S-switch-B-ospf-1-area-0.0.0.0] quit
[S-switch-B-ospf-1] quit
```

Configure S-switch-C.

```
[S-switch-C] ospf
[S-switch-C-ospf-1] area 0
[S-switch-C-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[S-switch-C-ospf-1-area-0.0.0.0] quit
[S-switch-C-ospf-1] quit
```

Configure S-switch-D.

```
[S-switch-D] ospf
[S-switch-D-ospf-1] area 0
[S-switch-D-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[S-switch-D-ospf-1-area-0.0.0.0] quit
[S-switch-D-ospf-1] quit
```

- Configure five static routes on S-switch-A and import these routes to OSPF.

```
[S-switch-A] ip route-static 172.1.16.0 24 NULL0
[S-switch-A] ip route-static 172.1.17.0 24 NULL0
[S-switch-A] ip route-static 172.1.18.0 24 NULL0
[S-switch-A] ip route-static 172.1.19.0 24 NULL0
[S-switch-A] ip route-static 172.1.20.0 24 NULL0
[S-switch-A] ospf
[S-switch-A-ospf-1] import-route static
[S-switch-A-ospf-1] quit
```

Check the IP routing table on S-switch-B. You view that the five static routes are imported to OSPF.

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

Routing Tables: Public

Destinations : 13 Routes : 13

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
192.168.1.0/24	Direct	0	0	D	192.168.1.2	Vlanif10
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 Vlanif30
192.168.2.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
192.168.3.0/24 Direct 0 0 D 192.168.3.1 Vlanif20
192.168.3.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0
172.1.16.0/24 O_ASE 150 1 D 192.168.1.1 Vlanif10
172.1.17.0/24 O_ASE 150 1 D 192.168.1.1 Vlanif10
172.1.18.0/24 O_ASE 150 1 D 192.168.1.1 Vlanif10
172.1.19.0/24 O_ASE 150 1 D 192.168.1.1 Vlanif10
172.1.20.0/24 O_ASE 150 1 D 192.168.1.1 Vlanif10

```

5. Configure the policy for advertising routes.

Set an IP prefix list named a2b on S-switch-A.

```

[S-switch-A] ip ip-prefix a2b index 10 permit 172.1.17.0 24
[S-switch-A] ip ip-prefix a2b index 20 permit 172.1.18.0 24
[S-switch-A] ip ip-prefix a2b index 30 permit 172.1.19.0 24

```

Set a policy for advertising routes on S-switch-A and use a2b to filter routes.

```

[S-switch-A] ospf
[S-switch-A-ospf-1] filter-policy ip-prefix a2b export static

```

Check the routing table on S-switch-B. You can view that S-switch-B receives only three routes defined in a2b.

```

[S-switch-B] 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
-----
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
192.168.1.0/24     Direct 0    0      D  192.168.1.2         Vlanif10
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         Vlanif30
192.168.2.1/32     Direct 0    0      D  127.0.0.1           InLoopBack0
192.168.3.0/24     Direct 0    0      D  192.168.3.1         Vlanif20
192.168.3.1/32     Direct 0    0      D  127.0.0.1           InLoopBack0
172.1.17.0/24      O_ASE 150  1      D  192.168.1.1         Vlanif10
172.1.18.0/24      O_ASE 150  1      D  192.168.1.1         Vlanif10
172.1.19.0/24      O_ASE 150  1      D  192.168.1.1         Vlanif10

```

6. Configure the policy for receiving routes.

Set an IP prefix list named in on S-switch-C.

```

[S-switch-C] ip ip-prefix in index 10 permit 172.1.18.0 24

```

Set a policy for receiving routes on S-switch-C and use in to filter routes.

```

[S-switch-C] ospf
[S-switch-C-ospf-1] filter-policy ip-prefix in import

```

Check the routing table on S-switch-C. You can find that S-switch-C in the local core routing table receives only one route defined in in.

```

[S-switch-C] 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
192.168.2.0/24     Direct 0    0      D  192.168.2.2         Vlanif20
192.168.2.2/32     Direct 0    0      D  127.0.0.1           InLoopBack0
172.1.18.0/24      O_ASE 150  1      D  192.168.2.1         Vlanif20

```

Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
vlan batch 10
#
interface Vlanif10
ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
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 S-switch-B

```
#
sysname S-switch-B
#
vlan batch 10 20 30
#
interface Vlanif10
ip address 192.168.1.2 255.255.255.0
#
interface Vlanif20
ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 30
#
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 S-switch-C

```
#
sysname S-switch-C
#
vlan batch 20
#
```

```
interface Vlanif20
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 20
#
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 S-switch-D

```
#
 sysname S-switch-D
#
 vlan batch 30
#
interface Vlanif30
 ip address 192.168.3.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 30
#
ospf 1
 area 0.0.0.0
 network 192.168.3.0 0.0.0.255
#
return
```

7 MCE Configuration

About This Chapter

Generally, a Customer Edge (CE) can connect to only one Virtual Private Network (VPN). If multiple VPNs need to be divided, multiple CEs are required. The Multi-VPN-Instance CE (MCE) technology enables a CE to be connected to multiple VPNs. This isolates services between different VPNs and reduces the investment on network devices.

[7.1 Introduction to MCE](#)

MCE isolates different services or users by using the route multi-instance on the CE.

[7.2 Configuring a VPN Instance](#)

This section describes how to configure a VPN instance.

[7.3 Configuring a Route Multi-Instance Between an MCE and a Site](#)

This section describes how to configure static routes, RIP, OSPF, IS-IS, and BGP between an MCE and a site.

[7.4 Configuring a Route Multi-Instance Between an MCE and a PE](#)

This section describes how to configure static routes, RIP, OSPF, IS-IS, and BGP between an MCE and a PE.

[7.5 MCE Configuration Examples](#)

This section provides several configuration examples of MCE.

7.1 Introduction to MCE

MCE isolates different services or users by using the route multi-instance on the CE.

7.1.1 MCE Overview

MCE isolates different services or users by using the route multi-instance on the CE.

