



Quidway S5300 Series Ethernet Switches
V100R002C02

Configuration Guide - Ethernet

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



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 Ethernet Interface Configuration.....	1-1
1.1 Introduction.....	1-3
1.1.1 Ethernet Interfaces.....	1-3
1.1.2 Interface Isolation.....	1-4
1.1.3 References.....	1-5
1.1.4 Logical Relationships Between Configuration Tasks.....	1-5
1.2 Configuring Basic Attributes of Ethernet Interfaces.....	1-5
1.2.1 Establishing the Configuration Task.....	1-5
1.2.2 (Optional) Setting the Description of an Interface.....	1-6
1.2.3 (Optional) Setting the Cable Type for an Interface.....	1-7
1.2.4 (Optional) Setting the Working Mode of an Interface.....	1-7
1.2.5 (Optional) Setting the Rate of an Interface.....	1-7
1.2.6 (Optional) Enabling Flow Control.....	1-8
1.2.7 Checking the Configuration.....	1-8
1.3 Configuring Advanced Attributes of Ethernet Interfaces.....	1-9
1.3.1 Establishing the Configuration Task.....	1-9
1.3.2 Configuring Traffic Suppression.....	1-10
1.3.3 (Optional) Enabling an Interface to Allow Jumbo Frames to Pass Through.....	1-10
1.3.4 (Optional) Configuring an Interface to Discard Incoming Tagged Frames.....	1-11
1.3.5 (Optional) Configuring an Interface to Process BPDUs.....	1-11
1.3.6 Checking the Configuration.....	1-11
1.4 Configuring Auto-negotiation of Ethernet Interfaces.....	1-12
1.4.1 Establishing the Configuration Task.....	1-12
1.4.2 (Optional) Enabling Auto-negotiation.....	1-13
1.4.3 (Optional) Enabling Auto-negotiation of Flow Control.....	1-13
1.4.4 Checking the Configuration.....	1-13
1.5 Configuring External Loopback Detection on Ethernet Interfaces.....	1-14
1.5.1 Establishing the Configuration Task.....	1-14
1.5.2 Enabling External Loopback Detection on Interfaces.....	1-15
1.5.3 (Optional) Setting the Interval for External Loopback Detection on Interfaces.....	1-15
1.5.4 (Optional) Configuring External Loopback Detection Actions on Interfaces.....	1-15
1.5.5 Checking the Configuration.....	1-16

1.6 Creating an Eth-Trunk.....	1-16
1.6.1 Establishing the Configuration Task.....	1-16
1.6.2 Creating an Eth-Trunk.....	1-17
1.6.3 Adding Member Interfaces to an Eth-Trunk.....	1-17
1.6.4 (Optional) Setting the Load Balancing Mode for an Eth-Trunk.....	1-18
1.6.5 Checking the Configuration.....	1-18
1.7 Deleting an Eth-Trunk.....	1-18
1.7.1 Establishing the Configuration Task.....	1-19
1.7.2 (Optional) Deleting a Member Interface from an Eth-Trunk.....	1-19
1.7.3 (Optional) Deleting an Eth-Trunk.....	1-19
1.7.4 Checking the Configuration.....	1-20
1.8 Configuring Interface Isolation.....	1-20
1.8.1 Establishing the Configuration Task.....	1-20
1.8.2 Configuring Interface Isolation.....	1-21
1.8.3 Checking the Configuration.....	1-22
1.9 Configuring Storm Control.....	1-22
1.9.1 Establishing the Configuration Task.....	1-22
1.9.2 Configuring Storm Control.....	1-23
1.9.3 Checking the Configuration.....	1-23
1.10 Maintaining Ethernet Interfaces.....	1-24
1.11 Configuration Examples.....	1-24
1.11.1 Example for Setting Attributes of Ethernet Interfaces.....	1-24
1.11.2 Example for Configuring Interface Isolation.....	1-27
2 LACP Configuration.....	2-1
2.1 Introduction to Link Aggregation.....	2-2
2.1.1 Link Aggregation Overview.....	2-2
2.1.2 Link Aggregation Modes Supported by the S-switch.....	2-2
2.1.3 Related Concepts of LACP.....	2-3
2.1.4 Logical Relationships Between Configuration Tasks.....	2-4
2.1.5 Update History.....	2-4
2.2 Configuring Link Aggregation in Manual Load Balancing Mode.....	2-4
2.2.1 Establishing the Configuration Task.....	2-5
2.2.2 Creating an Eth-Trunk.....	2-5
2.2.3 (Optional) Configuring the Eth-Trunk to Work in Manual Load Balancing Mode.....	2-6
2.2.4 Adding a Member Interface to the Eth-Trunk.....	2-6
2.2.5 (Optional) Setting the Load Balancing Mode.....	2-6
2.2.6 Checking the Configuration.....	2-7
2.3 Configuring Link Aggregation in Static LACP Mode.....	2-8
2.3.1 Establishing the Configuration Task.....	2-8
2.3.2 Creating an Eth-Trunk.....	2-9
2.3.3 Configuring the Eth-Trunk to Work in Static LACP Mode.....	2-9
2.3.4 Adding a Member Interface to the Eth-Trunk.....	2-10

2.3.5 Configuring the Eth-Trunk to Process BPDUs.....	2-10
2.3.6 (Optional) Setting the LACP Priority of the System.....	2-11
2.3.7 (Optional) Setting the Upper Threshold for the Number of Active Interfaces.....	2-11
2.3.8 (Optional) Setting the Lower Threshold for the Number of Active Interfaces.....	2-12
2.3.9 (Optional) Setting the LACP Priority of the Interface.....	2-12
2.3.10 (Optional) Enabling LACP Preemption and Setting the Delay for LACP Preemption.....	2-13
2.3.11 Checking the Configuration.....	2-13
2.4 Maintaining LACP.....	2-14
2.4.1 Clearing the Statistics of Received and Sent LACPDUs.....	2-14
2.4.2 Debugging LACP.....	2-15
2.4.3 Monitoring the Operation Status of the LAG.....	2-15
2.5 Configuration Examples.....	2-16
2.5.1 Example for Configuring Link Aggregation in Manual Load Balancing Mode.....	2-16
2.5.2 Example for Configuring Link Aggregation in Static LACP Mode.....	2-18
3 VLAN Configuration.....	3-1
3.1 Introduction.....	3-2
3.1.1 VLAN.....	3-2
3.1.2 VLAN Classification.....	3-2
3.1.3 VLAN Features Supported by the S-switch.....	3-2
3.1.4 Logical Relationships Between Configuration Tasks.....	3-3
3.1.5 Update History.....	3-3
3.2 Configuring a VLAN.....	3-3
3.2.1 Establishing the Configuration Task.....	3-3
3.2.2 (Optional) Creating a VLAN.....	3-4
3.2.3 (Optional) Creating VLANs in Batches.....	3-4
3.2.4 Checking the Configuration.....	3-5
3.3 Adding Interfaces to a VLAN.....	3-5
3.3.1 Establishing the Configuration Task.....	3-5
3.3.2 (Optional) Adding Access Interfaces to a VLAN.....	3-6
3.3.3 (Optional) Adding Trunk Interfaces to a VLAN.....	3-7
3.3.4 (Optional) Adding Hybrid Interfaces to a VLAN.....	3-7
3.3.5 (Optional) Adding QinQ Interfaces to a VLAN.....	3-8
3.3.6 Checking the Configuration.....	3-9
3.4 Configuring VLANIF Interfaces.....	3-9
3.4.1 Establishing the Configuration Task.....	3-10
3.4.2 Creating a VLANIF Interface.....	3-10
3.4.3 (Optional) Assigning IP Addresses to VLANIF Interfaces.....	3-11
3.4.4 Checking the Configuration.....	3-11
3.5 Configuring MAC Address-Based VLANs.....	3-11
3.5.1 Establishing the Configuration Task.....	3-12
3.5.2 Relating a MAC Address with a VLAN.....	3-12
3.5.3 Permitting Packets with the VLAN Tag to Pass the Current Interface.....	3-12

3.5.4 Enabling MAC Address-Based VLAN Classification.....	3-13
3.5.5 (Optional) Setting the Precedence for VLAN Matching.....	3-13
3.5.6 Checking the Configuration.....	3-13
3.6 Configuring Protocol-Based VLANs.....	3-14
3.6.1 Establishing the Configuration Task.....	3-14
3.6.2 Configuring Protocol-Based VLANs and Assigning the Protocol Template.....	3-14
3.6.3 Allowing Packets to Pass Through Protocol-Based VLANs.....	3-15
3.6.4 Relating a Protocol with a VLAN.....	3-15
3.6.5 Checking the Configuration.....	3-16
3.7 Configuring IP Subnet-Based VLAN Classification.....	3-16
3.7.1 Establishing the Configuration Task.....	3-16
3.7.2 Relating an IP Subnet with a VLAN.....	3-17
3.7.3 Allowing an IP Subnet-Based VLAN to Pass the Current Interface.....	3-17
3.7.4 Enabling an IP Subnet-Based VLAN.....	3-18
3.7.5 Checking the Configuration.....	3-18
3.8 Configuration Examples.....	3-18
3.8.1 Example for Configuring Trunk Links on the S-switch.....	3-18
3.8.2 Example for Configuring VLAN Integration.....	3-21
4 VLAN Aggregation Configuration.....	4-1
4.1 Introduction.....	4-2
4.1.1 Concept of VLAN Aggregation.....	4-2
4.1.2 VLAN Aggregation Supported by the S-switch.....	4-2
4.1.3 Logical Relationships Between Configuration Tasks.....	4-3
4.1.4 Update History.....	4-3
4.2 Configuring VLAN Aggregation.....	4-3
4.2.1 Establishing the Configuration Task.....	4-3
4.2.2 Configuring Sub VLANs.....	4-4
4.2.3 Configuring a Super VLAN.....	4-4
4.2.4 Assigning IP Addresses to VLANIF Interfaces.....	4-4
4.2.5 Enabling ARP Proxy in Sub VLANs.....	4-5
4.2.6 Checking the Configuration.....	4-5
4.3 Configuration Examples.....	4-6
4.3.1 Example for Configuring VLAN Aggregation.....	4-6
5 VLAN Mapping Configuration.....	5-1
5.1 Introduction to VLAN Mapping.....	5-2
5.1.1 VLAN Mapping Overview.....	5-2
5.1.2 VLAN Mapping Features Supported by the S-switch.....	5-3
5.1.3 Update History.....	5-4
5.2 Configuring VLAN Mapping.....	5-4
5.2.1 Establishing the Configuration Task.....	5-4
5.2.2 Creating an S-VLAN and a C-VLAN.....	5-5
5.2.3 Configuring the Type of an Interface Type as Hybrid.....	5-5

5.2.4 Adding Interfaces to an S-VLAN.....	5-5
5.2.5 Enabling Selective QinQ on an Interface.....	5-6
5.2.6 (Optional) Configuring an Interface to Trust the 802.1p Priorities Carried in Packets.....	5-6
5.2.7 Configuring VLAN Mapping.....	5-6
5.2.8 Checking the Configuration.....	5-7
5.3 Configuration Examples.....	5-7
5.3.1 Example for Configuring VLAN Mapping.....	5-8
6 Voice VLAN Configuration.....	6-1
6.1 Introduction.....	6-2
6.1.1 Identification of Voice Flows.....	6-2
6.1.2 Voice VLAN 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 Voice VLANs of the Automatic Mode.....	6-4
6.2.1 Establishing the Configuration Task.....	6-5
6.2.2 (Optional) Configuring Other Identifiable OUIs for the Voice VLAN.....	6-5
6.2.3 (Optional) Configuring the Device to Work in the Security Mode.....	6-5
6.2.4 (Optional) Setting the Aging Time of a Voice VLAN.....	6-6
6.2.5 Enabling the Voice VLAN Function Globally.....	6-6
6.2.6 Enabling the Voice VLAN Function on an Interface.....	6-6
6.2.7 Configuring a Voice VLAN to Work in Automatic Mode.....	6-7
6.2.8 Checking the Configuration.....	6-7
6.3 Configuring Voice VLANs of the Manual Mode.....	6-8
6.3.1 Establishing the Configuration Task.....	6-8
6.3.2 (Optional) Configuring Other Identifiable OUIs for the Voice VLAN.....	6-9
6.3.3 (Optional) Configuring the Device to Work in the Security Mode.....	6-9
6.3.4 (Optional) Setting the Aging Time of a Voice VLAN.....	6-9
6.3.5 Enabling the Voice VLAN Function Globally.....	6-10
6.3.6 Enabling the Voice VLAN Function on an Interface.....	6-10
6.3.7 Configuring a Voice VLAN to Work in Manual Mode.....	6-10
6.3.8 Adding Interfaces to the Voice VLAN.....	6-11
6.3.9 Checking the Configuration.....	6-11
6.4 Configuration Examples.....	6-12
6.4.1 Example for Configuring the Voice VLAN of the Automatic Mode.....	6-12
6.4.2 Example for Configuring the Voice VLAN of the Manual Mode.....	6-14
7 QinQ Configuration.....	7-1
7.1 Introduction.....	7-2
7.1.1 QinQ.....	7-2
7.1.2 Selective QinQ.....	7-2
7.1.3 References.....	7-2
7.1.4 Logical Relationships Between Configuration Tasks.....	7-2
7.2 Configure QinQ Interfaces.....	7-2

7.2.1 Establishing the Configuration Task.....	7-3
7.2.2 Setting the Interface Type.....	7-3
7.2.3 (Optional) Setting the TPID Etype Value in the Outer VLAN Tag.....	7-4
7.2.4 Setting the VLAN ID of the Outer VLAN Tag.....	7-4
7.2.5 Checking the Configuration.....	7-5
7.3 Configuring Selective QinQ.....	7-5
7.3.1 Establishing the Configuration Task.....	7-5
7.3.2 Configuring an Interface to Add Outer VLAN Tags to Frames.....	7-6
7.3.3 (Optional) Configuring an Interface to Discard Packets That Do Not Match Selective QinQ.....	7-7
7.3.4 Checking the Configuration.....	7-7
7.4 Configuration Examples.....	7-8
7.4.1 Example for Configuring QinQ.....	7-8
7.4.2 Example for Configuring Selective QinQ.....	7-11
7.4.3 Example for Setting the TPID Etype Value in the Outer VLAN Tags.....	7-15
8 MAC Table Configuration.....	8-1
8.1 Introduction.....	8-2
8.1.1 MAC Table.....	8-2
8.1.2 Capacity of a MAC Table and Limit to the Number of MAC Entries Learned by an Interface.....	8-2
8.1.3 Packet Forwarding Restriction.....	8-2
8.1.4 References.....	8-3
8.1.5 Logical Relationships Between Configuration Tasks.....	8-3
8.2 Configuring the MAC Table.....	8-3
8.2.1 Establishing the Configuration Task.....	8-3
8.2.2 (Optional) Adding MAC Entries.....	8-4
8.2.3 (Optional) Setting the Aging Time of Dynamic MAC Entries.....	8-4
8.2.4 Checking the Configuration.....	8-5
8.3 Configuration Examples.....	8-5
8.3.1 Example for Configuring the MAC Table.....	8-5
9 MSTP Configuration.....	9-1
9.1 Introduction.....	9-2
9.1.1 STP, RSTP, and MSTP.....	9-2
9.1.2 References.....	9-2
9.2 Enabling Basic Functions of MSTP on the S-switch.....	9-2
9.2.1 Establishing the Configuration Task.....	9-2
9.2.2 Enabling an Interface to Process BPDUs.....	9-3
9.2.3 Enabling MSTP.....	9-3
9.2.4 Checking the Configuration.....	9-4
9.3 Adding an S-switch to a Specified MST Region.....	9-4
9.3.1 Establishing the Configuration Task.....	9-4
9.3.2 Setting the MSTP Mode of the S-switch.....	9-5
9.3.3 Setting the MST Region.....	9-5
9.3.4 Activating the Configuration of an MST Region.....	9-6

9.3.5 (Optional) Setting the S-switch as the Root Switch or Secondary Root Switch.....	9-7
9.3.6 (Optional) Setting the Priority of the S-switch in a Specified MSTI.....	9-7
9.3.7 Checking the Configuration.....	9-8
9.4 Configuring MSTP Parameters of the S-switch.....	9-8
9.4.1 Establishing the Configuration Task.....	9-8
9.4.2 (Optional) Configuring MSTP Network Parameters of the S-switch.....	9-9
9.4.3 (Optional) Configuring MSTP Parameters of an Interface.....	9-10
9.4.4 (Optional) Switching an Interface to the MSTP Mode.....	9-11
9.5 Configuring MSTP Protection on the S-switch.....	9-12
9.5.1 Establishing the Configuration Task.....	9-12
9.5.2 (Optional) Configuring BPDU Protection on the S-switch.....	9-13
9.5.3 (Optional) Configuring Root Protection on an Interface.....	9-13
9.5.4 (Optional) Configuring Loop Protection on an Interface.....	9-14
9.5.5 Checking the Configuration.....	9-15
9.6 Maintaining MSTP.....	9-15
9.6.1 Displaying MSTP Running Information.....	9-15
9.6.2 Clearing MSTP Statistics.....	9-15
9.6.3 Debugging MSTP.....	9-16
9.7 Configuration Examples.....	9-16
9.7.1 Example for Configuring MSTP.....	9-16
10 RRPP Configuration.....	10-1
10.1 Introduction.....	10-2
10.1.1 RRPP.....	10-2
10.1.2 References.....	10-2
10.2 Configuring RRPP Functions.....	10-2
10.2.1 Establishing the Configuration Task.....	10-3
10.2.2 Creating an RRPP Domain and the Control VLAN.....	10-3
10.2.3 (Optional) Setting the Values of Timers in an RRPP Domain.....	10-4
10.2.4 Disabling the STP Function on the Interfaces to be Added to an RRPP Ring.....	10-5
10.2.5 Creating an RRPP Ring.....	10-5
10.2.6 Enabling an RRPP Ring.....	10-6
10.2.7 Enabling RRPP.....	10-6
10.2.8 Disabling Multiple Sub-Ring Protection.....	10-6
10.2.9 Checking the Configuration.....	10-7
10.3 Configuring RRPP Multi-Instance.....	10-8
10.3.1 Establishing the Configuration Task.....	10-9
10.3.2 Creating Instances.....	10-11
10.3.3 Creating an RRPP Domain and the Control VLAN.....	10-12
10.3.4 Disabling the STP Function on the Interfaces to be Added to an RRPP Ring.....	10-12
10.3.5 Configuring Protected VLAN.....	10-13
10.3.6 Creating an RRPP Ring.....	10-13
10.3.7 Enabling an RRPP Ring.....	10-14

10.3.8 Enabling RRPP.....	10-14
10.3.9 (Optional) Creating a RRPP Ring Group.....	10-15
10.3.10 (Optional) Configuring the Delay for Link Restoration.....	10-15
10.3.11 (Optional) Setting the Values of Timers in an RRPP Domain.....	10-16
10.3.12 Checking the Configuration.....	10-16
10.4 Maintaining RRPP.....	10-17
10.4.1 Clearing RRPP Running Information.....	10-17
10.4.2 Debugging RRPP.....	10-17
10.5 Configuration Examples.....	10-18
10.5.1 Example for Configuring a Single RRPP Ring.....	10-18
10.5.2 Example for Configuring Tangent RRPP Rings.....	10-23
10.5.3 Example for Configuring Intersectant Rings in a Single RRPP Domain.....	10-30
10.5.4 Example for Configuring Intersectant Rings in Multiple RRPP Domains.....	10-36
10.5.5 Example for Configuring Single RRPP Ring of Multi-Instance.....	10-43
10.5.6 Example for Configuring the Crossed RRPP Ring of Multi-Instance.....	10-54
10.5.7 Example for Configuring the Tangent RRPP Ring of Multi-Instance.....	10-77
11 BPDU Tunneling and Partitioned STP Configuration.....	11-1
11.1 Introduction.....	11-2
11.1.1 BPDU Tunneling.....	11-2
11.1.2 Partitioned STP.....	11-2
11.1.3 Logic Relationships Between Configuration Tasks.....	11-2
11.2 Configuring Interface-based Transparent Transmission of BPDUs from the Same Customer Network.....	11-3
11.2.1 Establishing the Configuration Task.....	11-3
11.2.2 Enabling STP on CEs.....	11-3
11.2.3 Configuring the Provider Mode for UPEs.....	11-4
11.2.4 Enabling UPEs to Process BPDUs.....	11-4
11.2.5 Checking the Configuration.....	11-5
11.3 Configuring Interface-based Transparent Transmission of BPDUs from Different Customer Networks.....	11-5
11.3.1 Establishing the Configuration Task.....	11-5
11.3.2 Enabling UPE Interfaces to Process BPDUs.....	11-6
11.3.3 Adding UPE Interfaces to Specified VLANs in Untagged Mode.....	11-6
11.3.4 Replacing the MAC Address of BPDUs with a Reserved Multicast MAC Address.....	11-7
11.3.5 Enabling BPDU Tunneling.....	11-7
11.3.6 Checking the Configuration.....	11-7
11.4 Configuring VLAN-based BPDU Tunneling.....	11-8
11.4.1 Establishing the Configuration Task.....	11-8
11.4.2 Setting VLAN IDs of the BPDUs that CE Interfaces Allow to Pass Through.....	11-9
11.4.3 Tagging BPDUs.....	11-9
11.4.4 (Optional) Replacing the MAC Address of BPDUs with a Multicast MAC Address.....	11-10
11.4.5 Configuring UPEs to Transmit Tagged BPDUs Through BPDU Tunnels.....	11-10
11.4.6 Checking the Configuration.....	11-10

11.5 Configuring QinQ-based BPDU Tunneling.....	11-11
11.5.1 Establishing the Configuration Task.....	11-11
11.5.2 Setting VLAN IDs of the BPDUs that CE Interfaces Allow to Pass Through.....	11-12
11.5.3 Tagging BPDUs.....	11-12
11.5.4 Tagging and Untagging the Tagged BPDUs.....	11-13
11.5.5 Replacing the MAC Address of BPDUs with a Reserved Multicast MAC Address.....	11-13
11.5.6 Configuring BPDU Tunneling.....	11-14
11.5.7 Checking the Configuration.....	11-14
11.6 Configuring Partitioned STP.....	11-15
11.6.1 Establishing the Configuration Task.....	11-15
11.6.2 Enabling STP.....	11-16
11.6.3 Enabling Interfaces Connected to the MAN to Tag BPDUs.....	11-16
11.6.4 Setting VLAN IDs for Inbound Interfaces.....	11-17
11.6.5 Configuring BPDU Tunneling.....	11-17
11.6.6 Enabling STP Snooping.....	11-18
11.6.7 Checking the Configuration.....	11-18
11.7 Configuration Examples.....	11-19
11.7.1 Example for Configuring Interface-based BPDU Tunnel of the Same Customer.....	11-19
11.7.2 Example for Configuring Interface-based BPDU Tunnel of Different Customer.....	11-22
11.7.3 Example for Configuring VLAN-based BPDU Tunneling.....	11-25
11.7.4 Example for Configuring QinQ-based BPDU Tunneling.....	11-30
11.7.5 Example for Configuring Partitioned STP.....	11-37

Figures

Figure 1-1 Networking for applying unidirectional interface isolation.....	1-4
Figure 1-2 Networking for applying bidirectional interface isolation.....	1-5
Figure 1-3 Networking for setting attributes of Ethernet interfaces.....	1-25
Figure 1-4 Networking for configuring interface isolation.....	1-27
Figure 2-1 Determining the active links by the Actor in static LACP mode.....	2-4
Figure 2-2 Networking diagram of link aggregation in manual load balancing mode.....	2-5
Figure 2-3 Networking diagram of link aggregation in static LACP mode.....	2-8
Figure 2-4 Networking diagram of link aggregation in manual load balancing mode.....	2-16
Figure 2-5 Networking diagram of link aggregation in static LACP mode.....	2-18
Figure 3-1 Networking diagram for configuring trunk links on the S-switch.....	3-19
Figure 3-2 Networking diagram for configuring VLAN integration.....	3-21
Figure 4-1 Networking diagram for configuring VLAN aggregation.....	4-7
Figure 5-1 Networking diagram of VLAN mapping.....	5-3
Figure 5-2 Networking for configuring VLAN mapping.....	5-8
Figure 6-1 Configuring voice VLANs of the automatic mode.....	6-12
Figure 6-2 Configuring voice VLANs of the manual mode.....	6-15
Figure 7-1 Networking diagram for configuring QinQ interfaces.....	7-9
Figure 7-2 Networking diagram for configuring selective QinQ.....	7-12
Figure 7-3 Networking diagram of configuring the compatibility of the TPID Etype value in the outer VLAN tags.....	7-15
Figure 9-1 Networking diagram for configuring basic MSTP functions.....	9-17
Figure 10-1 Networking diagram of RRPP multi-instance.....	10-10
Figure 10-2 Networking diagram for configuring a single RRPP ring.....	10-18
Figure 10-3 Networking diagram for configuring RRPP.....	10-23
Figure 10-4 Networking diagram for configuring RRPP.....	10-30
Figure 10-5 Networking diagram for configuring intersectant rings in multiple RRPP domains.....	10-37
Figure 10-6 Networking diagram of single RRPP ring of multi-instance.....	10-44
Figure 10-7 Networking diagram of crossed RRPP ring of multi-instance.....	10-57
Figure 10-8 Networking diagram of configuring the tangent RRPP ring of multi-instance.....	10-78
Figure 11-1 Tagging and Untagging the Tagged BPDUs.....	11-13
Figure 11-2 Networking of partitioned STP.....	11-15
Figure 11-3 Networking for configuring interface-based transparent transmission of BPDUs from the same customer network.....	11-20

Figure 11-4 Networking for configuring interface-based transparent transmission of BPDUs from different customer networks.....	11-22
Figure 11-5 Networking for configuring VLAN-based BPDU tunneling.....	11-26
Figure 11-6 Networking for configuring QinQ-based BPDU tunneling.....	11-30
Figure 11-7 Networking for configuring partitioned STP.....	11-37

Tables

Table 1-1 Attributes of FE interfaces.....	1-3
Table 1-2 Attributes of GE interfaces.....	1-4
Table 6-1 Default OUI addresses.....	6-2
Table 6-2 Packet processing methods in various voice VLAN modes.....	6-3
Table 10-1 Mapping between protected VLAN and instance.....	10-43
Table 10-2 Information table of master nodes.....	10-43
Table 10-3 Mapping between the protected VLAN and instance.....	10-55
Table 10-4 Information table of master nodes.....	10-55
Table 10-5 Information table of nodes and ports.....	10-55
Table 10-6 Mapping between protected VLANs and instances.....	10-77
Table 10-7 Information about the master node, primary port, and secondary port.....	10-77

About This Document

Purpose

This document describes the Ethernet feature that is supported by the S-switch. The Ethernet feature is described by providing configuration procedures and configuration examples.

This document covers the following topics:

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

This document guides you through the configuration and the applicable environment of the Ethernet feature of the S-switch.

Related Versions

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

Product Name	Related Versions
S5300	V100R002C02

Intended Audience

This document is intended for:

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

Organization


This document consists of 11 chapters whose contents are shown as follows:





Chapter	Description
1 Ethernet Interface Configuration	Describes the basics, methods, and examples for configuring the Ethernet interface.
2 LACP Configuration	Describes the basics, methods, and examples for configuring the Link Aggregation.
3 VLAN Configuration	Describes the basics, methods, and examples for configuring the Virtual Local Area Network (VLAN).
4 VLAN Aggregation Configuration	Describes the basics, methods, and examples for configuring the VLAN Aggregation.
5 VLAN Mapping Configuration	Describes the basics, methods, and examples for configuring the VLAN Mapping.
6 Voice VLAN Configuration	Describes the basics, methods, and examples for configuring the Voice VLAN.
7 QinQ Configuration	Describes the basics, methods, and examples for configuring QinQ.
8 MAC Table Configuration	Describes the basics, methods, and examples for configuring the MAC table.
9 MSTP Configuration	Describes the basics, methods, and examples for configuring the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP).
10 RRPP Configuration	Describes the basics, methods, and examples for configuring Rapid Ring Protection Protocol (RRPP).
11 BPDU Tunneling and Partitioned STP Configuration	Describes the basics, methods, and examples for configuring the Bridge Protocol Data Unit (BPDU) tunnel and partitioned STP.

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 injuries.

Symbol	Description
 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.
 NOTE	Provides additional information to emphasize or supplement important points of the main text.
 TIP	Indicates a tip that may help you solve a problem or save your time.

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	“Terminal display is in 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>italic</i> .
[]	Items (keywords or arguments) in brackets [] are optional.
{ 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.

Convention	Description
#	A line starting with the # sign is comments.

GUI Conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, 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

Format	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, A means the two keys should be pressed in turn.

Mouse Operation

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

Revision History

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

Updates in Issue 01 (12.26.08)

This is the first release.

1 Ethernet Interface Configuration

About This Chapter

This chapter describes the basics, procedures, and configuration examples of Ethernet interfaces.

[1.1 Introduction](#)

This section describes Ethernet interfaces and the interface isolation function supported by the S-switch.

[1.2 Configuring Basic Attributes of Ethernet Interfaces](#)

This section describes how to configure the description, cable type, working mode, and rate of Ethernet interfaces.

[1.3 Configuring Advanced Attributes of Ethernet Interfaces](#)

This section describes how to configure traffic suppression on Ethernet interfaces and how to configure Ethernet interfaces to allow jumbo frames to pass through, to discard incoming tagged frames, and to process Bridge Protocol Data Units (BPDUs).

[1.4 Configuring Auto-negotiation of Ethernet Interfaces](#)

This section describes how to configure auto-negotiation and auto-negotiation of flow control of Ethernet interfaces.

[1.5 Configuring External Loopback Detection on Ethernet Interfaces](#)

This section describes how to configure external loopback detection on Ethernet interfaces.

[1.6 Creating an Eth-Trunk](#)

This section describes how to create an Eth-Trunk.

[1.7 Deleting an Eth-Trunk](#)

Deleting an Eth-Trunk

[1.8 Configuring Interface Isolation](#)

This section describes how to configure interface isolation.

[1.9 Configuring Storm Control](#)

This section describes how to configure storm control.

[1.10 Maintaining Ethernet Interfaces](#)

This section describes how to maintain Ethernet interfaces.

[1.11 Configuration Examples](#)

This section provides several examples for configuring Ethernet interfaces.

1.1 Introduction

This section describes Ethernet interfaces and the interface isolation function supported by the S-switch.

1.1.1 Ethernet Interfaces

1.1.2 Interface Isolation

1.1.3 References

1.1.4 Logical Relationships Between Configuration Tasks

1.1.1 Ethernet Interfaces

The S-switch supports the following Ethernet interfaces:

- Fast Ethernet (FE) interfaces
- Gigabit Ethernet (GE) interfaces

FE Interfaces

FE interfaces can be either FE electrical interfaces or FE optical interfaces.

Table 1-1 shows the attributes of FE electrical interfaces and FE optical interfaces.

Table 1-1 Attributes of FE interfaces

Interface Type	Rate (Mbit/s)	Duplex Mode		Auto-negotiation Mode	Non-Automatic Negotiation Mode
		Full-Duplex	Half-Duplex		
FE electrical interface	10/100	√	√	√	√
FE optical interface	100	√	×	×	√

In auto-negotiation mode, FE interfaces and the directly connected devices negotiate and determine their common duplex mode and rate. This simplifies system configuration and management.

GE Interfaces

Table 1-2 shows the attributes of GE interfaces.

Table 1-2 Attributes of GE interfaces

Interface Type	Rate (Mbit/s)	Duplex Mode		Auto-negotiation Mode	Non-Automatic Negotiation Mode
		Full-Duplex	Half-Duplex		
GE optical interface	1000	√	×	√	√

In auto-negotiation mode, GE interfaces and the directly connected devices negotiate and determine whether to implement flow control.

1.1.2 Interface Isolation

The S-switch supports interface isolation, which implements Layer 2 isolation between interfaces. Interface isolation is supported by the following interfaces on the S-switch:

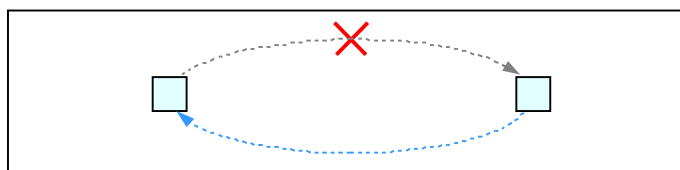
- FE interfaces
- GE interfaces
- Eth-Trunks

NOTE

Interface isolation cannot be configured on member interfaces of an Eth-Trunk.

Unidirectional Isolation

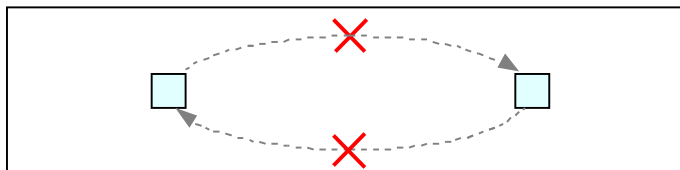
As shown in [Figure 1-1](#), if interface isolation is configured on Interface A, Interface A cannot send packets to Interface B; Interface B, however, can send packets to Interface A.

Figure 1-1 Networking for applying unidirectional interface isolation

Bidirectional Isolation

As shown in [Figure 1-2](#), if interface isolation is configured on Interface A and Interface B, Interface A and Interface B cannot exchange packets. This implements bidirectional isolation between Interface A and Interface B.

Figure 1-2 Networking for applying bidirectional interface isolation



Rules for Configuring Interface Isolation

On the S-switch, interface isolation can be configured on any two interfaces that support this function.

1.1.3 References

For details on Ethernet interfaces, refer to the *Quidway S5300 Series Ethernet Switches Feature Description*.

1.1.4 Logical Relationships Between Configuration Tasks

[1.2 Configuring Basic Attributes of Ethernet Interfaces](#) is a prerequisite to advanced configurations.

1.2 Configuring Basic Attributes of Ethernet Interfaces

This section describes how to configure the description, cable type, working mode, and rate of Ethernet interfaces.

[1.2.2 \(Optional\) Setting the Description of an Interface](#) to [1.2.6 \(Optional\) Enabling Flow Control](#) are optional and are not listed in sequence.

[1.2.1 Establishing the Configuration Task](#)

[1.2.2 \(Optional\) Setting the Description of an Interface](#)

[1.2.3 \(Optional\) Setting the Cable Type for an Interface](#)

[1.2.4 \(Optional\) Setting the Working Mode of an Interface](#)

[1.2.5 \(Optional\) Setting the Rate of an Interface](#)

[1.2.6 \(Optional\) Enabling Flow Control](#)

[1.2.7 Checking the Configuration](#)

1.2.1 Establishing the Configuration Task

Applicable Environment

The configuration task is applicable to the following:

- To identify an interface, set the description of the interface.

- By default, an FE electrical interface automatically identifies the type of the cable connected to it. When the FE electrical interface fails to identify the cable type, you can set the cable type for the interface.
- By default, an FE electrical interface and the directly connected device automatically negotiate and determine their common working mode and rate. If the peer device does not support auto-negotiation, you can set the working mode and rate of the FE electrical interface the same as those of the peer device.
- If the traffic received by an Ethernet interface on the S-switch exceeds its processing capability, and the interface directly connected to the local interface also supports flow control, you can enable flow control on the local interface. After flow control is enabled, the interface sends a special data frame called the Pause frame to the peer interface to notify the peer interface to stop sending traffic, if the received traffic reaches the set threshold. If the peer interface also supports flow control, it reduces the rate of sending frames so that the local interface can process received frames properly.

Pre-configuration Tasks

None.

Data Preparation

To set basic attributes of Ethernet interfaces, you need the following data.

No.	Data
1	Number of an Ethernet interface
2	(Optional) Description of the Ethernet interface
3	(Optional) Cable type for the FE electrical interface
4	(Optional) Duplex mode of the FE electrical interface
5	(Optional) Rate of the FE electrical interface

1.2.2 (Optional) Setting the Description of an Interface

Context

Do as follows on the S-switch where the description needs to be set for an Ethernet interface.

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 GE interface view.
- Step 3** Run the **description description** command to set the description of the interface.

By default, the description of an interface shows the type and number of the interface. For example, the description of GigabitEthernet 0/0/1 is "HUAWEI, Quidway Series, GigabitEthernet0/0/1 interface."

----End

1.2.3 (Optional) Setting the Cable Type for an Interface

Context

Do as follows on the S-switch where the cable type needs to be set for an Ethernet interface.

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 Ethernet interface view or GE interface view.

Step 3 Run the **mdi { across | auto | normal }** command to set the cable type for the FE electrical interface.

By default, an FE electrical interface automatically identifies the type of the cable connected to it.

----End

1.2.4 (Optional) Setting the Working Mode of an Interface

Context

Do as follows on the S-switch where the working mode needs to be set for an Ethernet electrical interface.

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 GE interface view.

Step 3 Run the **undo negotiation auto** command to set the FE electrical interface to work in non-automatic negotiation mode.

Step 4 Run the **duplex { full | half }** command to set the working mode of the FE electrical interface.

By default, the working mode of an FE electrical interface is full-duplex when it runs in non-automatic negotiation mode.

----End

1.2.5 (Optional) Setting the Rate of an Interface

Context

Do as follows on the S-switch where the working mode needs to be set for an Ethernet electrical interface.

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 Ethernet interface view.

Step 3 Run the **undo negotiation auto** command to set the FE electrical interface to work in non-automatic negotiation mode.

Step 4 Run the **speed { 10 | 100 }** command to set the rate of the FE electrical interface.

By default, the rate of an FE electrical interface is 100 Mbit/s when it works in non-automatic negotiation mode.

----End

1.2.6 (Optional) Enabling Flow Control

Context

Do as follows on the S-switch and the peer S-switch that need flow control on Ethernet interfaces.

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 GE interface view.

Step 3 Run the **flow-control** command to enable flow control on the Ethernet interface.

By default, flow control is disabled on an Ethernet interface.

----End

1.2.7 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the basic configuration of an Ethernet interface.	display interface [<i>interface-type</i> [<i>interface-number</i>]] [verbose] [{ begin exclude include } <i>regular-expression</i>]
Check the cable type and flow control status of an Ethernet interface.	display current-configuration interface <i>interface-type interface-number</i>

After the configurations succeed, the following results can be obtained with the preceding command:

- The basic configurations, including the description, working mode, and rate of the Ethernet interface are correctly set.
- The cable type of the Ethernet interface is correctly set.

- Flow control is enabled or disabled as configured.

1.3 Configuring Advanced Attributes of Ethernet Interfaces

This section describes how to configure traffic suppression on Ethernet interfaces and how to configure Ethernet interfaces to allow jumbo frames to pass through, to discard incoming tagged frames, and to process Bridge Protocol Data Units (BPDUs).

1.3.1 Establishing the Configuration Task

1.3.2 Configuring Traffic Suppression

1.3.3 (Optional) Enabling an Interface to Allow Jumbo Frames to Pass Through

1.3.4 (Optional) Configuring an Interface to Discard Incoming Tagged Frames

1.3.5 (Optional) Configuring an Interface to Process BPDUs

1.3.6 Checking the Configuration

1.3.1 Establishing the Configuration Task

Applicable Environment

The configuration task is applicable to the following:

- The S-switch supports the suppression of the broadcast packets, unknown multicast packets, and unknown unicast packets received by Ethernet interfaces. When the number of broadcast packets, unknown multicast packets, or unknown unicast packets exceeds the set threshold, the system discards the excessive packets. This reduces the traffic to an allowable range and ensures normal transmission of network services.
- When there are jumbo frames on the network and the frames need to pass through an Ethernet interface, you need to enable the Ethernet interface to allow jumbo frames to pass through.
- In normal situations, when an interface is not allowed to receive tagged frames, for example, the interface directly connects a user host, you can configure the interface to discard incoming tagged frames. This protects the system against hackers that use forged tags.
- When an interface needs to run the Multiple Spanning Tree Protocol (MSTP) or Huawei Group Management Protocol (HGMP), you need to enable the interface to process BPDUs. Otherwise, the interface discards all BPDUs it receives.

Pre-configuration Tasks

None.

Data Preparation

To set advanced attributes of Ethernet interfaces, you need the following data.

No.	Data
1	Number of an Ethernet interface

No.	Data
2	(Optional) Maximum percentage of broadcast traffic, unknown multicast traffic, and unknown unicast traffic that an Ethernet interface allows to pass through
3	(Optional) Type and number of the interface where the incoming tagged frames need to be discarded
4	(Optional) Type and number of the interface where BPDUs need to be processed

1.3.2 Configuring Traffic Suppression

Context

Do as follows on the S-switch where the description needs to be set for an Ethernet interface.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface { ethernet | gigabitethernet } interface-number** command to enter the Ethernet interface view or GE interface view.
- Step 3** Run the **broadcast-suppression { broadcast-pct | packets packets-per-second }** command to set the maximum percentage of broadcast traffic that the Ethernet interface allows to pass through.
- Step 4** Run the **multicast-suppression { multicast-pct | packets packets-per-second }** command to set the maximum percentage of multicast traffic that the Ethernet interface allows to pass through.
- Step 5** Run the **unicast-suppression { unicast-pct | packets packets-per-second }** command to set the maximum percentage of unknown unicast traffic that the Ethernet interface allows to pass through.

By default, the maximum percentage of broadcast traffic, unknown multicast traffic, and unknown unicast traffic that an Ethernet interface allows to pass through is 100% respectively. That is, the broadcast traffic, unknown multicast traffic, and unknown unicast traffic are not suppressed on an Ethernet interface.

----End

1.3.3 (Optional) Enabling an Interface to Allow Jumbo Frames to Pass Through

Context

Do as follows on the S-switch where you need to enable an Ethernet interface to allow jumbo frames to pass through.

Procedure

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

- Step 2** Run the **interface { ethernet | gigabitethernet } interface-number** command to enter the Ethernet interface view or GE interface view.
- Step 3** Run the **jumboframe enable** command to enable the Ethernet interface to allow jumbo frames to pass through.
- By default, an Ethernet interface does not allow jumbo frames to pass through.
- End

1.3.4 (Optional) Configuring an Interface to Discard Incoming Tagged Frames

Context

Do as follows on the S-switch where you need to configure an interface to discard incoming tagged frames.

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 GE interface view or Eth-Trunk interface view.
- Step 3** Run the **port discard tagged-packet** command to configure the interface to discard incoming tagged frames.
- By default, an interface does not discard incoming tagged frames.
- End

1.3.5 (Optional) Configuring an Interface to Process BPDUs

Context

Do as follows on the S-switch where you need to configure an interface to process BPDUs.

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 Ethernet interface view, GE interface view, or Eth-Trunk interface view.
- Step 3** Run the **bpdu enable** command to set the interface to process BPDUs.
- By default, an interface does not process BPDUs.
- End

1.3.6 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check whether the following functions are configured on an Ethernet interface: <ul style="list-style-type: none">• Traffic suppression.• Jumbo frames are allowed to pass through.• The incoming tagged frames are discarded.• BPDUs are processed.	display current-configuration interface <i>interface-type interface-number</i>

After the configurations succeed, the following results can be obtained with the preceding command:

- Flow control, auto-negotiation of flow control, and traffic suppression are correctly configured.
- The Ethernet interface allows jumbo frames to pass through, discards incoming tagged frames, and processes BPDUs.

1.4 Configuring Auto-negotiation of Ethernet Interfaces

This section describes how to configure auto-negotiation and auto-negotiation of flow control of Ethernet interfaces.

[1.4.2 \(Optional\) Enabling Auto-negotiation](#) to [1.4.3 \(Optional\) Enabling Auto-negotiation of Flow Control](#) are optional. You must perform [1.4.2 \(Optional\) Enabling Auto-negotiation](#) before performing [1.4.3 \(Optional\) Enabling Auto-negotiation of Flow Control](#).

[1.4.1 Establishing the Configuration Task](#)

[1.4.2 \(Optional\) Enabling Auto-negotiation](#)

[1.4.3 \(Optional\) Enabling Auto-negotiation of Flow Control](#)

[1.4.4 Checking the Configuration](#)

1.4.1 Establishing the Configuration Task

Applicable Environment

- FE interfaces and GE interfaces on the S-switch support auto-negotiation. An FE interface negotiates the duplex mode and rate with the peer interface. A GE interface and the peer interface can negotiate and determine whether to enable flow control only after the **flow-control negotiation** command is used to enable auto-negotiation of flow control on both sides.
- GE interfaces on the S-switch support auto-negotiation of flow control. Auto-negotiation of flow control allows an interface and the directly connected interface to negotiate and determine whether to enable flow control on both sides. This simplifies system configuration and management.

Pre-configuration Tasks

None.

Data Preparation

To configure auto-negotiation of Ethernet interfaces, you need the following data.

No.	Data
1	Number of an Ethernet interface

1.4.2 (Optional) Enabling Auto-negotiation

Context

Do as follows on the S-switch and the peer S-switch that need auto-negotiation on Ethernet interfaces.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface gigabitethernet *interface-number*** command to enter the GE interface view.
- Step 3** Run the **negotiation auto** command to set the GE interface to work in auto-negotiation mode.
- By default, GE interfaces work in non-automatic negotiation mode.
- End

1.4.3 (Optional) Enabling Auto-negotiation of Flow Control

Context

Do as follows on the S-switch and the peer S-switch that need auto-negotiation of flow control on Ethernet interfaces.

GE interfaces support auto-negotiation of flow control. This function, however, is not supported by FE interfaces.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface gigabitethernet *interface-number*** command to enter the GE interface view.
- Step 3** Run the **flow-control negotiation** command to enable auto-negotiation of flow control on the GE interface.
- By default, auto-negotiation of flow control is disabled on an Ethernet interface.
- End

1.4.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check auto-negotiation and auto-negotiation of flow control on an Ethernet interface.	display current-configuration interface <i>interface-type interface-number</i>

After the configuration succeeds, run the preceding command. You can view that auto-negotiation and auto-negotiation of flow control are correctly configured on the Ethernet interface.

1.5 Configuring External Loopback Detection on Ethernet Interfaces

This section describes how to configure external loopback detection on Ethernet interfaces.

[1.5.3 \(Optional\) Setting the Interval for External Loopback Detection on Interfaces](#) to [1.5.4 \(Optional\) Configuring External Loopback Detection Actions on Interfaces](#) are optional. You must perform [1.5.2 Enabling External Loopback Detection on Interfaces](#) before performing [1.5.3 \(Optional\) Setting the Interval for External Loopback Detection on Interfaces](#) and [1.5.4 \(Optional\) Configuring External Loopback Detection Actions on Interfaces](#).

[1.5.1 Establishing the Configuration Task](#)

[1.5.2 Enabling External Loopback Detection on Interfaces](#)

[1.5.3 \(Optional\) Setting the Interval for External Loopback Detection on Interfaces](#)

[1.5.4 \(Optional\) Configuring External Loopback Detection Actions on Interfaces](#)

[1.5.5 Checking the Configuration](#)

1.5.1 Establishing the Configuration Task

Applicable Environment

- After external loopback detection is enabled on Ethernet interfaces, the device detects whether an external loopback occurs on an interface at regular intervals. If an external loopback occurs on an interface, the device disables, restricts, or blocks the interface.

Pre-configuration Tasks

None.

Data Preparation

To configure external loopback detection on Ethernet interfaces, you need the following data.

No.	Data
1	Number of an Ethernet interface

No.	Data
2	Interval for external loopback detection

1.5.2 Enabling External Loopback Detection on Interfaces

Context

Do as follows on the S-switch where external loopback detection needs to be enabled on interfaces.

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 **loopback-detect enable** command to enable external loopback detection on the interface.



NOTE

You can run the **loopback-detect enable** command in the system view to enable external loopback detection for all interfaces.

----End

1.5.3 (Optional) Setting the Interval for External Loopback Detection on Interfaces

Context

Do as follows on the S-switch where external loopback detection needs to be enabled on interfaces.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **loopback-detect interval** *time* command to set the interval for external loopback detection on interfaces.

----End

1.5.4 (Optional) Configuring External Loopback Detection Actions on Interfaces

Context

Do as follows on the S-switch where external loopback detection needs to be enabled on interfaces.

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 **loopback-detect action shutdown** command to shut down the interface when an external loop occurs.

----End

1.5.5 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check external loopback detection on an Ethernet interface.	display current-configuration interface <i>interface-type interface-number</i>

After the configuration succeeds, run the preceding command. You can view that external loopback detection is correctly configured on the Ethernet interface.

```
[Quidway] display current-configuration interface GigabitEthernet0/0/1
# interface GigabitEthernet0/0/1
    loopback-detect enable
    loopback-detect interval 9
    loopback-detect action shutdown
# return
```

1.6 Creating an Eth-Trunk

This section describes how to create an Eth-Trunk.

[1.6.1 Establishing the Configuration Task](#)

[1.6.2 Creating an Eth-Trunk](#)

[1.6.3 Adding Member Interfaces to an Eth-Trunk](#)

[1.6.4 \(Optional\) Setting the Load Balancing Mode for an Eth-Trunk](#)

[1.6.5 Checking the Configuration](#)

1.6.1 Establishing the Configuration Task

Applicable Environment

You can configure Eth-Trunks in the following scenarios:

- The bandwidth is insufficient when two S-switches are connected through a single link.
- The connection reliability cannot be satisfied when two S-switches are connected through a single link.

In the preceding situations, Eth-Trunks can be applied to balance the outgoing and incoming traffic among all physical links. This increases the bandwidth and connection reliability between the two S-switchs.

Pre-configuration Tasks

None.

Data Preparation

To configure Eth-Trunks, you need the following data.

No.	Data
1	IDs of Eth-Trunks
2	Types and numbers of member interfaces

1.6.2 Creating an Eth-Trunk

Context

Do as follows on the S-switch and the peer S-switch where an Eth-Trunk needs to be created.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface eth-trunk *trunk-id*** command to create an Eth-Trunk.
- End

1.6.3 Adding Member Interfaces to an Eth-Trunk

Context

Do as follows on the S-switch and the peer S-switch where an Eth-Trunk needs to be configured.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface { **ethernet** | **gigabitethernet** } *interface-number*** command to enter the Ethernet interface view or GE interface view.
- Step 3** Run the **eth-trunk *trunk-id*** command to add the Ethernet interface or GE interface to an Eth-Trunk.

When you add an Ethernet interface to an Eth-Trunk, the interface must adopt the default values of certain attributes. Otherwise, the interface cannot be added to the Eth-Trunk.

 **NOTE**

If the Multiple Spanning Tree Protocol (MSTP) is enabled on the device where the interface to be added to an Eth-Trunk resides, you must shut down the interface before adding the interface to the Eth-Trunk. After the interface is added to the Eth-Trunk, you can enable the interface. Otherwise, a temporary broadcast storm occurs.

----End

1.6.4 (Optional) Setting the Load Balancing Mode for an Eth-Trunk

Context

Do as follows on the S-switch and the peer S-switch where an Eth-Trunk needs to be configured.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface eth-trunk *trunk-id*** command to enter the Eth-Trunk interface view.
- Step 3** Run the **load-balance { *dmac* | *smac* | *smacxordmac* }** command to set the load balancing mode for the Eth-Trunk.

By default, the load balancing mode of an Eth-Trunk is **smacxordmac**.

----End

1.6.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the member interfaces of an Eth-Trunk.	display trunkmembership eth-trunk <i>trunk-id</i>
Check the load balancing mode of an Eth-Trunk.	display interface eth-trunk [<i>trunk-id</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]

After the configuration succeeds, the following results can be obtained with the preceding commands:

- The member interfaces are properly configured for the Eth-Trunk.
- The load balancing mode is properly set for the Eth-Trunk.

1.7 Deleting an Eth-Trunk

Deleting an Eth-Trunk

1.7.2 (Optional) Deleting a Member Interface from an Eth-Trunk is the prerequisite to **1.7.3 (Optional) Deleting an Eth-Trunk**. You must delete all member interfaces of an Eth-Trunk before deleting the Eth-Trunk.

[1.7.1 Establishing the Configuration Task](#)

[1.7.2 \(Optional\) Deleting a Member Interface from an Eth-Trunk](#)

[1.7.3 \(Optional\) Deleting an Eth-Trunk](#)

[1.7.4 Checking the Configuration](#)

1.7.1 Establishing the Configuration Task

Applicable Environment

The configuration task is applicable to the following:

- A member interface needs to be deleted from an Eth-Trunk.
- An Eth-Trunk needs to be deleted.

Pre-configuration Tasks

Before deleting an Eth-Trunk, you must configure the Eth-Trunk or member interfaces of the Eth-Trunk.

Data Preparation

To delete member interfaces from an Eth-Trunk or delete an Eth-Trunk, you need the following data.

No.	Data
1	(Optional) Numbers of the member interfaces to be deleted
2	(Optional) ID of the Eth-Trunk to be deleted

1.7.2 (Optional) Deleting a Member Interface from an Eth-Trunk

Context

Do as follows to delete a member interface from an Eth-Trunk.

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 Ethernet interface view.
- Step 3** Run the **undo eth-trunk** *trunk-id* command to delete the Ethernet interface from a specified Eth-Trunk.
- End

1.7.3 (Optional) Deleting an Eth-Trunk

Context

Do as follows to delete an Eth-Trunk.

Procedure

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

Step 2 Run the **undo interface eth-trunk *trunk-id*** command to delete the specified Eth-Trunk.



NOTE

Ensure that all member interfaces of an Eth-Trunk are deleted before deleting the Eth-Trunk. Otherwise, the Eth-Trunk cannot be deleted.

----End

1.7.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check member interfaces of an Eth-Trunk.	display trunkmembership eth-trunk <i>trunk-id</i>
Check an Eth-Trunk.	display current-configuration [{ begin exclude include } <i>regular-expression</i>]

After the configuration succeeds, the following results can be obtained with the preceding commands:

- The member interfaces are properly configured for the Eth-Trunk.
- The current configuration is displayed in the system view and you can find that the specified Eth-Trunk is deleted.

1.8 Configuring Interface Isolation

This section describes how to configure interface isolation.

[1.8.1 Establishing the Configuration Task](#)

[1.8.2 Configuring Interface Isolation](#)

[1.8.3 Checking the Configuration](#)

1.8.1 Establishing the Configuration Task

Applicable Environment

When two Ethernet interfaces, two Eth-Trunks, or an Ethernet interface and an Eth-Trunk do not need to communicate, or only unidirectional communication is required, you can configure interface isolation to implement unidirectional isolation or bidirectional isolation.

Pre-configuration Tasks

None.

Data Preparation

To configure interface isolation, you need the following data.

No.	Data
1	Number of the Ethernet interface to be isolated

1.8.2 Configuring Interface Isolation

Context

Do as follows on the S-switch that needs interface isolation.

If you want to implement unidirectional isolation between Interface A and Interface B so that packets sent by interface A cannot reach interface B whereas packets sent by interface B can reach interface A, specify the parameters as follows:

- *interface-type interface-number* in **Step 2** should specify the type and number of Interface A.
- { *interface-type interface-number* } &<1-8> in **Step 3** should specify the type and number of Interface B.

If you want to implement bidirectional isolation between Interface A and Interface B so that packets sent from Interface A and Interface B cannot reach each other, use the following ways:

- To isolate Interface B from Interface A, in addition to the preceding configuration, specify the parameters as follows:
 - *interface-type interface-number* in **Step 2** should specify the type and number of Interface B.
 - { *interface-type interface-number* } &<1-8> in **Step 3** should specify the type and number of Interface A.
- To add Interface A and Interface B to an isolation group, specify the parameters as follows:
 - *interface-type interface-number* of **interface** in **Step 2** should specify the type and number of Interface A and that of Interface B.
 - The **port-isolateenable** command in **Step 3** should be run on Interface A and Interface B.

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 Ethernet interface view, Eth-Trunk interface view, or GE interface view.

Step 3 Run the **am isolate** { *interface-type interface-number* }&<1-8> command or the **port-isolate enable** command to configure interface isolation.

----End

1.8.3 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the configuration of interface isolation on an Ethernet interface or an Eth-Trunk.	display current-configuration interface <i>interface-type interface-number</i>
Check information about the interfaces added to an isolation group.	display port-isolate group

After the configuration succeeds, run the preceding command. You can view that interface isolation is correctly configured on an Ethernet interface or an Eth-Trunk.

1.9 Configuring Storm Control

This section describes how to configure storm control.

[1.9.1 Establishing the Configuration Task](#)

[1.9.2 Configuring Storm Control](#)

[1.9.3 Checking the Configuration](#)

1.9.1 Establishing the Configuration Task

Applicable Environment

When an interface receives packets, you can configure storm control to regulate broadcast or multicast packets in the inbound direction of the interface. In the interval for checking storm control, when the average receiving rate of packets on an interface is greater than the specified upper threshold, storm control is performed to block packets or shut down the interface.

Pre-configuration Tasks

Before configuring storm control, complete the following tasks:

- Configuring physical parameters for the interface
- Configuring the data link layer for the interface

Data Preparation

To configure storm control, you need the following data.

No.	Data
1	Type of the packet, the lower and the upper threshold of the rate
2	Action of storm control
3	Interval for checking storm control
4	Status of traps and logs

1.9.2 Configuring Storm Control

Context

Do as follows on the interface that needs to be configured with storm control.

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 **storm-control** { **broadcast** | **multicast** } **min-rate** *min-rate-value* **max-rate** *max-rate-value* command to perform storm control on multicast or broadcast packets on an interface.
- Step 4** Run the **storm-control action** { **block** | **shutdown** } command to configure the storm control action.
- By default, storm control is disabled.
- Step 5** Run the **storm-control enable** { **log** | **trap** } command to enable the function of recording logs or reporting traps during storm control.
- By default, functions of recording logs and reporting traps during storm control are disabled.
- Step 6** Run the **storm-control interval** *interval-value* command to set the interval for checking storm control.
- By default, the interval for checking storm control is 3 seconds.
- End

1.9.3 Checking the Configuration

Prerequisite

The configurations of the storm control function are complete.

Procedure

Run the **display storm-control** [**interface** { *interface-name* | *interface-type interface-number* }] command to check information about storm control on an interface.

----End

Example

Run the **display storm-control** command to check the name of the interface, the type of the packet, the lower threshold and the upper threshold of the rate, the action of storm control, the status of packets, the status of traps and logs, and the interval for checking storm control. Take the following as an example:

```
<Quidway> system-view
[Quidway] display storm-control interface GigabitEthernet 0/0/1
PortName           Type      MinRate  MaxRate  Action  Status  Trap Log
Interval
-----
GigabitEthernet0/0/1 Broadcast 3000     5000     Block   Normal  Off  Off  3
```

1.10 Maintaining Ethernet Interfaces

This section describes how to maintain Ethernet interfaces.



CAUTION

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

When a fault occurs on an Ethernet interface or an Eth-Trunk, you can run the following **debugging** command in the user view to debug the Ethernet interface or Eth-Trunk, view the debugging information, locate the fault, and analyze the cause. For the procedure for displaying the debugging information, refer to the chapter "Maintenance and Debugging" in the *Quidway S5300 Series Ethernet Switches Configuration Guide - Device Management*.

Action	Command
Enable the debugging of data link layer features.	debugging l2if [error event msg updown]

1.11 Configuration Examples

This section provides several examples for configuring Ethernet interfaces.

[1.11.1 Example for Setting Attributes of Ethernet Interfaces](#)

[1.11.2 Example for Configuring Interface Isolation](#)

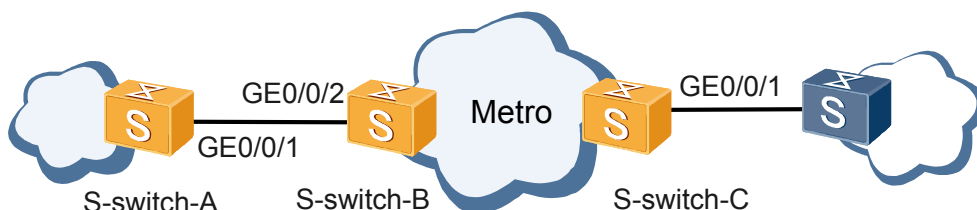
1.11.1 Example for Setting Attributes of Ethernet Interfaces

Networking Requirements

As shown in [Figure 1-3](#), GE 0/0/1 on S-switch-A is connected to GE 0/0/2 on S-switch-B; GE 0/0/1 on S-switch-C is connected to a LAN switch (LSW).

- To prevent congestion on the links, it is required that auto-negotiation of flow control be enabled on S-switch-A and S-switch-B.
- To ensure normal transmission of services, it is required that the following be achieved on the Ethernet interfaces of all the S-switches:
 - The maximum percentage of broadcast, multicast, and unknown unicast traffic that an Ethernet interface allows to pass through is not more than 15%.
 - Jumbo frames are allowed to pass through.

Figure 1-3 Networking for setting attributes of Ethernet interfaces



Configuration Roadmap

The configuration roadmap is as follows:

- Configure traffic suppression on S-switch-A, S-switch-B, and S-switch-C.
- Configure auto-negotiation of flow control on S-switch-A and S-switch-B.
- Configure S-switch-A, S-switch-B, and S-switch-C to allow jumbo frames to pass through.

Data Preparation

To complete the configuration, you need the following data:

- Numbers of interfaces that connect S-switch-A and S-switch-B
- Number of the interface on S-switch-C that connects the LSW

Configuration Procedure

1. Configure traffic suppression on S-switch-A, S-switch-B, and S-switch-C.

Configure S-switch-A.

```

<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] broadcast-suppression 15
[Quidway-GigabitEthernet0/0/1] multicast-suppression 15
[Quidway-GigabitEthernet0/0/1] unicast-suppression 15
    
```

Configure S-switch-B.

```

<Quidway> system-view
[Quidway] interface gigabitethernet 1/0/2
[Quidway-GigabitEthernet0/0/2] broadcast-suppression 15
[Quidway-GigabitEthernet0/0/2] multicast-suppression 15
[Quidway-GigabitEthernet0/0/2] unicast-suppression 15
    
```

Configure S-switch-C.

```

<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] broadcast-suppression 15
[Quidway-GigabitEthernet0/0/1] multicast-suppression 15
[Quidway-GigabitEthernet0/0/1] unicast-suppression 15

```

2. Configure auto-negotiation of flow control on S-switch-A and S-switch-B.

Configure S-switch-A.

```

<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] negotiation auto
[Quidway-GigabitEthernet0/0/1] flow-control negotiation

```

Configure S-switch-B.

```

<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] negotiation auto
[Quidway-GigabitEthernet0/0/2] flow-control negotiation

```

3. Configure S-switch-A, S-switch-B, and S-switch-C to allow jumbo frames to pass through.

Configure S-switch-A.

```

<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet1/0/1] jumboframe enable

```

Configure S-switch-B.

```

<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] jumboframe enable

```

Configure S-switch-C.

```

<Quidway> system-view
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] jumboframe enable

```

Configuration Files

- Configuration file of S-switch-A

```

#
interface gigabitethernet0/0/1
 broadcast-suppression 15
 multicast-suppression 15
 unicast-suppression 15
 negotiation auto
 flow-control negotiation
 jumboframe enable
#
return

```

- Configuration file of S-switch-B

```

#
interface gigabitethernet0/0/2
 broadcast-suppression 15
 multicast-suppression 15
 unicast-suppression 15
 negotiation auto
 flow-control negotiation
 jumboframe enable
#
return

```

- Configuration files of S-switch-C

```

#
interface gigabitethernet0/0/1
 broadcast-suppression 15
 multicast-suppression 15

```

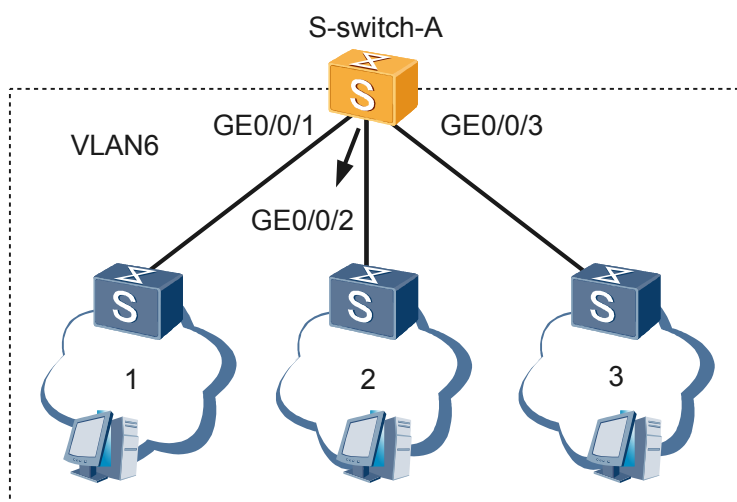
```
unicast-suppression 15
jumboframe enable
#
return
```

1.11.2 Example for Configuring Interface Isolation

Networking Requirements

As shown in [Figure 1-4](#), security threats exist in the network connected to GigabitEthernet 0/0/2. Thus, it is required that GigabitEthernet 0/0/2 be isolated from GigabitEthernet 0/0/1, and GigabitEthernet 0/0/2 and GigabitEthernet 0/0/3 be isolated from each other.

Figure 1-4 Networking for configuring interface isolation



Configuration Roadmap

The configuration roadmap is as follows:

- Isolate GigabitEthernet 0/0/2 from GigabitEthernet 0/0/1 and GigabitEthernet 0/0/3.
- Isolate GigabitEthernet 0/0/3 from GigabitEthernet 0/0/2.

Data Preparation

To complete the configuration, you need the following data:

- Numbers of interfaces that connect S-switch-A to the three LSWs

Configuration Procedure

1. Isolate GigabitEthernet 0/0/2 from GigabitEthernet 0/0/1 and GigabitEthernet 0/0/3.

```
[Quidway] interface ethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] am isolate ethernet 0/0/1
[Quidway-GigabitEthernet0/0/2] am isolate ethernet 0/0/3
[Quidway-GigabitEthernet0/0/2] quit
```

2. Isolate GigabitEthernet 0/0/3 from GigabitEthernet 0/0/2.

```
[Quidway] interface ethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] am isolate ethernet 0/0/2
```

Add GigabitEthernet 0/0/2 and GigabitEthernet 0/0/3 to an isolation group to implement bidirectional isolation between GigabitEthernet 0/0/2 and GigabitEthernet 0/0/3.

```
[Quidway] interface ethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port-isolate enable
[Quidway-GigabitEthernet0/0/2] quit
[Quidway] interface ethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port-isolate enable
```

3. Verify the configuration.

Do as follows to verify the configuration:

- Ping a host in Network 2 from a host in Network 1. The ping fails. The host in Network 2 can receive packets sent from Network 1; the host in Network 1, however, cannot receive the packets replied from Network 2. This indicates that Ethernet 0/0/2 is isolated from GigabitEthernet 0/0/1.
- Ping a host in Network 2 from a host in Network 3. The ping fails; the host in Network 2 cannot receive packets sent from Network 3. Ping a host in Network 3 from a host in Network 2. The ping fails; the host in Network 3 cannot receive packets sent from Network 2. This indicates that GigabitEthernet 0/0/2 and GigabitEthernet 0/0/3 are isolated from each other.

Configuration Files

Configuration file of S-switch-A

```
#
 sysname Quidway
#
vlan batch 6
#
interface ethernet0/0/1
 port default vlan 6
#
interface ethernet0/0/2
 port default vlan 6
 am isolate ethernet0/0/1 ethernet0/0/3
#
interface ethernet0/0/3
 port default vlan 6
 am isolate ethernet0/0/2
#
return
```

Or, configuration file of S-switch-A

```
#
 sysname Quidway
#
vlan batch 6
#
interface ethernet0/0/1
 port default vlan 6
#
interface ethernet0/0/2
 port default vlan 6
 am isolate ethernet0/0/1 ethernet0/0/3
 port-isolate enable
#
interface ethernet0/0/3
 port default vlan 6
 port-isolate enable
```

```
#  
return
```


2 LACP Configuration

About This Chapter

This chapter describes basic knowledge, configuration methods, and configuration examples of the Link Aggregation Control Protocol (LACP).

[2.1 Introduction to Link Aggregation](#)

This section describes the concepts of link aggregation and the classification of link aggregation supported by the S-switch.

[2.2 Configuring Link Aggregation in Manual Load Balancing Mode](#)

This section describes how to configure link aggregation in manual load balancing mode.

[2.3 Configuring Link Aggregation in Static LACP Mode](#)

This section describes how to configure link aggregation in static LACP mode.

[2.4 Maintaining LACP](#)

This section describes how to maintain LACP.

[2.5 Configuration Examples](#)

This section provides several configuration examples of LACP.

2.1 Introduction to Link Aggregation

This section describes the concepts of link aggregation and the classification of link aggregation supported by the S-switch.

[2.1.1 Link Aggregation Overview](#)

[2.1.2 Link Aggregation Modes Supported by the S-switch](#)

[2.1.3 Related Concepts of LACP](#)

[2.1.4 Logical Relationships Between Configuration Tasks](#)

[2.1.5 Update History](#)

2.1.1 Link Aggregation Overview

Link aggregation refers to a method of binding a group of physical interfaces together as a logical interface to increase the bandwidth. Link aggregation is also called the multi-interface load sharing group or Link Aggregation Group (LAG). For more information about link aggregation, refer to IEEE802.3ad.

By setting up an LAG between two devices, you can obtain higher bandwidth and greater reliability. Link aggregation provides redundancy protection for communications among devices without upgrading the hardware.

2.1.2 Link Aggregation Modes Supported by the S-switch

Manual Load Balancing Mode

In manual load balancing mode, you can manually add member interfaces to an LAG. All interfaces are in the forwarding state to transmit packets. Load balancing that the S-switch supports can be based on the following:

- Destination MAC address
- Source MAC address
- Exclusive-OR operation of the source MAC address and the destination MAC address

In manual load balancing mode, you must set up an Eth-Trunk and add interfaces to the Eth-Trunk. You must also configure member interfaces in the active state. The Link Aggregation Control Protocol Data Units (LACPDU) are not required.

The manual load balancing mode is used when the peer device does not support LACP.

Static LACP Mode

The static LACP mode refers to a link aggregation method of determining active and inactive interfaces by negotiating aggregation parameters through LACPDU. In static LACP mode, you must manually set up an Eth-Trunk and add member interfaces to the Eth-Trunk. The active and inactive interfaces are negotiated through parameters in the LACPDU.

The static LACP mode is called M:N mode. The static LACP mode can implement load balancing and backup. In an LAG, M links are active to forward data and perform load balancing.

In addition, other N links are inactive. They act as backup links that do not forward data. When a fault occurs on one of the M links, the system selects the link with the highest priority from the N backup links to replace the faulty link. At the same time, the link becomes active and starts to forward data.

There is the dynamic LACP mode in comparison to the static LACP mode. In dynamic LACP mode, the creation of the Eth-Trunk and the addition of the member interfaces are automatically negotiated through parameters in the LACPDUs without manual interference. The dynamic LACP mode can be easily configured. It is, however, too flexible and thus hard to manage. The S-switch does not support link aggregation in dynamic LACP mode.

2.1.3 Related Concepts of LACP

Active and Inactive Interfaces

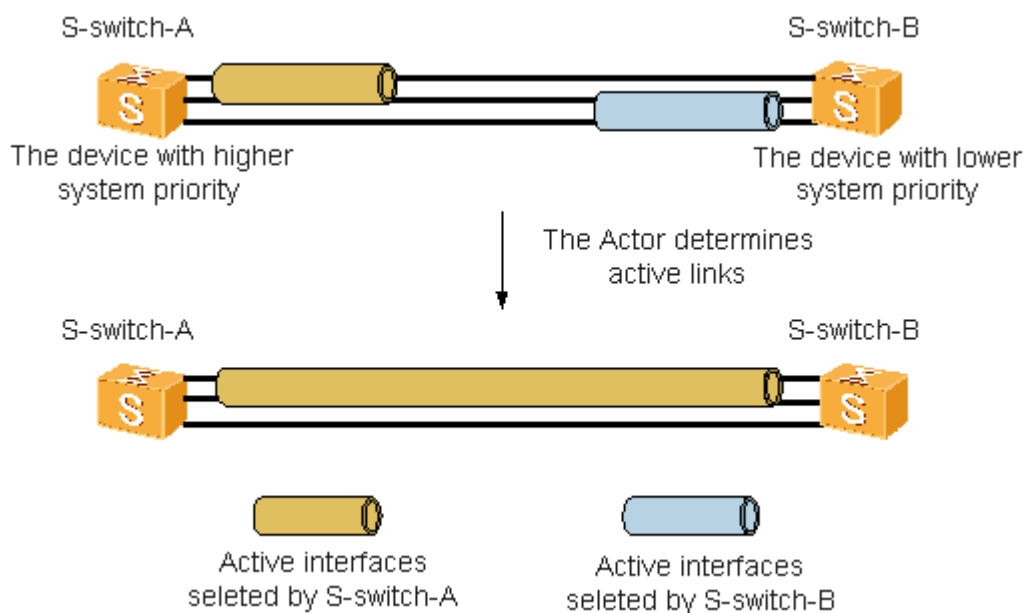
The interfaces that are responsible for forwarding data are active interfaces. In contrary, the interfaces that do not forward data are inactive interfaces. According to the operation modes, active and inactive interfaces are classified as follows:

- Manual load balancing mode: Generally, all member interfaces are active ones unless faults occur on these interfaces.
- Static LACP mode: The interfaces connected to M links are active interfaces that are responsible for forwarding data; the interfaces connected to N links are inactive interfaces that are responsible for redundancy.

Actor and Partner

In static LACP mode, the device with a higher LACP priority at both ends of an LAG is the Actor and the device with a lower LACP priority is the Partner.

Differentiating the Actor and the Partner is to ensure that active interfaces of devices at both ends are the same. If devices at both ends select active interfaces according to the priority of their own interfaces, the active interfaces may be different and the active links cannot be set up. Therefore, the Actor is first determined. The Partner selects active interfaces according to the priority of the interfaces of the Actor, as shown in [Figure 2-1](#).

Figure 2-1 Determining the active links by the Actor in static LACP mode

2.1.4 Logical Relationships Between Configuration Tasks

There is no strict logical relationship between configuration tasks. You can perform any configuration task as required.

2.1.5 Update History

Version	Revision
V200R002C01B010	This is the first release.

2.2 Configuring Link Aggregation in Manual Load Balancing Mode

This section describes how to configure link aggregation in manual load balancing mode.

[2.2.1 Establishing the Configuration Task](#)

[2.2.2 Creating an Eth-Trunk](#)

[2.2.3 \(Optional\) Configuring the Eth-Trunk to Work in Manual Load Balancing Mode](#)

[2.2.4 Adding a Member Interface to the Eth-Trunk](#)

[2.2.5 \(Optional\) Setting the Load Balancing Mode](#)

[2.2.6 Checking the Configuration](#)

2.2.1 Establishing the Configuration Task

Applicable Environment

As shown in [Figure 2-2](#), when the bandwidth or the reliability of two devices needs to be increased, you can create an Eth-Trunk in manual load balancing mode on the S-switch and add multiple member interfaces to the Eth-Trunk to increase the bandwidth and reliability of devices.

Figure 2-2 Networking diagram of link aggregation in manual load balancing mode



Pre-configuration Tasks

Before configuring link aggregation in manual load balancing mode, complete the following task:

- Powering on the S-switch

Data Preparation

Before configuring link aggregation in manual load balancing mode, you need the following data.

No.	Data
1	Number of the Eth-Trunk in manual load balancing mode
2	Type and number of the member interface

2.2.2 Creating an Eth-Trunk

Context

Do as follows on the S-switches at both ends.

Procedure

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

Step 2 Run the **interface eth-trunk** *trunk-id* command to create an Eth-Trunk and enter the Eth-Trunk interface view.

NOTE

The IDs of the Eth-Trunks created on the S-switches at both ends can be different. To identify and maintain the Eth-Trunks at both ends, using the same ID for the Eth-Trunks at both ends is recommended.

----End

2.2.3 (Optional) Configuring the Eth-Trunk to Work in Manual Load Balancing Mode

Context

**NOTE**

Ensure that an Eth-Trunk does not contain any member interface before you configure the operation mode of the Eth-Trunk; otherwise, the operation mode of the Eth-Trunk cannot be changed. Run the **undo eth-trunk trunk-id** command in the interface view to delete the existing member interfaces.

Do as follows on the S-switchs at both ends.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface eth-trunk trunk-id** command to enter the Eth-Trunk interface view.
- Step 3** Run the **mode manual [load-balance]** command to configure the Eth-Trunk to work in manual load balancing mode.

By default, an Eth-Trunk works in manual load balancing mode. If you do not adjust the operation mode of an Eth-Trunk to the static LACP mode during or after the establishment of the Eth-Trunk, you can choose not to configure the manual load balancing mode.

----End

2.2.4 Adding a Member Interface to the Eth-Trunk

Context

Do as follows on the S-switchs at both ends.

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 **eth-trunk trunk-id** command to add the current interface to the Eth-Trunk.

**NOTE**

When adding an interface to an Eth-Trunk, ensure that no configuration such as the cable type, duplex mode, and rate exists on the interface. Run the **display this** command to check whether the configuration exists on the interface. If the configuration exists on the interface, first delete the configuration, and then add the interface to the Eth-Trunk.