7.1.2 MCE Functions Supported by the S-switch

When the S-switch functions as an MCE, multiple routing protocols can be run between an MCE and a PE, and between an MCE and a site, including static routes, the Routing Information Protocol (RIP), the Open Shortest Path First (OSPF), the Intermediate System-to-Intermediate System (IS-IS), and BGP.

7.1.3 Logical Relationships Between Configuration Tasks

The following lists the logical relationships between several configuration tasks of MCE functions.

7.1.4 Update History

This section describes the function that varies with the version of the product.

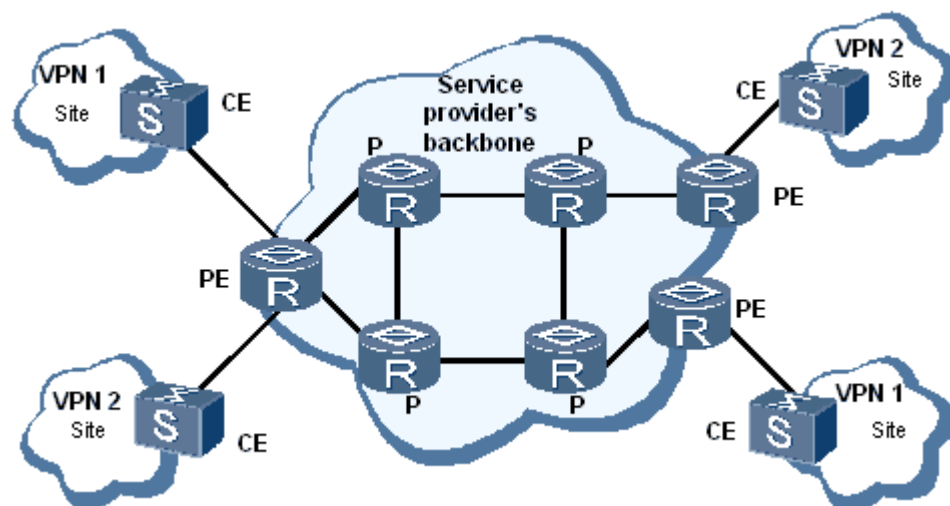
7.1.1 MCE Overview

MCE isolates different services or users by using the route multi-instance on the CE.

Background

The Border Gateway Protocol (BGP) or Multiprotocol Label Switching (MPLS) IP VPN technology transmits data of a private network in a public network by setting up tunnels. The traditional BGP or MPLS IP VPN technology, however, requires that each VPN instance should use a CE to connect a Provider Edge (PE), as shown in [Figure 7-1](#).

Figure 7-1 Traditional BGP or MPLS IP VPN model

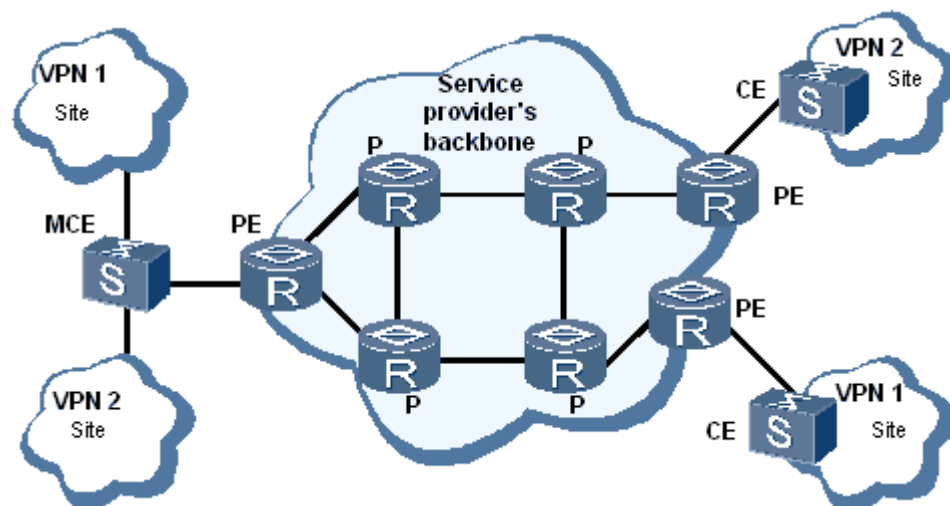


With increasing diversification of user services and higher requirements on the security, multiple VPNs are required in a private network in most cases and services of different VPNs need to be isolated. In this case, using a CE for each VPN increases the device expenditure and maintenance

cost; the security of data cannot be ensured if multiple VPNs share a CE and a route forwarding table.

As shown in **Figure 7-2**, MCE can effectively solve issues of security of the data and network costs in a VPN. MCE isolates services of different VPNs by binding VLANIF interfaces to VPNs, and creating and maintaining an independent multi-VRF table for each VPN.

Figure 7-2 Typical MCE networking diagram



Basic Concepts

- **CE**
An edge device that is located in a user network. A CE provides interfaces that are directly connected to the Service Provider (SP) network. A CE can be a router, a switch, or a host. In most situations, a CE neither senses a VPN nor supports MPLS.
- **MCE**
A CE configured with MCE functions. An MCE can connect to multiple VPNs whose services are isolated completely.
- **PE**
An edge router that is located in an SP network. A PE is an edge device in the SP network and is directly connected to the CE and MCE. In an MPLS network, PEs process all VPN services.
- **Provider (P)**
A backbone router that is located in an SP network. A P device is not directly connected to CEs. The P devices only need the basic MPLS forwarding capability, without maintaining information about a VPN.
- **Site**
A group of IP systems with IP connectivity between each other. Their connectivity need not be implemented through an SP network. The site is connected to the SP network through a CE or an MCE.

7.1.2 MCE Functions Supported by the S-switch

When the S-switch functions as an MCE, multiple routing protocols can be run between an MCE and a PE, and between an MCE and a site, including static routes, the Routing Information

Protocol (RIP), the Open Shortest Path First (OSPF), the Intermediate System-to-Intermediate System (IS-IS), and BGP.