----End

2.2.5 (Optional) Setting the Load Balancing Mode

Context

Do as follows on the S-switchs at both ends.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface eth-trunk** *trunk-id* command to enter the Eth-Trunk interface view.
- Step 3** Run the **load-balance { dmac | smac | smacxordmac }** command to set the manual load balancing mode of the Eth-Trunk.

By default, the load balancing mode of an Eth-Trunk is **smacxordmac**.

The load balancing mode of the local end and that of the peer end can be different because they do not interact with each other.

----End

2.2.6 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the member interface of the Eth-Trunk.	display trunkmembership eth-trunk <i>trunk-id</i>
Check the manual load balancing mode of the Eth-Trunk.	display eth-trunk [<i>trunk-id</i> [interface <i>interface-type</i> <i>interface-number</i>]]

Run the **display trunkmembership eth-trunk** command. If you can view the operation mode of the Eth-Trunk as Normal, number of member interfaces, number of member interfaces in the Up state, and information about member interfaces, it means that the configuration succeeds.

```
<Quidway> display trunkmembership eth-trunk 1
Trunk ID: 1
used status: VALID
TYPE: ethernet
Working Mode : Normal
Working State: Normal
Number Of Ports in Trunk = 3
Number Of UP Ports in Trunk = 3
operate status: up

Interface Ethernet0/0/1, valid, selected, operate up, weight=1,
standby interface NULL

Interface Ethernet0/0/2, valid, selected, operate up, weight=1,
standby interface NULL

Interface Ethernet0/0/3, valid, selected, operate up, weight=1,
standby interface NULL
```

Run the **display eth-trunk** command to check the load balancing mode of an Eth-Trunk. If the load balancing mode is displayed as Normal, it means that the configuration succeeds.

```
<Quidway> display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL          Hash arithmetic: According to MAC
Least Active-linknumber: 1    Max Bandwidth-affected-linknumber: 8
Operate status: up           Number Of Up Port In Trunk: 3
-----
PortName      Status      Weight
Ethernet0/0/1 Up          1
```

Ethernet0/0/2	Up	1
Ethernet0/0/3	Up	1

2.3 Configuring Link Aggregation in Static LACP Mode

This section describes how to configure link aggregation in static LACP mode.

2.3.1 Establishing the Configuration Task

2.3.2 Creating an Eth-Trunk

2.3.3 Configuring the Eth-Trunk to Work in Static LACP Mode

2.3.4 Adding a Member Interface to the Eth-Trunk

2.3.5 Configuring the Eth-Trunk to Process BPDUs

2.3.6 (Optional) Setting the LACP Priority of the System

2.3.7 (Optional) Setting the Upper Threshold for the Number of Active Interfaces

2.3.8 (Optional) Setting the Lower Threshold for the Number of Active Interfaces

2.3.9 (Optional) Setting the LACP Priority of the Interface

2.3.10 (Optional) Enabling LACP Preemption and Setting the Delay for LACP Preemption

2.3.11 Checking the Configuration

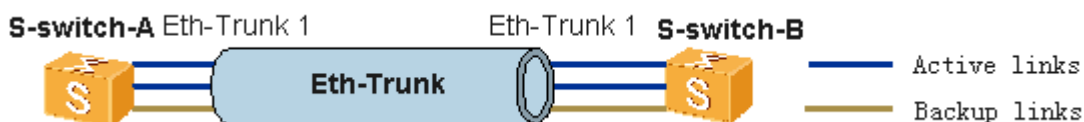
2.3.1 Establishing the Configuration Task

Applicable Environment

To improve the bandwidth and the reliability of two devices, you should create an LAG on two directly connected S-switchs. The requirements are as follows:

- The links between two devices can implement redundancy. When a fault occurs on certain links, the backup links are used to replace the faulty ones to keep data transmission uninterrupted.
- The active links can perform load balancing.

Figure 2-3 Networking diagram of link aggregation in static LACP mode



NOTE

An Eth-Trunk in static LACP mode does not support the following interfaces to be aggregated:

- Gigabit Ethernet interfaces and 100M Ethernet interfaces
- Interfaces in half duplex mode

Pre-configuration Tasks

Before configuring link aggregation in static LACP mode, complete the following task:

- Powering on the S-switch

Data Preparation

To configure link aggregation in static LACP mode, you need the following data.

No.	Data
1	Number of the Eth-Trunk
2	Type and number of the member interface
3	Upper threshold for the number of active interfaces

2.3.2 Creating an Eth-Trunk

Context

Do as follows on the S-switches at both ends.

Procedure

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

Step 2 Run the **interface eth-trunk trunk-id** command to create an Eth-Trunk and enter the Eth-Trunk interface view.

NOTE

The IDs of the Eth-Trunks created on the S-switches at both ends can be different. To identify and maintain the Eth-Trunks at both ends, using the same ID for the Eth-Trunks at both ends is recommended.

----End

2.3.3 Configuring the Eth-Trunk to Work in Static LACP Mode

Context

NOTE

Ensure that the Eth-Trunk does not contain any member interface before you configure the operation mode of the Eth-Trunk; otherwise, the operation mode of the Eth-Trunk cannot be modified. Run the **undo eth-trunk trunk-id** command in the interface view to delete the existing member interfaces.

Do as follows on the S-switches at both ends.

Procedure

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

Step 2 Run the **interface eth-trunk trunk-id** command to enter the Eth-Trunk interface view.

Step 3 Run the **mode lacp-static** command to configure the Eth-Trunk to work in static LACP mode.

By default, an Eth-Trunk works in manual load balancing mode.

Step 4 Using the **lacp timeout { fast | slow }** command, you can set the timeout duration of LACP packets.

By default, the timeout duration of LACP packets is thirty seconds.

----End

2.3.4 Adding a Member Interface to the Eth-Trunk

Context

Do as follows on the S-switchs at both ends.

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 **eth-trunk trunk-id** command to add the interface to the Eth-Trunk.

NOTE

- When adding an interface to an Eth-Trunk, ensure that no configuration exists on the interface. You can configure the cable type, duplex mode, and rate for the interface. Run the **display this** command to check whether the configuration exists on the interface. If the configuration exists on the interface, first delete the configuration, and then add the interface to the Eth-Trunk.
- The number of interfaces added to the LAG should not be greater than eight.

----End

2.3.5 Configuring the Eth-Trunk to Process BPDUs

Context

Do as follows on the S-switchs at both ends.

Procedure

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

Step 2 Run the **interface eth-trunk trunk-id** command to enter the Eth-Trunk interface view.

Step 3 Run the **bpdu enable** command to configure the interface to process Bridge Protocol Data Units (BPDUs).

By default, an interface does not process BPDUs.

When configuring link aggregation in static LACP mode, you need run the **bpdu enable** command in the Eth-Trunk view so that the S-switch can receive and process LACPDUs. If the

bpdu enable command is not run, the S-switch discards LACPDUs. As a result, the Eth-Trunk becomes Down.

----End

2.3.6 (Optional) Setting the LACP Priority of the System

Context

Do as follows on the S-switchs at both ends.

Procedure

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

Step 2 Run the **lacp priority *priority*** command to set the LACP priority for the system of the S-switch.

The lower the LACP priority of the system is, the higher the priority of the S-switch is.

You can select a S-switch at one end as the Actor and set the LACP priority of the system to a smaller value. By default, the LACP priority of the system is 32768. Therefore, one end can be the Actor only when its LACP priority of the system is smaller than 32768.

----End

2.3.7 (Optional) Setting the Upper Threshold for the Number of Active Interfaces

Context

Do as follows on the S-switchs at both ends.

Procedure

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

Step 2 Run the **interface eth-trunk *trunk-id*** command to enter the Eth-Trunk interface view.

Step 3 Run the **max bandwidth-affected-linknumber *link-number*** command to set the upper threshold for the number of active interfaces.

By default, the upper threshold for the number of active interfaces is 8.

In static LACP mode, you can control maximum number M of active interfaces in an Eth-Trunk by setting the upper threshold for the number of active interfaces. The remaining member interfaces are backup ones.

If the upper threshold is not set, a maximum of eight interfaces in the Eth-Trunk can be active.

 **NOTE**

- The upper threshold for the number of active interfaces should not be smaller than the lower threshold for the number of active interfaces.
- The upper threshold for the number of active interfaces of the local S-switch and that of the remote S-switch can be different. If the upper threshold for the number of active interfaces at both ends is different, take the smaller upper threshold.

----End

2.3.8 (Optional) Setting the Lower Threshold for the Number of Active Interfaces

Context

Do as follows on the S-switchs at both ends.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **interface eth-trunk** *trunk-id* command to enter the Eth-Trunk interface view.
- Step 3** Run the **least active-linknumber** *link-number* command to set the lower threshold for the number of active interfaces.

By default, the lower threshold for the number of active interfaces is 1.

In static LACP mode, you can determine the minimum number of active interfaces in an Eth-Trunk by setting the lower threshold for the number of active interfaces. If the number of active interfaces in static LACP mode is smaller than the value, the interface of the Eth-Trunk becomes Down.

 **NOTE**

- The lower threshold for the number of active interfaces should not be greater than the upper threshold for the number of active interfaces.
- The lower threshold for the number of active interfaces of the local S-switch and that of the remote S-switch can be different. If the lower threshold at both ends are different, take the greater lower threshold.

----End

2.3.9 (Optional) Setting the LACP Priority of the Interface

Context

Do as follows on the S-switchs at both ends.

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 **lacp priority** *priority* command to set the LACP priority for the interface.

By default, the LACP priority of an interface is 32768.

 **NOTE**

The LACP priority of the interface indicates the priority when the interface becomes the active interface. The lower the LACP priority of the interface is, the higher the priority of the interface is. By default, the LACP priority of an interface is 32768.

----End

2.3.10 (Optional) Enabling LACP Preemption and Setting the Delay for LACP Preemption

Context

Do as follows on the S-switches at both ends.

Procedure

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

Step 2 Run the **interface eth-trunk** *trunk-id* command to enter the Eth-Trunk interface view.

Step 3 Run the **lacp preempt enable** command to enable LACP preemption for the Eth-Trunk.

By default, LACP preemption is disabled.

Step 4 Run the **lacp preempt delay** *delay-time* command to set the delay for LACP preemption on the Eth-Trunk.

By default, the delay for LACP preemption is 30s.

 **NOTE**

Before enabling LACP preemption, you should set the upper threshold for the number of active interfaces.

The preemption function takes effect only on the active interface. The preemption function must be configured together with the upper limit of active interfaces. To guarantee that the preemption function works normally, it is recommended that the preemption function and the upper limit of active interfaces be configured on only the active interface before you use the preemption function.

When LACP preemption is enabled, the interface with the highest LACP priority can be an active interface. For example, when an interface with a high priority switches to inactive due to failure and then recovers, the interface can become the active interface if LACP preemption is enabled; the interface cannot become the active interface if the LACP preemption function is disabled.

The delay for LACP preemption refers to the period when an inactive interface of the Eth-Trunk in static LACP mode switches to active.

----End

2.3.11 Checking the Configuration

Run the following commands on both S-switches to check the previous configuration.

Action	Command
Check the member interface of the Eth-Trunk.	display trunkmembership eth-trunk <i>trunk-id</i>
Check information about the Eth-Trunk and active interfaces.	display eth-trunk [<i>trunk-id</i> [interface <i>interface-type interface-number</i>]]

Run the **display trunkmembership eth-trunk** command. If you can view the operation mode of the Eth-Trunk as Static, number of member interfaces, number of member interfaces in the Up state, and information about member interfaces, it means that the configuration succeeds.

```
<Quidway> display trunkmembership eth-trunk 1
Trunk ID: 1
used status: VALID
TYPE: ethernet
Working Mode : Static
Number Of Ports in Trunk = 3
Number Of UP Ports in Trunk = 3
operate status: up
Interface GigabitEthernet0/0/1, valid, selected, operate up, weight=1,
standby interface NULL
Interface GigabitEthernet0/0/2, valid, selected, operate up, weight=1,
standby interface NULL
Interface GigabitEthernet0/0/3, valid, selected, operate down, weight=1,
standby interface NULL
```

Run the **display eth-trunk** command to check the working mode.

```
<Quidway> display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                               WorkingMode: STATIC
Preempt Delay Time: 60 Sec              Hash arithmetic: According to MAC
System Priority: 50                      System ID: 0001-0168-0182
Least Active-linknumber: 1              Max Bandwidth-affected-linknumber: 8
Operate status: down                    Number Of Up Port In Trunk: 0
-----
ActorPortName      Status    PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/1 Selected 100M    32768 1      289    11111100 1
GigabitEthernet0/0/2 Selected 100M    32768 2      289    11111100 1
GigabitEthernet0/0/3 Selected 100M    32768 3      289    11111100 1
Partner:
-----
ActorPortName      SysPri    SystemID PortPri PortNo PortKey PortState
GigabitEthernet0/0/1 32768    0077-7777-7777 32768 1      289    11111100
GigabitEthernet0/0/2 32768    0077-7777-7777 32768 2      289    11111100
GigabitEthernet0/0/3 32768    0077-7777-7777 32768 3      289    11111100
```

2.4 Maintaining LACP

This section describes how to maintain LACP.

[2.4.1 Clearing the Statistics of Received and Sent LACPDUs](#)

[2.4.2 Debugging LACP](#)

[2.4.3 Monitoring the Operation Status of the LAG](#)

2.4.1 Clearing the Statistics of Received and Sent LACPDUs



CAUTION

The statistics of received and sent LACPDUs cannot be restored after you clear them. So, confirm the action before you use the command.

To clear the statistics of received and sent LACPDUs, run the following command in the user view.

Action	Command
Clear the statistics of received and sent LACPDUs.	reset lacp statistics eth-trunk [<i>trunk-id</i> [interface <i>interface-type interface-number</i>]]

2.4.2 Debugging LACP



CAUTION

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

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

Action	Command
Debug Eth-Trunk errors.	debugging trunk error [<i>slot slot-number</i>]
Debug Eth-Trunk events.	debugging trunk event [<i>slot slot-number</i>]
Debug LACPDUs.	debugging trunk lacp-pdu [<i>slot slot-number</i>]
Debug LACP messages.	debugging trunk lagmsg [<i>slot slot-number</i>]
Debug Eth-Trunk messages.	debugging trunk msg [<i>slot slot-number</i>]
Debug Eth-Trunk state machines.	debugging trunk state-machine [<i>slot slot-number</i>]
Debug information when the Eth-Trunk is Up and Down.	debugging trunk updown [<i>slot slot-number</i>]

2.4.3 Monitoring the Operation Status of the LAG

During routine maintenance, you can run the following commands in any view to check the operation status of the LAG.

Action	Command
Check the status of the LAG.	display eth-trunk [<i>trunk-id</i> [interface <i>interface-type</i> <i>interface-number</i>]]
Check the statistics of received and sent LACPDUs.	display lacp statistics eth-trunk [<i>trunk-id</i> [interface <i>interface-type</i> <i>interface-number</i>]]
Check the member interface of the Eth-Trunk.	display trunkmembership eth-trunk <i>trunk-id</i>

2.5 Configuration Examples

This section provides several configuration examples of LACP.

[2.5.1 Example for Configuring Link Aggregation in Manual Load Balancing Mode](#)

[2.5.2 Example for Configuring Link Aggregation in Static LACP Mode](#)

2.5.1 Example for Configuring Link Aggregation in Manual Load Balancing Mode

Networking Requirements

As shown in [Figure 2-4](#), S-switch-A and S-switch-B are two switches and the link between S-switch-A and S-switch-B is one of the backbone transmission links of the Metropolitan Area Network (MAN). The link is required to be of high reliability and load balancing of data traffic can be performed between S-switch-A and S-switch-B.

Figure 2-4 Networking diagram of link aggregation in manual load balancing mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Create an Eth-Trunk.
2. Add member interfaces to the Eth-Trunk.

NOTE

After the Eth-Trunk is created, the Eth-Trunk works in manual load balancing mode by default. That is, you do not need to configure the Eth-Trunk in manual load balancing mode by default. If the current operation mode is configured as another mode, use the **mode** command to change the mode.

Data Preparation

To complete the configuration, you need the following data:

- Number of the LAG
- Type and number of the member interface of the Eth-Trunk

Configuration Procedure

1. Create an Eth-Trunk.

Configure S-switch-A.

```
<Quidway> system-view
[Quidway] sysname S-switch-A
[S-switch-A] interface eth-trunk 1
[S-switch-A-Eth-Trunk1] quit
```

Configure S-switch-B.

```
<Quidway> system-view
[Quidway] sysname S-switch-B
[S-switch-B] interface eth-trunk 1
[S-switch-B-Eth-Trunk1] quit
```

2. Add member interfaces to the Eth-Trunk.

Configure S-switch-A.

```
[S-switch-A] interface GigabitEthernet0/0/1
[S-switch-A-GigabitEthernet0/0/1] eth-trunk 1
[S-switch-A-GigabitEthernet0/0/1] quit
[S-switch-A] interface GigabitEthernet0/0/2
[S-switch-A-GigabitEthernet0/0/2] eth-trunk 1
[S-switch-A-GigabitEthernet0/0/2] quit
[S-switch-A] interface GigabitEthernet0/0/3
[S-switch-A-GigabitEthernet0/0/3] eth-trunk 1
[S-switch-A-GigabitEthernet0/0/3] quit
```

Configure S-switch-B.

```
[S-switch-B] interface GigabitEthernet0/0/1
[S-switch-B-GigabitEthernet0/0/1] eth-trunk 1
[S-switch-B-GigabitEthernet0/0/1] quit
[S-switch-B] interface GigabitEthernet0/0/2
[S-switch-B-GigabitEthernet0/0/2] eth-trunk 1
[S-switch-B-GigabitEthernet0/0/2] quit
[S-switch-B] interface GigabitEthernet0/0/3
[S-switch-B-GigabitEthernet0/0/3] eth-trunk 1
[S-switch-B-GigabitEthernet0/0/3] quit
```

3. Verify the configuration.

Run the **display trunkmembership** command in any view to check whether Eth-Trunk 1 is created successfully and whether member interfaces are added correctly. Take S-switch-A as an example.

```
[S-switch-A] display trunkmembership eth-trunk 1
Trunk ID: 1
used status: VALID
TYPE: ethernet
Working Mode : Normal
Working State: Normal
Number Of Ports in Trunk = 3
Number Of UP Ports in Trunk = 3
operate status: up
Interface GigabitEthernet0/0/1, valid, selected, operate up, weight=1,
standby interface NULL

Interface GigabitEthernet0/0/2, valid, selected, operate up, weight=1,
standby interface NULL
```

```
Interface GigabitEthernet0/0/3, valid, selected, operate up, weight=1,
standby interface NULL
```

Configuration Files

- Configuration file of S-switch-A


```
#
sysname S-switch-A
#
interface Eth-Trunk1
#
interface GigabitEthernet0/0/1
eth-trunk 1
#
interface GigabitEthernet0/0/2
eth-trunk 1
#
interface GigabitEthernet0/0/3
eth-trunk 1
#
return
```
- Configuration file of S-switch-B


```
#
sysname S-switch-B
#
interface Eth-Trunk1
#
interface GigabitEthernet0/0/1
eth-trunk 1
#
interface GigabitEthernet0/0/2
eth-trunk 1
#
interface GigabitEthernet0/0/3
eth-trunk 1
#
return
```

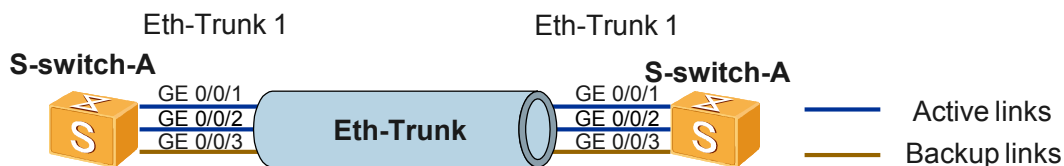
2.5.2 Example for Configuring Link Aggregation in Static LACP Mode

Networking Requirements

As shown in [Figure 2-5](#), to improve the bandwidth and the reliability of two devices, configure the link aggregation group on two directly connected S-switches. The requirements are as follows:

- M active links can perform load balancing.
- N links between two devices can act as backup links to perform redundancy. When a fault occurs on a link of active links, the backup link replaces the faulty link to keep the reliability of data transmission.

Figure 2-5 Networking diagram of link aggregation in static LACP mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Create an Eth-Trunk on the S-switch and configure the Eth-Trunk to work in static LACP mode.
2. Add member interfaces to the Eth-Trunk.
3. Configure the Eth-Trunk to process BPDUs.
4. Set the LACP priority of the system and determine the Actor.
5. Set the upper threshold for the number of active interfaces.
6. Set the LACP priority of the interface and determine the active link.

Data Preparation

To complete the configuration, you need the following data:

- Number of the LAG of the S-switches at both ends
- LACP priority of the system of S-switch-A
- Upper threshold for the number of active interfaces
- LACP priority of the active interface

Configuration Procedure

1. Create an Eth-Trunk numbered one and configure Eth-Trunk 1 to work in static LACP mode.

Configure S-switch-A.

```
<Quidway> system-view
[Quidway] sysname S-switch-A
[S-switch-A] interface eth-trunk 1
[S-switch-A-Eth-Trunk1] mode lacp-static
[S-switch-A-Eth-Trunk1] quit
```

Configure S-switch-B.

```
<Quidway> system-view
[Quidway] sysname S-switch-B
[S-switch-B] interface eth-trunk 1
[S-switch-B-Eth-Trunk1] mode lacp-static
[S-switch-B-Eth-Trunk1] quit
```

2. Add member interfaces to the Eth-Trunk.

Configure S-switch-A.

```
[S-switch-A] interface ethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] eth-trunk 1
[S-switch-A-GigabitEthernet0/0/1] quit
[S-switch-A] interface ethernet 0/0/2
[S-switch-A-GigabitEthernet0/0/2] eth-trunk 1
[S-switch-A-GigabitEthernet0/0/2] quit
[S-switch-A] interface ethernet 0/0/3
[S-switch-A-GigabitEthernet0/0/3] eth-trunk 1
[S-switch-A-GigabitEthernet0/0/3] quit
```

Configure S-switch-B.

```
[S-switch-B] interface ethernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] eth-trunk 1
```

```
[S-switch-B-GigabitEthernet0/0/1] quit
[S-switch-B] interface ethernet 0/0/2
[S-switch-B-GigabitEthernet0/0/2] eth-trunk 1
[S-switch-B-GigabitEthernet0/0/2] quit
[S-switch-B] interface ethernet 0/0/3
[S-switch-B-GigabitEthernet0/0/3] eth-trunk 1
[S-switch-B-GigabitEthernet0/0/3] quit
```

3. Configure the Eth-Trunk to process BPDUs.

Configure S-switch-A.

```
[S-switch-A] interface eth-trunk 1
[S-switch-A-Eth-Trunk1] bpdu enable
[S-switch-A-Eth-Trunk1] quit
```

Configure S-switch-B.

```
[S-switch-B] interface eth-trunk 1
[S-switch-B-Eth-Trunk1] bpdu enable
[S-switch-B-Eth-Trunk1] quit
```

4. On S-switch-A, set the LACP priority of the system to 100 so that CX-A becomes the Actor.

```
[CX-A] lacp priority 100
```

5. On CX-A, set upper threshold M for the number of active interfaces to 2.

```
[S-switch-A] interface eth-trunk 1
[S-switch-A-Eth-Trunk1] max bandwidth-affected-linknumber 2
[S-switch-A-Eth-Trunk1] quit
```

NOTE

CX-A functions as the Actor, so CX-B does not need to set the upper threshold. In Step 6, the LACP priority of the interface needs to be set on CX-A only.

6. On CX-A, set the LACP priority of the interface and determine active links.

```
[S-switch-A] interface ethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] lacp priority 100
[S-switch-A-GigabitEthernet0/0/1] quit
[S-switch-A] interface ethernet 0/0/2
[S-switch-A-GigabitEthernet0/0/2] lacp priority 100
[S-switch-A-GigabitEthernet0/0/2] quit
```

7. Verify the configuration.

Check the information about the Eth-Trunks of the S-switchs and check whether the negotiation succeeds on the link.

```
[S-switch-A] display eth-trunk 1
Eth-Trunk1's state information is:
```

Local:

```
LAG ID: 1 WorkingMode: STATIC
Preempt Delay: Disabled Hash arithmetic: According to MAC
System Priority: 100 System ID: 0077-7777-7777
Least Active-linknumber: 1 Max Bandwidth-affected-linknumber: 2
Operate status: up Number Of Up Port In Trunk: 2
```

--

ActorPortName	Status	PortType	PortPri	PortNo	PortKey	PortState
Ethernet0/0/1	Selected	100M	100	1	289	11111100 1
Ethernet0/0/2	Selected	100M	100	2	289	11111100 1
Ethernet0/0/3	Unselect	100M	32768	3	289	11100000 1

Partner:

--

ActorPortName	SysPri	SystemID	PortPri	PortNo	PortKey	PortState
Ethernet0/0/1	32768	0001-0168-0182	32768	1	289	11111100
Ethernet0/0/2	32768	0001-0168-0182	32768	2	289	11111100
Ethernet0/0/3	32768	0001-0168-0182	32768	3	289	11100000

```
[S-switch-B] display eth-trunk 1
```

Eth-Trunk1's state information is:

Local:

```
LAG ID: 1 WorkingMode: STATIC
Preempt Delay: Disabled Hash arithmetic: According to MAC
System Priority: 32768 System ID: 0001-0168-0182
Least Active-linknumber: 1 Max Bandwidth-affected-linknumber: 8
Operate status: up Number Of Up Port In Trunk: 2
```

```
-----
--
ActorPortName      Status   PortType PortPri PortNo PortKey PortState
Weight
Ethernet0/0/1      Selected 100M     32768   1      289     11111100 1
Ethernet0/0/2      Selected 100M     32768   2      289     11111100 1
Ethernet0/0/3      Unselect 100M     32768   3      289     11100000 1
```

Partner:

```
-----
--
ActorPortName      SysPri   SystemID PortPri PortNo PortKey PortState
Ethernet0/0/1      100      0077-7777-7777 100    1      289     11111100
Ethernet0/0/2      100      0077-7777-7777 100    2      289     11111100
Ethernet0/0/3      100      0077-7777-7777 32768  3      289     11100000
```

The preceding information shows that the LACP priority of the system on CX-A is 100, which is higher than that on CX-B. The two member interfaces of the Eth-Trunk, GigabitEthernet 0/0/1 and Ethernet 0/0/2, become active interfaces. They are in the **Selected** state. Ethernet 0/0/3 is in the **Unselected** state. Load balancing can be implemented on M links and redundancy can be performed on N links.

Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
lacp priority 100
#
interface Eth-Trunk1
bpdu enable
mode lacp-static
max bandwidth-affected-linknumber 2
#
interface GigabitEthernet0/0/1
eth-trunk 1
lacp priority 100
#
interface GigabitEthernet0/0/2
eth-trunk 1
lacp priority 100
#
interface GigabitEthernet0/0/3
eth-trunk 1
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
interface Eth-Trunk1
bpdu enable
mode lacp-static
#
interface GigabitEthernet0/0/1
eth-trunk 1
#
interface GigabitEthernet0/0/2
eth-trunk 1
```

```
#  
interface GigabitEthernet0/0/3  
  eth-trunk 1  
#  
return
```

3 VLAN Configuration

About This Chapter

This chapter describes the basics of Virtual Local Area Networks (VLANs) and the procedures and examples for configuring VLANs.

[3.1 Introduction](#)

This section describes the definition and functions of VLANs, references related to VLANs, and logical relationships between configuration tasks.

[3.2 Configuring a VLAN](#)

This section describes how to configure a VLAN.

[3.3 Adding Interfaces to a VLAN](#)

This section describes how to add access interfaces, QinQ interfaces, hybrid interfaces, and trunk interfaces to a VLAN. To allow user packets to pass an interface, you need to perform this task.

[3.4 Configuring VLANIF Interfaces](#)

This section describes how to configure VLANIF interfaces. To implement interconnection at the network layer through logical interfaces, you need to perform this task.

[3.5 Configuring MAC Address-Based VLANs](#)

This section describes how to configure MAC address-based VLANs. You can perform this task to ensure the secure and flexible access of terminals.

[3.6 Configuring Protocol-Based VLANs](#)

This section describes how to configure protocol-based VLANs. You need to perform this task to bind service types to VLANs, which facilitates management and maintenance.

[3.7 Configuring IP Subnet-Based VLAN Classification](#)

This section describes how to configure IP subnet-based VLAN classification. To transmit packets from a specified network segment or a specified IP address over a specified VLAN, you need to perform this task. Compared with configuring MAC address-based VLAN classification, configuring IP subnet-based VLAN classification can change network structures more easily.

[3.8 Configuration Examples](#)

This section provides an example for configuring VLAN mapping.

3.1 Introduction

This section describes the definition and functions of VLANs, references related to VLANs, and logical relationships between configuration tasks.

[3.1.1 VLAN](#)

[3.1.2 VLAN Classification](#)

[3.1.3 VLAN Features Supported by the S-switch](#)

[3.1.4 Logical Relationships Between Configuration Tasks](#)

[3.1.5 Update History](#)

3.1.1 VLAN

Definition

A Local Area Network (LAN) can be divided into several logical LANs. Each logical LAN is a broadcast domain, which is called a VLAN.

Function

This isolates broadcast domains, reduces broadcast storms, and improves the security of information.

3.1.2 VLAN Classification

The S-switch classifies VLANs into the following types:

- Interface VLANs
VLAN members are defined according to device interfaces. An interface can forward packets of a VLAN after being added to the VLAN.
- MAC VLANs
VLAN members are defined according to source MAC addresses of packets. Packets are forwarded after being added with the VLAN tag.
- Protocol VLANs
VLAN IDs are allocated to packets received on an interface according to the protocol (suite) type and encapsulation format of the packets.
- IP subnet VLANs
VLAN members are defined according to the source IP address and the subnet mask of packets. After receiving untagged packets from an interface, the S-switch determines the VLAN that the packets belong to according to the source IP address of the packets, and then allocates the packets to a specified VLAN for transmission.

3.1.3 VLAN Features Supported by the S-switch

VLAN Capacity

The S-switch supports up to 4094 VLANs numbered 1 to 4094.

VLAN Types

The S-switch supports interface-based VLANs, that is, the S-switch classifies a VLAN by adding interfaces to the VLAN.

Types of VLAN Links

VLAN links are classified into the following:

- Access links, which connect user hosts and the S-switch
- Trunk links, which connect S-switches and the S-switches.

For detailed information about link types, refer to the *Quidway S5300 Series Ethernet Switches Feature Description - Ethernet*.

3.1.4 Logical Relationships Between Configuration Tasks

To configure a VLAN, perform [3.2 Configuring a VLAN](#).

To configure VLAN mapping, perform the following tasks in order:

- [3.2 Configuring a VLAN](#)
- [5.2 Configuring VLAN Mapping](#)

3.1.5 Update History

Version	Revision
V200R002C01B010	This is the first release.

3.2 Configuring a VLAN

This section describes how to configure a VLAN.

[3.2.1 Establishing the Configuration Task](#)

[3.2.2 \(Optional\) Creating a VLAN](#)

[3.2.3 \(Optional\) Creating VLANs in Batches](#)

[3.2.4 Checking the Configuration](#)

3.2.1 Establishing the Configuration Task

Applicable Environment

Through VLANs, hosts that do not need to communicate are isolated. VLANs improve network security, reduce broadcast traffic, and suppress broadcast storms.

Pre-configuration Tasks

None.

Data Preparation

To create a VLAN, you need the following data.

No.	Data
1	VLAN ID

3.2.2 (Optional) Creating a VLAN

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 **vlan *vlan-id*** command to create a VLAN and enter the VLAN view.

NOTE

You can configure a management VLAN on the S-switch to forward Huawei Group Management Protocol (HGMP) packets. Using management VLANs in other scenarios is not recommended. By default, the management VLAN on the S-switch is VLAN 1.

For detailed information about management VLANs, refer to *Quidway S5300 Series Ethernet Switches Configuration Guide - Network Management*.

Step 3 (Optional) Run the **description *description*** command to set the description of the VLAN.

Setting VLAN description facilitates the management and memorization of the VLAN. By default, the description of a VLAN indicates the VLAN ID. For example, the description of VLAN 15 is "VLAN 0015."

----End

3.2.3 (Optional) Creating VLANs in Batches

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 **vlan batch { *vlan-id1* [to *vlan-id2*] }&<1-10>** command to create VLANs in batches.

----End

3.2.4 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check information about a VLAN.	display vlan [<i>vlan-id</i> [verbose]]

Run the **display vlan** command to check information about the VLANs created.

```
<Quidway> display vlan
VLAN ID   Type           Status          MAC Learning
-----
1          common         enable          enable
4          common         enable          enable
7          common         enable          enable
8          common         enable          enable
9          common         enable          enable
```

Total vlan displayed = 5

Run the **display vlan *vlan-id* verbose** command to check whether the VLAN description is correct.

```
<Quidway> display vlan 4 verbose
VLAN ID       : 4
VLAN Type     : Common
Description   : VLAN 0004 huawei
Status        : Enable
Statistics    : Disable
```

3.3 Adding Interfaces to a VLAN

This section describes how to add access interfaces, QinQ interfaces, hybrid interfaces, and trunk interfaces to a VLAN. To allow user packets to pass an interface, you need to perform this task.

[3.3.1 Establishing the Configuration Task](#)

[3.3.2 \(Optional\) Adding Access Interfaces to a VLAN](#)

[3.3.3 \(Optional\) Adding Trunk Interfaces to a VLAN](#)

[3.3.4 \(Optional\) Adding Hybrid Interfaces to a VLAN](#)

[3.3.5 \(Optional\) Adding QinQ Interfaces to a VLAN](#)

[3.3.6 Checking the Configuration](#)

3.3.1 Establishing the Configuration Task

Applicable Environment

VLANs are classified according to interfaces. You can group interfaces that process the same type of services into a VLAN. In this manner, interfaces that process different types of services are isolated. For example, interface 1 and interface 2 both connect to broadband access users; interface 3 connects to users of video services. In this case, interface 1 and interface 2 are grouped into a VLAN; interface 3 is grouped into another VLAN.

Pre-configuration Tasks

Before adding interfaces to a VLAN, complete the following task:

- [3.2 Configuring a VLAN](#)

Data Preparation

To add interfaces to a VLAN, you need the following data.

No.	Data
1	Types of the interfaces to be added to a VLAN
2	VLAN IDs

3.3.2 (Optional) Adding Access Interfaces to a VLAN

Context

Adding Access Interfaces to a VLAN

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 **port link-type access** command to set the interface type.

By default, the link type is hybrid.

Step 4 Run the **quit** command to return to the system view.

Step 5 Run the **vlan** *vlan-id* command to enter the VLAN view.

Step 6 Run the **port interface-type { interface-number1 [to interface-number2] }&<1-10>** command to add access interfaces to their default VLAN.

----End

Configuring a Default VLAN for Interfaces

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 **port link-type access** command to set the interface type.
- By default, the interface type is hybrid.
- Step 4** Run the **port default vlan** *vlan-id* command to set the default VLAN of interfaces.
- End

3.3.3 (Optional) Adding Trunk Interfaces to a VLAN

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 **port link-type trunk** command to set the interface type to trunk.
- By default, the interface type is hybrid.
- Step 4** Run the **port trunk allow-pass vlan** { { *vlan-id1* [*to vlan-id2*] } &<1-10> | **all** } command to add trunk interfaces to the VLAN.
- End

3.3.4 (Optional) Adding Hybrid Interfaces to a VLAN

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 **port link-type hybrid** command to set the interface type to hybrid.
- By default, the interface type is hybrid.
- Step 4** Run the following commands as required.
- Run the **port default vlan** *vlan-id* command to set the default VLAN of hybrid interfaces.

- Run the **port interface-type** { *interface-number1* [**to** *interface-number2*] } <1-10> command in the VLAN view to set the default VLAN of the hybrid interface. You can use this command to set the default VLAN for multiple hybrid interfaces.
- Run the **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] } <1-10> | **all** } command to add hybrid interfaces to the VLAN in tagged mode.
- Run the **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } <1-10> | **all** } command to add hybrid interfaces to the VLAN in untagged mode.

----End

3.3.5 (Optional) Adding QinQ Interfaces to a VLAN

Context

Adding QinQ Interfaces to a VLAN

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 **port link-type dot1q-tunnel** command to set the interface type.
- By default, the interface type is hybrid.
- Step 4** Run the **quit** command to return to the system view.
- Step 5** Run the **vlan vlan-id** command to enter the VLAN view.
- Step 6** Run the **port interface-type** { *interface-number1* [**to** *interface-number2*] } <1-10> command to add QinQ interfaces to the default VLAN of the interfaces.

----End

Configuring a Default VLAN for Interfaces

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 **port link-type dot1q-tunnel** command to set the interface type.
- By default, the interface type is hybrid.

Step 4 Run the **port default vlan *vlan-id*** command to set the default VLAN of interfaces.

----End

3.3.6 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the VLAN to which an interface is added.	display interface [<i>interface-type</i> [<i>interface-number</i>]]
Check information about a VLAN.	display vlan <i>vlan-id</i>

Run the **display interface** [*interface-type* [*interface-number*]] command. You can view that GE 0/0/1 is added to VLAN 2.

```
<Quidway> display interface gigabitethernet 0/0/1
GigabitEthernet2/0/1 current state : UP
Description : HUAWEI, Quidway Series, GigabitEthernet0/0/1 Interface, Switch Port
PVID : 2
The Maximum Transmit Unit is 1500 bytes
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0010-8300-0026
NO AUTO NEGOTIATION, SPEED 1000M, DUPLEX FULL, LOOPBACK NOT SET;
Transmitter's pause : enable, Receiver's pause : enable ;

Last 300 seconds input rate: 82 bytes/sec, 1 packets/sec
Last 300 seconds output rate: 74 bytes/sec, 1 packets/sec

Last 300 seconds Multicast input rate: 1 packets/sec
Last 300 seconds Multicast output rate: 1 packets/sec
Input: 16328 Packets, 1068290 Bytes
       256 Broadcasts, 29 Multicasts
       0 Oversizes, 0 Undersizes
       0 FCSs, 0 Pauses
Output: 16322 Packets, 1176245 Bytes
       148 Broadcasts, 6 Multicasts
       0 Oversizes, 0 Defers
       0 FCSs, 0 Pauses
       0 Collisions
```

Run the **display vlan *vlan-id*** command. You can view that GE 0/0/1 is added to VLAN 2.