Multiple Routing Protocols Run Between an MCE and a PE

When the S-switch functions as an MCE, multiple routing protocols can be run between the S-switch and a PE, including:

- Static routes
- RIP
- OSPF
- IS-IS
- BGP

Multiple Routing Protocols Run Between an MCE and a Site

When the S-switch functions as an MCE, multiple routing protocols can be run between the S-switch and a site, including:

- Static routes
- RIP
- OSPF
- IS-IS
- BGP

7.1.3 Logical Relationships Between Configuration Tasks

The following lists the logical relationships between several configuration tasks of MCE functions.

If you want to...	Then...
Configure MCE functions	<ul style="list-style-type: none"> • 7.2 Configuring a VPN Instance • 7.3 Configuring a Route Multi-Instance Between an MCE and a Site • 7.4 Configuring a Route Multi-Instance Between an MCE and a PE <p>The last two configuration tasks are optional and can be configured as required.</p>

7.1.4 Update History

This section describes the function that varies with the version of the product.

Version	Revision
V100R002C01B050	This is the first release.

7.2 Configuring a VPN Instance

This section describes how to configure a VPN instance.

[7.2.1 Establishing the Configuration Task](#)

[7.2.2 Creating a VPN instance](#)

[7.2.3 Binding a VPN Instance to a VLANIF Interface](#)

[7.2.4 Checking the Configuration](#)

7.2.1 Establishing the Configuration Task

Applicable Environment

To connect a CE to multiple VPNs and isolate services of these VPNs, you need to configure MCE functions. Before configuring MCE functions, you need to configure VPN instances on an MCE and a PE.

Pre-configuration Tasks

Before configuring a VPN instance, complete the following tasks:

- Creating a VLAN on the MCE and adding the interface connecting the site and PE to the VLAN
- Creating a VLAN on the PE and adding the sub-interface connecting the MCE to the VLAN
- Creating a VLAN on the device connected to the MCE in a site and adding the interface connected to the MCE on the device to the VLAN

Data Preparation

To configure a VPN instance, you need the following data.

No.	Data
1	Name of the VPN instance
2	Route Distinguisher (RD) of the VPN instance
3	(Optional) Description of the VPN instance
4	(Optional) Maximum number of routes supported by the VPN instance
5	ID of the VLAN corresponding to the VPN instance

7.2.2 Creating a VPN instance

Context

Do as follows on the MCE.

You need to perform similar configurations on the PE; however, configuration commands and methods may be different because device manufacturers and types are different. For details, refer to manuals of corresponding products.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ip vpn-instance** *vpn-instance-name* command to create a VPN instance and enter the VPN instance view.



NOTE

The name of a VPN instance is case-sensitive. For example, "vpn1" and "VPN1" are taken as different VPN instances.

Step 3 Run the **route-distinguisher** *route-distinguisher* command to configure an RD for the VPN instance.

The RD does not have a default value; therefore, you must configure an RD when creating a VPN instance.

A VPN instance takes effect only after it is configured with an RD. The RDs of different VPN instances on a device should be different.

Before configuring an RD, you can configure only the description.

Step 4 (Optional) Run the **description** *description-information* command to configure the description for the VPN instance.

By default, no description is configured for a VPN instance.

The description is similar to that of the host name and interface, which can be used to record information about the relationship between a VPN instance and a VPN.

Step 5 (Optional) Run the **routing-table limit** *number* { *alert-percent* | **simply-alert** } command to set the maximum number of routes supported by the VPN instance.

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

To prevent excessive routes from being imported, set the maximum number of routes supported by a VPN instance.

----End

7.2.3 Binding a VPN Instance to a VLANIF Interface

Context

Do as follows on the MCE.

You also need to bind the sub-interface connected to the MCE to a VPN instance on a PE. For details, refer to manuals of corresponding products.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface vlanif *vlan-id*** command to enter the VLANIF interface view.
- Step 3** Run the **ip binding vpn-instance *vpn-instance-name*** command to bind the VPN instance to a VLANIF interface.

By default, a VLANIF interface is not bound to any VPN instance.



NOTE

The **ip binding vpn-instance** command deletes Layer 3 features such as the IP address and routing protocols configured on the interface. To use these features, you need to reconfigure them.

- Step 4** Run the **ip address *ip-address* { *mask* | *mask-length* }** command to assign an IP address to the VLANIF interface.

----End

7.2.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about a VPN instance.	display ip vpn-instance [<i>verbose</i>] [<i>vpn-instance-name</i>]

Run the **display ip vpn-instance** command. If the configuration is correct, you can view:

- VPN instance created correctly
- Name of the VPN instance
- RD
- Description
- Maximum number of routes supported by the VPN instance
- Interface configured correctly

```
<Quidway> display ip vpn-instance verbose
Total VPN-Instances configured : 1

VPN-Instance Name and ID : vpn1, 1
Create date : 2008/09/10 16:58:42
Up time : 0 days, 21 hours, 42 minutes and 10 seconds
Route Distinguisher : 101:1
Description : vpn for areal
Maximum Routes Limit : 2000
Thresh Hold Value(%): 80
Interfaces : Vlanif55
```

7.3 Configuring a Route Multi-Instance Between an MCE and a Site

This section describes how to configure static routes, RIP, OSPF, IS-IS, and BGP between an MCE and a site.

For configuring a route multi-instance between an MCE and a site, [7.3.2 \(Optional\) Configuring a Static Route Between an MCE and a Site](#) to [7.3.6 \(Optional\) Configuring BGP Between an MCE and a Site](#) are optional and can be configured as required.

[7.3.1 Establishing the Configuration Task](#)

[7.3.2 \(Optional\) Configuring a Static Route Between an MCE and a Site](#)

[7.3.3 \(Optional\) Configuring RIP Between an MCE and a Site](#)

[7.3.4 \(Optional\) Configuring OSPF Between an MCE and a Site](#)

[7.3.5 \(Optional\) Configuring IS-IS Between an MCE and a Site](#)

[7.3.6 \(Optional\) Configuring BGP Between an MCE and a Site](#)

[7.3.7 Checking the Configuration](#)

7.3.1 Establishing the Configuration Task

Applicable Environment

To connect a CE to multiple VPNs and isolate services of these VPNs, you need to configure MCE functions. Before configuring MCE functions, you need to perform the task of [7.2 Configuring a VPN Instance](#) on the MCE and PE and then configure a route multi-instance between an MCE and a site.

Pre-configuration Tasks

Before configuring a route multi-instance between an MCE and a site, complete the following task:

- [7.2 Configuring a VPN Instance](#)

Data Preparation

To configure a route multi-instance between an MCE and a site, you need the following data.

No.	Data
1	Name of the VPN instance
2	(Optional) Destination address of a static route to the site, name of the destination VPN instance, mask or mask length, next hop IP address, priority of the route, and description of the route

No.	Data
3	(Optional) RIP process number, address of the network segment where the VLANIF interface bound to the VPN instance is located, type and process number of the routing protocol run between an MCE and a PE, cost of the imported route, and name of the routing policy during route importing
4	(Optional) OSPF process number, router ID of OSPF, area ID of OSPF, address of the network segment where the VLANIF interface bound to the VPN instance is located, type and process number of the routing protocol run between an MCE and a PE, cost of the imported route, metric of the imported route, tag in the external Link State Advertisement (LSA) of the imported route, and name of the routing policy during route importing
5	(Optional) IS-IS process number, Network Entity Title (NET) of the IS-IS process, number of the VLANIF interface bound to the VPN instance, type and process number of the routing protocol run between an MCE and a PE, type and value of the cost of the imported route, administrative tag of the imported route, and level of the routing table for storing the imported route
6	(Optional) Autonomous System (AS) number, IP address of the VLANIF interface connecting a CE and an MCE, type and process number of the routing protocol run between an MCE and a PE, Multi-Exit Discriminator (MED) of the imported route, and name of the routing policy during route importing

7.3.2 (Optional) Configuring a Static Route Between an MCE and a Site

Context

Do as follows on the MCE.

You need to configure only routing protocols on a device in a site.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ip route-static vpn-instance** *vpn-source-name destination-address { mask | mask-length } { interface-type interface-number [gateway-address] | vpn-instance vpn-destination-name gateway-address | gateway-address }* [**preference** *preference*] [**track bfd-session** *cfg-name*] [**description** *description*] command to configure a static route to the site.

You must specify the next hop address on the local device.

----End

7.3.3 (Optional) Configuring RIP Between an MCE and a Site

Context

Do as follows on the MCE.

You need to configure only routing protocols on a device in a site.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **rip** [*process-id*] **vpn-instance** *vpn-instance-name* command to create and enable a RIP process used by a VPN instance and enter the RIP view.
- Step 3** Run the **network** *network-address* command to enable RIP routes on the network segment where the IP address of the VLANIF interface bound to the VPN instance belongs.
- Step 4** (Optional) Run the **import-route** *protocol* [*process-id*] [**cost** *cost*] [**route-policy** *route-policy-name*] command to import routes from other routing protocols.
If another routing protocol is run between an MCE and a PE in this VPN, you need to perform this step.
- End


7.3.4 (Optional) Configuring OSPF Between an MCE and a Site

Context

Do as follows on the MCE.

You need to configure only routing protocols on a device in a site.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] * command to create an OSPF process used by a VPN instance and enter the OSPF view.
-  **NOTE**
In this step, you must specify **vpn-instance** *vpn-instance-name*.
- Step 3** Run the **area** { *area-id* | *area-id-address* } command to create an OSPF area and enter the OSPF area view.
- Step 4** Run the **network** *network-address* command to enable OSPF routes on the network segment where the IP address of the VLANIF interface bound to the VPN instance belongs.
- Step 5** (Optional) Run the **import-route** *protocol* [*process-id*] [**cost** *cost* | **tag** *tag* | **type** *type* | **route-policy** *route-policy-name*] * command to import routes from other routing protocols.
If another routing protocol is run between an MCE and a PE in this VPN, you need to perform this step.
- End

7.3.5 (Optional) Configuring IS-IS Between an MCE and a Site

Context

Do as follows on the MCE.

You need to configure only routing protocols on a device in a site.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **isis** [*process-id*] **vpn-instance** *vpn-instance-name* command to create an IS-IS process used by a VPN instance and enter the IS-IS view.
- Step 3** Run the **network-entity** *net* command to configure an NET.
- By default, no NET is configured for an IS-IS process.
- Step 4** Run the **interface** **vlanif** *vlan-id* command to enter the view of the VLANIF interface bound to the VPN instance.
- Step 5** Run the **isis enable** [*process-id*] command to enable IS-IS on the VLANIF interface.
- By default, IS-IS is disabled on a VLANIF interface.
- Step 6** 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 routes from other routing protocols.
- If another routing protocol is run between an MCE and a PE in this VPN, you need to perform this step.
- End

7.3.6 (Optional) Configuring BGP Between an MCE and a Site

Context

Do as follows on the MCE.

You need to configure only routing protocols on a device in a site.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bgp** *as-number* command to enable BGP and enter the BGP view.
- By default, BGP is disabled.
- Step 3** Run the **ipv4-family** **vpn-instance** *vpn-instance-name* command to enter the BGP-VPN instance view.
- Step 4** Run the **peer** *ipv4-address* **as-number** *as-number* command to configure the device connected to an MCE in a site as the peer of a VPN private network.
- Step 5** (Optional) Run the **import-route** **protocol** [*process-id*] [**med** *med* | **route-policy** *route-policy-name*] * command to import routes from other routing protocols.
- If another routing protocol is run between an MCE and a PE in this VPN, you need to perform this step.
- Step 6** Run the **peer** *ipv4-address* **allow-as-loop** [*number*] command to configure BGP to allow routing loops.

By default, routing loops are denied.



NOTE

Generally, BGP detects routing loops through the AS number. Assume that BGP is run between an MCE and a site. When the MCE advertises the routing information with the AS number to the site, the MCE cannot receive this routing update from the site because the routing update carries the AS number. In this case, you need to configure BGP to allow routing loops.