```
<Quidway> display vlan 2
VLAN ID    Type           Status          MAC Learning
-----
2          common        enable         enable
-----
Untagged   Port: GigabitEthernet0/0/1
-----
Interface   Physical
GigabitEthernet0/0/1  UP
```

3.4 Configuring VLANIF Interfaces

This section describes how to configure VLANIF interfaces. To implement interconnection at the network layer through logical interfaces, you need to perform this task.

3.4.3 (Optional) Assigning IP Addresses to VLANIF Interfaces is optional and can be configured as required.

[3.4.1 Establishing the Configuration Task](#)

[3.4.2 Creating a VLANIF Interface](#)

[3.4.3 \(Optional\) Assigning IP Addresses to VLANIF Interfaces](#)

[3.4.4 Checking the Configuration](#)

3.4.1 Establishing the Configuration Task

Applicable Environment

- On the S-switch, you can create a logical interface for a VLAN, that is, a VLANIF interface. A VLANIF interface is a network layer interface to which you can assign an IP address. The S-switch can communicate with other devices through the IP address of its VLANIF interface.
- The S-switch supports static routes to implement the communication between devices in different VLANs.

Pre-configuration Tasks

Before configuring VLANIF interfaces and static routes, complete the following task:

- [3.2.2 \(Optional\) Creating a VLAN](#)

Data Preparation

To configure VLANIF interfaces and static routes, you need the following data.

No.	Data
1	ID of a VLAN
2	IP address of each VLANIF interface
3	Destination IP address, mask, and IP address of the next hop

3.4.2 Creating a VLANIF Interface

Context

Do as follows on the S-switch that needs to be configured with static routes.

Procedure

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

Step 2 Run the **interface vlanif** *vlan-id* command to create a VLANIF interface and enter the VLANIF interface view.

Step 3 Run the **ip address** *ip-address* { *mask* | *mask-length* } [**sub**] command to assign an IP address to the VLANIF interface.

----End

3.4.3 (Optional) Assigning IP Addresses to VLANIF Interfaces

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 vlanif** *vlan-id* command to create a VLANIF interface and enter the VLANIF interface view.

Step 3 Run the **ip address** *ip-address* { *mask* | *mask-length* } [**sub**] command to assign an IP address to the VLANIF interface.

----End

3.4.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the status and basic configuration of a VLANIF interface.	display interface vlanif [<i>vlan-id</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]
Check the routing table.	display ip routing-table protocol { direct static } [inactive verbose]

After the configuration succeeds, the following results can be obtained with the preceding commands:

- The IP address of the VLANIF interface is correct.
- The static route is properly configured.

3.5 Configuring MAC Address-Based VLANs

This section describes how to configure MAC address-based VLANs. You can perform this task to ensure the secure and flexible access of terminals.

[3.5.1 Establishing the Configuration Task](#)

[3.5.2 Relating a MAC Address with a VLAN](#)

[3.5.3 Permitting Packets with the VLAN Tag to Pass the Current Interface](#)

[3.5.4 Enabling MAC Address-Based VLAN Classification](#)

[3.5.5 \(Optional\) Setting the Precedence for VLAN Matching](#)[3.5.6 Checking the Configuration](#)

3.5.1 Establishing the Configuration Task

Applicable Environment

MAC address-based VLANs need not to be reconfigured when the physical addresses of terminal users change. This improves the security of terminal users and ensures the flexible access.

Pre-configuration Tasks

None.

Data Preparation

To configure a MAC address-based VLAN, you need the following data.

No.	Data
1	VLAN ID
2	VLAN-related MAC address
3	Type and number of the interface where a MAC address-based VLAN is configured

3.5.2 Relating a MAC Address with a VLAN

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 **vlan *vlan-id*** command to create a VLAN and enter the VLAN view.

----End

3.5.3 Permitting Packets with the VLAN Tag to Pass the Current Interface

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 **port link-type hybrid** command to set the link type to hybrid.
- By default, the interface type is hybrid.
- Step 4** Run the **port trunk allow-pass vlan** *vlan-id* command to permit the packets with the VLAN tag to pass the current interface.
- End

3.5.4 Enabling MAC Address-Based VLAN Classification

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 **mac-vlan enable** command to enable MAC address-based VLAN classification.
- By default, MAC address-based VLAN classification is disabled.
- End

3.5.5 (Optional) Setting the Precedence for VLAN Matching

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 **vlan precedence { mac-vlan | ip-subnet-vlan }** command to set the precedence for VLAN matching.
- By default, the S-switch matches a VLAN according to the MAC address preferentially.
- End

3.5.6 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the entries in a MAC-VLAN table.	display mac-vlan { all dynamic mac-address <i>mac-address</i> static vlan <i>vlan-id</i> }

Run the **display mac-vlan** command to check whether the MAC address is correctly related to the VLAN.

<Quidway> **display mac-vlan all**

3.6 Configuring Protocol-Based VLANs

This section describes how to configure protocol-based VLANs. You need to perform this task to bind service types to VLANs, which facilitates management and maintenance.

[3.6.1 Establishing the Configuration Task](#)

[3.6.2 Configuring Protocol-Based VLANs and Assigning the Protocol Template](#)

[3.6.3 Allowing Packets to Pass Through Protocol-Based VLANs](#)

[3.6.4 Relating a Protocol with a VLAN](#)

[3.6.5 Checking the Configuration](#)

3.6.1 Establishing the Configuration Task

Applicable Environment

You can bind service types to VLANs by configuring protocol-based VLANs. This facilitates management and maintenance.

Pre-configuration Tasks

None.

Data Preparation

To configure protocol-based VLANs, you need the following data.

No.	Data
1	VLAN ID
2	VLAN-related protocol
3	Type and number of the interface where a protocol-based VLAN is configured

3.6.2 Configuring Protocol-Based VLANs and Assigning the Protocol Template

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 **vlan *vlan-id*** command to create a VLAN and enter the VLAN view.
- Step 3** Run the **protocol-vlan [*protocol-index*] { at | ipv4 | ipv6 | ipx { ethernetii | llc | raw | snap } | mode { ethernetii-etype *etype-id1* | llc { dsap *dsap-id* ssap *ssap-id* } | snap-etype *etype-id2* } }** command to configure the protocol-based VLAN and assign the protocol template.
- End

3.6.3 Allowing Packets to Pass Through Protocol-Based VLANs

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 **port link-type hybrid** command to set the link type to hybrid.
- By default, the interface type is hybrid.
- Step 4** Run the **port trunk allow-pass vlan *vlan-id*** command to allow packets to pass through the protocol-based VLAN.
- End

3.6.4 Relating a Protocol with a VLAN

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 **protocol-vlan *vlan* *vlan-id* { all | *protocol-index1* [to *protocol-index2*] } [priority *priority*]** command to relate a protocol with a VLAN.
- End

3.6.5 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check the relation between the protocol and VLAN on the interface.	display protocol-vlan interface { all <i>interface-type interface-number</i> }
Check the protocol configured on the VLAN and protocol template index.	display protocol-vlan vlan { all <i>vlan-id1</i> [to <i>vlan-id2</i>] }

Run the **display protocol-vlan interface** command, and you can view whether the protocol is correctly related to the VLAN.

```
<Quidway> display protocol-vlan interface ethernet 0/0/1
```

Interface	VLAN	Protocol Index	Protocol Type	Priority
Ethernet0/0/1	4	0	ipv4	0

Run the **display protocol-vlan vlan** command, and you can view whether the protocol template is correctly configured on the VLAN.

```
<Quidway> display protocol-vlan vlan 4
```

VLAN	Protocol Index	Protocol Type
4	0	ipv4

3.7 Configuring IP Subnet-Based VLAN Classification

This section describes how to configure IP subnet-based VLAN classification. To transmit packets from a specified network segment or a specified IP address over a specified VLAN, you need to perform this task. Compared with configuring MAC address-based VLAN classification, configuring IP subnet-based VLAN classification can change network structures more easily.

3.7.1 Establishing the Configuration Task

3.7.2 Relating an IP Subnet with a VLAN

3.7.3 Allowing an IP Subnet-Based VLAN to Pass the Current Interface

3.7.4 Enabling an IP Subnet-Based VLAN

3.7.5 Checking the Configuration

3.7.1 Establishing the Configuration Task

Applicable Environment

You can transmit packets from a specified network segment or a specified IP address over a specified VLAN by configuring IP subnet-based VLANs.

Pre-configuration Tasks

None.

Data Preparation

To configure an IP subnet-based VLAN, you need the following data.

No.	Data
1	VLAN ID
2	VLAN-related IP address
3	Type and number of the interface where an IP subnet-based VLAN is configured

3.7.2 Relating an IP Subnet with a VLAN

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 **vlan *vlan-id*** command to create a VLAN and enter the VLAN view.
- Step 3** Run the **ip-subnet-vlan [*ip-subnet-index*] ip *ip-address* [*mask*] [**priority** *priority*]** command to relate the IP subnet with the VLAN.



NOTE

An IP network segment cannot be configured as a multicast network segment; an IP address cannot be configured as a multicast address.

----End

3.7.3 Allowing an IP Subnet-Based VLAN to Pass the Current Interface

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 **port link-type hybrid** command to set the interface type to hybrid.
- By default, the interface type is hybrid.
- Step 4** Run the **port hybrid untagged vlan *vlan-id*** command to allow the IP subnet-based VLAN to pass the current interface.

----End

3.7.4 Enabling an IP Subnet-Based VLAN

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 **ip-subnet-vlan enable** command to enable the IP subnet-based VLAN.
- By default, IP subnet-based VLANs are disabled.
- End

3.7.5 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the IP subnet configured on the VLAN.	display ip-subnet-vlan vlan { all vlan-id1 [to vlan-id2] }

Run the **display ip-subnet-vlan vlan** command, and you can check whether the IP subnet is correctly related to the VLAN.

```
<Quidway> display ip-subnet-vlan vlan 2
-----
Vlan      Index  IpAddress      SubnetMask      Priority
-----
2         1      10.10.10.1     255.255.255.0   0
-----
ip-subnet-vlan count: 1                total count: 1
```

3.8 Configuration Examples

This section provides an example for configuring VLAN mapping.

3.8.1 Example for Configuring Trunk Links on the S-switch

3.8.2 Example for Configuring VLAN Integration

3.8.1 Example for Configuring Trunk Links on the S-switch

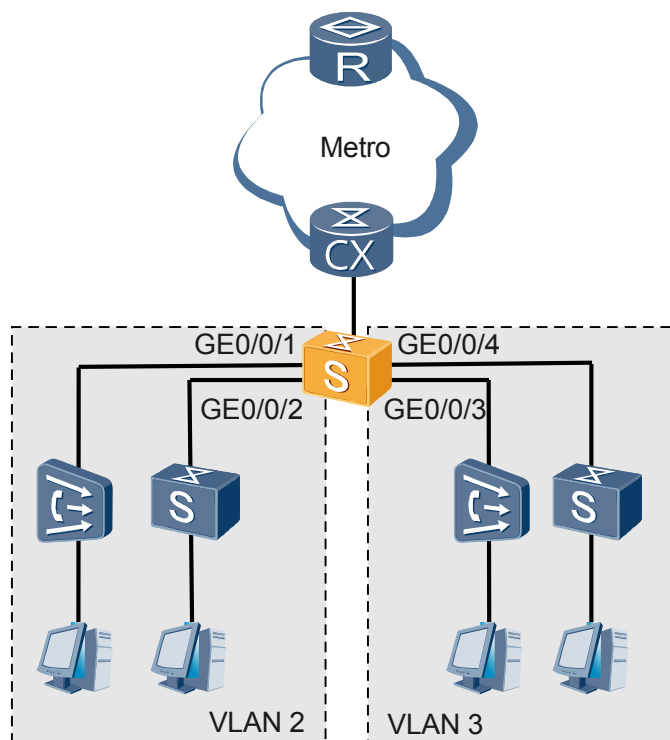
Networking Requirements

As shown in [Figure 3-1](#), an enterprise is composed of four departments. Department 1 is connected to GE 0/0/1 on the S-switch through DSLAM-A. Department 2 is connected to GE 0/0/2 on the S-switch through LSW-A. Department 3 is connected to GE 0/0/3 on the S-

switch through LSW-B. Department 4 is connected to GE 0/0/4 on the S-switch through DSLAM-B. The networking requirements are as follows:

- Department 1 and Department 2 in VLAN 2 are isolated from Department 3 and Department 4 in VLAN 3.
- Department 1 and Department 2 in VLAN 2 can communicate with each other.
- Department 3 and Department 4 in VLAN 3 can communicate with each other.

Figure 3-1 Networking diagram for configuring trunk links on the S-switch



Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN.
2. Add interfaces to the VLAN.

Data Preparation

To complete the configuration, you need the following data:

- GE 0/0/1 and GE 0/0/2, which belong to VLAN 2
- GE 0/0/3 and GE 0/0/4, which belong to VLAN 3

Configuration Procedure

The following provides only the configurations on the S-switch. For the configurations on other devices in [Figure 3-1](#), refer to the manuals of other devices.

1. Configure the S-switch.

Create VLAN 2.

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] quit
```

Set the link type of GE 0/0/1 to trunk and add GE 0/0/1 to VLAN 2.

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] port link-type trunk
[Quidway-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[Quidway-GigabitEthernet0/0/1] quit
```

Set the link type of GE 0/0/2 to trunk and add GE 0/0/2 to VLAN 2.

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] port link-type trunk
[Quidway-GigabitEthernet0/0/2] port trunk allow-pass vlan 2
[Quidway-GigabitEthernet0/0/2] quit
```

Create VLAN 3.

```
[Quidway] vlan 3
[Quidway-vlan3] quit
```

Set the link type of GE 0/0/3 to trunk and add GE 0/0/3 to VLAN 3.

```
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] port link-type trunk
[Quidway-GigabitEthernet0/0/3] port trunk allow-pass vlan 3
[Quidway-GigabitEthernet0/0/3] quit
```

Set the link type of GE 0/0/4 to trunk and add GE 0/0/4 to VLAN 3.

```
[Quidway] interface gigabitethernet 0/0/4
[Quidway-GigabitEthernet0/0/4] port link-type trunk
[Quidway-GigabitEthernet0/0/4] port trunk allow-pass vlan 3
[Quidway-GigabitEthernet0/0/4] quit
```

2. Verify the configuration.

No host in VLAN 2, which Department 1 and Department 2 belong to, can successfully ping any host in VLAN 3, which Department 3 and Department 4 belong to. This shows that Department 1 and Department 2 are isolated from Department 3 and Department 4.

Each host of Department 1 can successfully ping any host of Department 2. This shows that Department 1 is interconnected with Department 2.

Each host of Department 3 can also successfully ping any host of Department 4. This shows that Department 3 is interconnected with Department 4.

Configuration Files

The following lists the configuration files of the S-switch.

```
#
 sysname Quidway
#
 vlan batch 2 to 3
#
 interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
 interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2
#
 interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 3
```

```
#
interface GigabitEthernet0/0/4
port link-type trunk
port trunk allow-pass vlan 3
#
return
```

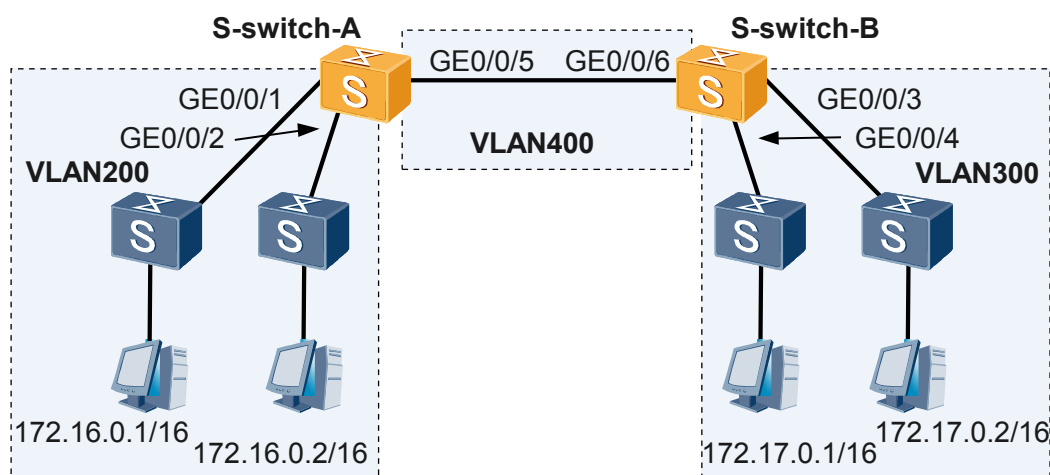
3.8.2 Example for Configuring VLAN Integration

Networking Requirements

As shown in [Figure 3-2](#), User 1 and User 2 are connected to S-switch-A through GE 0/0/1 and GE 0/0/2 on a LAN switch; User 3 and User 4 are connected to S-switch-B through GE 0/0/3 and GE 0/0/4 on another LAN switch. The networking requirements are as follows:

- Each host in VLAN 2 can communicate with any host in VLAN 3.

Figure 3-2 Networking diagram for configuring VLAN integration



Configuration Roadmap

The configuration roadmap is as follows:

- Create VLANs on S-switch-A and S-switch-B and add interfaces on S-switch-A and S-switch-B to the VLANs.
- Create VLANIF interfaces on S-switch-A and S-switch-B and assign IP addresses to the VLANIF interfaces.
- Configure static routes on S-switch-A and S-switch-B.

Data Preparation

To complete the configuration, you need the following data:

- GE 0/0/1 and GE 0/0/2, which belong to VLAN 2

- GE 0/0/3 and GE 0/0/4, which belong to VLAN 3
- GE 0/0/5 and GE 0/0/6, which belong to VLAN 4
- IP address of VLANIF 2 on S-switch-A, which is 10.10.1.1/24
- IP address of VLANIF 4 on S-switch-A, which is 10.10.20.1/24
- IP address of VLANIF 3 on S-switch-B, which is 10.10.2.1/24
- IP address of VLANIF 4 on S-switch-B, which is 10.10.20.2/24

Configuration Procedure

The following provides only the configurations on the S-switch. For the configurations on other devices in [Figure 3-2](#), refer to the manuals of other devices.

1. Create VLANs and add interfaces to the corresponding VLANs.

Create VLAN 2 on S-switch-A.

```
<Quidway> system-view
[Quidway] sysname S-switch-A
[S-switch-A] vlan 2
[S-switch-A-vlan2] quit
```

Add GE 0/0/1 and GE 0/0/2 to VLAN 2.

```
[S-switch-A] interface gigabitethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] port link-type trunk
[S-switch-A-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[S-switch-A-GigabitEthernet0/0/1] quit
[S-switch-A] interface gigabitethernet 0/0/2
[S-switch-A-GigabitEthernet0/0/2] port link-type trunk
[S-switch-A-GigabitEthernet0/0/2] port trunk allow-pass vlan 2
[S-switch-A-GigabitEthernet0/0/2] quit
```

Create VLAN 4 on S-switch-A.

```
[S-switch-A] vlan 4
```

Add GE 0/0/5 to VLAN 4.

```
[S-switch-A-vlan4] port gigabitethernet 0/0/5
[S-switch-A-vlan4] quit
```

Create VLAN 3 on S-switch-B.

```
<Quidway> system-view
[Quidway] sysname S-switch-B
[S-switch-B] vlan 3
[S-switch-B-vlan3] quit
```

Add GE 0/0/3 and GE 0/0/4 to VLAN 3.

```
[S-switch-B] interface gigabitethernet 0/0/3
[S-switch-B-GigabitEthernet0/0/3] port link-type trunk
[S-switch-B-GigabitEthernet0/0/3] port trunk allow-pass vlan 3
[S-switch-B-GigabitEthernet0/0/3] quit
[S-switch-B] interface gigabitethernet 0/0/4
[S-switch-B-GigabitEthernet0/0/4] port link-type trunk
[S-switch-B-GigabitEthernet0/0/4] port trunk allow-pass vlan 3
[S-switch-B-GigabitEthernet0/0/4] quit
```

Create VLAN 4 on S-switch-B.

```
[S-switch-B] vlan 4
```

Add GE 0/0/6 to VLAN 4.

```
[S-switch-B-vlan4] port gigabitethernet 0/0/6
[S-switch-B-vlan4] quit
```

2. Create VLANIF interfaces and assign IP addresses to the VLANIF interfaces.

Create VLANIF 2 on S-switch-A.

- ```
[S-switch-A] interface vlanif 2
Assign the IP address of 10.10.1.1/24 to VLANIF 2.
[S-switch-A-Vlanif2] ip address 10.10.1.1 24
[S-switch-A-Vlanif2] quit
Create VLANIF 4 on S-switch-A.
[S-switch-A] interface vlanif 4
Assign the IP address of 10.10.20.1/24 to VLANIF 4.
[S-switch-A-Vlanif4] ip address 10.10.20.1 24
[S-switch-A-Vlanif4] quit
Create VLANIF 3 on S-switch-B.
[S-switch-B] interface vlanif 3
Assign the IP address of 10.10.2.1/24 to VLANIF 3.
[S-switch-B-Vlanif3] ip address 10.10.2.1 24
[S-switch-B-Vlanif3] quit
Create VLANIF 4 on S-switch-B.
[S-switch-B] interface vlanif 4
Assign the IP address of 10.10.20.2/24 to VLANIF 4.
[S-switch-B-Vlanif4] ip address 10.10.20.2 24
[S-switch-B-Vlanif4] quit
```
3. Configure static routes.
 

```
Configure a static route on S-switch-A with the destination IP address as 10.10.2.0, the
mask as 255.255.255.0, and the IP address of the next hop as 10.10.20.2.
[S-switch-A] ip route-static 10.10.2.0 255.255.255.0 10.10.20.2
Configure a static route on S-switch-B with the destination IP address as 10.10.1.0, the
mask as 255.255.255.0, and the IP address of the next hop as 10.10.20.1.
[S-switch-B] ip route-static 10.10.1.0 255.255.255.0 10.10.20.1
```
  4. Verify the configuration.
 

Ping any host in VLAN 2 from any host in VLAN 3. If the ping operations succeed, it indicates that the configuration succeeds.

Ping any host in VLAN 3 from any host in VLAN 2. If the ping operations succeed, it indicates that the configuration succeeds.

## Configuration Files

The following lists the configuration files of the S-switch.

- Configuration files of S-switch-A
 

```
#
sysname S-switch-A
#
vlan batch 2 4
#
interface Vlanif2
ip address 10.10.1.1 255.255.255.0
#
interface Vlanif4
ip address 10.10.20.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/2
port link-type trunk
```

```
port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/5
port default vlan 4
#
ip route-static 10.10.2.0 255.255.255.0 10.10.20.2
#
return
```

- Configuration files of S-switch-B

```
#
sysname S-switch-B
#
vlan batch 3 4
#
interface Vlanif3
ip address 10.10.2.1 255.255.255.0
#
interface Vlanif4
ip address 10.10.20.2 255.255.255.0
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 3
#
interface GigabitEthernet0/0/4
port link-type trunk
port trunk allow-pass vlan 3
#
interface GigabitEthernet0/0/6
port default vlan 4
#
ip route-static 10.10.1.0 255.255.255.0 10.10.20.1
#
return
```

# 4 VLAN Aggregation Configuration

---

## About This Chapter

This chapter describes the basics, methods, and examples for configuring VLAN aggregation.

### [4.1 Introduction](#)

This section describes the concepts of VLAN aggregation and VLAN aggregation features supported by the S-switch.

### [4.2 Configuring VLAN Aggregation](#)

This section describes how to configure VLAN aggregation. You can perform this task to enable multiple VLANs to share an IP address. This can save IP addresses.

### [4.3 Configuration Examples](#)

This section provides configuration examples for VLAN aggregation.

## 4.1 Introduction

This section describes the concepts of VLAN aggregation and VLAN aggregation features supported by the S-switch.

### 4.1.1 Concept of VLAN Aggregation

#### 4.1.2 VLAN Aggregation Supported by the S-switch

#### 4.1.3 Logical Relationships Between Configuration Tasks

#### 4.1.4 Update History

### 4.1.1 Concept of VLAN Aggregation

To interconnect VLANs on the S-switch, you need to assign an IP address to each VLANIF interface. If there is a large number of VLANs, many IP addresses are used. VLAN aggregation can solve the problem that each VLAN interface uses an IP address.

An aggregated VLAN is also called a super VLAN. Multiple VLANs can be aggregated to a super VLAN. The VLANs that form into a super VLAN are called sub VLANs.

### 4.1.2 VLAN Aggregation Supported by the S-switch

#### Super VLANs and Sub VLANs

Each super VLAN supports up to 16 sub VLANs.

A sub VLAN does not need a separate subnet segment. In a super VLAN, the IP address of a host is in the subnet segment corresponding to the super VLAN, irrespective of the sub VLAN that the host belongs to.

Different from a common VLAN, a super VLAN includes only Layer 3 interfaces rather than physical interfaces. A super VLAN is also different from a VLAN without physical interfaces. The Layer 3 virtual interface of a super VLAN is Up when the sub VLANs of the super VLAN has physical interfaces that are in the Up state.

A sub VLAN has only physical interfaces. VLANIF interfaces cannot be set up in a sub VLAN. The Layer 3 switching between a sub VLAN and other sub VLANs and networks is implemented through the VLANIF interfaces of the super VLAN.

#### Sub VLAN Communications

To implement Layer 3 communications in a sub VLAN, users can use the IP address of the VLANIF interface of the super VLAN as the gateway address.

To implement Layer 3 interconnections between a sub VLAN with another sub VLAN or other networks, you need to use the Address Resolution Protocol (ARP) proxy function. After ARP proxy is enabled, ARP request and response packets can be forwarded and processed. This can implement Layer 3 interconnection between isolated interfaces at Layer 2. By default, ARP proxy is disabled in sub VLANs.

## 4.1.3 Logical Relationships Between Configuration Tasks

The configuration tasks in this chapter are independent. You can perform the task in the order at your desire.

## 4.1.4 Update History

| Version         | Revision                   |
|-----------------|----------------------------|
| V200R002C01B010 | This is the first release. |

## 4.2 Configuring VLAN Aggregation

This section describes how to configure VLAN aggregation. You can perform this task to enable multiple VLANs to share an IP address. This can save IP addresses.

[4.2.1 Establishing the Configuration Task](#)

[4.2.2 Configuring Sub VLANs](#)

[4.2.3 Configuring a Super VLAN](#)

[4.2.4 Assigning IP Addresses to VLANIF Interfaces](#)

[4.2.5 Enabling ARP Proxy in Sub VLANs](#)

[4.2.6 Checking the Configuration](#)

### 4.2.1 Establishing the Configuration Task

#### Applicable Environment

When a large number of VLANs exists in the network, you can configure VLAN aggregation to simplify configuration and facilitate network planning.

#### Pre-configuration Tasks

Before configuring VLAN aggregation, complete the following task:

- Configuring Basic Attributes of Ethernet Interfaces

#### Data Preparation

To configure VLAN aggregation, you need the following data.

| No. | Data                                        |
|-----|---------------------------------------------|
| 1   | Sub VLAN IDs and interface numbers          |
| 2   | Super VLAN ID                               |
| 3   | IP address and mask of the VLANIF interface |

## 4.2.2 Configuring Sub VLANs

### 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 **vlan *vlan-id*** command to create a VLAN and enter the VLAN view.
- Step 3** Run the **port *interface-type* { *interface-number1* [ to *interface-number2* ] } &<1-10>** command to add interfaces to sub VLANs.

By default, a newly created VLAN functions the same as a sub VLAN.

To configure a sub VLAN, add interfaces to the created VLAN.

----End

## 4.2.3 Configuring a Super VLAN

### 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 **vlan *vlan-id*** command to create a VLAN and enter the VLAN view.
- Step 3** Run the **aggregate-vlan** command to set a created VLAN as a super VLAN.

 **NOTE**

- The ID of the super VLAN must differ from that of sub VLANs. The super VLAN cannot contain any physical interfaces.
- Using the **undo aggregate-vlan** command in the VLAN view, you can change a super VLAN interface to a sub VLAN interface.

- Step 4** Run the **access-vlan { *vlan-id1* [ to *vlan-id2* ] } &<1-10>** command to add a sub VLAN to a super VLAN.

----End

## 4.2.4 Assigning IP Addresses to VLANIF Interfaces

### 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 vlanif** *vlan-id* command to create a VLANIF interface.

You can create VLANIF interfaces for super VLANs rather than sub VLANs. Therefore, *vlan-id* specifies the ID of a super VLAN.

**Step 3** Run the **ip address** *ip-address* { *mask* | *mask-length* } [ **sub** ] command to assign an IP address to the VLANIF interface.



### NOTE

The network segment that contains the IP address of the VLANIF interface must also contain subnet segments of sub VLAN users.

----End

## 4.2.5 Enabling ARP Proxy in Sub VLANs

### 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 vlanif** *vlan-id* command to create a VLANIF interface.

You can create VLANIF interfaces for super VLANs rather than sub VLANs. Therefore, *vlan-id* is the ID of a super VLAN.

**Step 3** Run the **arp-proxy enable** command to enable ARP proxy on the VLANIF interface.

**Step 4** Run the **arp-proxy inter-sub-vlan-proxy enable** command to enable ARP proxy between sub VLANs.

----End

## 4.2.6 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                          | Command                                                                                                                                                |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display VLAN information.                       | <b>display vlan</b> [ <i>vlan-id</i> [ <b>verbose</b> ] ]                                                                                              |
| Display information about the VLANIF interface. | <b>display interface vlanif</b> [ <i>vlan-id</i> ] [ <b>verbose</b> ] [ { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ] |

Run the **display vlan** command. You can view the VLAN type and sub VLAN configuration. Take VLAN 2 as an example:

```
<Quidway> display vlan 2 verbose
VLAN ID : 2
VLAN Type : Super
Description : VLAN 0002
Status : Enable
Broadcast : Enable
MAC learning : Enable
Statistics : Disable

sub-VLAN List: 2-3
```

Run the **display interface vlanif** command. You can view whether the VLANIF interface is properly configured.

```
<Quidway> display interface vlanif 2
Vlanif2 current state : UP
Line protocol current state : UP
Description : HUAWEI, Quidway Series, Vlanif2 Interface, Route Port
The Maximum Transmit Unit is 1500 bytes
Internet Address is 100.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc10-3e00
Physical is VLANIF
 Last 5 minutes input rate 0 bytes/sec, 0 packets/sec
 Last 5 minutes output rate 0 bytes/sec, 0 packets/sec
 0 packets input, 0 bytes, 0 drops
 0 packets output, 0 bytes, 0 drops
```

## 4.3 Configuration Examples

This section provides configuration examples for VLAN aggregation.

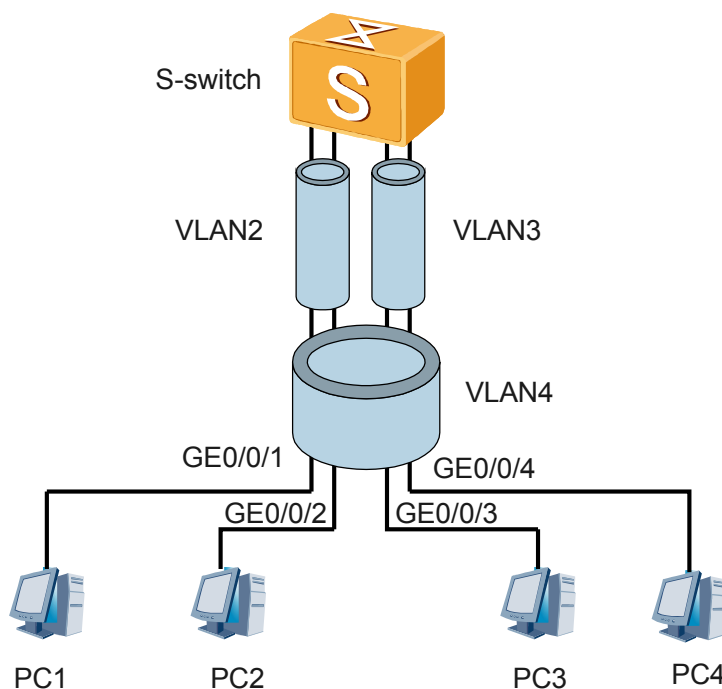
### [4.3.1 Example for Configuring VLAN Aggregation](#)

#### 4.3.1 Example for Configuring VLAN Aggregation

##### Networking Requirements

As shown in [Figure 4-1](#), the S-switch is connected to PC 1, PC 2, PC 3, and PC 4 through GE 0/0/1, GE 0/0/2, GE 0/0/3, and GE 0/0/4. It is required that VLAN 2 and VLAN 3 should be able to communicate with each other after ARP proxy is enabled.

**Figure 4-1** Networking diagram for configuring VLAN aggregation



## Configuration Roadmap

The configuration roadmap is as follows:

1. Create sub VLANs.
2. Aggregate sub VLANs to a super VLAN.
3. Assign IP Addresses to VLANIF interfaces.
4. Enable ARP proxy between sub VLANs.

### NOTE

PC 1, PC 2, PC 3, and PC 4 must be assigned with IP addresses that are in the same network segment with VLAN 4.

## Data Preparation

To complete the configuration, you need the following data:

- Sub VLAN IDs, which are 2 and 3, and super VLAN ID, which is 4
- GE 0/0/1 and GE 0/0/2 belonging to VLAN 2
- GE 0/0/3 and GE 0/0/4 belonging to VLAN 3
- IP address of the super VLAN, which is 10.10.10.1

## Configuration Procedure

1. Create sub VLAN 2.

```
<S-switch> system-view
[S-switch] vlan 2
```

2. Add GE 0/0/1 and GE 0/0/2 to VLAN 2.  

```
[S-switch-vlan2] port gigabitethernet 0/0/1 0/0/2
[S-switch-vlan2] quit
```
3. Create sub VLAN 3.  

```
[S-switch] vlan 3
```
4. Add GE 0/0/3 and GE 0/0/4 to VLAN 3.  

```
[S-switch-vlan3] port gigabitethernet 0/0/3 0/0/4
[S-switch-vlan3] quit
```
5. Create super VLAN 4.  

```
[S-switch] vlan 4
[S-switch-vlan4] aggregate-vlan
[S-switch-vlan4] access-vlan 2 to 3
[S-switch-vlan4] quit
```
6. Assign the IP address of 10.10.10.1 to the super VLAN.  

```
[S-switch] interface vlanif 4
[S-switch-Vlanif4] ip address 10.10.10.1 255.255.255.0
```
7. Enable ARP proxy.  

```
[S-switch-Vlanif4] arp-proxy enable
[S-switch-Vlanif4] arp-proxy inter-sub-vlan-proxy enable
```
8. Verify the configuration.  
The PCs in VLAN 2 and VLAN 3 can communicate each other.

## Configuration Files

The following lists the configuration files of the S-switch.

```

sysname S-switch

vlan batch 2 to 4

vlan 4
aggregate-vlan
access-vlan 2 to 3

interface Vlanif4
ip address 10.10.10.1 255.255.255.0
arp-proxy enable
arp-proxy inter-sub-vlan-proxy enable

interface GigabitEthernet0/0/1
port default vlan 2

interface GigabitEthernet0/0/2
port default vlan 2

interface GigabitEthernet0/0/3
port default vlan 3

interface GigabitEthernet0/0/4
port default vlan 3

return
```

# 5 VLAN Mapping Configuration

---

## About This Chapter

This chapter describes the basics, configuration methods, and configuration examples of VLAN mapping.

### [5.1 Introduction to VLAN Mapping](#)

This section describes the concepts of VLAN mapping and the VLAN mapping features supported by the S-switch.

### [5.2 Configuring VLAN Mapping](#)

This section describes how to configure VLAN mapping.

### [5.3 Configuration Examples](#)

This section provides several examples for configuring VLAN Mapping.

## 5.1 Introduction to VLAN Mapping

This section describes the concepts of VLAN mapping and the VLAN mapping features supported by the S-switch.

### 5.1.1 VLAN Mapping Overview

#### 5.1.2 VLAN Mapping Features Supported by the S-switch

#### 5.1.3 Update History

### 5.1.1 VLAN Mapping Overview

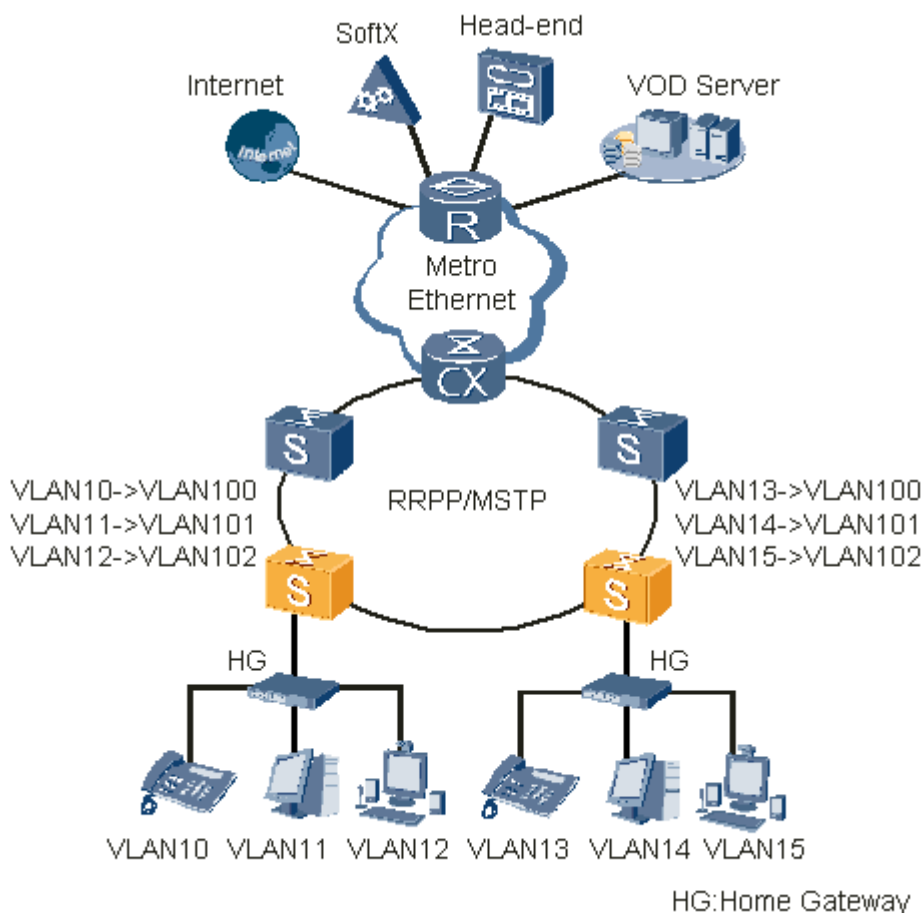
#### Definition

VLAN mapping is used to implement the mapping between Customer-VLAN (C-VLAN) tags and Service-VLAN (S-VLAN) tags by replacing the outer VLAN tags of data frames. In this manner, VLAN convergence is implemented; thus, services are transmitted according to the provider's network planning.