----End

7.3.7 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the routing table of the VPN instance.	display ip routing-table vpn-instance <i>vpn-instance-name</i> [verbose]

Run the **display ip routing-table vpn-instance** command on the MCE. If you can view the route to the local VPN in the display, it means that the configuration succeeds. Take RIP used between an MCE and a site as an example. The information is displayed as follows:

```
[MCE] display ip routing-table vpn-instance vpnb
Route Flags: R - relay, D - download to fib
```

```
-----
Routing Tables: vpnb
Destinations : 7          Routes : 7

Destination/Mask    Proto  Pre  Cost    Flags NextHop          Interface
-----
172.16.0.0/16      Direct 0    0        D  172.16.1.2        Vlanif10
172.16.1.1/32      Direct 0    0        D  172.16.1.1        Vlanif10
172.16.1.2/32      Direct 0    0        D  127.0.0.1         InLoopBack0
172.18.0.0/16      Direct 0    0        D  172.18.1.2        Vlanif30
172.18.1.1/32      Direct 0    0        D  172.18.1.1        Vlanif30
172.18.1.2/32      Direct 0    0        D  127.0.0.1         InLoopBack0
192.168.0.0/16     RIP    100  1        D  172.16.1.1        Vlanif10
```

7.4 Configuring a Route Multi-Instance Between an MCE and a PE

This section describes how to configure static routes, RIP, OSPF, IS-IS, and BGP between an MCE and a PE.

For configuring a route multi-instance between an MCE and a PE, [7.4.2 \(Optional\) Configuring a Static Route Between an MCE and a PE](#) to [7.4.6 \(Optional\) Configuring BGP Between an MCE and a PE](#) are optional and can be configured as required.

[7.4.1 Establishing the Configuration Task](#)

[7.4.2 \(Optional\) Configuring a Static Route Between an MCE and a PE](#)

[7.4.3 \(Optional\) Configuring RIP Between an MCE and a PE](#)

[7.4.4 \(Optional\) Configuring OSPF Between an MCE and a PE](#)

[7.4.5 \(Optional\) Configuring IS-IS Between an MCE and a PE](#)

7.4.6 (Optional) Configuring BGP Between an MCE and a PE

7.4.7 Checking the Configuration

7.4.1 Establishing the Configuration Task

Applicable Environment

To connect a CE to multiple VPNs and isolate services of these VPNs, you need to configure MCE functions. Before configuring MCE functions, you need to perform the task of [7.2 Configuring a VPN Instance](#) on the MCE and PE and then configure a route multi-instance between the MCE and PE.

Pre-configuration Tasks

Before configuring a route multi-instance between an MCE and a PE, complete the following task:

- [7.2 Configuring a VPN Instance](#)

Data Preparation

To configure a route multi-instance between an MCE and a PE, you need the following data.

No.	Data
1	Name of the VPN instance
2	(Optional) Destination address of a static route to the PE, name of the destination VPN instance, mask or mask length, next hop IP address, priority of the route, and description of the route
3	(Optional) RIP process number, address of the network segment where the VLANIF interface bound to the VPN instance is located, type and process number of the routing protocol run between an MCE and a site, cost of the imported route, and name of the routing policy used during route importing
4	(Optional) OSPF process number, router ID of OSPF, area ID of OSPF, address of the network segment where the VLANIF interface bound to the VPN instance is located, type and process number of the routing protocol run between an MCE and a site, cost of the imported route, metric of the imported route, tag in the external LSA of the imported route, and name of the routing policy during route importing
5	(Optional) IS-IS process number, NET of the IS-IS process, number of the VLANIF interface bound to the VPN instance, type and process number of the routing protocol run between an MCE and a site, type and value of the cost of the imported route, administrative tag of the imported route, and level of the routing table for storing the imported route

No.	Data
6	(Optional) AS number, IP address of the VLANIF interface connecting a CE and an MCE, type and process number of the routing protocol run between an MCE and a site, MED of the imported route, and name of the routing policy during route importing

7.4.2 (Optional) Configuring a Static Route Between an MCE and a PE

Context

Do as follows on the MCE.

You can use a static route on a PE, and can also use RIP, OSPF, IS-IS, or BGP. For details, refer to manuals of corresponding products.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **ip route-static vpn-instance vpn-source-name destination-address { mask | mask-length } { interface-type interface-number [gateway-address] | vpn-instance vpn-destination-name gateway-address | gateway-address } [preference preference] [track bfd-session cfg-name] [description description]** command to configure a static route to a PE.

You must specify the next hop address on the local device.

----End

7.4.3 (Optional) Configuring RIP Between an MCE and a PE

Context

Do as follows on the MCE.

You need to perform similar configurations on a PE. For details, refer to manuals of corresponding products.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **rip [process-id] vpn-instance vpn-instance-name** command to create and enable a RIP process used by a VPN instance and enter the RIP view.
- Step 3** Run the **network network-address** command to enable RIP routes on the network segment where the IP address of the VLANIF interface bound to the VPN instance belongs.
- Step 4** (Optional) Run the **import-route protocol [process-id] [cost cost] [route-policy route-policy-name]** command to import routes from other routing protocols.

If another routing protocol is run between an MCE and a site in this VPN, you need to perform this step.

----End

7.4.4 (Optional) Configuring OSPF Between an MCE and a PE

Context

Do as follows on the MCE.

You need to perform similar configurations on a PE. For details, refer to manuals of corresponding products.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] * command to create an OSPF process used by a VPN instance and enter the OSPF view.



NOTE

In this step, you must specify **vpn-instance** *vpn-instance-name*.

Step 3 Run the **area** { *area-id* | *area-id-address* } command to create an OSPF area and enter the OSPF area view.

Step 4 Run the **network** *network-address* command to enable OSPF routes on the network segment where the IP address of the VLANIF interface bound to the VPN instance belongs.

Step 5 (Optional) Run the **import-route** *protocol* [*process-id*] [**cost** *cost* | **tag** *tag* | **type** *type* | **route-policy** *route-policy-name*] * command to import routes from other routing protocols.

If another routing protocol is run between an MCE and a site in this VPN, you need to perform this step.

----End

7.4.5 (Optional) Configuring IS-IS Between an MCE and a PE

Context

Do as follows on the MCE.

You need to perform similar configurations on a PE. For details, refer to manuals of corresponding products.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **isis** [*process-id*] **vpn-instance** *vpn-instance-name* command to create an IS-IS process used by a VPN instance and enter the IS-IS view.

Step 3 Run the **network-entity** *net* command to configure a NET.