#### Background

In the metropolitan Ethernet network shown in [Figure 5-1](#), services such as Internet, IPTV, and VoIP of home users are transmitted through different VLANs. The number of VLANs in the network of the provider, however, is limited; therefore, VLAN convergence needs to be performed on the switch at the access layer. Thus, the same services of different customers sent through different VLANs can be sent through the same VLAN.

**Figure 5-1** Networking diagram of VLAN mapping



## 5.1.2 VLAN Mapping Features Supported by the S-switch

### Mapping Mode

The S-switch maps the outermost C-VLAN tag carried in a received packet to the S-VLAN tag based on the interface and the C-VLAN; the S-switch maps the outermost S-VLAN tag carried in a packet to be sent to the C-VLAN tag based on the S-VLAN and destination MAC address.

The S-switch supports 1:1 mapping and n:1 mapping.

- 1:1 VLAN mapping  
Map a C-VLAN tag to an S-VLAN tag or map an S-VLAN tag to a C-VLAN tag.
- N:1 VLAN mapping  
Map multiple C-VLAN tags to an S-VLAN tag.

### Specification

After VLAN mapping is configured on an interface, the interface can be connected to a maximum of 1000 customers and a device can be connected to a maximum of 1000 customers.

## 5.1.3 Update History

| Version         | Revision                   |
|-----------------|----------------------------|
| V200R002C01B010 | This is the first release. |

## 5.2 Configuring VLAN Mapping

This section describes how to configure VLAN mapping.

[5.2.1 Establishing the Configuration Task](#)

[5.2.2 Creating an S-VLAN and a C-VLAN](#)

[5.2.3 Configuring the Type of an Interface Type as Hybrid](#)

[5.2.4 Adding Interfaces to an S-VLAN](#)

[5.2.5 Enabling Selective QinQ on an Interface](#)

[5.2.6 \(Optional\) Configuring an Interface to Trust the 802.1p Priorities Carried in Packets](#)

[5.2.7 Configuring VLAN Mapping](#)

[5.2.8 Checking the Configuration](#)

### 5.2.1 Establishing the Configuration Task

#### Applicable Environment

In the metropolitan Ethernet network, services such as Internet, IPTV, and VoIP of home users are transmitted through different VLANs. The number of VLANs in S-VLAN, however, is limited; therefore, VLAN convergence needs to be performed on the switch at the access layer. Thus, the same services of different users sent by different VLANs can be sent by the same VLAN.

#### Pre-configuration Tasks

None.

#### Data Preparation

To configure VLAN mapping, you need the following data.

| No. | Data                                                 |
|-----|------------------------------------------------------|
| 1   | Number of the interface configured with VLAN mapping |
| 2   | IDs of C-VLANs                                       |
| 3   | IDs of S-VLANs                                       |

## 5.2.2 Creating an S-VLAN and a C-VLAN

### Context

Do as follows on the S-switch that needs to be configured with VLAN mapping.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
  - Step 2** Run the **vlan batch** { *vlan-id1* [ **to** *vlan-id2* ] } &<1-10> command to create S-VLANs in batches.
  - Step 3** Run the **vlan batch** { *vlan-id1* [ **to** *vlan-id2* ] } &<1-10> command to create C-VLANs in batches.
- End

## 5.2.3 Configuring the Type of an Interface Type as Hybrid

### Context

Do as follows on the S-switch that needs to be configured with VLAN mapping.

### 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 view of the interface at the customer side.
- Step 3** Run the **port link-type hybrid** command to configure the type of the interface as Hybrid.

By default, the type of the interface is hybrid.

#### NOTE

On the S-switch, VLAN mapping can be configured on hybrid interfaces only.

----End

## 5.2.4 Adding Interfaces to an S-VLAN

### Context

Do as follows on the S-switch that needs to be configured with VLAN mapping.

### 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 view of the interface at the customer side.
- Step 3** Run the **port trunk allow-pass vlan** { { *vlan-id1* [ **to** *vlan-id2* ] } &<1-10> | **all** } command to add the interface at the customer side to the S-VLAN.

- Step 4** Run the **quit** command to exit from the view of the interface at the customer side.
- Step 5** Run the **interface** *interface-type interface-number* command to enter the view of the interface at the network side.
- Step 6** Run the **port trunk allow-pass vlan** { { *vlan-id1* [ **to** *vlan-id2* ] } &<1-10> | **all** } command to add the interface at the network side to the S-VLAN.
- End

## 5.2.5 Enabling Selective QinQ on an Interface

### Context

Do as follows on the S-switch that needs to be configured with VLAN mapping.

### 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 view of the interface at the customer side.
- Step 3** Run the **qinq vlan-translation enable** command to enable selective QinQ on the interface.
- By default, selective QinQ is disabled on the interface.
- End

## 5.2.6 (Optional) Configuring an Interface to Trust the 802.1p Priorities Carried in Packets

### Context

When [5.2.7 Configuring VLAN Mapping](#) and configuring the S-VLAN to inherit the priority of the C-LVLAN, configure an interface to trust the 802.1p priorities carried in packets

Do as follows on the S-switch that needs to be configured with VLAN mapping.

### 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 view of the interface at the customer side.
- Step 3** Run the **trust 8021p** command to configure the interface to trust the 802.1p priorities carried in received packets.
- By default, the interface does not trust the 802.1p priorities carried in received packets.
- End

## 5.2.7 Configuring VLAN Mapping

## Context

If the S-VLAN inherits the priority of the C-VLAN when the C-VLAN tag is mapped to the S-VLAN tag, perform the action of [5.2.6 \(Optional\) Configuring an Interface to Trust the 802.1p Priorities Carried in Packets](#) before configuring VLAN mapping.

Do as follows on the S-switch that needs to be configured with VLAN mapping.

## 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 view of the interface at the customer side.
- Step 3** Run the **port vlan-mapping external-vlan** *vlan-id1* [ **to** *vlan-id2* ] **map-external-vlan** *vlan-id3* { **priority-inherit** | **remark-8021p** *priority* } command to configure VLAN mapping and set up the mapping between C-VLANs and S-VLANs.
- *vlan-id1* specifies the start C-VLAN ID to be replaced.
  - *vlan-id2* specifies the end C-VLAN ID to be replaced.
  - *vlan-id3* specifies the S-VLAN ID.

----End

## 5.2.8 Checking the Configuration

Run the following command to check the previous configuration.

| Action                                                   | Command                                                                               |
|----------------------------------------------------------|---------------------------------------------------------------------------------------|
| Check the configuration of VLAN mapping on an interface. | <b>display current-configuration interface</b> <i>interface-type interface-number</i> |

Run the **display current-configuration interface** command in any view, and you can check whether VLAN mapping is correctly configured on the interface. In this example, C-VLANs 13 and 14 are mapped to S-VLAN 100, and C-VLAN 15 is mapped to S-VLAN 101 on GigabitEthernet 0/0/2.

```
<Quidway> display current-configuration interface ethernet 0/0/2
#
interface Ethernet0/0/2
 port trunk allow-pass vlan 100 to 101
 trust 8021p
 qinq vlan-translation enable
 port vlan-mapping external-vlan 13 to 14 map-external-vlan 100 priority-inherit
 port vlan-mapping external-vlan 15 map-external-vlan 101 priority-inherit
#
return
```

## 5.3 Configuration Examples

This section provides several examples for configuring VLAN Mapping.

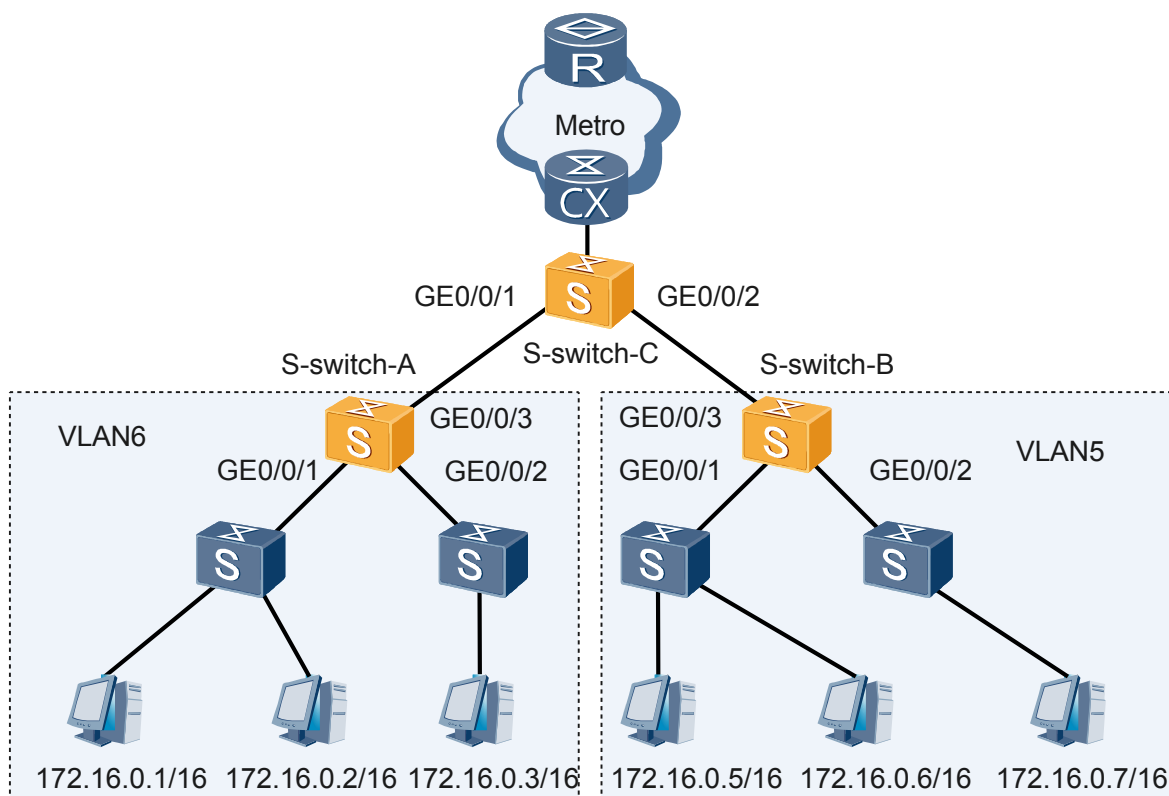
### 5.3.1 Example for Configuring VLAN Mapping

## 5.3.1 Example for Configuring VLAN Mapping

### Networking Requirements

As shown in [Figure 5-2](#), the home users are connected to the S-switch through home gateways. The home users, therefore, can access the network of the provider. The home users require one or more types of voice telephony, Internet, BTV, and VoD services. The services need to be isolated through VLANs. To save VLAN resources, services of the same type are transmitted in the same VLAN in the networks of providers.

**Figure 5-2** Networking for configuring VLAN mapping



### Configuration Roadmap

The configuration roadmap is as follows:

1. Create S-VLANs on S-switch-A and S-switch-B and configure interfaces at the provider side and the customer side to permit packets from the S-VLANs to pass through.
2. Create C-VLANs on S-switch-A and S-switch-B.
3. Configure VLAN mapping on the interfaces through which S-switch-A and S-switch-B are connected to customers.

### Data Preparation

To complete the configuration, you need the following data:

- IDs of C-VLANs
- IDs of S-VLANs

## Configuration Procedure

The following presents only the configurations on the S-switch. For the configurations on other devices in [Figure 5-2](#), refer to corresponding manuals.

### 1. Create S-VLANs.

# Create VLAN 100, VLAN 101, and VLAN 102 on S-switch-A.

```
<Quidway> system-view
[Quidway] sysname S-switch-A
[S-switch-A] vlan batch 100 to 102
```

# Create VLAN 100 and VLAN 101 on S-switch-B.

```
<Quidway> system-view
[Quidway] sysname S-switch-B
[S-switch-B] vlan batch 100 101
```

### 2. Configure interfaces at the provider side to permit packets from the VLANs to pass through.

# Configure GE 0/0/1 and GE 0/0/2 on S-switch-A to permit packets from VLAN 100, VLAN 101, and VLAN 102 to pass through.

```
[S-switch-A] interface gigabitethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 102
[S-switch-A-GigabitEthernet0/0/1] quit
[S-switch-A] interface gigabitethernet 0/0/2
[S-switch-A-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 102
[S-switch-A-GigabitEthernet0/0/2] quit
```

# Configure GE 0/0/1 and GE 0/0/2 on S-switch-B to permit packets from VLAN 100 to VLAN 101 to pass through.

The configurations on S-switch-B are the same as that of S-switch-A, and are not mentioned here.

### 3. Configure the type of the interface at the customer side to hybrid and configure the interface to permit packets from the S-VLAN to pass through.

# Configure the type of GigabitEthernet 0/0/1 on S-switch-A as hybrid and configure the interface to permit packets from VLAN 100, VLAN 101, and VLAN 102 to pass through.

```
[S-switch-A] interface ethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] port link-type hybrid
[S-switch-A-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 102
[S-switch-A-GigabitEthernet0/0/1] quit
```

# Configure Ethernet 0/0/2 on S-switch-B to permit packets from VLAN 100 to VLAN 101 to pass through.

The configurations on S-switch-B are the same as that of S-switch-A, and are not mentioned here.

### 4. Create C-VLANs.

# Create VLAN 10, VLAN 11, and VLAN 12 on S-switch-A.

```
[S-switch-A] vlan batch 10 to 12
```

# Create VLAN 13, VLAN 14, and VLAN 15 on S-switch-B.

```
[S-switch-B] vlan batch 13 to 15
```

### 5. Configure VLAN mapping on the interface at the customer side.

# Configure selective QinQ on the interface at the customer side on S-switch-A.

```
[S-switch-A] interface ethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] qinq vlan-translation enable
```

# Configure the interface at the customer side of S-switch-A to trust the 802.1p priorities carried in packets.

```
[S-switch-A-GigabitEthernet0/0/1] trust 8021p
```

# Configure VLAN mapping on the interface at the customer side of S-switch-A.

```
[S-switch-A-GigabitEthernet0/0/1] port vlan-mapping external-vlan 10 map-external-vlan 100 priority-inher
[S-switch-A-GigabitEthernet0/0/1] port vlan-mapping external-vlan 11 map-external-vlan 101 priority-inher
[S-switch-A-GigabitEthernet0/0/1] port vlan-mapping external-vlan 12 map-external-vlan 102 priority-inher
```

# Configure selective QinQ on the interfaces at the customer side of S-switch-B.

```
[S-switch-B] interface ethernet 0/0/2
[S-switch-B-GigabitEthernet0/0/2] qinq vlan-translation enable
```

# Configure the interface at the customer side of S-switch-B to trust the 802.1p priorities carried in packets.

```
[S-switch-B-GigabitEthernet0/0/2] trust 8021p
```

# Configure VLAN mapping on the interface at the customer side of S-switch-B.

```
[S-switch-B-GigabitEthernet0/0/2] port vlan-mapping external-vlan 13 to 14 map-external-vlan 100 priority-inher
[S-switch-B-GigabitEthernet0/0/2] port vlan-mapping external-vlan 15 map-external-vlan 101 priority-inher
```

## 6. Verify the configuration.

# Run the **display current-configuration interface** command in the system view to check the VLAN mapping configuration. Take the display on S-switch-A as an example.

```
[S-switch-A] display current-configuration interface ethernet 0/0/1
#
interface Ethernet0/0/1
port trunk allow-pass vlan 100 to 102
trust 8021p
qinq vlan-translation enable
port vlan-mapping external-vlan 10 map-external-vlan 100 priority-inherit
port vlan-mapping external-vlan 11 map-external-vlan 101 priority-inherit
port vlan-mapping external-vlan 12 map-external-vlan 102 priority-inherit
#
return
```

From the command output, you can find the following information:

- VLAN 10, VLAN 13, and VLAN 14 can communicate with the SoftX server of the provider.
- VLAN 11 and VLAN 15 can communicate with the Internet server of the provider.
- VLAN 12 can communicate with the Head-end server and VoD server of the provider.

## Configuration Files

Only the configuration files about the S-switch are provided.

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
vlan batch 10 to 12 100 to 102
#
interface Ethernet0/0/1
port trunk allow-pass vlan 100 to 102
trust 8021p
qinq vlan-translation enable
port vlan-mapping external-vlan 10 map-external-vlan 100 priority-inherit
port vlan-mapping external-vlan 11 map-external-vlan 101 priority-inherit
```

```
port vlan-mapping external-vlan 12 map-external-vlan 102 priority-inherit
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 100 to 102
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 100 to 102
#
return
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
vlan batch 13 to 15 100 to 101
#
interface Ethernet0/0/2
port trunk allow-pass vlan 100 to 101
trust 8021p
qinq vlan-translation enable
port vlan-mapping external-vlan 13 to 14 map-external-vlan 100 priority-
inherit
port vlan-mapping external-vlan 15 map-external-vlan 101 priority-inherit
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 100 to 101
#
return
```



# 6 Voice VLAN Configuration

---

## About This Chapter

This chapter describes the basics, methods, and examples for configuring voice VLANs.

### [6.1 Introduction](#)

This section describes the concept of voice VLANs and voice VLAN function supported by the S-switch.

### [6.2 Configuring Voice VLANs of the Automatic Mode](#)

This section describes how to configure voice VLANs of the automatic mode. To automatically add interfaces connected to voice devices to a voice VLAN, you need to perform this task.

### [6.3 Configuring Voice VLANs of the Manual Mode](#)

This section describes how to configure voice VLANs of the manual mode. To manually add interfaces connected to voice devices to a voice VLAN, you need to perform this task.

### [6.4 Configuration Examples](#)

This section provides several examples for configuring voice VLANs.

## 6.1 Introduction

This section describes the concept of voice VLANs and voice VLAN function supported by the S-switch.

A voice VLAN is dedicated to voice flows. After the interfaces connected to voice devices are added to a voice VLAN, all voice flows are transmitted in the voice VLAN.

Using voice VLANs, you can effectively configure the Quality of Services (QoS) of voice flows and increase the transmission priority of voice flows. In this way, the quality of voice services can be guaranteed.

### 6.1.1 Identification of Voice Flows

### 6.1.2 Voice VLAN Features Supported by the S-switch

### 6.1.3 Logical Relationships Between Configuration Tasks

### 6.1.4 Update History

## 6.1.1 Identification of Voice Flows

The S-switch judges whether a flow entering an interface is a voice flow according to the source MAC address field of the flow. The flow whose source MAC address complies with the Organizationally Unique Identifiers (OUIs) of voice devices set by the system is regarded as a voice flow. The interface receiving voice flows is automatically added to the voice VLAN. Then, the voice flow that is sent by the voice device connected to the interface and carries a voice VLAN tag can be transmitted through this interface.

You can preset OUIs or use the default OUIs.

The first 24 bits of a MAC address is an OUI, which is a unique identifier allocated to a device supplier by the Institute of Electrical and Electronics Engineers (IEEE). An OUI indicates the supplier of a device. The S-switch supports OUI masks. You can set various masks to adjust the degree of MAC address matching.

By default, the S-switch can identify seven OUIs, as shown in [Table 6-1](#).

**Table 6-1** Default OUI addresses

| No. | OUI            | Supplier          |
|-----|----------------|-------------------|
| 1   | 0001-e300-0000 | Simens phone      |
| 2   | 0003-6b00-0000 | Cisco phone       |
| 3   | 0004-0d00-0000 | Avaya phone       |
| 4   | 0060-b900-0000 | Philips/NEC phone |
| 5   | 00d0-1e00-0000 | Pingtel phone     |
| 6   | 00e0-7500-0000 | Polycom phone     |
| 7   | 00e0-bb00-0000 | 3Com phone        |

## 6.1.2 Voice VLAN Features Supported by the S-switch

### Working Modes of Voice VLANs

You can set the working mode of voice VLANs on an interface according to the voice flows passing through the interface. A voice VLAN can work in the following modes:

- Automatic mode

The S-switch automatically adds the interfaces connected to voice devices to the voice VLAN through learning the source MAC address of the packets that the voice devices send when being powered on. The S-switch controls the number of the interfaces in the voice VLAN through the interface aging mechanism. When the aging time of the interfaces expires, the interfaces that cannot update OUIs, that is, the interfaces that no voice data passes through are automatically deleted from the voice VLAN.

- Manual mode

Interfaces are manually added to or deleted from the voice VLAN through commands.

### Working Modes of Voice VLANs

#### NOTE

It is recommended that voice and data services should not be transmitted in the voice VLAN together. If the voice and data services need to be transmitted together, ensure that the voice VLAN works in ordinary mode.

To meet customers' diversified requirements, interfaces enabled with the voice VLAN function can process packets in the following modes as shown in [Table 6-2](#):

- Security mode
- Ordinary mode

**Table 6-2** Packet processing methods in various voice VLAN modes

| Modes of Voice VLANs | Packet Type                               | Mode                                                                                                                |
|----------------------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Security mode        | Packets that are untagged                 | Only the packets whose source MAC address contains an identifiable OUI can be transmitted through the voice VLAN.   |
| Security mode        | Packets carrying voice VLAN tags          | Only the packets whose source MAC address contains an identifiable OUI can be transmitted through the voice VLAN.   |
| Security mode        | Packets carrying other types of VLAN tags | Packets are forwarded if the specified interface permits the specified VLAN tag, regardless of the voice VLAN mode. |

| Modes of Voice VLANs | Packet Type                               | Mode                                                                                                                |
|----------------------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Ordinary mode        | Packets that are untagged                 | The source MAC address of the packets is not checked. All packets can be transmitted through the voice VLAN.        |
| Ordinary mode        | Packets carrying voice VLAN tags          | The source MAC address of the packets is not checked. All packets can be transmitted through the voice VLAN.        |
| Ordinary mode        | Packets carrying other types of VLAN tags | Packets are forwarded if the specified interface permits the specified VLAN tag, regardless of the voice VLAN mode. |

### 6.1.3 Logical Relationships Between Configuration Tasks

In this chapter, all configuration tasks are optional and are not listed in sequence. You can configure them as required

### 6.1.4 Update History

| Version         | Revision                   |
|-----------------|----------------------------|
| V200R002C01B010 | This is the first release. |

## 6.2 Configuring Voice VLANs of the Automatic Mode

This section describes how to configure voice VLANs of the automatic mode. To automatically add interfaces connected to voice devices to a voice VLAN, you need to perform this task.

[6.2.1 Establishing the Configuration Task](#)

[6.2.2 \(Optional\) Configuring Other Identifiable OUIs for the Voice VLAN](#)

[6.2.3 \(Optional\) Configuring the Device to Work in the Security Mode](#)

[6.2.4 \(Optional\) Setting the Aging Time of a Voice VLAN](#)

[6.2.5 Enabling the Voice VLAN Function Globally](#)

[6.2.6 Enabling the Voice VLAN Function on an Interface](#)

[6.2.7 Configuring a Voice VLAN to Work in Automatic Mode](#)

[6.2.8 Checking the Configuration](#)

## 6.2.1 Establishing the Configuration Task

### Applicable Environment

After the voice VLAN of the automatic mode is configured, interfaces connected to voice devices can be added to or deleted from the voice VLAN automatically and voice flows are transmitted over this voice VLAN.

### Pre-configuration Tasks

Before configuring the voice VLAN of the automatic mode, complete the following task:

- [3.2 Configuring a VLAN](#)

### Data Preparation

To configure the voice VLAN of the automatic mode, you need the following data.

| No. | Data                              |
|-----|-----------------------------------|
| 1   | Aging time of the voice VLAN      |
| 2   | OUI                               |
| 3   | Interface enabled with voice VLAN |

## 6.2.2 (Optional) Configuring Other Identifiable OUIs for the Voice VLAN

### 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 **voice-vlan mac-address mac-address mask oui-mask [ description text ]** command to configure an identifiable OUI for the voice VLAN.

By default, the S-switch identifies voice flows according to default OUIs.

----End

## 6.2.3 (Optional) Configuring the Device to Work in the Security Mode

### 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 **voice-vlan security enable** command to configure the S-switch to work in the security mode.
- By default, the S-switch works in security mode.
- End

## 6.2.4 (Optional) Setting the Aging Time of a Voice VLAN

### 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 **voice-vlan aging-time** *minutes* command to set the aging time of the voice VLAN.
- By default, the aging time is 1440 minutes.
- End

## 6.2.5 Enabling the Voice VLAN Function Globally

### 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 **voice-vlan** *vlan-id* **enable** command to enable the voice VLAN function globally.
- You cannot set several VLANs as voice VLANs together.
- End

## 6.2.6 Enabling the Voice VLAN Function on an Interface

### 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.  
The link must be of the trunk or hybrid type.
- Step 3** Run the **voice-vlan enable** command to enable the voice VLAN function on the interface.  
By default, the voice VLAN function is disabled on interfaces.
- End

## 6.2.7 Configuring a Voice VLAN to Work in Automatic Mode

### 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 **voice-vlan mode auto** command to configure the voice VLAN to work in automatic mode.  
By default, a voice VLAN works in automatic mode.
- End

## 6.2.8 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                                                           | Command                          |
|----------------------------------------------------------------------------------|----------------------------------|
| Check the OUIs, OUI masks, and description supported by the system.              | <b>display voice-vlan oui</b>    |
| Check the working mode, security mode, and aging time of the current voice VLAN. | <b>display voice-vlan status</b> |

Run the **display voice-vlan oui** command to check whether the other identifiable OUIs of the voice VLAN are correctly configured.

```
<Quidway> display voice-vlan oui

OuiAddress Mask Description

0001-e300-0000 ffff-ff00-0000 Simens phone
0003-6b00-0000 ffff-ff00-0000 Cisco phone
0004-0d00-0000 ffff-ff00-0000 Avaya phone
0060-b900-0000 ffff-ff00-0000 Philips/NEC phone
00d0-1e00-0000 ffff-ff00-0000 Pingtel phone
00e0-7500-0000 ffff-ff00-0000 Polycom phone
00e0-bb00-0000 ffff-ff00-0000 3come phone
0011-2200-0000 ffff-ff00-0000 huawei
```

Run the **display voice-vlan-status** command to check whether the working mode, security mode, and aging time of the voice VLAN are correctly configured.

```
<Quidway> display voice-vlan status
Voice VLAN Configurations:

Voice VLAN status : Enable
Voice VLAN ID : 2
Voice VLAN security mode : Security
Voice VLAN aging time : 100

Port Information:

Port Mode

Ethernet0/0/1 Auto
Ethernet0/0/2 Manual
```

## 6.3 Configuring Voice VLANs of the Manual Mode

This section describes how to configure voice VLANs of the manual mode. To manually add interfaces connected to voice devices to a voice VLAN, you need to perform this task.

### 6.3.1 Establishing the Configuration Task

#### 6.3.2 (Optional) Configuring Other Identifiable OUIs for the Voice VLAN

#### 6.3.3 (Optional) Configuring the Device to Work in the Security Mode

#### 6.3.4 (Optional) Setting the Aging Time of a Voice VLAN

#### 6.3.5 Enabling the Voice VLAN Function Globally

#### 6.3.6 Enabling the Voice VLAN Function on an Interface

#### 6.3.7 Configuring a Voice VLAN to Work in Manual Mode

#### 6.3.8 Adding Interfaces to the Voice VLAN

#### 6.3.9 Checking the Configuration

## 6.3.1 Establishing the Configuration Task

### Applicable Environment

After the voice VLAN of the manual mode is configured, interfaces connected to voice devices can be added to or deleted from the voice VLAN manually and voice flows are transmitted over this voice VLAN.

### Pre-configuration Tasks

Before configuring the voice VLAN of the manual mode, complete the following task:

- [3.2 Configuring a VLAN](#)

### Data Preparation

To configure the voice VLAN of the manual mode, you need the following data.

| No. | Data                         |
|-----|------------------------------|
| 1   | Aging time of the voice VLAN |

| No. | Data                              |
|-----|-----------------------------------|
| 2   | OUI                               |
| 3   | Interface enabled with voice VLAN |

## 6.3.2 (Optional) Configuring Other Identifiable OUIs for the Voice VLAN

### 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 **voice-vlan mac-address mac-address mask oui-mask [ description text ]** command to configure the identifiable OUIs for the voice VLAN.

By default, the S-switch judges voice flows according to default OUIs.

----End

## 6.3.3 (Optional) Configuring the Device to Work in the Security Mode

### 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 **voice-vlan security enable** command to configure the S-switch to work in the security mode.

By default, the S-switch works in the security mode.

----End

## 6.3.4 (Optional) Setting the Aging Time of a Voice VLAN

### 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 **voice-vlan aging-time** *minutes* command to set the aging time of the voice VLAN.

By default, the aging time is 1440 minutes.

----End

## 6.3.5 Enabling the Voice VLAN Function Globally

### 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 **voice-vlan** *vlan-id* **enable** command to enable the voice VLAN function globally.

You cannot set several VLANs as voice VLANs together.

----End

## 6.3.6 Enabling the Voice VLAN Function on an Interface

### 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 **voice-vlan enable** command to enable the voice VLAN function on the interface.

By default, the voice VLAN function is disabled on interfaces.

----End

## 6.3.7 Configuring a Voice VLAN to Work in Manual Mode

### 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 **undo voice-vlan mode auto** command to configure the voice VLAN to work in manual mode.

By default, the voice VLAN works in automatic mode.

----End

## 6.3.8 Adding Interfaces to the Voice VLAN

### Context

Do as follows on the S-switch

### Procedure

**Step 1** If the interface is of the access type, see "[3.3.2 \(Optional\) Adding Access Interfaces to a VLAN](#)."

**Step 2** If the interface is of the trunk type, see "[3.3.3 \(Optional\) Adding Trunk Interfaces to a VLAN](#)."

**Step 3** If the interface is of the hybrid type, see "[3.3.4 \(Optional\) Adding Hybrid Interfaces to a VLAN](#)."

----End

## 6.3.9 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                                                           | Command                          |
|----------------------------------------------------------------------------------|----------------------------------|
| Check the OUIs, OUI masks, and description supported by the system.              | <b>display voice-vlan oui</b>    |
| Check the working mode, security mode, and aging time of the current voice VLAN. | <b>display voice-vlan status</b> |

Run the **display voice-vlan oui** command to check whether the other identifiable OUIs of the voice VLAN are correctly configured.

```
<Quidway> display voice-vlan oui

OuiAddress Mask Description

0001-e300-0000 ffff-ff00-0000 Simens phone
0003-6b00-0000 ffff-ff00-0000 Cisco phone
0004-0d00-0000 ffff-ff00-0000 Avaya phone
0060-b900-0000 ffff-ff00-0000 Philips/NEC phone
00d0-1e00-0000 ffff-ff00-0000 Pingtel phone
00e0-7500-0000 ffff-ff00-0000 Polycom phone
00e0-bb00-0000 ffff-ff00-0000 3come phone
0011-2200-0000 ffff-ff00-0000 huawei
```

Run the **display voice-vlan-status** command to check whether the working mode, security mode, and aging time of the voice VLAN are correctly configured.

```
<Quidway> display voice-vlan status
Voice VLAN Configurations:

Voice VLAN status : Enable
Voice VLAN ID : 2
Voice VLAN security mode : Security
Voice VLAN aging time : 100

Port Information:

Port Mode

Ethernet0/0/1 Auto
Ethernet0/0/2 Manual
```

## 6.4 Configuration Examples

This section provides several examples for configuring voice VLANs.

[6.4.1 Example for Configuring the Voice VLAN of the Automatic Mode](#)

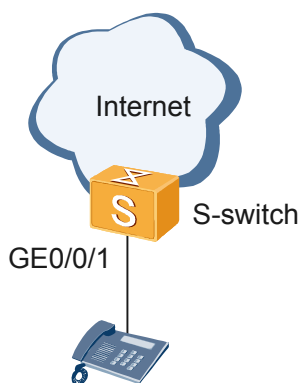
[6.4.2 Example for Configuring the Voice VLAN of the Manual Mode](#)

### 6.4.1 Example for Configuring the Voice VLAN of the Automatic Mode

#### Networking Requirements

As shown in [Figure 6-1](#), Voice over IP (VoIP) services access GE 0/0/1 on the S-switch. It is required that this interface should be added to or deleted from the voice VLAN automatically and voice flows should be transmitted through the voice VLAN.

**Figure 6-1** Configuring voice VLANs of the automatic mode



#### Configuration Roadmap

The configuration roadmap is as follows:

1. Create a voice VLAN.
2. Configure other identifiable OUIs for the voice VLAN.

3. Enable the security mode in the voice VLAN.
4. Set the aging time of the voice VLAN.
5. Enable the voice VLAN function globally.
6. Configure the interface type.
7. Configure the default VLAN of the interface.
8. Enable the voice VLAN function on the interface.
9. Configure the voice VLAN to work in automatic mode.

## Data Preparation

To complete the configuration, you need the following data:

- Voice VLAN ID, which is 2
- Aging time of the voice VLAN, which is 100 minutes
- Default VLAN of GE 0/0/1, which is VLAN 6
- OUI of 0011-2200-0000 and mask of ffff-ff00-0000

## Configuration Procedure

1. Create VLAN 2 and VLAN 6.  

```
<S-switch> system-view
[S-switch] vlan batch 2 6
```
2. Set the OUI to 0011-2200-0000; set the mask to ffff-ff00-0000; set the description to Huawei.  

```
[S-switch] voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
description huawei
```
3. Enable the security mode in the voice VLAN.  

```
[S-switch] voice-vlan security enable
```
4. Set the aging time of the voice VLAN to 100 minutes.  

```
[S-switch] voice-vlan aging-time 100
```
5. Enable voice VLAN 2 globally.  

```
[S-switch] voice-vlan 2 enable
```
6. Set the type of GE 0/0/1 to hybrid.  

```
[S-switch] interface gigabitethernet 0/0/1
[S-switch-GigabitEthernet0/0/1] port link-type hybrid
```
7. Set the default VLAN of GE 0/0/1 to VLAN 6.  

```
[S-switch-GigabitEthernet0/0/1] port default vlan 6
```
8. Enable the voice VLAN function on GE 0/0/1.  

```
[S-switch-GigabitEthernet0/0/1] voice-vlan enable
```
9. Configure the voice VLAN to work in automatic mode.  

```
[S-switch-GigabitEthernet0/0/1] voice-vlan mode auto
```
10. Verify the configuration.

Run the **display voice-vlan oui** command. You can view whether the other identifiable OUIs of the voice VLAN are correctly configured.

```
<Quidway> display voice-vlan oui

OuiAddress Mask Description

```

```

0001-e300-0000 ffff-ff00-0000 Simens phone
0003-6b00-0000 ffff-ff00-0000 Cisco phone
0004-0d00-0000 ffff-ff00-0000 Avaya phone
0060-b900-0000 ffff-ff00-0000 Philips/NEC phone
00d0-1e00-0000 ffff-ff00-0000 Pingtel phone
00e0-7500-0000 ffff-ff00-0000 Polycom phone
00e0-bb00-0000 ffff-ff00-0000 3come phone
0011-2200-0000 ffff-ff00-0000 huawei

```

Run the **display voice vlan-status** command. You can view whether the working mode, security mode, and aging time of the voice VLAN are correctly configured.

```

<Quidway> display voice-vlan status
Voice VLAN Configurations:

```

```

Voice VLAN status : Enable
Voice VLAN ID : 2
Voice VLAN security mode : Security
Voice VLAN aging time : 100

```

```

Port Information:

```

```

Port Mode

GigabitEthernet0/0/1 Auto

```

## Configuration Files

```

#
 sysname S-switch
#
 vlan batch 2 6
#
 voice-vlan 2 enable
#
 voice-vlan aging-time 100
#
 voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000 description huawei
#
interface GigabitEthernet0/0/1
 port default vlan 6
 voice-vlan enable
#
return

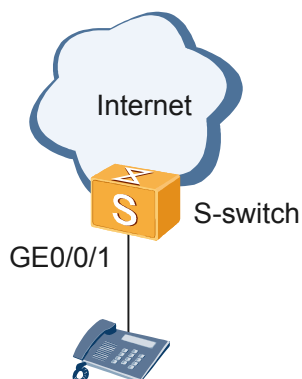
```

## 6.4.2 Example for Configuring the Voice VLAN of the Manual Mode

### Networking Requirements

As shown in [Figure 6-2](#), VoIP services access GE 0/0/1 on the S-switch. It is required that this interface should be added to or deleted from the voice VLAN manually and voice flows should be transmitted through the voice VLAN.

**Figure 6-2** Configuring voice VLANs of the manual mode



## Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the security mode in the voice VLAN.
2. Create a voice VLAN.
3. Configure other identifiable OUIs for the voice VLAN.
4. Enable the voice VLAN function globally.
5. Configure the voice VLAN to work in manual mode.
6. Configure the interface type.
7. Configure the default VLAN of the interface.
8. Enable the voice VLAN function on the interface.

## Data Preparation

To complete the configuration, you need the following data:

- Voice VLAN ID, which is 2
- Interface accessing VoIP services, which is GE 0/0/1
- OUI of 0011-2200-0000 and mask of ffff-ff00-0000

## Configuration Procedure

1. Enable the security mode in the voice VLAN.  

```
[S-switch] voice-vlan security enable
```
2. # Create VLAN 2.  

```
<S-switch> system-view
[S-switch] vlan 2
[S-switch-vlan2] quit
```
3. Set the OUI to 0011-2200-0000; set the mask to ffff-ff00-0000; set the description to Huawei.  

```
[S-switch] voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000
description huawei
```
4. Enable voice VLAN 2 globally.

- ```
[S-switch] voice-vlan 2 enable
```
- Set the type of GE 0/0/1 to hybrid.

```
[S-switch-GigabitEthernet0/0/1] port link-type hybrid
```
 - Enable the voice VLAN function on GE 0/0/1.

```
[S-switch-GigabitEthernet0/0/1] voice-vlan enable
```
 - Configure the voice VLAN to work in manual mode.

```
[S-switch] interface gigabitethernet 0/0/1  
[S-switch-GigabitEthernet0/0/1] undo voice-vlan mode auto
```
 - Set the voice VLAN as the default VLAN of GE 0/0/1.

```
[S-switch-GigabitEthernet0/0/1] port default vlan 2
```
 - Verify the configuration.

Run the **display voice-vlan oui** command. You can view whether the other identifiable OUIs of the voice VLAN are correctly configured.

```
<Quidway> display voice-vlan oui
```

OuiAddress	Mask	Description
0001-e300-0000	ffff-ff00-0000	Simens phone
0003-6b00-0000	ffff-ff00-0000	Cisco phone
0004-0d00-0000	ffff-ff00-0000	Avaya phone
0060-b900-0000	ffff-ff00-0000	Philips/NEC phone
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3come phone
0011-2200-0000	ffff-ff00-0000	huawei

Run the **display voice vlan-status** command. You can view whether the working mode, security mode, and aging time of the voice VLAN are correctly configured.

```
<Quidway> display voice-vlan status
```

Voice VLAN Configurations:

```
-----
Voice VLAN status      : Enable
Voice VLAN ID          : 2
Voice VLAN security mode : Security
Voice VLAN aging time  : 1440
-----
```

Port Information:

```
-----
Port          Mode
-----
GigabitEthernet0/0/1  Manual
```

Configuration Files

```
#
sysname S-switch
#
vlan batch 2
#
voice-vlan 2 enable
#
voice-vlan mac-address 0011-2200-0000 mask ffff-ff00-0000 description huawei
#
interface GigabitEthernet0/0/1
port default vlan 2
voice-vlan enable
undo voice-vlan mode auto
#
return
```

7 QinQ Configuration

About This Chapter

This chapter describes the basic concepts, and methods and examples for configuring QinQ.

[7.1 Introduction](#)

This section describes the concepts of QinQ and selective QinQ.

[7.2 Configure QinQ Interfaces](#)

This section describes how to configure QinQ interfaces.

[7.3 Configuring Selective QinQ](#)

This section describes how to configure selective QinQ.

[7.4 Configuration Examples](#)

This section provides several examples for configuring QinQ and selective QinQ.

7.1 Introduction

This section describes the concepts of QinQ and selective QinQ.

[7.1.1 QinQ](#)

[7.1.2 Selective QinQ](#)

[7.1.3 References](#)

[7.1.4 Logical Relationships Between Configuration Tasks](#)

7.1.1 QinQ

The 802.1Q-in-802.1Q protocol is a Layer 2 tunnel protocol based on the IEEE 802.1Q technology. The frame transmitted in the public network has double 802.1Q tags. One tag identifies a public network and the other identifies a private network. It is thus called the QinQ protocol.

The core concept of QinQ is to encapsulate a private VLAN tag in a public VLAN tag; Thus, a packet carrying double VLAN tags traverses the backbone network of the Internet service provider (ISP). This provides a simpler Layer 2 Virtual Private Network (VPN) tunnel for users.

7.1.2 Selective QinQ

As an extension of QinQ, selective QinQ enables an interface to flexibly add the outer VLAN tags with different public VLAN IDs to frames according to the private VLAN IDs of the frames. Selective QinQ also isolates the ISP network from the user network, and provides rich service features and flexible networking capabilities according to the different 802.1p priorities. In addition, you can configure an interface to discard packets that do not match selective QinQ and VLAN mapping.

7.1.3 References

For detailed information about QinQ, refer to the *Quidway S5300 Series Ethernet Switches - Feature Description*.

7.1.4 Logical Relationships Between Configuration Tasks

The configuration of basic QinQ and that of selective QinQ are independent of each other.

7.2 Configure QinQ Interfaces

This section describes how to configure QinQ interfaces.

[7.2.1 Establishing the Configuration Task](#)

[7.2.2 Setting the Interface Type](#)

[7.2.3 \(Optional\) Setting the TPID Etype Value in the Outer VLAN Tag](#)

7.2.4 Setting the VLAN ID of the Outer VLAN Tag

7.2.5 Checking the Configuration

7.2.1 Establishing the Configuration Task

Applicable Environment

A Layer 2 network can support up to 4094 VLANs. This number of VLANs cannot meet the requirement in the actual application. QinQ interfaces provided by the S-switch can add double tags to a frame. With QinQ interfaces, you can transmit frames by using the private VLAN tags in the internal networks such as the enterprise networks, and using the public VLAN tags in the external networks such as the ISP networks. In this manner, QinQ interfaces can support up to 4094 x 4094 VLAN IDs. This meets the need of isolating a large number of users.

Pre-configuration Tasks

None.

Data Preparation

To configure QinQ, you need the following data.

No.	Data
1	Number of the QinQ interface
2	(Optional) TPID Etype value in the outer VLAN tag
3	VLAN ID of the outer VLAN tag

7.2.2 Setting the Interface Type

Context

Do as follows on the S-switch on which QinQ needs to be configured.

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 Ethernet interface view or the GE interface view; run the **interface eth-trunk trunk-id** command to enter the Eth-Trunk interface view.
- Step 3** Run the **port link-type dot1q-tunnel** command to set an interface as the QinQ interface.

By default, the interface type is hybrid.

----End

7.2.3 (Optional) Setting the TPID Etype Value in the Outer VLAN Tag

Context

Do as follows on the S-switch on which QinQ needs to be configured.

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 Ethernet interface view or the VE interface view; run the **interface eth-trunk** *trunk-id* command to enter the Eth-Trunk interface view.
- Step 3** Run the **qinq protocol** *protocol-id* command to set the TPID Etype value in the outer VLAN tag.

By default, the TPID Etype value in the outer VLAN tag is 0x8100.

 **NOTE**

When an interface receives a packet that has the different TPID Etype value in the outer VLAN tag from that set on the interface, the interface processes the packet as an untagged packet.

On an interface, the TPID Etype value in the outer VLAN tag needs to be identified by the device directly connected to this interface.

----End

7.2.4 Setting the VLAN ID of the Outer VLAN Tag

Context

Do as follows on the S-switch on which QinQ needs to be configured.

 **NOTE**

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan** *vlan-id* command to create a VLAN and enter the VLAN view.
- Step 3** Run the **quit** command to quit the VLAN view.
- Step 4** Run the **interface** *interface-type interface-number* command to enter the Ethernet interface view or the Virtual Ethernet (VE) interface view; run the **interface eth-trunk** *trunk-id* command to enter the Eth-Trunk interface view.
- Step 5** Run the **port default vlan** *vlan-id* command to set the VLAN ID of the outer VLAN tag, that is, the default VLAN for an interface.

----End

7.2.5 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the QinQ configuration of an interface.	display current-configuration interface [<i>interface-type</i> [<i>interface-number</i>]] [{ begin exclude include } <i>regular-expression</i>]

After the configuration succeeds, run the **display current-configuration interface** [*interface-type* [*interface-number*]] [{ **begin** | **exclude** | **include** } *regular-expression*] command to check the QinQ configuration of an interface. You can obtain the following results:

- The interface type is set correctly.
- The TPID Etype value in the outer VLAN tag is set correctly.
- The VLAN ID of the outer VLAN tag, that is, the default VLAN of an interface, is set correctly.

7.3 Configuring Selective QinQ

This section describes how to configure selective QinQ.

[7.3.1 Establishing the Configuration Task](#)

[7.3.2 Configuring an Interface to Add Outer VLAN Tags to Frames](#)

[7.3.3 \(Optional\) Configuring an Interface to Discard Packets That Do Not Match Selective QinQ](#)

[7.3.4 Checking the Configuration](#)

7.3.1 Establishing the Configuration Task

Applicable Environment

As an extension of QinQ, selective QinQ is more flexible than QinQ. Selective QinQ applies to the scenario where the S-switch needs to add an outer tag with a different public Virtual Local Area Network (VLAN) ID to a frame based on its private VLAN ID. In this manner, the Internet Service Provider (ISP) network is isolated from the user network, and provides rich service features and flexible networking capabilities. When an outer VLAN tag is added, the 802.1p priority of the Customer-VLAN (C-VLAN) is mapped to the Service-VLAN (S-VLAN). In this manner, the 802.1p priority of the C-VLAN is applied to the entire ISP network. You can re-set the 802.1p priority of the S-VLAN as required.

Selective QinQ can be configured only on the following types of interfaces:

- Fast Ethernet (FE) interfaces
- Gigabit Ethernet (GE) interfaces
- Eth-Trunk interfaces

The type of all the interfaces must be hybrid.

Before configuring selective QinQ, deploy the entire network to determine which interfaces to be configured with this function. Generally, an outbound interface automatically removes the

outer VLAN tags of frames after selective QinQ is enabled. You need to configure the interface to add the outer VLAN tags of the frames for the realization of selective QinQ. You can also configure the interface to discard packets that do not match selective QinQ and VLAN mapping.

Pre-configuration Tasks

Before configuring selective QinQ, complete the following task:

- Configuring VLANs

Data Preparation

To configure selective QinQ, you need the following data.

No.	Data
1	Number of the interface to be configured with selective QinQ
2	VLAN ID of the inner VLAN tag
4	VLAN ID of the outer VLAN tag
3	802.1p priority in the outer VLAN tag

7.3.2 Configuring an Interface to Add Outer VLAN Tags to Frames

Context

Do as follows on the S-switch on which QinQ needs to be configured.

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 Ethernet interface view or the GE interface view; run the **interface eth-trunk** *trunk-id* command to enter the Eth-Trunk interface view.

Step 3 Run the **qinq vlan-translation enable** command to enable selective QinQ on an interface.

NOTE

After selective QinQ is enabled on an interface, the interface adds the default VLAN tag to each received frame, irrespective of whether the frame carries a VLAN tag. If VLAN mapping is not configured, the interface automatically removes the outer VLAN tag from the frame to be sent.

Step 4 Run the **port default vlan** *vlan-id* command to set the default VLAN for an interface.

NOTE

When using the **qinq vlan-translation enable** command to implement selective QinQ, you also need to use the **port default vlan** command to allow traffic to pass through.

Step 5 Run the **trust 8021p** command to set the priority carried in the frames received from an interface to trusted.

Step 6 Run the **port vlan-stacking vlan** *vlan-id1* [**to** *vlan-id2*] **push vlan** *vlan-id3* { **remark-8021p** *priority-id* | **priority-inherit** } command to add the outer VLAN tags specified by *vlan-id3* to frames on an interface.

Step 7 Run the **port trunk allow-pass vlan** *vlan-id3* command to add an interface to a specified VLAN.

Before running the **port vlan-stacking push** command, you must add an interface to the VLAN specified by *vlan-id3* through the **port trunk allow-pass vlan** command to enable the interface to add the outer VLAN tags to received frames.

----End

7.3.3 (Optional) Configuring an Interface to Discard Packets That Do Not Match Selective QinQ

Context

Do as follows on the S-switch on which QinQ needs to be configured.

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 Ethernet interface view or the GE interface view; run the **interface eth-trunk** *trunk-id* command to enter the Eth-Trunk interface view.

Step 3 Using the **qinq vlan-translation miss-drop** command, you can configure an interface to discard the packets that do not match selective QinQ.

----End

7.3.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check whether an interface is added to the local VLAN.	display vlan <i>vlan-id</i>
Check the configuration of selective QinQ on a specified interface.	display current-configuration interface [<i>interface-type</i> [<i>interface-number</i>]] [{ begin exclude include } <i>regular-expression</i>]

If the configurations succeed, you can obtain the following results by running the preceding commands:

- The interface is added to the local VLAN.
- VLAN mapping is configured properly on the interface.

7.4 Configuration Examples

This section provides several examples for configuring QinQ and selective QinQ.

[7.4.1 Example for Configuring QinQ](#)

[7.4.2 Example for Configuring Selective QinQ](#)

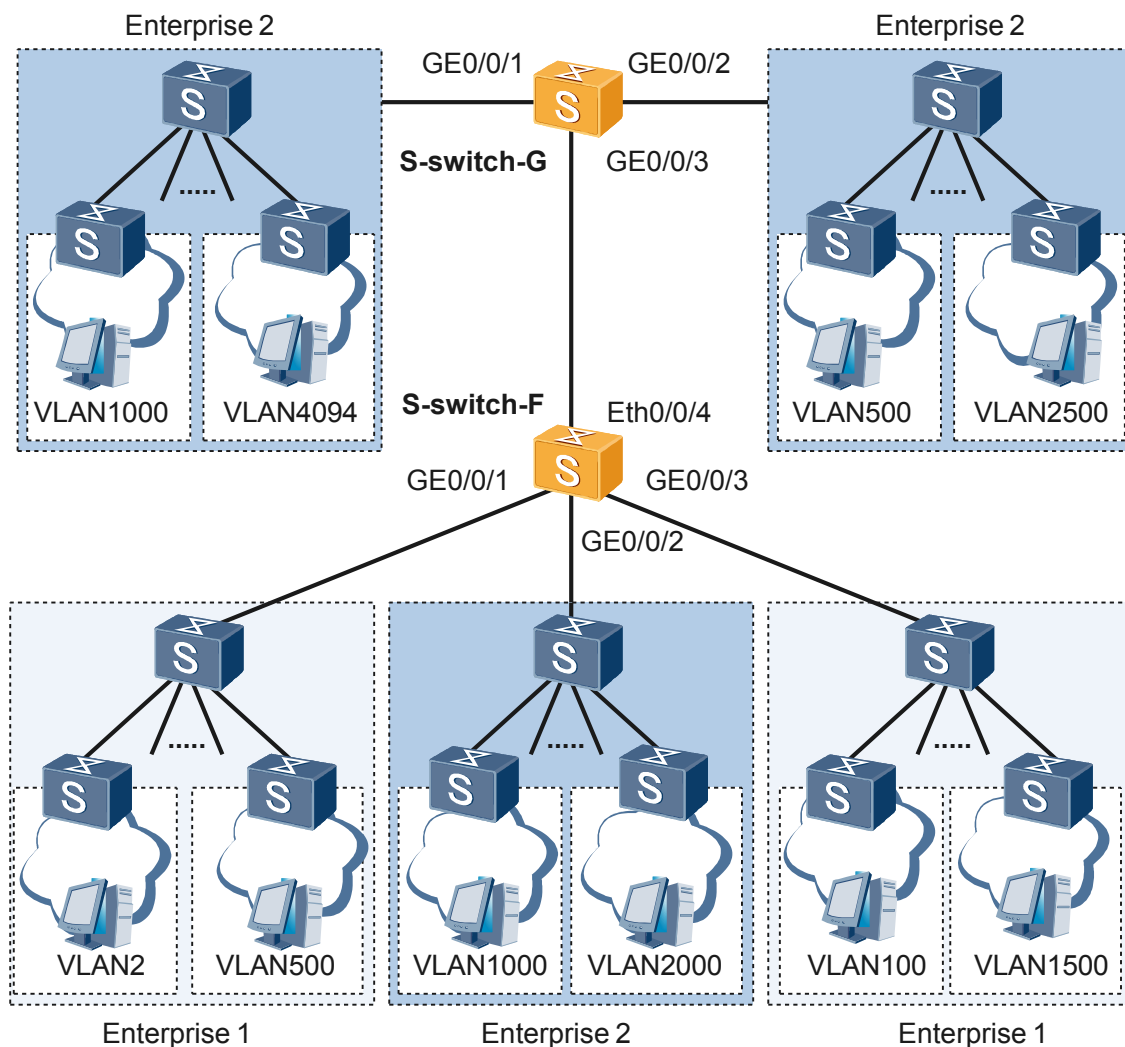
[7.4.3 Example for Setting the TPID Etype Value in the Outer VLAN Tags](#)

7.4.1 Example for Configuring QinQ

Networking Requirements

As shown in [Figure 7-1](#), there are two enterprises in the network. Enterprise 1 has two office locations and Enterprise 2 has three. Their enterprise networks are connected respectively with S-switch-G or S-switch-F in the ISP network. Enterprise 1 uses VLAN 2 to VLAN 1500 and Enterprise 2 uses VLAN 500 to VLAN 4094 to identify their intranets. The office locations of the same enterprise can communicate with each other. The two enterprises, however, are isolated from each other.

Figure 7-1 Networking diagram for configuring QinQ interfaces



Configuration Roadmap

The configuration roadmap is as follows:

- Create VLAN 10 and VLAN 20 on S-switch-F, and VLAN 20 on S-switch-G.
- Set GigabitEthernet 0/0/1, GigabitEthernet 0/0/2, and GigabitEthernet 0/0/3 as QinQ interfaces on S-switch-F.
- Set GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 as QinQ interfaces on S-switch-G.
- Add GigabitEthernet 0/0/4 of S-switch-F and GigabitEthernet 0/0/3 of S-switch-G to VLAN 20 in tagged mode.

Data Preparation

To complete the configuration, you need the following data:

- VLAN 10 to which Enterprise 1 belongs in the ISP network

- VLAN 20 to which Enterprise 2 belongs in the ISP network

Configuration Procedure

1. Create VLANs.

Create VLAN 10 and VLAN 20 on S-switch-F.

```
<Quidway> system-view
[Quidway] sysname S-switch-F
[S-switch-F] vlan batch 10 20
```

Create VLAN 20 on S-switch-G.

```
[S-switch-G] vlan batch 20
```

2. Configure QinQ interfaces.

Set GigabitEthernet 0/0/1, GigabitEthernet 0/0/2, and GigabitEthernet 0/0/3 as QinQ interfaces on S-switch-F.

```
[S-switch-F] interface ethernet 0/0/1
[S-switch-F-GigabitEthernet0/0/1] port link-type dot1q-tunnel
[S-switch-F-GigabitEthernet0/0/1] port default vlan 10
[S-switch-F-GigabitEthernet0/0/1] quit
[S-switch-F] interface ethernet 0/0/2
[S-switch-F-GigabitEthernet0/0/2] port link-type dot1q-tunnel
[S-switch-F-GigabitEthernet0/0/2] port default vlan 20
[S-switch-F-GigabitEthernet0/0/2] quit
[S-switch-F] interface ethernet 0/0/3
[S-switch-F-GigabitEthernet0/0/3] port link-type dot1q-tunnel
[S-switch-F-GigabitEthernet0/0/3] port default vlan 10
[S-switch-F-GigabitEthernet0/0/3] quit
```

Set GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 as QinQ interfaces on S-switch-G.

```
<Quidway> system-view
[Quidway] sysname S-switch-G
[S-switch-G] interface ethernet 0/0/1
[S-switch-G-GigabitEthernet0/0/1] port link-type dot1q-tunnel
[S-switch-G-GigabitEthernet0/0/1] port default vlan 20
[S-switch-G-GigabitEthernet0/0/1] quit
[S-switch-G] interface ethernet 0/0/2
[S-switch-G-GigabitEthernet0/0/2] port link-type dot1q-tunnel
[S-switch-G-GigabitEthernet0/0/2] port default vlan 20
[S-switch-G-GigabitEthernet0/0/2] quit
```

3. Configure other interfaces.

Add GigabitEthernet 0/0/4 to VLAN 20 on S-switch-F.

```
[S-switch-F] interface ethernet 0/0/4
[S-switch-F-GigabitEthernet0/0/4] port trunk allow-pass vlan 20
[S-switch-F-GigabitEthernet0/0/4] quit
```

Add GigabitEthernet 0/0/3 to VLAN 20 on S-switch-G.

```
[S-switch-F] interface ethernet 0/0/3
[S-switch-G-GigabitEthernet0/0/3] port trunk allow-pass vlan 20
[S-switch-G-GigabitEthernet0/0/3] quit
```

4. Verify the configuration.

From a host in one office location of Enterprise 1, ping a remote host in the same VLAN in another office location of Enterprise 1. If it can ping through the remote host, hosts in different locations of Enterprise 1 can communicate with each other.

From a host in one office location of Enterprise 2, ping a remote host in the same VLAN in another office location of Enterprise 2. If it can ping through the remote host, hosts in different locations of Enterprise 2 can communicate with each other.

From a host in any office location of Enterprise 1, ping a host of Enterprise 2. If it fails to ping through the host of Enterprise 2, this means that the two enterprises are isolated from each other.

Configuration Files

- S-switch-F


```
#
sysname S-switch-F
#
vlan batch 10 20
#
interface GigabitEthernet0/0/1
port link-type dot1q-tunnel
port default vlan 10
#
interface GigabitEthernet0/0/2
port link-type dot1q-tunnel
port default vlan 20
#
interface GigabitEthernet0/0/3
port link-type dot1q-tunnel
port default vlan 10
#
interface GigabitEthernet0/0/4
port trunk allow-pass vlan 20
#
return
```
- S-switch-G

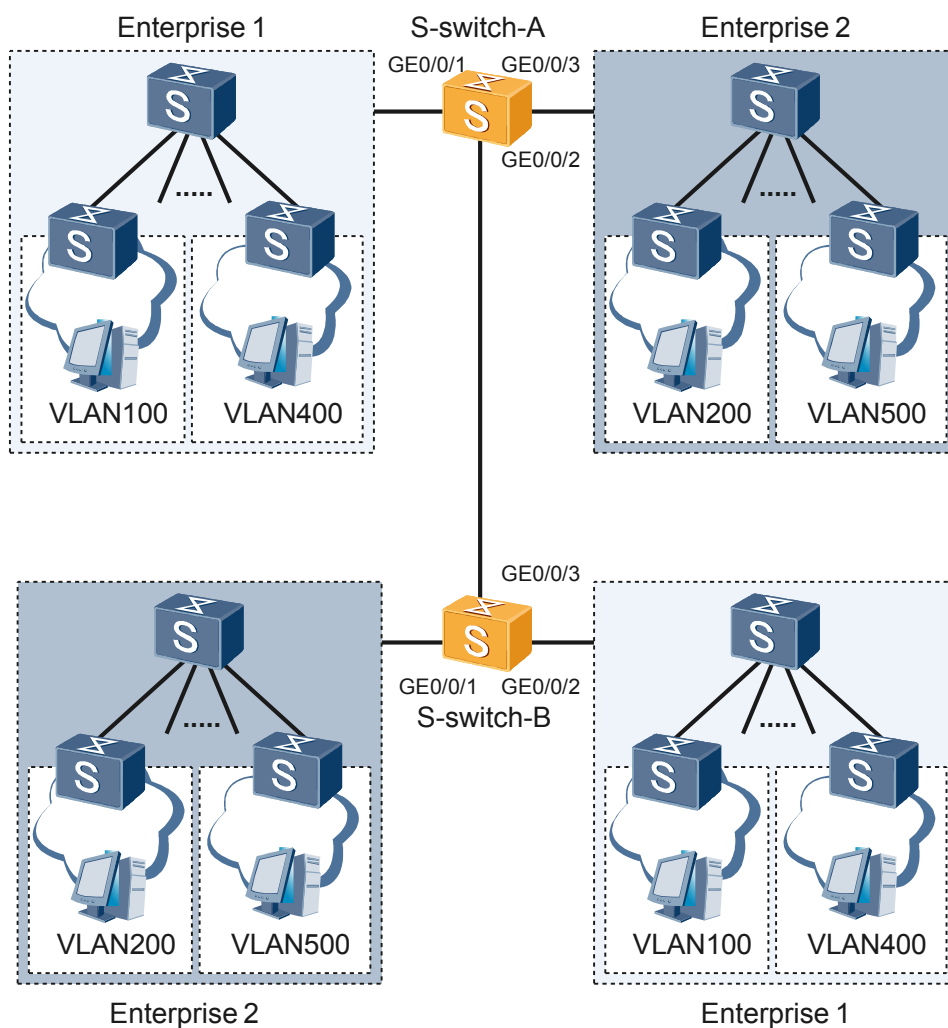

```
#
sysname S-switch-G
#
vlan batch 20
#
interface GigabitEthernet0/0/1
port link-type dot1q-tunnel
port default vlan 20
#
interface GigabitEthernet0/0/2
port link-type dot1q-tunnel
port default vlan 20
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 20
#
return
```

7.4.2 Example for Configuring Selective QinQ

Networking Requirements

As shown in [Figure 7-2](#), there are two enterprises in the network. Enterprise 1 has two office locations and Enterprise 2 has two. Their enterprise networks are connected respectively with S-switch-A or S-switch-B in the ISP network. Enterprise 1 uses VLAN 100 to VLAN 400 and Enterprise 2 uses VLAN 200 to VLAN 500 to identify their intranets.

It is required that the office locations of the same enterprise communicate with each other. The two enterprises, however, are isolated from each other. Data transmission services of Enterprise 1 use the VLAN ID of the ISP as 10; video services of Enterprise 2 use the VLAN ID of the ISP as 20. When the services of each enterprise are transmitted across the ISP network, the 802.1p priority in the outer VLAN tag inherits that in the inner VLAN tag.

Figure 7-2 Networking diagram for configuring selective QinQ

Configuration Roadmap

The configuration roadmap is as follows:

- Create VLAN 10 and VLAN 20 on S-switch-A and S-switch-B.
- Configure selective QinQ on GigabitEthernet 0/0/1 and Ethernet 0/0/3 of S-switch-A, GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 of S-switch-B to enable the interfaces to add or strip the outer VLAN tags to or off frames from a specified VLAN.
- Add GigabitEthernet 0/0/1 of S-switch-A and GigabitEthernet 0/0/2 of S-switch-B to VLAN 10 in tagged mode; add GigabitEthernet 0/0/3 of S-switch-A and Ethernet 0/0/1 of S-switch-B to VLAN 20 in tagged mode.
- Add GigabitEthernet 0/0/2 of S-switch-A and GigabitEthernet 0/0/3 of S-switch-B to VLAN 10 and VLAN 20 in tagged mode.
- Configure VLAN stacking based on the 802.1p priority to transmit different services.

Data Preparation

To complete the configuration, you need the following data:

- VLAN 10 to which Enterprise 1 belongs in the ISP network
- VLAN 20 to which Enterprise 2 belongs in the ISP network

Configuration Procedure

1. Create VLANs.

Create VLAN 10, VLAN 20, and VLAN 300 on S-switch-A.

```
<S-switch-A> system-view
[S-switch-A] vlan batch 10 20 300
```

Create VLAN 10 and VLAN 20 on S-switch-B.

```
<S-switch-B> system-view
[S-switch-B] vlan batch 10 20 300
```

2. Configure selective QinQ on interfaces to enable the inbound interfaces to add or strip the outer tags to or off frames from a specified VLAN. The priority of the inner VLAN is inherited.

Configure GigabitEthernet 0/0/1 of S-switch-A.

```
[S-switch-A] interface ethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] qinq vlan-translation enable
[S-switch-A-GigabitEthernet0/0/1] port default vlan 300
[S-switch-A-GigabitEthernet0/0/1] trust 8021p
[S-switch-A-GigabitEthernet0/0/1] port vlan-stacking vlan 100 to 400 push vlan
10 priority-inherit
[S-switch-A-GigabitEthernet0/0/1] quit
```

Configure GigabitEthernet 0/0/3 of S-switch-A.

```
[S-switch-A] interface ethernet 0/0/3
[S-switch-A-GigabitEthernet0/0/3] qinq vlan-translation enable
[S-switch-A-GigabitEthernet0/0/3] port default vlan 300
[S-switch-A-GigabitEthernet0/0/3] trust 8021p
[S-switch-A-GigabitEthernet0/0/3] port vlan-stacking vlan 200 to 500 push vlan
20 priority-inherit
[[S-switch-A-GigabitEthernet0/0/3] port trunk allow-pass vlan 20
[[S-switch-A-GigabitEthernet0/0/3] quit
```

Configure GigabitEthernet 0/0/1 of S-switch-B.

```
[S-switch-B] interface ethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] qinq vlan-translation enable
[S-switch-B-GigabitEthernet0/0/1] port default vlan 300
[S-switch-B-GigabitEthernet0/0/1] trust 8021p
[S-switch-A-GigabitEthernet0/0/1] port vlan-stacking vlan 100 to 400 push vlan
10 priority-inherit
[[S-switch-A-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[S-switch-B-GigabitEthernet0/0/1] quit
```

Configure GigabitEthernet 0/0/2 of S-switch-B.

```
[S-switch-B] interface ethernet 0/0/2
[S-switch-B-GigabitEthernet0/0/2] qinq vlan-translation enable
[S-switch-B-GigabitEthernet0/0/2] port default vlan 300
[S-switch-B-GigabitEthernet0/0/2] trust 8021p
[S-switch-B-GigabitEthernet0/0/2] port vlan-stacking vlan 100 to 400 push vlan
10 priority-inherit
[S-switch-B-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[S-switch-B-GigabitEthernet0/0/2] quit
```

3. Configure other interfaces.

Add GigabitEthernet 0/0/2 to VLAN 10 and VLAN 20 on S-switch-A.

```
[S-switch-A] interface ethernet 0/0/2
```

```
[S-switch-A-GigabitEthernet0/0/2] port trunk allow-pass vlan 10 20
[S-switch-A-GigabitEthernet0/0/2] quit
```

Add GigabitEthernet 0/0/3 to VLAN 10 and VLAN 20 on S-switch-B.

```
[S-switch-B] interface ethernet 0/0/3
[S-switch-A-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
[S-switch-A-GigabitEthernet0/0/3] quit
```

4. Verify the configuration.

From a host in one office location of Enterprise 1, ping a remote host in the same VLAN in another office location of Enterprise 1. If it can ping through the remote host, hosts in different locations of Enterprise 1 can communicate with each other.

From a host in one office location of Enterprise 2, ping a remote host in the same VLAN in another office location of Enterprise 2. If it can ping through the remote host, hosts in different locations of Enterprise 2 can communicate with each other.

From a host in any office location of Enterprise 1, ping a host of Enterprise 2. If it fails to ping through the host of Enterprise 2, this means that the two enterprises are isolated from each other.

Configuration Files

- S-switch-A

```
#
system-view
sysname S-switch-A
#
vlan batch 10 20 300
#
interface ethernet 0/0/1
port trunk allow-pass vlan 10
qinq vlan-translation enable
port default vlan 300
trust 8021p
port vlan-stacking vlan 100 to 400 push vlan 10 priority-inherit
#
interface ethernet 0/0/2
port trunk allow-pass vlan 10 20
#
interface ethernet 0/0/3
port trunk allow-pass vlan 20
qinq vlan-translation enable
port default vlan 300
trust 8021p
port vlan-stacking vlan 200 to 500 push vlan 20 priority-inherit
#
return
```

- S-switch-B

```
#
system-view
sysname S-switch-B
#
vlan batch 10 20 300
#
interface ethernet 0/0/1
port trunk allow-pass vlan 20
qinq vlan-translation enable
port default vlan 300
trust 8021p
port vlan-stacking vlan 200 to 500 push vlan 20 priority-inherit
interface ethernet 0/0/2
port trunk allow-pass vlan 10
qinq vlan-translation enable
port default vlan 300
trust 8021p
```

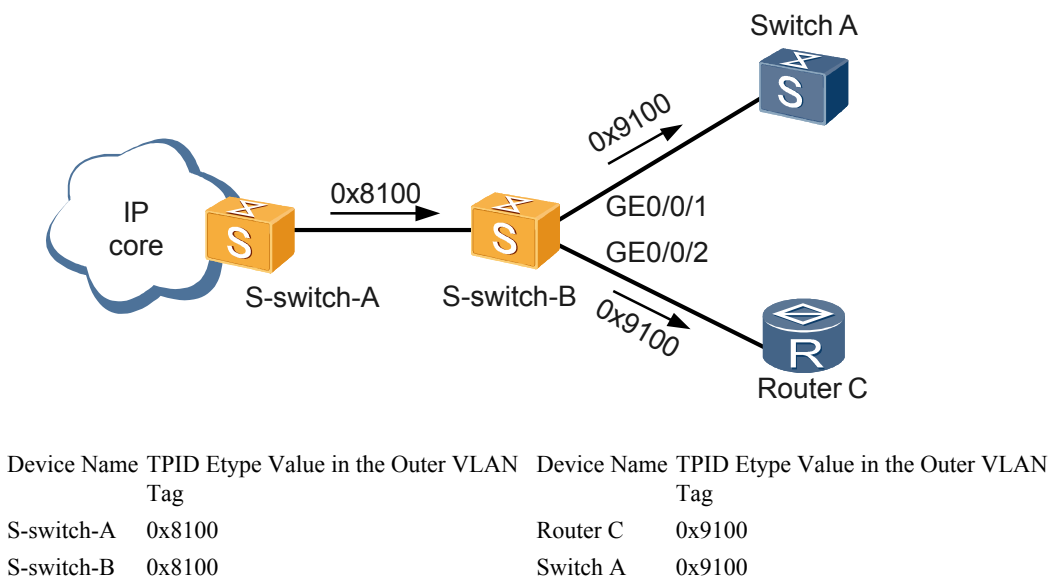
```
port vlan-stacking vlan 100 to 400 push vlan 10 priority-inherit
#
interface ethernet 0/0/3
port trunk allow-pass vlan 10 20
#
return
```

7.4.3 Example for Setting the TPID Etype Value in the Outer VLAN Tags

Networking Requirements

S-switch-A and S-switch-B are Huawei datacom devices using the Versatile Routing Platform (VRP). Router C and Switch A are non-Huawei devices. The networking and the TPID Etype value in the outer VLAN tag are shown in [Figure 7-3](#). You can set the TPID Etype value on the interfaces of S-switch-B. In this manner, the devices of different manufacturers can communicate with each other.

Figure 7-3 Networking diagram of configuring the compatibility of the TPID Etype value in the outer VLAN tags



Configuration Roadmap

The configuration roadmap is as follows:

- Set the TPID Etype value for the outer tag of Switch A on the physical interface on S-switch-B connected to Switch A.
- Set the TPID Etype value for the outer tag of Router C on the physical interface on S-switch-B connected to Router C.

Data Preparation

To complete the configuration, you need the following data:

- TPID Etype value in the outer VLAN tag added by the non-Huawei devices
- Names of the physical interfaces connecting the non-Huawei devices on S-switch-B

Configuration Procedure

1. Set the TPID Etype value for the outer VLAN tag on the physical interfaces connecting the non-Huawei devices on S-switch-B.

```
<Quidway> system-view
[Quidway] sysname S-switch-B
[S-switch-B] interface ethernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] qinq protocol 9100
[S-switch-B-GigabitEthernet0/0/1] quit
[S-switch-B] interface ethernet 0/0/2
[S-switch-B-GigabitEthernet0/0/2] qinq protocol 9100
```

Configuration Files

Configuration file of S-switch-B

```
#
sysname S-switch-B
#
interface GigabitEthernet0/0/1
qinq protocol 9100
#
interface GigabitEthernet0/0/2
qinq protocol 8100
#
return
```

8 MAC Table Configuration

About This Chapter

This chapter describes the basics, methods, and examples for configuring the Medium Access Control (MAC) table.

[8.1 Introduction](#)

This section describes the MAC table, capacity of the MAC table, and limit to the number of MAC entries learned by an interface.

[8.2 Configuring the MAC Table](#)

This section describes how to configure the MAC table.

[8.3 Configuration Examples](#)

This section provides examples for configuring the MAC address table.

8.1 Introduction

This section describes the MAC table, capacity of the MAC table, and limit to the number of MAC entries learned by an interface.

[8.1.1 MAC Table](#)

[8.1.2 Capacity of a MAC Table and Limit to the Number of MAC Entries Learned by an Interface](#)

[8.1.3 Packet Forwarding Restriction](#)

[8.1.4 References](#)

[8.1.5 Logical Relationships Between Configuration Tasks](#)

8.1.1 MAC Table

The S-switch holds one MAC address table (MAC table for short). The MAC table records MAC addresses of all the devices connected to all the interfaces of the S-switch. When forwarding a data frame, the S-switch searches the MAC table for the outbound interface according to the destination MAC address in the frame. This helps the S-switch reduce the broadcasting of frames.

8.1.2 Capacity of a MAC Table and Limit to the Number of MAC Entries Learned by an Interface

Capacity of a MAC Table

The MAC table on the S-switch can hold a maximum of 16384 entries.

Limit to the Number of MAC Entries Learned by an Interface

The capacity of a MAC table is limited; therefore, when hackers forge a large quantity of packets with different source MAC addresses and send the packets to the S-switch, the MAC table of the S-switch may be filled to its full capacity. After the MAC table of the S-switch is crammed with MAC entries, the system cannot learn the source MAC address in the normal packets received by the interface any more.

The S-switch supports the limit to the number of MAC entries learned by an interface. That is, you can set the maximum number of dynamic MAC entries learned by the interface. After this function is configured, the interface cannot learn new MAC entries if the interface has learned the maximum MAC entries. The interface can learn new MAC entries only when the previously learned MAC entries aged.

In most cases, the attack packets sent by a hacker enter the S-switch through the same interface. Thus, you can prevent the MAC table of the S-switch from being fully filled by configuring the limit to the number of MAC entries learned by an interface.

8.1.3 Packet Forwarding Restriction

Packet forwarding restriction indicates that the S-switch can restrict the known multicast packets and broadcast packets with specified MAC addresses in the specified VLAN from being forwarded to an interface or certain interfaces.

8.1.4 References

For details on the principle of the MAC table technology, refer to the chapter "Ethernet and Switching Technology" in the *Quidway S5300 Series Ethernet Switches Feature Description*.

8.1.5 Logical Relationships Between Configuration Tasks

Configuring the MAC table is the basis for configuring the capacity of the MAC table and limit to the amount of MAC entries learned by an interface. You are required to first configure the MAC table, and then choose to configure the capacity of the MAC table and limit to the number of MAC entries learned by an interface as required.

8.2 Configuring the MAC Table

This section describes how to configure the MAC table.

The configuration procedures are optional and not listed in sequence.

[8.2.1 Establishing the Configuration Task](#)

[8.2.2 \(Optional\) Adding MAC Entries](#)

[8.2.3 \(Optional\) Setting the Aging Time of Dynamic MAC Entries](#)

[8.2.4 Checking the Configuration](#)

8.2.1 Establishing the Configuration Task

Applicable Environment

You should manually add MAC entries or adjust the aging time of dynamic entries in the MAC table in the following situations to optimize the MAC table and meet different requirements:

- Sending the packets with a specified destination MAC address from a designated interface
- Discarding the packets with a specified source or destination MAC address
- Modifying the aging time of dynamic MAC entries

Pre-configuration Tasks

None.

Data Preparation

To configure the MAC table, you need the following data.

No.	Data
1	(Optional) Destination MAC address, number of the outbound interface, and ID of the VLAN
2	(Optional) Aging time of dynamic MAC entries

8.2.2 (Optional) Adding MAC Entries

Context

Do as follows on the S-switch where static or blackhole MAC entries need to be added.

The S-switch can learn 16384 MAC addresses, among which the number of non-dynamic MAC addresses cannot exceed 1024.

When you configure static or blackhole entries, you may meet either of the following cases if the MAC table is full:

- If there are less than 1024 non-dynamic MAC entries, the system deletes a dynamic MAC entry and adds a static or blackhole MAC entry.
- If there are 1024 non-dynamic entries, the system prompts "Number of MAC address entries has reached the limit".

Procedure

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

Step 2 Run the **mac-address { blackhole | static } mac-address interface-type interface-number vlan vlan-id** command to add MAC entries.

Through this configuration, you can add static MAC entries and blackhole MAC entries.

----End

8.2.3 (Optional) Setting the Aging Time of Dynamic MAC Entries

Context

Do as follows on the S-switch on which the aging time of dynamic MAC entries needs to be adjusted.

Procedure

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

Step 2 Run the **mac-address aging-time aging-time** command to set the aging time of dynamic MAC entries.

By default, the aging time of dynamic MAC entries is 300 seconds.

----End

8.2.4 Checking the Configuration

Run the following commands to check the previous configuration.

Action	Command
Check information about the MAC table.	display mac-address [[<i>mac-address</i> { vlan <i>vlan-id</i> }] [blackhole static] [dynamic [<i>interface-type interface-number</i> vlan <i>vlan-id</i>]]]
Check the aging time of MAC entries.	display mac-address aging-time

Run the preceding commands, and you can obtain the following information:

- The static and blackhole MAC entries are configured correctly.
- The aging time of MAC entries is set correctly.

8.3 Configuration Examples

This section provides examples for configuring the MAC address table.

8.3.1 Example for Configuring the MAC Table

8.3.1 Example for Configuring the MAC Table

Networking Requirements

The MAC address of the PC is 0002-0002-0002 and the PC belongs to VLAN 2, and the interface connecting the PC to the S-switch is Ethernet 0/0/8. To prevent MAC addresses from being attacked, you need to add a static entry to the MAC address table for the PC on the S-switch, and set the aging time of dynamic MAC entries on the S-switch to 500 seconds.

Configuration Roadmap

The configuration roadmap is as follows:

- Create a VLAN and add Ethernet 0/0/8 to the VLAN.
- Configure static MAC entries.
- Set the aging time of dynamic entries to 500 seconds.

Data Preparation

To complete the configuration, you need the following data:

- MAC address: 00-02-00-02-00-02
- VLAN to which the S-switch belongs: VLAN 2
- Interface connecting the PC and the S-switch being Ethernet 0/0/8
- Aging time of dynamic MAC entries on the S-switch being 500 seconds

Configuration Procedure

1. Add static MAC entries.

Create VLAN 2 and add Ethernet 0/0/8 to VLAN 2.