By default, no NET is configured for an IS-IS process.

Step 4 Run the **interface vlanif** *vlan-id* command to enter the view of the VLANIF interface bound to the VPN instance.

Step 5 Run the **isis enable** [*process-id*] command to enable IS-IS on the VLANIF interface.

By default, IS-IS is disabled on a VLANIF interface.

Step 6 (Optional) 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 routes from other routing protocols.

If another routing protocol is run between an MCE and a site in this VPN, you need to perform this step.

----End

7.4.6 (Optional) Configuring BGP Between an MCE and a PE

Context

Do as follows on the MCE.

You need to perform similar configurations on a PE. For details, refer to manuals of corresponding products.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp as-number** command to start BGP and enter the BGP view.

By default, BGP is disabled.

Step 3 Run the **ipv4-family vpn-instance** *vpn-instance-name* command to enter the BGP-VPN instance view.

Step 4 Run the **peer** *ipv4-address* **as-number** *as-number* command to configure the device connected to an MCE in a site as the peer of a VPN private network.

Step 5 (Optional) Run the **import-route protocol** [*process-id*] [**med** *med* | **route-policy** *route-policy-name*] * command to import routes from other routing protocols.

If another routing protocol is run between an MCE and a site in this VPN, you need to perform this step.

----End

7.4.7 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the routing table of the VPN instance.	display ip routing-table vpn-instance <i>vpn-instance-name</i> [verbose] NOTE The preceding command is used to check the routing table of the VPN instance on Huawei Quidway CX600 that functions as a PE. In actual networks, the command used to check the routing table of the VPN instance varies with the type of a PE. For details on using these commands, refer to manuals of corresponding products.

Run the **display ip routing-table vpn-instance** command on the PE, and you can find the routes to the local VPN. Take Huawei Quidway CX600 as an example. The information is displayed as follows:

```
[PE1] display ip routing-table vpn-instance vpnb
Route Flags: R - relay, D - download to fib
-----
Routing Tables: vpnb
          Destinations : 5          Routes : 5

Destination/Mask    Proto  Pre  Cost    Flags NextHop          Interface
172.18.0.0/16       Direct 0    0        D  172.18.1.1        GigabitEthernet8/
0/0.1
172.18.1.1/32       Direct 0    0        D  127.0.0.1         InLoopBack0
172.18.255.255/32   Direct 0    0        D  127.0.0.1         InLoopBack0
192.168.0.0/16      O_ASE  150  1        D  172.16.1.1        GigabitEthernet8/
0/0.1
255.255.255.255/32 Direct 0    0        D  127.0.0.1         InLoopBack0
```

7.5 MCE Configuration Examples

This section provides several configuration examples of MCE.

7.5.1 Example for Configuring MCE

7.5.1 Example for Configuring MCE

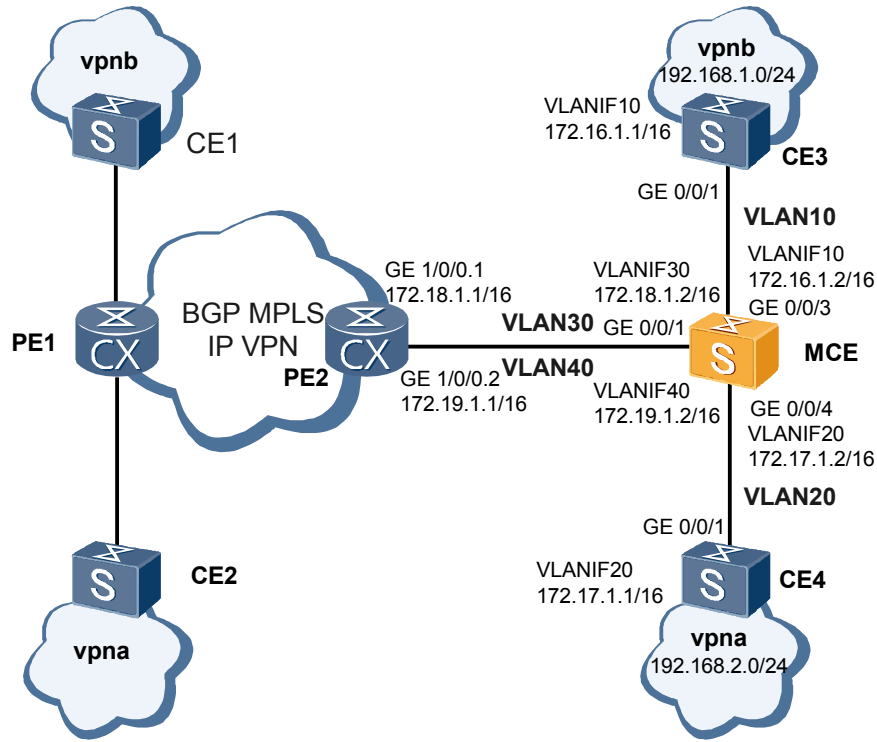
Networking Requirements

As shown in [Figure 7-3](#), the networking is as follows:

- CE1, CE2, CE3, and CE4 are edge devices of the VPN.
- CE1 and CE3 belong to a VPN instance named **vpnb**, and CE2 and CE4 belong to a VPN instance named **vpna**.
- PE1 and PE2 are edge routers of the backbone network. PE2 is Huawei Quidway CX600. BGP or MPLS IP VPN is configured on the backbone network between PE1 and PE2.
- The MCE functions as a Multi-VPN-Instance CE located in the user network.
- RIP is run between the MCE, CE3, and CE4.
- OSPF is run between the MCE and PE.

It is required that route isolation between VPNs be implemented on the MCE and routes of VPNs be advertised to the PE through OSPF.

Figure 7-3 Networking diagram for configuring MCE



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs on the MCE, PE2, CE3, and CE4, and add the interfaces connecting these devices to the VLANs.
2. Create and configure VPN instances on the MCE and PE2.
3. Configure the OSPF route multi-instance on the MCE and PE2.
4. Configure RIP between the MCE and CE3, and between the MCE and CE4.