```
<Quidway> system-view
[Quidway] vlan 2
[Quidway-vlan2] port ethernet 0/0/8
[Quidway-vlan2] quit
```

Configure static MAC entries.

```
[Quidway] mac-address static 2-2-2 ethernet 0/0/8 vlan 2
```

2. Set the aging time of dynamic MAC entries.

```
[Quidway] mac-address aging-time 500
```

3. Verify the configuration.

Run the **display mac-address** command in any view to check whether the static entry is added successfully.

```
[Quidway] display mac-address 2-2-2 vlan 2
```

MAC Address	VLAN/VSI	Port	Type	Lsp
0002-0002-0002	2	Ethernet0/0/8	static	0/-

Total matching items displayed = 1

Run the **display mac-address aging-time** command to check whether the aging time of dynamic entries is set successfully.

```
[Quidway] display mac-address aging-time
Aging time: 500 seconds
```

Configuration Files

```
#
 sysname Quidway
#
 vlan batch 2
#
 mac-address aging-time 500
#
 interface Ethernet0/0/8
 port default vlan 2
 mac-address static 0002-0002-0002 Ethernet0/0/8 vlan 2
#
 return
```

9 MSTP Configuration

About This Chapter

This chapter describes the basics, methods, and examples for configuring the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP).

[9.1 Introduction](#)

This section describes the basic knowledge you need to know before configuring MSTP.

[9.2 Enabling Basic Functions of MSTP on the S-switch](#)

This section describes how to enable basic functions of MSTP on the S-switch.

[9.3 Adding an S-switch to a Specified MST Region](#)

This section describes how to add an S-switch to a specified multiple spanning tree (MST) region.

[9.4 Configuring MSTP Parameters of the S-switch](#)

This section describes how to configure MSTP parameters of the S-switch.

[9.5 Configuring MSTP Protection on the S-switch](#)

This section describes how to configure MSTP protection on the S-switch.

[9.6 Maintaining MSTP](#)

This section describes how to maintain MSTP.

[9.7 Configuration Examples](#)

This section provides MSTP configuration examples.

9.1 Introduction

This section describes the basic knowledge you need to know before configuring MSTP.

[9.1.1 STP, RSTP, and MSTP](#)

[9.1.2 References](#)

9.1.1 STP, RSTP, and MSTP

STP is used in the local area network (LAN) to eliminate loops. The S-switches running STP discover loops in the network by exchanging information with one another, and block certain interfaces to eliminate loops. With the growing LAN scale, STP has become an important protocol.

RSTP is described in Institute of Electrical and Electronics Engineers (IEEE) 802.1w in detail. RSTP is based on and supplements STP. Nowadays, RSTP is employed in the actual networking instead of STP.

MSTP is a new spanning tree protocol defined in IEEE 802.1s and introduces concepts of region and instance. Based on different requirements, MSTP divides a big network into regions where multiple spanning tree instances (MSTIs) are created. These MSTIs are mapped to virtual LANs (VLANs) and bridge protocol data units (BPDUs) are transmitted between network bridges. Network bridges determine regions to which they belong according to BPDUs. RSTP with multiple instances are used within regions. Protocols which RSTP are compatible with are used between regions.

MSTP is compatible with STP and RSTP. RSTP is compatible with STP.

9.1.2 References

For details about the principles of STP, RSTP, and MSTP, refer to chapter "MSTP" in the *Quidway S5300 Series Ethernet Switches Feature Description*.

9.2 Enabling Basic Functions of MSTP on the S-switch

This section describes how to enable basic functions of MSTP on the S-switch.

[9.2.1 Establishing the Configuration Task](#)

[9.2.2 Enabling an Interface to Process BPDUs](#)

[9.2.3 Enabling MSTP](#)

[9.2.4 Checking the Configuration](#)

9.2.1 Establishing the Configuration Task

Applicable Environment

MSTP functions are enabled on the S-switch.

Pre-configuration Tasks

None.

Data Preparation

None.

9.2.2 Enabling an Interface to Process BPDUs

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 **bpdudisable** command to enable the interface to process BPDUs.

By default, an interface does not process BPDUs.

----End

9.2.3 Enabling MSTP

Context

Do as follows on the S-switch on which MSTP needs to be enabled.

Procedure

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

Step 2 Run the **mstp enable** command to enable the MSTP function on the S-switch.

By default, the MSTP function on the S-switch is disabled.

NOTE

After you run the **mstp enable** command, the system prompts "Are you sure to change global STP status? [Y/N]" for you to determine whether MSTP needs to be enabled.

When the MSTP function is enabled on the S-switch, the MSTP function is enabled on all interfaces on the S-switch by default.

NOTE

If two or more interfaces on the S-switch enabled with MSTP need to be added to the Eth-Trunk, you must disable the interfaces before adding them to the Eth-Trunk. Then, you can enable these interfaces of the Eth-Trunk. Otherwise, a temporary broadcast storm occurs.

----End

9.2.4 Checking the Configuration

Run the following commands to check the previous configuration in the user view.

Action	Command
Check the STP configuration in the system view.	display stp
Check whether an interface is enabled to process BPDUs in the Ethernet interface view.	display current-configuration interface

9.3 Adding an S-switch to a Specified MST Region

This section describes how to add an S-switch to a specified multiple spanning tree (MST) region.

[9.3.1 Establishing the Configuration Task](#)

[9.3.2 Setting the MSTP Mode of the S-switch](#)

[9.3.3 Setting the MST Region](#)

[9.3.4 Activating the Configuration of an MST Region](#)

[9.3.5 \(Optional\) Setting the S-switch as the Root Switch or Secondary Root Switch](#)

[9.3.6 \(Optional\) Setting the Priority of the S-switch in a Specified MSTI](#)

[9.3.7 Checking the Configuration](#)

9.3.1 Establishing the Configuration Task

Applicable Environment

An S-switch that is not enabled with MSTP is added to an MST region. Or an S-switch is enabled with MSTP and needs to be added to another MST region by modifying its MST region attributes.

Pre-configuration Tasks

Before adding the S-switch to the specified MST region, complete the following tasks:

- Configuring physical attributes of the interface
- Configuring VLAN features of the interface

Data Preparation

Before adding the S-switch to the specified MST region, you need the following data.

No.	Data
1	Name of the MST region that the S-switch belongs to
2	Mapping between MSTIs and VLANs

No.	Data
3	MSTP revision level of the MST region
4	(Optional) Priority of the S-switch in the specified MSTI

9.3.2 Setting the MSTP Mode of the S-switch

Context



CAUTION

When an S-switch is configured in multiple MSTIs, other MSTIs except MSTI 0 fail to communicate if the S-switch is switched to the STP mode. MSTI 0 refers to the internal spanning tree (IST).

Do as follows on each S-switch that needs to be added to the MST region.

Procedure

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

Step 2 Run the **stp mode { mstp | stp }** command to set the MSTP mode of the S-switch.

By default, an S-switch runs in MSTP mode.



NOTE

On the S-switch running MSTP, if an interface is connected to a device running STP, the interface automatically switches to the STP compatible mode. If the device running STP is powered off or removed, the interface cannot automatically switch to the MSTP mode. In this case, you must run the **stp mcheck** command to manually switch the interface to the MSTP mode.

----End

9.3.3 Setting the MST Region

Context

Do as follows on each S-switch that needs to be added to the MST region.



NOTE

The two S-switches belong to the same MST region when the following configurations are the same:

- MST region name
- Mapping between MSTIs and VLANs
- Revision level of the MST region

Procedure

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

Step 2 Run the **stp region-configuration** command to enter the MST region view.

Step 3 Run the **region-name** *name* command to set the name of the MST region.

By default, the name of an MST region is the MAC address of an S-switch.

Step 4 Run the **instance** *instance-id* **vlan** { *vlan-id* [*to* *vlan-id*] } <1-10> command to set the mapping between MSTIs and VLANs.

By default, all VLANs in an MST region are mapped to MSTI 0.

Step 5 Run the **revision-level** *level* command to set the MSTP revision level of the MST region.

By default, the revision level of the MST region is 0.

----End

9.3.4 Activating the Configuration of an MST Region

Context

NOTE

When you change parameter values of an MST region on the S-switch after enabling the MSTP feature, you can run the following commands to activate the configuration of the MST region.

The change of related parameters (especially the VLAN mapping table) in an MST region causes recalculation of spanning trees and route flapping in a network. You are recommended to run the **check region-configuration** command to check the parameter settings of the current region in the MST region view before activating them. If the parameter settings are correct, you can run the **active region-configuration** command to activate them.

The activated configuration of the MST region by running the **active region-configuration** command includes:

- MST region name
- Revision level
- Mapping between VLANs and MSTIs

Procedure

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

Step 2 Run the **stp region-configuration** command to enter the MST region view.

Step 3 Run the **check region-configuration** command to check the configuration of parameters in the MST region.

Step 4 Run the **active region-configuration** command to activate the configuration of the MST region.

----End

9.3.5 (Optional) Setting the S-switch as the Root Switch or Secondary Root Switch

Context

Do as follows on the S-switch that needs to join the MST region and to be the root switch or secondary root switch.

Root types of the S-switches in different MSTIs are independent of each other. The S-switch can serve as the root switch or secondary root switch of any MSTI. However, the S-switch cannot serve as both the root switch and secondary root switch in the same MSTI.

It is not recommended that you specify two or more root switches for an MSTI. You can designate multiple secondary root switches for an MSTI. In general, you are recommended to designate one root switch and multiple secondary root switches for an MSTI.

Procedure

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

Step 2 Run the **stp [instance *instance-id*] root primary** command to set the S-switch as the root switch; run the **stp [instance *instance-id*] root secondary** command to set the S-switch as the secondary root switch.

By default, the S-switch serves as neither the root switch nor the secondary root switch of the spanning tree.

This configuration procedure is optional. If you need to set the S-switch as the root switch or the secondary root switch, perform this configuration procedure.

----End

9.3.6 (Optional) Setting the Priority of the S-switch in a Specified MSTI

Context



CAUTION

If the current S-switch has been configured as the root switch or secondary root switch, its priority cannot be set. To set the priority of the current S-switch, you must first disable the root switch or secondary root switch function.

Do as follows on the S-switch whose priority in the specified MSTI needs to be set.

Procedure

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

Step 2 Run the **stp [instance *instance-id*] priority *priority*** command to set the priority of the S-switch in the specified MSTI.

The lower value of the priority, the higher the priority of the S-switch and the more the possibility of the S-switch being selected as the root switch. The priority of the root switch or secondary root switch must be higher than that of other S-switches. Otherwise, the root switch or the secondary root switch may lose its position. By default, the priority of the S-switch is 32768.

----End

9.3.7 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the MST region configuration that has taken effect.	display stp region-configuration

After the configuration succeeds, the MST region of the S-switch is correctly configured when you run the **display stp region-configuration** command to view the configuration of the MST region of the S-switch.

9.4 Configuring MSTP Parameters of the S-switch

This section describes how to configure MSTP parameters of the S-switch.

[9.4.1 Establishing the Configuration Task](#)

[9.4.2 \(Optional\) Configuring MSTP Network Parameters of the S-switch](#)

[9.4.3 \(Optional\) Configuring MSTP Parameters of an Interface](#)

[9.4.4 \(Optional\) Switching an Interface to the MSTP Mode](#)

9.4.1 Establishing the Configuration Task

Applicable Environment

In some specific networks, it is necessary to adjust MSTP parameters of some S-switches to optimize their performance.

Pre-configuration Tasks

Before adjusting MSTP parameters of the S-switch, you need to complete the following tasks:

- Configuring physical attributes of the interface
- Configuring VLAN features of the interface
- Adding an S-switch to a specified MST region

Data Preparation

Before adjusting MSTP parameters of the S-switch, you need the following data.

No.	Data
1	(Optional) Value of Hello Time
2	(Optional) Value of Forward Delay
3	(Optional) Value of Max Age
4	(Optional) Priority of the S-switch in the specified MSTI
5	(Optional) Network diameter
6	(Optional) Maximum number of hops of the spanning tree in an MST region
7	(Optional) Number of the interface on which to enable or disable MSTP
8	(Optional) Priority of the interface in the specified MSTI
9	(Optional) Path cost of an interface
10	(Optional) Maximum transmission speed of an interface

9.4.2 (Optional) Configuring MSTP Network Parameters of the S-switch

Context

Do as follows on the S-switch where MSTP network parameters need to be configured.

It is not recommended to directly set the value of **Hello Time**, **Forward Delay**, or **Max Age**. It is recommended to run the **stp bridge-diameter** command to set the network diameter. The S-switch automatically calculates optimum values of **Hello Time**, **Forward Delay**, and **Max Age** according to the network diameter.



NOTE

To prevent frequent route flapping, values of **Hello Time**, **Forward Delay**, and **Max Age** must meet the following conditions:

$$2 \times (\text{Forward Delay} - 1.0 \text{ second}) \geq \text{Max Age}$$

$$\text{Max Age} \geq 2 \times (\text{Hello Time} + 1.0 \text{ second})$$

Procedure

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

Step 2 Run the **stp bridge-diameter** *diameter* command to set the network diameter.

By default, the value of the network diameter is 7.

Step 3 Run the **stp timer forward-delay** *forward-delay* command to set the value of **Forward Delay** of the S-switch.

By default, the value of **Forward Delay** is 1500, in centiseconds, that is, 15, in seconds.

Step 4 Run the **stp timer hello** *hello-time* command to set the value of **Hello Time** of the S-switch.

By default, the value of **Hello Time** is 200, in centiseconds, that is, 2, in seconds.

Step 5 Run the **stp timer max-age max-age** command to set the value of **Max Age** of the S-switch.

By default, the value of **Max Age** is 2000, in centiseconds, that is, 20, in seconds.

Step 6 Run the **stp max-hops hop** command to set the maximum number of hops in an MST region.

By default, the maximum number of hops in an MST region is 20.

Step 7 Run the **stp pathcost-standard { dot1d-1998 | dot1t | legacy }** command to specify the standard to calculate the path cost of an interface.

By default, IEEE 802.1t standard method is used to calculate the default value of the path cost. It is recommended that you use the same standard to calculate path costs of interfaces on all S-switches in the same network.

 **NOTE**

When you change the method to calculate the path cost of an interface, the path cost of the interface is restored to the default value.

----End

9.4.3 (Optional) Configuring MSTP Parameters of an Interface

Context



CAUTION

When MSTP is disabled on an interface, a loop may occur.

Do as follows on the S-switch where MSTP parameters need to be set on an interface.

Step 6 and **Step 11** are optional and not listed in sequence.

Procedure

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

Step 2 Run the **stp interface { interface-type interface-number [to interface-number] } &<1-10> { enable | disable }** command to enable MSTP on an interface.

Step 3 Run the **interface interface-type interface-number** command to enter the Ethernet interface view or the virtual Ethernet (VE) interface view. Or, run the **interface eth-trunk trunk-id** command to enter the Eth-Trunk interface view.

Step 4 Run the **bpdu enable** command to enable an interface to process BPDUs.

By default, an interface does not process BPDUs.

Step 5 Run the **quit** command to quit the interface view.

Step 6 Run the **stp interface { interface-type interface-number [to interface-number] } &<1-10> edged-port { enable | disable }** command to set an interface to an edge interface.

The interface type can be Ethernet, Eth-Trunk, or Gigabit Ethernet (GE).

By default, an interface is a non-edge interface.

- Step 7** Run the **stp interface** { *interface-type interface-number* [**to interface-number**] } <1-10> **point-to-point** { **auto** | **force-false** | **force-true** } command to connect the interface to a point-to-point (P2P) link.

By default, an interface automatically identifies whether it is connected to a P2P link.

- Step 8** Run the **stp interface** { *interface-type interface-number* [**to interface-type interface-number**] } <1-10> **instance instance-id port priority priority** command to set the priority of an interface in the specified MSTI.

By default, the priority of an interface in the specified MSTI is 128.

- Step 9** Run the **stp interface** { *interface-type interface-number* [**to interface-number**] } <1-10> [**instance instance-id**] **cost cost** command to set the path cost of an interface in the specified MSTI.

By default, MSTP calculates the path cost of an interface.

- Step 10** Run the **stp interface** { *interface-type interface-number* [**to interface-number**] } <1-10> **transmit-limit packet-number** command to set the maximum number of BPDUs that an interface can send in a Hello Time.

By default, the maximum number of BPDUs that an interface can send in a Hello Time is 3.

- Step 11** Run the **stp converge** { **fast** | **normal** } command to set the STP convergence mode of an interface.

By default, the STP convergence mode of an interface is **fast**.

----End

9.4.4 (Optional) Switching an Interface to the MSTP Mode

Switching One or More Interfaces to the MSTP Mode

Context

Do as follows on the S-switch where one or more interfaces need to be switched to the MSTP mode.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **stp interface** *interface-type interface-number* [**to interface-number**] } <1-10> **mcheck** command to perform the MCheck operation.

----End

Switching One Interface to the MSTP Mode

Context

Do as follows on the S-switch where one interface needs to be switched to the MSTP mode.

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 Ethernet interface view or the VE interface view; run the **interface eth-trunk** *trunk-id* command to enter the Eth-Trunk interface view.
- Step 3** Run the **stp mcheck** command to perform the MCheck operation.

 **NOTE**

The MCheck operation can be performed only if the S-switch runs MSTP. The MCheck operation is invalid when the S-switch runs in STP compatible mode.

----End

9.5 Configuring MSTP Protection on the S-switch

This section describes how to configure MSTP protection on the S-switch.

[9.5.2 \(Optional\) Configuring BPDU Protection on the S-switch](#) to [9.5.4 \(Optional\) Configuring Loop Protection on an Interface](#) are optional and not listed in sequence.

[9.5.1 Establishing the Configuration Task](#)

[9.5.2 \(Optional\) Configuring BPDU Protection on the S-switch](#)

[9.5.3 \(Optional\) Configuring Root Protection on an Interface](#)

[9.5.4 \(Optional\) Configuring Loop Protection on an Interface](#)

[9.5.5 Checking the Configuration](#)

9.5.1 Establishing the Configuration Task

Applicable Environment

It is recommended to configure:

- BPDU protection on the S-switch with edge interfaces
- Root protection on the root switch
- Loop protection on the root interface and the alternate interface

Each interface can be set with only one protection function. If you set BPDU protection on the S-switch and set root protection or loop protection on an interface of the S-switch, the interface cannot be set as an edge interface any longer. Thus, BPDU protection cannot take effect on the interface.

Pre-configuration Tasks

Before configuring MSTP protection on the S-switch, you need to complete the following tasks:

- Configuring physical attributes of the interface
- Configuring VLAN features of the interface
- Adding an S-switch to a specified MST region
- Setting the interface as an edge interface before configuring BPDU protection

Data Preparation

To configure MSTP protection on the S-switch, you need the following data.

No.	Data
1	(Optional) Number of the interface on which root protection is to be enabled
2	(Optional) Number of the interface on which loop protection is to be enabled

9.5.2 (Optional) Configuring BPDU Protection on the S-switch

Context

Do as follows on the S-switch on which BPDU protection needs to be configured.

Procedure

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

Step 2 Run the **stp bpd protection** command to configure BPDU protection on the S-switch.

----End

9.5.3 (Optional) Configuring Root Protection on an Interface

Configuring Root Protection on an Interface in the System View

Context

Do as follows on the S-switch on which root protection needs to be configured.

Procedure

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

Step 2 Run the **stp interface interface-type interface-number [to interface-number] }&<1-10> root-protection** command to configure root protection on an interface.

----End

Configuring Root Protection on an Interface in the Interface View

Context

Do as follows on the S-switch on which root protection needs to be configured.

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 Ethernet interface view or the GE interface view; run the **interface eth-trunk** *trunk-id* command to enter the Eth-Trunk interface view.
- Step 3** Run the **stp root-protection** command to configure root protection on the S-switch.



NOTE

The interface to be configured with root protection must be a specified interface in all MSTIs.

----End

9.5.4 (Optional) Configuring Loop Protection on an Interface

Configuring Loop Protection on an Interface in the System View

Context

Do as follows on the S-switch on which loop protection needs to be configured.

Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **stp interface** { *interface-type interface-number* [**to** *interface-number*] } &<1-10> **loop-protection** command to configure loop protection on the S-switch.

----End

Configuring Loop Protection on an Interface in the Interface View

Context

Do as follows on the S-switch on which loop protection needs to be configured.

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 Ethernet interface view or the GE interface view; run the **interface eth-trunk** *trunk-id* command to enter the Eth-Trunk interface view.

Step 3 Run the **stp loop-protection** command to configure loop protection on the S-switch.

----End

9.5.5 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the status of an interface in the MSTI.	display stp [instance <i>instance-id</i>] [slot <i>slot-number</i> interface { <i>interface-type interface-number</i> [to interface-number] }&<1-10>] [brief]

If the configuration succeeds, you can find that the protection function of the interface is correctly set.

9.6 Maintaining MSTP

This section describes how to maintain MSTP.

9.6.1 Displaying MSTP Running Information

9.6.2 Clearing MSTP Statistics

9.6.3 Debugging MSTP

9.6.1 Displaying MSTP Running Information

After the previous configurations are complete, run the following command in any view to check MSTP running information and verify the configuration. For details on MSTP running information, refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.

Action	Command
Display the status and statistics of the spanning tree.	display stp [instance <i>instance-id</i>] [slot <i>slot-number</i> interface { <i>interface-type interface-number</i> [to interface-number] }&<1-10>] [brief]

9.6.2 Clearing MSTP Statistics



CAUTION

MSTP statistics cannot be restored after you clear them. Therefore, confirm the action before you use the command.

After you confirm that MSTP statistics need to be cleared, run the following command in the user view.

Action	Command
Clear MSTP statistics on the spanning tree.	reset stp [interface { <i>interface-type interface-number</i> [to interface-number] }&<1-10>] statistics

9.6.3 Debugging MSTP



CAUTION

Enabling debugging affects the system performance. Therefore, after debugging, run the **undo debugging all** command to disable debugging immediately.

When an MSTP fault occurs, run the following commands in the user view to debug MSTP, view debugging information, locate and analyze the fault. For how to enable debugging, refer to the chapter "Monitoring and Debugging" in the *Quidway S5300 Series Ethernet Switches Configuration Guide - Device Management*. For descriptions of the **debugging** commands, refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.

Action	Command
Enable debugging of a specified MSTI.	debugging stp instance <i>instance-id</i> event
Enable MSTP debugging.	debugging stp { all global-event global-error msti { <i>instance-id1</i> [to instance-id2] }&<1-10> }
Enable BPDU and event debugging on a specified interface.	debugging stp [interface <i>interface-type interface-number</i>] { event packet { all receive send } }

9.7 Configuration Examples

This section provides MSTP configuration examples.

9.7.1 Example for Configuring MSTP

9.7.1 Example for Configuring MSTP

Networking Requirements

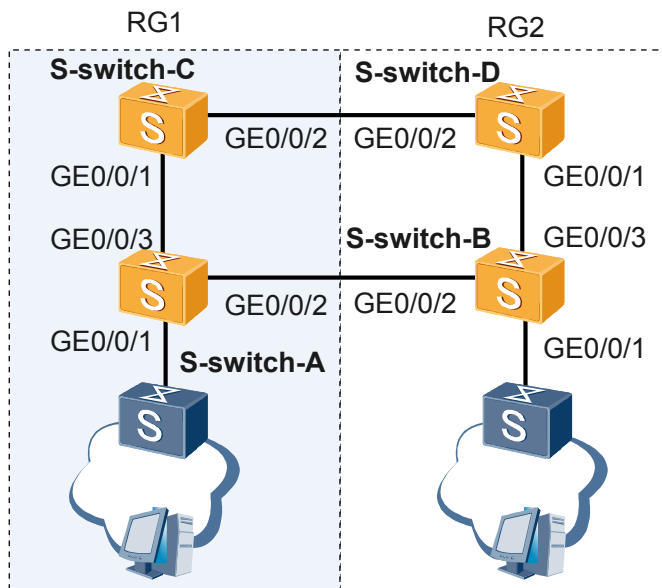
As shown in [Figure 9-1](#), S-switch-A and S-switch-C are configured to work in a region named RG 1, and MSTI 1 is created. S-switch-B and S-switch-D are configured to work in another region named RG 2 and MSTI 1 is created.

S-switch-C is configured to be the common and internal spanning tree (CIST) root. In region RG 1, S-switch-C is the region root of CIST and the region root of MSTI 1. Root protection is applied on GigabitEthernet 0/0/2 and Ethernet 0/0/1 of S-switch-C. In region RG 2, S-switch-D is the region root of CIST and S-switch-B is the region root of MSTI 1.

Both S-switch-A and S-switch-B are downstream attached with a L2 Switch through Ethernet 0/0/1. Set GigabitEthernet 0/0/1 as the edge interface and apply BPDU protection on S-switch-A and S-switch-B.

S-switch-A, S-switch-B, S-switch-C, and S-switch-D all use Huawei private algorithm for calculating path costs.

Figure 9-1 Networking diagram for configuring basic MSTP functions



Configuration Roadmap

The configuration roadmap is as follows:

- Configuring an MST region on S-switch-C, S-switch-D, S-switch-A and S-switch-B
- Setting priorities of S-switch-C, S-switch-D, and S-switch-B in MSTIs
- Configuring VLANs
- Configuring the protection function
- Configuring interfaces on the S-switch-A and S-switch-B to allow BPDU messages
- Enabling MSTP on S-switch-C, S-switch-D, S-switch-A and S-switch-B

Data Preparation

To complete the configuration, you need the following data:

- Names of two MST regions: RG1 and RG2.
- S-switch-A, S-switch-B, S-switch-C and S-switch-D all use Huawei legacy standard to calculate the path cost of their interfaces

Configuration Procedure

1. Configure S-switch-C.

Configure the MST region on S-switch-C.

```
<Quidway> system-view
[Quidway] sysname S-switch-C
[S-switch-C] stp region-configuration
[S-switch-C-mst-region] region-name RG1
[S-switch-C-mst-region] instance 1 vlan 1 to 10
```

Activate the region configuration on S-switch-C.

```
[S-switch-C-mst-region] active region-configuration
[S-switch-C-mst-region] quit
```

Set the priority of S-switch-C in MSTI 0 to 0 to ensure that S-switch-C serves as the CIST root.

```
[S-switch-C] stp instance 0 priority 0
```

Set the priority of S-switch-C in MSTI 1 to 0 to ensure that S-switch-C serves as the region root of MSTI 1.

```
[S-switch-C] stp instance 1 priority 0
```

Configure the algorithm for calculating interface path costs to Huawei private algorithm.

```
[S-switch-C] stp pathcost-standard legacy
```

Create VLAN 1 to VLAN 20.

```
[S-switch-C] vlan batch 1 to 20
```

Add GigabitEthernet 0/0/2 to the VLANs.

```
[S-switch-C] interface ethernet 0/0/2
[S-switch-C-GigabitEthernet0/0/2] port trunk allow-pass vlan 1 to 20
[S-switch-C-GigabitEthernet0/0/2] quit
```

Add GigabitEthernet 0/0/1 to the VLANs.

```
[S-switch-C] interface ethernet 0/0/1
[S-switch-C-GigabitEthernet0/0/1] port trunk allow-pass vlan 1 to 20
[S-switch-C-GigabitEthernet0/0/1] quit
```

Enable root protection on GigabitEthernet 0/0/2.

```
[S-switch-C] interface ethernet 0/0/2
[S-switch-C-GigabitEthernet0/0/2] stp root-protection
[S-switch-C-GigabitEthernet0/0/2] quit
```

Enable root protection on GigabitEthernet 0/0/1.

```
[S-switch-C] interface ethernet 0/0/1
[S-switch-C-GigabitEthernet0/0/1] stp root-protection
[S-switch-C-GigabitEthernet0/0/1] quit
```

Configure GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 to allow BPDUs to pass through.

```
[S-switch-C] interface ethernet 0/0/1
[S-switch-C-GigabitEthernet0/0/1] bpdu enable
[S-switch-C-GigabitEthernet0/0/1] quit
[S-switch-C] interface ethernet 0/0/2
[S-switch-C-GigabitEthernet0/0/2] bpdu enable
[S-switch-C-GigabitEthernet0/0/2] quit
```

Enable MSTP.

```
[S-switch-C] stp enable
```

2. Configure S-switch-D.

Configure the MST region on S-switch-D.

```
<Quidway> system-view
[Quidway] sysname S-switch-D
[S-switch-D] stp region-configuration
[S-switch-D-mst-region] region-name RG2
[S-switch-D-mst-region] instance 1 vlan 1 to 10
```

Activate the region configuration on S-switch-D.

```
[S-switch-D-mst-region] active region-configuration
[S-switch-D-mst-region] quit

# Set the priority of S-switch-D in MSTI 0 to 4096 to ensure that S-switch-D serves as the
region root of MSTI 0 in RG 2.
[S-switch-D] stp instance 0 priority 4096

# Configure the algorithm for calculating interface path costs to Huawei private algorithm.
[S-switch-D] stp pathcost-standard legacy

# Create VLAN 1 to VLAN 20.
[S-switch-D] vlan batch 1 to 20

# Add GigabitEthernet 0/0/2 to the VLANs.
[S-switch-D] interface ethernet 0/0/2
[S-switch-D-GigabitEthernet0/0/2] port trunk allow-pass vlan 1 to 20
[S-switch-D-GigabitEthernet0/0/2] quit

# Add GigabitEthernet 0/0/1 to the VLANs.
[S-switch-D] interface ethernet 0/0/1
[S-switch-D-GigabitEthernet0/0/1] port trunk allow-pass vlan 1 to 20
[S-switch-D-GigabitEthernet0/0/1] quit

# Configure GigabitEthernet 0/0/1 and Ethernet 0/0/2 to allow BPDUs to pass through.
[S-switch-D] interface ethernet 0/0/1
[S-switch-D-GigabitEthernet0/0/1] bpdu enable
[S-switch-D-GigabitEthernet0/0/1] quit
[S-switch-D] interface ethernet 0/0/2
[S-switch-D-GigabitEthernet0/0/2] bpdu enable
[S-switch-D-GigabitEthernet0/0/2] quit

# Enable MSTP.
[S-switch-D] stp enable
```

3. Configure S-switch-A.

```
# Configure the MST region on S-switch-A.
<Quidway> system-view
[Quidway] sysname S-switch-A
[S-switch-A] stp region-configuration
[S-switch-A-mst-region] region-name RG1
[S-switch-A-mst-region] instance 1 vlan 1 to 10

# Activate the region configuration on S-switch-A.
[S-switch-A-mst-region] active region-configuration
[S-switch-A-mst-region] quit

# Configure the algorithm for calculating interface path costs to Huawei private algorithm.
[S-switch-A] stp pathcost-standard legacy

# Enable BPDU protection.
[S-switch-A]] stp bpdu-protection

# Create VLAN 1 to VLAN 20.
[S-switch-A]] vlan batch 1 to 20

# Add Ethernet 0/0/2 to the VLANs.
[S-switch-A] interface gigabitethernet 0/0/2
[S-switch-A-GigabitEthernet0/0/2] port trunk allow-pass vlan 1 to 20
[S-switch-A-GigabitEthernet0/0/2] quit

# Add GigabitEthernet 0/0/2 to the VLANs.
[S-switch-A] interface gigabitethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/2] port trunk allow-pass vlan 1 to 20
[S-switch-A-GigabitEthernet0/0/2] quit

# Add GigabitEthernet 0/0/3 to the VLANs.
[S-switch-A] interface ethernet 0/0/3
```

```
[S-switch-A-GigabitEthernet0/0/3] port trunk allow-pass vlan 1 to 20
[S-switch-A-GigabitEthernet0/0/3] quit
```

Set GigabitEthernet 0/0/1 as the edge interface.

```
[S-switch-A] interface ethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] stp edged-port enable
[S-switch-A-GigabitEthernet0/0/1] quit
```

Configure GigabitEthernet 0/0/1, GigabitEthernet 0/0/2, and Ethernet 0/0/3 to allow BPDUs to pass through.

```
[S-switch-A] interface ethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] bpdu enable
[S-switch-A-GigabitEthernet0/0/1] quit
[S-switch-A] interface ethernet 0/0/2
[S-switch-A-GigabitEthernet0/0/2] bpdu enable
[S-switch-A-Ethernet0/0/22] quit
[S-switch-A] interface ethernet 0/0/3
[[S-switch-A-GigabitEthernet0/0/3] bpdu enable
[[S-switch-A-GigabitEthernet0/0/3] quit
```

Enable MSTP.

```
[S-switch-A] stp enable
```

4. Configure S-switch-B.

Configure the MST region on S-switch-B.

```
<Quidway> system-view
[Quidway] sysname S-switch-B
[S-switch-B] stp region-configuration
[S-switch-B-mst-region] region-name RG2
[S-switch-B-mst-region] instance 1 vlan 1 to 10
```

Activate the region configuration on S-switch-B.

```
[S-switch-B-mst-region] active region-configuration
[S-switch-B-mst-region] quit
```

Set the priority of S-switch-B in MSTI 1 to 0 to ensure that S-switch-B serves as the region root of MSTI 1.

```
[S-switch-B] stp instance 1 priority 0
```

Configure the algorithm for calculating interface path costs to Huawei private algorithm.

Enable BPDU protection.

```
[S-switch-B] stp bpdu-protection
```

Create VLAN 1 to VLAN 20.

```
[S-switch-B] vlan batch 1 to 20
```

Add GigabitEthernet 0/0/2 to the VLANs.

```
[S-switch-B] interface ethernet 0/0/2
[S-switch-B-GigabitEthernet0/0/2] port trunk allow-pass vlan 1 to 20
[S-switch-B-GigabitEthernet0/0/2] quit
```

Add GigabitEthernet 0/0/3 to the VLANs.

```
[S-switch-B] interface ethernet 0/0/3
[S-switch-B-GigabitEthernet0/0/3] port trunk allow-pass vlan 1 to 20
[S-switch-B-GigabitEthernet0/0/3] quit
```

Set GigabitEthernet 0/0/1 as the edge interface.

```
[S-switch-B] interface ethernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] stp edged-port enable
[S-switch-B-GigabitEthernet0/0/1] quit
```

Configure Ethernet 0/0/1, GigabitEthernet 0/0/2, and GigabitEthernet 0/0/3 to allow BPDUs to pass through.

```
[S-switch-B] interface ethernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] bpdu enable
[S-switch-B-GigabitEthernet0/0/1] quit
```

```
[S-switch-B] interface ethernet 0/0/2
[S-switch-B-GigabitEthernet0/0/2] bpdu enable
[S-switch-B-GigabitEthernet0/0/2] quit
[S-switch-B] interface ethernet 0/0/3
[[S-switch-B-GigabitEthernet0/0/3] bpdu enable
[[S-switch-B-GigabitEthernet0/0/3] quit
```

Enable MSTP.

```
[S-switch-B] stp enable
```

5. Verify the configuration.

After the previous configurations are complete, run the following commands to verify the configuration:

Run the **display stp brief** command on S-switch-C to view the interface status and protection type. The displayed information is as follows:

```
<S-switch-C> display stp brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/2	DESI	FORWARDING	ROOT
0	GigabitEthernet0/0/1	DESI	FORWARDING	ROOT
1	GigabitEthernet0/0/2	DESI	FORWARDING	ROOT
1	GigabitEthernet0/0/1	DESI	FORWARDING	ROOT

The priority of S-switch-C is the highest in CIST. Therefore, S-switch-C serves as both the CIST root and the region root of RG 1. GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 on S-switch-C are specified interfaces in CIST.

The priority of S-switch-C is the highest in MSTI 1 in region RG 1. Therefore, S-switch-C serves as the region root of MSTI 1. GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 serve as specified interfaces in MSTI 1.

Run the **display stp interface brief** command on S-switch-A. The displayed information is as follows:

```
<S-switch-A> display stp interface ethernet 0/0/3 brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/3	ROOT	FORWARDING	NONE
1	GigabitEthernet0/0/3	ROOT	FORWARDING	NONE

```
<S-switch-A> display stp interface gigabitethernet 1/0/2 brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/2	DESI	FORWARDING	NONE
1	GigabitEthernet0/0/2	DESI	FORWARDING	NONE

GigabitEthernet 0/0/3 of S-switch-A is the root interface in CIST and MSTI 1.

GigabitEthernet 0/0/2 of S-switch-A is the specified interface of CIST and that of MSTI 1.