Data Preparation

To complete the configuration, you need the following data:

- VLANs between the MCE, PE, CE3, and CE4, as shown in [Figure 7-3](#)
- IP addresses of VLANIF interfaces, as shown in [Figure 7-3](#)

Configuration Procedure

1. Create VLANs on the MCE, PE2, CE3, and CE4, and add the interfaces connecting these devices to the VLANs.

Create VLANs on the MCE.

```
<Quidway> system-view
[Quidway] sysname MCE
[MCE] vlan batch 10 20 30 40
```

Add interfaces to the VLANs on the MCE.

```
[MCE] interface gigabitethernet 0/0/1
[MCE-GigabitEthernet0/0/1] port trunk allow-pass vlan 30 40
[MCE-GigabitEthernet0/0/1] quit
[MCE] interface ethernet 0/0/3
[MCE-Ethernet0/0/3] port trunk allow-pass vlan 10
[MCE-Ethernet0/0/3] quit
[MCE] interface ethernet 0/0/4
[MCE-Ethernet0/0/4] port trunk allow-pass vlan 20
[MCE-Ethernet0/0/4] quit
```

Create sub-interfaces on PE2 and add these sub-interfaces to the VLAN.

```
<Quidway> system-view
[Quidway] sysname PE2
[PE2] interface gigabitethernet 1/0/0.1
[PE2-GigabitEthernet1/0/0.1] vlan-type dot1q 30
[PE2-GigabitEthernet1/0/0.1] quit
[PE2] interface gigabitethernet 1/0/0.2
[PE2-GigabitEthernet1/0/0.2] vlan-type dot1q 40
[PE2-GigabitEthernet1/0/0.2] quit
```

Create a VLAN on CE3.

```
<Quidway> system-view
[Quidway] sysname CE3
[CE3] vlan 10
```

Add an interface to the VLAN on CE3.

```
[CE3-A] interface ethernet 0/0/1
[CE3-Ethernet0/0/1] port trunk allow-pass vlan 10
[CE3-Ethernet0/0/1] quit
```

Create a VLAN on CE4.

The configuration on CE4 is similar to that on CE3, and is not mentioned here.

Add an interface to the VLAN on CE4.

The configuration on CE4 is similar to that on CE3, and is not mentioned here.

2. Create and configure VPN instances.

Create VPN instances on the MCE.

```
[MCE] ip vpn-instance vpna
[MCE-vpn-instance-vpna] route-distinguisher 100:1
[MCE-vpn-instance-vpna] quit
[MCE] ip vpn-instance vpnb
[MCE-vpn-instance-vpnb] route-distinguisher 100:2
[MCE-vpn-instance-vpnb] quit
```

Bind VPN instances to VLANIF interfaces on the MCE and assign IP addresses to the VLANIF interfaces.

```
[MCE] interface vlanif 10
[MCE-Vlanif10] ip binding vpn-instance vpnb
[MCE-Vlanif10] ip address 172.16.1.2 16
[MCE-Vlanif10] quit
[MCE] interface vlanif 20
[MCE-Vlanif20] ip binding vpn-instance vpna
[MCE-Vlanif20] ip address 172.17.1.2 16
[MCE-Vlanif20] quit
[MCE] interface vlanif 30
[MCE-Vlanif30] ip binding vpn-instance vpnb
[MCE-Vlanif30] ip address 172.18.1.2 16
[MCE-Vlanif30] quit
[MCE] interface vlanif 40
[MCE-Vlanif40] ip binding vpn-instance vpna
[MCE-Vlanif40] ip address 172.19.1.2 16
[MCE-Vlanif40] quit
```

Create VPN instances on PE2.

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance-vpna] route-distinguisher 100:1
[PE2-vpn-instance-vpna] quit
[PE2] ip vpn-instance vpnb
[PE2-vpn-instance-vpnb] route-distinguisher 100:2
[PE2-vpn-instance-vpnb] quit
```

Bind VPN instances to sub-interfaces on PE2 and assign IP addresses to the sub-interfaces.

```
[PE2] interface gigabitethernet 1/0/0.1
[PE2-GigabitEthernet1/0/0.1] ip binding vpn-instance vpnb
[PE2-GigabitEthernet1/0/0.1] ip address 172.18.1.1 255.255.0.0
[PE2-GigabitEthernet1/0/0.1] quit
[PE2] interface gigabitethernet 1/0/0.2
[PE2-GigabitEthernet1/0/0.2] ip binding vpn-instance vpna
[PE2-GigabitEthernet1/0/0.2] ip address 172.19.1.1 255.255.0.0
[PE2-GigabitEthernet1/0/0.2] quit
```

3. Configure the OSPF route multi-instance between the MCE and PE2.

Configure the OSPF route multi-instance on PE2.

```
[PE2] ospf 100 vpn-instance vpna
[PE2-ospf-100] area 0
[PE2-ospf-100-area-0.0.0.0] network 172.19.0.0 0.0.255.255
[PE2-ospf-100-area-0.0.0.0] quit
[PE2-ospf-100] quit
[PE2] ospf 200 vpn-instance vpnb
[PE2-ospf-200] area 0
[PE2-ospf-200-area-0.0.0.0] network 172.18.0.0 0.0.255.255
[PE2-ospf-200-area-0.0.0.0] quit
[PE2-ospf-200] quit
```

Configure the OSPF route multi-instance on the MCE.

```
[MCE] ospf 100 vpn-instance vpna
[MCE-ospf-100] area 0
[MCE-ospf-100-area-0.0.0.0] network 172.19.0.0 0.0.255.255
[MCE-ospf-100-area-0.0.0.0] quit
[MCE-ospf-100] quit
[MCE] ospf 200 vpn-instance vpnb
[MCE-ospf-200] area 0
[MCE-ospf-200-area-0.0.0.0] network 172.18.0.0 0.0.255.255
[MCE-ospf-200-area-0.0.0.0] return
```

4. Configure RIP between the MCE and CE3, and between the MCE and CE4.

Configure RIP-2 on the MCE.

```
[MCE] rip 100 vpn-instance vpna
[MCE-rip-100] version 2
[MCE-rip-100] network 172.17.0.0
[MCE-rip-100] import-route ospf 100
[MCE-rip-100] quit
[MCE] rip 200 vpn-instance vpnb
[MCE-rip-200] version 2
[MCE-rip-200] network 172.16.0.0
[MCE-rip-200] import-route ospf 200
```

Configure RIP-2 on CE3.

```
[S-sw1ch-A] rip 100
[S-sw1ch-A-rip-100] version 2
[S-sw1ch-A-rip-100] network 172.17.0.0
[S-sw1ch-A-rip-100] import-route direct
```

Configure RIP-2 on CE4.

```
[S-sw1ch-B] rip 200
[S-sw1ch-B-rip-200] version 2
[S-sw1ch-B-rip-200] network 172.16.0.0
[S-sw1ch-A-rip-200] network 192.168.2.0
[S-sw1ch-B-rip-200] import-route direct
```

Import RIP routes on the MCE.

```
[MCE] ospf 100
[MCE-ospf-100] import-route rip 100
[MCE-ospf-100] quit [MCE] ospf 200
[MCE-ospf-200] import-route rip 200
```

5. Verify the configuration.

After the configuration, run the **display ip routing-table vpn-instance** command on the MCE, and you can view the routes to the local VPN.

Take **vpnb** as an example:

```
[MCE] display ip routing-table vpn-instance vpnb
Route Flags: R - relay, D - download to fib
```

```
-----
Routing Tables: vpnb
Destinations : 7          Routes : 7

Destination/Mask    Proto  Pre  Cost    Flags NextHop          Interface
-----
172.16.0.0/16       Direct 0    0        D  172.16.1.2          Vlanif10
172.16.1.1/32       Direct 0    0        D  172.16.1.1          Vlanif10
172.16.1.2/32       Direct 0    0        D  127.0.0.1           InLoopBack0
172.18.0.0/16       Direct 0    0        D  172.18.1.2          Vlanif30
172.18.1.1/32       Direct 0    0        D  172.18.1.1          Vlanif30
172.18.1.2/32       Direct 0    0        D  127.0.0.1           InLoopBack0
192.168.0.0/16      RIP    100   1        D  172.16.1.1          Vlanif10
```

Run the **display ip routing-table vpn-instance** command on the PE, and you can view the routes to the local VPN.

Take **vpnb** on PE2 as an example:

```
[PE1] display ip routing-table vpn-instance vpnb
Route Flags: R - relay, D - download to fib
```

```
-----
Routing Tables: vpnb
Destinations : 5          Routes : 5

Destination/Mask    Proto  Pre  Cost    Flags NextHop          Interface
-----
172.18.0.0/16       Direct 0    0        D  172.18.1.1          GigabitEthernet8/
0/0.1
172.18.1.1/32       Direct 0    0        D  127.0.0.1           InLoopBack0
172.18.255.255/32   Direct 0    0        D  127.0.0.1           InLoopBack0
192.168.0.0/16      O_ASE  150   1        D  172.16.1.1          GigabitEthernet8/
0/0.1
255.255.255.255/32 Direct 0    0        D  127.0.0.1           InLoopBack0
```

Configuration Files

- Configuration file of the MCE

```
#
sysname MCE
#
vlan batch 10 20 30 40
#
ip vpn-instance vpna
route-distinguisher 100:1
#
ip vpn-instance vpnb
route-distinguisher 100:2
#
interface Vlanif10
ip binding vpn-instance vpnb
ip address 172.16.1.2 255.255.0.0
#
interface Vlanif20
ip binding vpn-instance vpna
ip address 172.17.1.2 255.255.0.0
#
```

```

interface Vlanif30
 ip binding vpn-instance vpnb
 ip address 172.18.1.2 255.255.0.0
#
interface Vlanif40
 ip binding vpn-instance vpna
 ip address 172.19.1.2 255.255.0.0
#
interface Ethernet0/0/3
 port trunk allow-pass vlan 10
#
interface Ethernet0/0/4
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30 40
#
ospf 100 vpn-instance vpna
 import-route rip 100
 area 0.0.0.0
  network 172.17.0.0 0.0.255.255
  network 172.19.0.0 0.0.255.255
#
ospf 200 vpn-instance vpnb
 import-route rip 200
 area 0.0.0.0
  network 172.16.0.0 0.0.255.255
  network 172.18.0.0 0.0.255.255
#
rip 100 vpn-instance vpna
 version 2
 network 172.17.0.0
 import-route ospf 100
#
rip 200 vpn-instance vpnb
 version 2
 network 172.16.0.0
 import-route ospf 200
#
return

```

- Configuration file of PE2

```

#
 sysname PE2
#
ip vpn-instance vpna
 route-distinguisher 100:1
#
ip vpn-instance vpnb
 route-distinguisher 100:2
#
interface GigabitEthernet1/0/0
 undo shutdown
#
interface GigabitEthernet1/0/0.1
 vlan-type dot1q 30
 ip binding vpn-instance vpnb
 ip address 172.18.1.3 255.255.0.0
#
interface GigabitEthernet1/0/0.2
 vlan-type dot1q 40
 ip binding vpn-instance vpna
 ip address 172.19.1.3 255.255.0.0
#
#
ospf 100 vpn-instance vpna
 area 0.0.0.0
  network 172.19.0.0 0.0.255.255
#

```

```
ospf 200 vpn-instance vpnb
 area 0.0.0.0
  network 172.18.0.0 0.0.255.255
#
return
```

 **NOTE**

The following lists only configuration files related to the MCE. For details on configuring BGP or MPLS IP VPN, refer to manuals of corresponding devices.

- Configuration file of CE3

```
#
 sysname CE3
#
vlan batch 10
#
interface Vlanif10
 ip address 172.16.1.1 255.255.0.0
#
interface Ethernet0/0/1
 port trunk allow-pass vlan 10
#
rip 200
 version 2
 network 172.16.0.0
 network 192.168.1.0
 import-route direct
#
return
```

- Configuration file of CE4

```
#
 sysname CE4
#
vlan batch 20
#
interface Vlanif20
 ip address 172.17.1.1 255.255.0.0
#
interface Ethernet0/0/1
 port trunk allow-pass vlan 10
#
rip 200
 version 2
 network 172.17.0.0
 network 192.168.2.0
 import-route direct
#
return
```