Run the **display stp brief** command on S-switch-D. The displayed information is as follows:

```
<S-switch-D> display stp brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/2	ROOT	FORWARDING	NONE
0	GigabitEthernet0/0/2	DESI	FORWARDING	NONE
1	GigabitEthernet0/0/2	MAST	FORWARDING	NONE
1	GigabitEthernet0/0/2	ROOT	FORWARDING	NONE

The priority of S-switch-D in CIST is lower than that of S-switch-C. Therefore, GigabitEthernet 0/0/2 serves as the root interface in CIST. Meanwhile, S-switch-C and S-switch-D belong to different regions. Therefore, Ethernet 0/0/2 serves as the Master interface in MSTI 1.

In MSTI 1, the priority of S-switch-D is lower than that of S-switch-B. Therefore, GigabitEthernet 0/0/1 serves as the root interface. The priority of S-switch-D in CIST is higher than that of S-switch-B. Therefore, Ethernet 0/0/1 serves as the specified interface in CIST.

Run the **display stp interface brief** command on S-switch-B. The displayed information is as follows:

```

<S-switch-B> display stp interface ethernet 0/0/3 brief
MSTID      Port      Role      STP State      Protection
0           GigabitEthernet0/0/3      ROOT      FORWARDING      NONE
1           GigabitEthernet0/0/3      DESI      FORWARDING      NONE
<S-switch-B> display stp interface ethernet 0/0/2 brief
MSTID      Port      Role      STP State      Protection
0           GigabitEthernet0/0/2      ALTE      DISCARDING      NONE
1           GigabitEthernet0/0/2      ALTE      DISCARDING      NONE

```

On S-switch-B, GigabitEthernet 0/0/2 serves as the alternate interface in CIST. Meanwhile, S-switch-B and S-switch-A are in different regions. Therefore, GigabitEthernet 0/0/2 also serves as the alternate interface in MSTI 1. GigabitEthernet 0/0/3 serves as the root interface in CIST. The priority of S-switch-B in MSTI 1 is higher than that of S-switch-D in MSTI 1. Therefore, GigabitEthernet 0/0/3 serves as the specified interface in MSTI 1.

Configuration Files

- Configuration file of S-switch-A

```

#
 sysname S-switch-A
#
 stp bpdu-protection
 stp pathcost-standard legacy
 stp enable
 stp region-configuration
  region-name RG1
  instance 1 vlan 1 to 10
  active region-configuration
#
 interface GigabitEthernet0/0/1
  stp edged-port enable
  bpdu enable
#
 interface GigabitEthernet0/0/2
  port trunk allow-pass vlan 1 to 20
  bpdu enable
#
 interface thernet0/0/3
  port trunk allow-pass vlan 1 to 20
  bpdu enable
#
return

```

- Configuration file of S-switch-B

```

#
 sysname S-switch-B
#
 vlan batch 1 to 20
#
 stp instance 1 priority 0
 stp bpdu-protection
 stp pathcost-standard legacy
 stp enable
 stp region-configuration
  region-name RG2
  instance 1 vlan 1 to 10
  active region-configuration
#
 interface GigabitEthernet0/0/1
  stp edged-port enable
  bpdu enable
#
 interface GigabitEthernet0/0/2
  port trunk allow-pass vlan 1 to 20
  bpdu enable
#
 interface GigabitEthernet0/0/3
  port trunk allow-pass vlan 1 to 20

```

```
    bpdu enable
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
vlan batch 1 to 20
#
stp instance 0 priority 0
stp instance 1 priority 0
stp pathcost-standard legacy
stp enable
stp region-configuration
    region-name RG1
    instance 1 vlan 1 to 10
    active region-configuration
#
interface GigabitEthernet0/0/2
    port trunk allow-pass vlan 1 to 20
    stp root-protection
    bpdu enable
#
interface GigabitEthernet0/0/1
    port trunk allow-pass vlan 1 to 20
    stp root-protection
    bpdu enable
#
return
```

- Configuration file of S-switch-D

```
#
sysname S-switch-D
#
vlan batch 1 to 20
#
stp instance 0 priority 4096
stp pathcost-standard legacy
stp enable
stp region-configuration
    region-name RG2
    instance 1 vlan 1 to 10
    active region-configuration
#
interface GigabitEthernet0/0/2
    port trunk allow-pass vlan 1 to 20
    bpdu enable
#
interface GigabitEthernet0/0/1
    port trunk allow-pass vlan 1 to 20
    bpdu enable
#
return
```


10 RRPP Configuration

About This Chapter

This chapter describes the basic concepts about the Rapid Ring Protection Protocol (RRPP), and methods and examples for configuring RRPP.

[10.1 Introduction](#)

This section describes the principle and concepts of RRPP.

[10.2 Configuring RRPP Functions](#)

This section describes how to configure basic RRPP functions.

[10.3 Configuring RRPP Multi-Instance](#)

This section describes how to configuring RRPP multi-instance.

[10.4 Maintaining RRPP](#)

This section describes how to clear the RRPP statistics and debug RRPP.

[10.5 Configuration Examples](#)

This section provides several configuration examples of RRPP.

10.1 Introduction

This section describes the principle and concepts of RRPP.

[10.1.1 RRPP](#)

[10.1.2 References](#)

10.1.1 RRPP

Concept

RRPP is a link layer protocol specially used for the Ethernet ring. When the Ethernet ring is complete, RRPP can prevent the broadcast storm caused by data loop. When a link on the Ethernet ring is disconnected, RRPP helps to quickly enable the standby link and then recover the communication channels between nodes on the ring network.

The networking of RRPP is relatively flexible. It can be a single ring topology, a tangent ring topology, or an intersectant ring topology.

An RRPP domain consists of the elements such as the RRPP major ring, RRPP sub-ring, control Virtual Local Area Network (VLAN), master node, transit node, common interface, edge interface, primary interface, and secondary interface.

Fundamentals of RRPP

- All the nodes in each domain are configured with the same RRPP domain ID and the same control VLAN.
- Each domain has two control VLANs: the major control VLAN and the sub control VLAN.
- The protocol packets of the major ring are transmitted in the major control VLAN; the protocol packets of the sub-ring are transmitted in the sub control VLAN.
- The RRPP interfaces on the nodes of the major ring can be added to the major control VLAN and the sub control VLAN at the same time; the interfaces on the sub-ring, however, can be added to only the sub control VLAN.
- The protocol packets of the sub-ring are processed as data packets on the major ring, and they are blocked/unblocked at the same time with data packets.

10.1.2 References

For detailed information about the RRPP principle, refer to the chapter "RRPP" in the *Quidway S5300 Series Ethernet Switches Feature Description*.

10.2 Configuring RRPP Functions

This section describes how to configure basic RRPP functions.

[10.2.1 Establishing the Configuration Task](#)

[10.2.2 Creating an RRPP Domain and the Control VLAN](#)

[10.2.3 \(Optional\) Setting the Values of Timers in an RRPP Domain](#)

[10.2.4 Disabling the STP Function on the Interfaces to be Added to an RRPP Ring](#)

[10.2.5 Creating an RRPP Ring](#)

[10.2.6 Enabling an RRPP Ring](#)

[10.2.7 Enabling RRPP](#)

[10.2.8 Disabling Multiple Sub-Ring Protection](#)

[10.2.9 Checking the Configuration](#)

10.2.1 Establishing the Configuration Task

Applicable Environment

RRPP is used for the networking of the single-ring or multiple intersectant rings. When configuring RRPP, you need to configure the role of each node on an RRPP ring.

 **NOTE**

You can configure either RRPP or STP on an interface.

Pre-configuration Tasks

Before configuring RRPP functions, complete the following tasks:

- Constructing the physical ring topology networking
- Configuring the link attributes of interfaces

Data Preparation

To configure RRPP functions, you need the following data:

No.	Data
1	ID of an RRPP domain
2	ID of the control VLAN in the RRPP domain
3	IDs of all RRPP rings in the RRPP domain
4	Values of the Hello timer and Fail timer in the RRPP domain
5	Interface names of the RRPP rings

10.2.2 Creating an RRPP Domain and the Control VLAN

Context

Do as follows on each S-switch in an RRPP domain:

Procedure

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

Step 2 Run the **rrpp domain** *domain-id* command to create an RRPP domain.

When creating an RRPP domain, you need to specify the domain ID. If the domain already exists, you can directly enter the RRPP domain view.

Step 3 Run the **control-vlan** *vlan-id* command to create the control VLAN.

The control VLAN specified by *vlan-id* must not have been created. According to the protocol, the control VLAN specified by *vlan-id+1* is the sub control VLAN that must not have been created.

After configuring the control VLAN, you cannot directly modify it. You can delete the control VLAN only by deleting the domain, and then reconfigure the control VLAN. The sub control VLAN is also deleted when you delete the domain.

 **NOTE**

Configuring VLAN stacking in the control VLAN of an RRPP domain is prohibited; otherwise, the control VLAN cannot transmit data normally from the secondary interface, and loops occur.

Configuring other services in the control VLAN is prohibited.

----End

10.2.3 (Optional) Setting the Values of Timers in an RRPP Domain

Context

Do as follows on the master nodes, edge nodes, and assistant edge nodes in RRPP domains.

 **NOTE**

The timers of the nodes in the same domain must be set with the same value.

Procedure

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

Step 2 Run the **rrpp domain** *domain-id* command to enter the RRPP domain view.

Step 3 Run the **timer hello-timer** *hello-value* **fail-timer** *fail-value* command to set the values of timers in the RRPP domain.

The value of the Fail timer is equal to or greater than three times the value of the Hello timer.

The value of the Fail timer must be greater than the value of the delay timer for link recovery.

The value of the Hello timer of the edge node, also called the Edge-Hello timer, is smaller than or equal to the value of the Hello timer of the master node on the major ring. By default, the value of the Edge-Hello timer is a half of the value of the Hello timer configured on the master node on the major ring.

----End

10.2.4 Disabling the STP Function on the Interfaces to be Added to an RRPP Ring

Context



NOTE

After the data frames are forwarded by the S-switch, the priorities of the RRPP protocol packets are cleared. Therefore, you need to run the **trust 8021p** command on each interface of the RRPP ring to guarantee the priorities of the packets. By default, the priority of the data frame is 7.

For details about the **trust 8021p** command, refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.

Before creating an RRPP ring, you need to run the **stp disable** command to disable the STP function on the interfaces to be added to the RRPP ring.

Do as follows on each S-switch in the RRPP domain:

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 **trust 8021p** command to configure the interface to trust the priorities of the RRPP packets.

Step 4 Run the **stp disable** command to disable the STP function on the interface.

By default, the Multiple Spanning Tree Protocol (MSTP) function is disabled on the S-switch.

----End

10.2.5 Creating an RRPP Ring

Context

Do as follows on each S-switch in an RRPP domain:



NOTE

Configuring the following functions on the interfaces of an RRPP ring is prohibited.

- Interface isolation function
- Function of discarding the tagged packets

Procedure

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

Step 2 Run the **rrpp domain domain-id** command to enter the RRPP domain view.

Step 3 Run the **ring ring-id node-mode { master | transit } primary-port interface-type interface-number secondary-port interface-type interface-number level level-value** command to create the RRPP major ring, specify the current S-switch as the master node or transmit node on the RRPP ring to be created, and specify the primary and secondary interfaces for the node.

In an RRPP domain, there must be only one primary ring. The primary ring has only one master node. You can create the sub-ring only after the primary ring is created. Level 0 refers to the major ring, while level 1 refers to the sub-ring.

 **NOTE**

In an RRPP domain, any two rings must be configured with different IDs.

RRPP can be used on the Ethernet interface, GigabitEthernet (GE) interface, Eth-Trunk interface, and Virtual-Ethernet (VE) interface.

Step 4 Run the **ring ring-id node-mode { edge | assistant-edge } common-port interface-type interface-number edge-port interface-type interface-number** command to create the RRPP sub-ring, specify the current S-switch as the edge node or assistant edge node on the RRPP ring to be created, and specify the common interface and edge interface for the node.

The common interface of the edge node and assistant edge node must reside on the major ring.

----End

10.2.6 Enabling an RRPP Ring

Context

Do as follows on each S-switch in an RRPP domain:

Procedure

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

Step 2 Run the **rrpp domain domain-id** command to enter the RRPP domain view.

Step 3 Run the **ring ring-id enable** command to enable an RRPP ring.

----End

10.2.7 Enabling RRPP

Context

Do as follows on each S-switch in an RRPP domain:

Procedure

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

Step 2 Run the **rrpp enable** command to enable RRPP.

 **NOTE**

An RRPP ring can be activated only when both the RRPP ring and RRPP are enabled.

----End

10.2.8 Disabling Multiple Sub-Ring Protection

Context

In the scenario where only one sub-ring exists, you need to disable multiple sub-ring protection on each S-switch in an RRPP domain.

Procedure

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

Step 2 Run the **rrpp domain domain-id** command to enter the RRPP domain view.

Step 3 Run the **undo rrpp multi-sub-ring protection enable** command to disable multiple sub-ring protection.

By default, multiple sub-ring protection is enabled.

In the scenario where only one sub-ring exists, when a fault occurs on the link of the primary ring, RRPP blocks the edge interface of the edge node, if multiple sub-ring protection is enabled. Traffic is thus interrupted. As a result, multiple sub-ring protection must be disabled when a single sub-ring is applied.

----End

10.2.9 Checking the Configuration

Run the following command to check the previous configuration.

Action	Command
Check the brief information about an RRPP domain.	display rrpp brief
Check the detailed information about the RRPP domain.	display rrpp verbose domain domain-id [ring ring-id]
Check the statistics on packets of the RRPP domain.	display rrpp statistics domain domain-id [ring ring-id]

Run the **display rrpp brief** command. You can view the node mode, RRPP status, control VLAN, and values of timers. For example:

```
<Quidway> display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
Number of RRPP Domains: 2

Domain Index : 1
Control VLAN : major 400 sub 401
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 6 sec(default is 6 sec)
Ring Ring Node Primary/Common Secondary/Edge Is
ID Level Mode Port Port Enabled
-----
1 0 M GigabitEthernet0/0/6 GigabitEthernet0/0/1
Yes

Domain Index : 2
Control VLAN : major 200 sub 201
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 6 sec(default is 6 sec)
```

Ring ID	Ring Level	Node Mode	Primary/Common Port	Secondary/Edge Port	Is Enabled
1	0	M	GigabitEthernet0/0/3	GigabitEthernet0/0/4	
No 2	1	E	GigabitEthernet0/0/3	GigabitEthernet0/0/5	
No					

Run the **display rrpp statistics** command. You can view the statistics on all types of sent and received packets. For example:

```
<Quidway> display rrpp statistics domain 1 ring 1
RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Is Activated   : Yes
Primary port   : GigabitEthernet0/0/6
Packet        LINK      COMMON    COMPLETE  EDGE      MAJOR      Packet
Direct  HEALTH  DOWN    FDB       FDB       HELLO     FAULT      Total
-----
Send    5386      0        0        0        0        0        0
Rcv     0         0        0        0        0        0        0
Secondary port: GigabitEthernet0/0/1
Packet        LINK      COMMON    COMPLETE  EDGE      MAJOR      Packet
Direct  HEALTH  DOWN    FDB       FDB       HELLO     FAULT      Total
-----
Send    0         0        0        0        0        0        0
Rcv     0         0        0        0        0        0        0
```

Run the **display rrpp verbose** command. You can view the detailed information about the control VLAN, timers, node mode, and interface status. For example:

```
<Quidway> display rrpp verbose domain 2 ring 2
Domain Index   : 2
Control VLAN   : major 200    sub 201
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
RRPP Ring      : 2
Ring Level     : 1
Node Mode      : Edge
Ring State     : Unknown
Is Enabled     : Disable     Is Activated : No
Common port    : GigabitEthernet0/0/3      Port status: DOWN
Edge port      : GigabitEthernet0/0/5      Port status: DOWN
```

10.3 Configuring RRPP Multi-Instance

This section describes how to configuring RRPP multi-instance.

10.3.1 Establishing the Configuration Task

10.3.2 Creating Instances

10.2.2 Creating an RRPP Domain and the Control VLAN

10.2.4 Disabling the STP Function on the Interfaces to be Added to an RRPP Ring

10.3.5 Configuring Protected VLAN

10.2.5 Creating an RRPP Ring

10.2.6 Enabling an RRPP Ring

[10.2.7 Enabling RRPP](#)

[10.3.9 \(Optional\) Creating a RRPP Ring Group](#)

[10.3.10 \(Optional\) Configuring the Delay for Link Restoration](#)

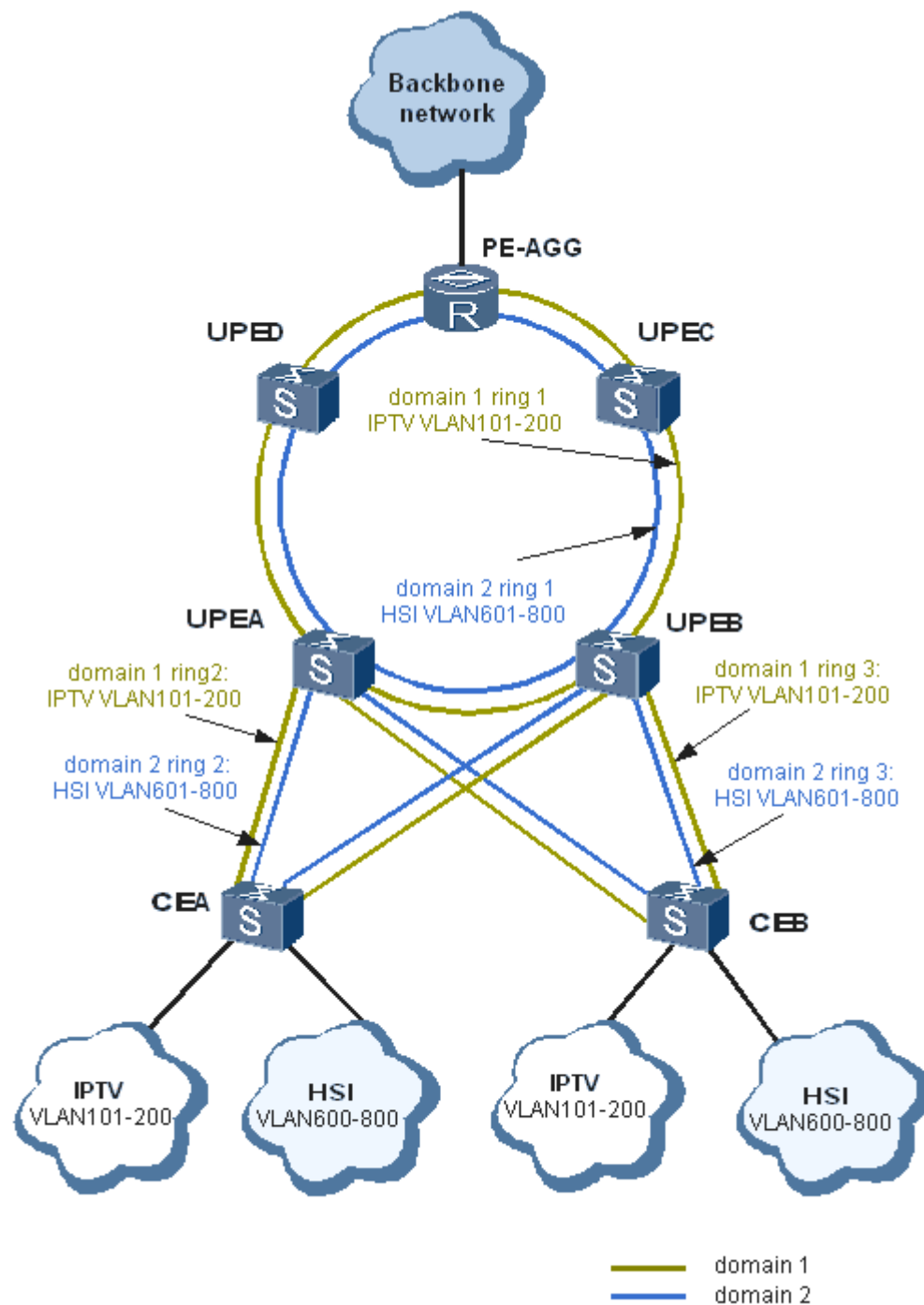
[10.2.3 \(Optional\) Setting the Values of Timers in an RRPP Domain](#)

[10.3.12 Checking the Configuration](#)

10.3.1 Establishing the Configuration Task

Applicable Environment

RRPP multi-instance can be applied to a more complicated networking. As shown in [Figure 10-1](#), two RRPP sub-rings are formed after CEs are dual-homed to UPEs, and an RRPP ring is constructed by four UPEs and one PE-AGG. The PE-AGG delivers the user data to the backbone network.

Figure 10-1 Networking diagram of RRPP multi-instance

CE: indicates Customer Edge

PE-AGG: indicates PE-Aggregation

HSI: indicates High Speed Internet

UPE: indicates Underlayer Provider Edge

IPTV: indicates Internet Protocol Television

In the preceding figure, the IPTV service and HSI service are respectively carried in two domains that share the same RRPP ring. By applying RRPP multi-instance, you can realize balanced

traffic loads for both services, that is, the IPTV service is carried in domain 1, and the HSI service is carried in domain 2.

 **NOTE**

Only either RRPP or STP can be configured on one port.

RRPP has no auto-selection mechanism. Ring detection and protection can be enabled in the corresponding protocol only when each node in the ring is correctly configured. Therefore, make sure that all the configurations are correct.

Pre-configuration Tasks

Before configuring RRPP multi-instance, complete the following tasks:

- Establishing the ring networking
- Configuring link attributes for interfaces

Data Preparation

To configure RRPP multi-instance, you need the following data.

No.	Data
1	IDs of RRPP domains
2	IDs of control VLANs in RRPP domains
3	IDs of protected VLANs in RRPP domains
4	IDs of RRPP rings in RRPP domains
5	Names of the interfaces in RRPP rings
6	(Optional) IDs of the ring groups
7	(Optional) Delay for link restoration
8	(Optional) Values of the Hello timer and Fail timer in RRPP domains

10.3.2 Creating Instances

Context

Do as follows on the S-switch in the RRPP domain:

Procedure

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

Step 2 Run the **stp region-configuration** command to enter the Multiple Spanning Tree (MST) region view.

Step 3 Perform following steps to map the VLAN to the instance.

- Run the **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] } <1-10> command to map the VLAN to the instance.
- Alternatively, run the **vlan-mapping modulo** *modulo* command to map the VLAN to the instance according to the default algorithm.

The **vlan-mapping modulo** command is used to map the VLAN to the instance with the instance number as $(\text{VLAN ID} - 1) \% \text{modulo} + 1$. For example, if the modulo value is 16, VLAN 1 is mapped to instance 1, VLAN 2 is mapped to instance 2, and the rest is deduced by analogy. Note that VLAN 17 is mapped to instance 1 at last.

The control VLANs in the major ring and sub-ring must be in the VLAN list.

In a domain, a maximum of 49 instances can be created. By default, instance 0 already exists in the domain and needs not be created.

In addition, all VLANs in the MST region are mapped to instance 0 by default.

Step 4 Run the **active region-configuration** command to activate the configurations of the MST region.

----End

10.3.3 Creating an RRPP Domain and the Control VLAN

Context

Do as follows on each S-switch in an RRPP domain:

Procedure

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

Step 2 Run the **rrpp domain** *domain-id* command to create an RRPP domain.

When creating an RRPP domain, you need to specify the domain ID. If the domain already exists, you can directly enter the RRPP domain view.

Step 3 Run the **control-vlan** *vlan-id* command to create the control VLAN.

The control VLAN specified by *vlan-id* must not have been created. According to the protocol, the control VLAN specified by *vlan-id+1* is the sub control VLAN that must not have been created.

After configuring the control VLAN, you cannot directly modify it. You can delete the control VLAN only by deleting the domain, and then reconfigure the control VLAN. The sub control VLAN is also deleted when you delete the domain.

NOTE

Configuring VLAN stacking in the control VLAN of an RRPP domain is prohibited; otherwise, the control VLAN cannot transmit data normally from the secondary interface, and loops occur.

Configuring other services in the control VLAN is prohibited.

----End

10.3.4 Disabling the STP Function on the Interfaces to be Added to an RRPP Ring

Context

NOTE

After the data frames are forwarded by the S-switch, the priorities of the RRPP protocol packets are cleared. Therefore, you need to run the **trust 8021p** command on each interface of the RRPP ring to guarantee the priorities of the packets. By default, the priority of the data frame is 7.

For details about the **trust 8021p** command, refer to the *Quidway S5300 Series Ethernet Switches Command Reference*.

Before creating an RRPP ring, you need to run the **stp disable** command to disable the STP function on the interfaces to be added to the RRPP ring.

Do as follows on each S-switch in the RRPP domain:

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 **trust 8021p** command to configure the interface to trust the priorities of the RRPP packets.

Step 4 Run the **stp disable** command to disable the STP function on the interface.

By default, the Multiple Spanning Tree Protocol (MSTP) function is disabled on the S-switch.

----End

10.3.5 Configuring Protected VLAN

Context

Do as follows on the S-switch in the RRPP domain:

Procedure

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

Step 2 Run the **rrpp domain** command to enter the RRPP domain view.

Step 3 Run the **protected-vlan reference-instance { { instance-id1 [to instance-id2] } &<1-10> | all }** command to configure the list of protected VLANs in the RRPP domain.

The VLANs that are allowed to pass the RRPP port must be all configured as the protected VLANs. These protected VLANs can be data VLANs and control VLANs.

----End

10.3.6 Creating an RRPP Ring

Context

Do as follows on each S-switch in an RRPP domain:

**NOTE**

Configuring the following functions on the interfaces of an RRPP ring is prohibited.

- Interface isolation function
- Function of discarding the tagged packets

Procedure

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

Step 2 Run the **rrpp domain domain-id** command to enter the RRPP domain view.

Step 3 Run the **ring ring-id node-mode { master | transit } primary-port interface-type interface-number secondary-port interface-type interface-number level level-value** command to create the RRPP major ring, specify the current S-switch as the master node or transmit node on the RRPP ring to be created, and specify the primary and secondary interfaces for the node.

In an RRPP domain, there must be only one primary ring. The primary ring has only one master node. You can create the sub-ring only after the primary ring is created. Level 0 refers to the major ring, while level 1 refers to the sub-ring.

**NOTE**

In an RRPP domain, any two rings must be configured with different IDs.

RRPP can be used on the Ethernet interface, GigabitEthernet (GE) interface, Eth-Trunk interface, and Virtual-Ethernet (VE) interface.

Step 4 Run the **ring ring-id node-mode { edge | assistant-edge } common-port interface-type interface-number edge-port interface-type interface-number** command to create the RRPP sub-ring, specify the current S-switch as the edge node or assistant edge node on the RRPP ring to be created, and specify the common interface and edge interface for the node.

The common interface of the edge node and assistant edge node must reside on the major ring.

----End

10.3.7 Enabling an RRPP Ring

Context

Do as follows on each S-switch in an RRPP domain:

Procedure

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

Step 2 Run the **rrpp domain domain-id** command to enter the RRPP domain view.

Step 3 Run the **ring ring-id enable** command to enable an RRPP ring.

----End

10.3.8 Enabling RRPP

Context

Do as follows on each S-switch in an RRPP domain:

Procedure

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

Step 2 Run the **rrpp enable** command to enable RRPP.



NOTE

An RRPP ring can be activated only when both the RRPP ring and RRPP are enabled.

----End

10.3.9 (Optional) Creating a RRPP Ring Group

Context

Do as follows on the edge node or assistant edge node:

Procedure

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

Step 2 Run the **rrpp ring-group ring-group-id** command to create an RRPP ring group.

The ring group can be only created on edge nodes or assistant edge nodes.

In an RRPP ring group, the nodes of all sub-rings must have the same type. That is, all of them must be all edge nodes or assistant edge nodes.

Step 3 Run the **domain domain-id ring { ring-id1 [to ring-id2] } <1-10>** command to add a sub-ring to the ring group.

The edge nodes of sub-rings in a ring group are the same device. Similarly, the assistant edge nodes of sub-rings in a ring group are the same device.

A sub-ring can belong to only one ring group, and a ring group can contain maximum 15 sub-rings.

When creating a sub-ring or deleting a sub-ring, pay attention to the following:

- To add activated sub-rings in the ring group, configure relevant commands firstly on the assistant edge node and then on the edge node.
- To delete activated sub-rings from the ring group, configure relevant commands firstly on the edge node and then on the assistant edge node.

----End

10.3.10 (Optional) Configuring the Delay for Link Restoration

Context

Do as follows on the master node:

Procedure

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

Step 2 Run the **rrpp linkup-delay-timer** *linkup-delay-timer-value* command to set the delay for the RRPP link to go Up.

----End

10.3.11 (Optional) Setting the Values of Timers in an RRPP Domain

Context

Do as follows on the master nodes, edge nodes, and assistant edge nodes in RRPP domains.



NOTE

The timers of the nodes in the same domain must be set with the same value.

Procedure

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

Step 2 Run the **rrpp domain** *domain-id* command to enter the RRPP domain view.

Step 3 Run the **timer hello-timer** *hello-value* **fail-timer** *fail-value* command to set the values of timers in the RRPP domain.

The value of the Fail timer is equal to or greater than three times the value of the Hello timer.

The value of the Fail timer must be greater than the value of the delay timer for link recovery.

The value of the Hello timer of the edge node, also called the Edge-Hello timer, is smaller than or equal to the value of the Hello timer of the master node on the major ring. By default, the value of the Edge-Hello timer is a half of the value of the Hello timer configured on the master node on the major ring.

----End

10.3.12 Checking the Configuration

Prerequisite

The configurations of RRPP function are complete.

Procedure

- Run the **display stp region-configuration** command to check the mapping between the VLAN and instance.
- Run the **display rrpp brief** command to check the brief information about the RRPP domain.
- Run the **display rrpp verbose domain** *domain-id* [**ring** *ring-id*] command to check the detailed information about the RRPP domain.
- Run the **display rrpp ring-group** [*ring-group-id*] command to check information about the ring group.

- Run the **display rrpp statistics domain** *domain-id* [**ring** *ring-id*] command to check the packet statistics of the RRPP domain.

----End

Example

Run the **display stp region-configuration** command, and you can check the mapping between the VLAN and instance. Take the following as an example:

```
<Quidway> display stp region-configuration
Oper configuration
Format selector      :0
Region name          :00e0cd568d00
Revision level       :0

Instance  Vlans Mapped
  0        3 to 99, 301 to 4094
  1        1, 100 to 200
  2        2, 201 to 300
```

10.4 Maintaining RRPP

This section describes how to clear the RRPP statistics and debug RRPP.

10.4.1 Clearing RRPP Running Information

10.4.2 Debugging RRPP

10.4.1 Clearing RRPP Running Information



CAUTION

RRPP statistics cannot be restored after you clear it. So, confirm the action before you use the command.

To clear the RRPP statistics, run the following **reset** command in the user view:

Action	Command
Clear the statistics on RRPP.	reset rrpp statistics domain <i>domain-id</i> [ring <i>ring-id</i>]

10.4.2 Debugging RRPP



CAUTION

Debugging affects the performance of the system. After the debugging, run the **undo debugging all** command to disable it at once.

When an RRPP running fault occurs, run the following **debugging** command in the user view to view the debugging information, and locate and analyze the fault.

To enable debugging, refer to the chapter "Debugging and Diagnosis" in the *Quidway S5300 Series Ethernet Switches Configuration Guide - Device Management*.

Action	Command
Enable RRPP debugging.	debugging rrpp [domain <i>domain-id</i> [ring <i>ring-id</i>]] { error event packet all }

10.5 Configuration Examples

This section provides several configuration examples of RRPP.

[10.5.1 Example for Configuring a Single RRPP Ring](#)

[10.5.2 Example for Configuring Tangent RRPP Rings](#)

[10.5.3 Example for Configuring Intersectant Rings in a Single RRPP Domain](#)

[10.5.4 Example for Configuring Intersectant Rings in Multiple RRPP Domains](#)

[10.5.5 Example for Configuring Single RRPP Ring of Multi-Instance](#)

[10.5.6 Example for Configuring the Crossed RRPP Ring of Multi-Instance](#)

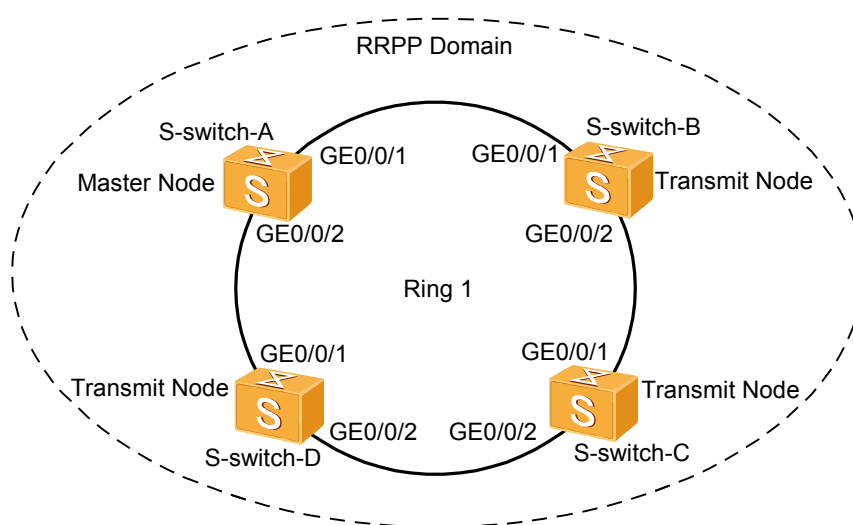
[10.5.7 Example for Configuring the Tangent RRPP Ring of Multi-Instance](#)

10.5.1 Example for Configuring a Single RRPP Ring

Networking Requirements

As shown in [Figure 10-2](#), S-switch-A, S-switch-B, S-switch-C, and S-switch-D support the RRPP function. The four S-switches are configured to be an RRPP ring in domain 1.

Figure 10-2 Networking diagram for configuring a single RRPP ring



Configuration Roadmap

The configuration roadmap is as follows:

- Configure S-switch-A, S-switch-B, S-switch-C, and S-switch-D to form RRPP domain 1.
- Configure the control VLAN in RRPP domain 1 to be VLAN 10.
- Configure S-switch-A, S-switch-B, S-switch-C, and S-switch-D to be major ring 1.
- Configure S-switch-A as the master node on the major ring, Ethernet 0/0/1 as the primary interface, and GigabitEthernet 0/0/2 as the secondary interface.
- Configure S-switch-B, S-switch-C, and S-switch-D as the transit nodes of the major ring, their GigabitEthernet 0/0/1 as primary interfaces, and their GigabitEthernet 0/0/2 as secondary interfaces.

Data Preparation

To complete the configuration, you need the following data:

- Number of an RRPP interface
- ID of the control VLAN

Configuration Procedure

Do as follows on the devices on which an RRPP ring needs to be configured.

1. Create an RRPP domain and its control VLAN.

Do as follows on each S-switch in the RRPP domain:

Configure the domain of S-switch-A, the master node on the major ring, to be domain 1, and the ID of the major control VLAN to be 10.

```
<S-switch-A> system-view
[S-switch-A] rrpp domain 1
[S-switch-A-rrpp-domain-region1] control-vlan 10
[S-switch-A-rrpp-domain-region1] quit
```

Configure the domain of S-switch-B, the transmit node on the major ring, to be domain 1, and the ID of the major control VLAN to be 10.

```
<S-switch-B> system-view
[S-switch-B] rrpp domain 1
[S-switch-B-rrpp-domain-region1] control-vlan 10
[S-switch-B-rrpp-domain-region1] quit
```

Configure the domain of S-switch-C, the transmit node on the major ring, to be domain 1, and the ID of the major control VLAN to be 10.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 1
[S-switch-C-rrpp-domain-region1] control-vlan 10
[S-switch-C-rrpp-domain-region1] quit
```

Configure the domain of S-switch-D, the transmit node on the major ring, to be domain 1, and the ID of the major control VLAN to be 10.

```
<S-switch-D> system-view
[S-switch-D] rrpp domain 1
[S-switch-D-rrpp-domain-region1] control-vlan 10
[S-switch-D-rrpp-domain-region1] quit
```

2. Set the values for timers in the RRPP domain.

Do as follows on the master node and transit nodes in the RRPP domain:

Configure the timer of S-switch-A, the master node of the major ring.

```
<S-switch-A> system-view
[S-switch-A] rrpp domain 1
[S-switch-A-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

Configure the timer of S-switch-B, the transit node on the major ring.

```
<S-switch-B> system-view
[S-switch-B] rrpp domain 1
[S-switch-B-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

Configure the timer of S-switch-C, the transit node on the major ring.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 1
[S-switch-C-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

Configure the timer of S-switch-D, the transit node on the major ring.

```
<S-switch-D> system-view
[S-switch-D] rrpp domain 1
[S-switch-D-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

3. Disable the Spanning Tree Protocol (STP) function of the interfaces to be added to an RRPP ring. Set the interfaces to trust the priorities carried in RRPP packets.

Do as follows on each S-switch in the RRPP domain:

Disable the STP function of the interfaces to be added to an RRPP ring on S-switch-A. Set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-A> system-view
[S-switch-A] interface ethernet0/0/1
[S-switch-A-GigabitEthernet0/0/1] trust 8021p
[S-switch-A-GigabitEthernet0/0/1] stp disable
[S-switch-A-GigabitEthernet0/0/1] quit
[S-switch-A] interface ethernet0/0/2
[S-switch-A-GigabitEthernet0/0/2] trust 8021p
[S-switch-A-GigabitEthernet0/0/2] stp disable
[S-switch-A-GigabitEthernet0/0/2] quit
```

Disable the STP function of the interfaces to be added to an RRPP ring on S-switch-B. Set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-B> system-view
[S-switch-B] interface ethernet0/0/1
[S-switch-B-GigabitEthernet0/0/1] trust 8021p
[S-switch-B-GigabitEthernet0/0/1] stp disable
[S-switch-B-GigabitEthernet0/0/1] quit
[S-switch-B] interface ethernet0/0/2
[S-switch-B-GigabitEthernet0/0/2] trust 8021p
[S-switch-B-GigabitEthernet0/0/2] stp disable
[S-switch-B-GigabitEthernet0/0/2] quit
```

Disable the STP function of the interfaces to be added to an RRPP ring on S-switch-C. Set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-C> system-view
[S-switch-C] interface ethernet0/0/1
[S-switch-C-GigabitEthernet0/0/1] trust 8021p
[S-switch-C-GigabitEthernet0/0/1] stp disable
[S-switch-C-GigabitEthernet0/0/1] quit
[S-switch-C] interface ethernet0/0/2
[S-switch-C-GigabitEthernet0/0/2] trust 8021p
[S-switch-C-GigabitEthernet0/0/2] stp disable
[S-switch-C-GigabitEthernet0/0/2] quit
```

Disable the STP function of the interfaces to be added to an RRPP ring on S-switch-D. Set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-D> system-view
```

```
[S-switch-D] interface ethernet0/0/1
[S-switch-D-GigabitEthernet0/0/1] trust 8021p
[S-switch-D-GigabitEthernet0/0/1] stp disable
[S-switch-D-GigabitEthernet0/0/1] quit
[S-switch-D] interface ethernet0/0/2
[S-switch-D-GigabitEthernet0/0/2] trust 8021p
[S-switch-D-GigabitEthernet0/0/2] stp disable
[S-switch-D-GigabitEthernet0/0/2] quit
```

4. Create an RRPP Ring.

Configure S-switch-A as the master node on the RRPP major ring, and specify the primary and secondary interfaces.

```
<S-switch-A> system-view
[S-switch-A] rrpp domain 1
[S-switch-A-rrpp-domain-region1] ring 1 node-mode master primary-port ethernet
0/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-A-rrpp-domain-region1] ring 1 enable
[S-switch-A-rrpp-domain-region1] quit
```

Configure S-switch-B as the transmit node on the RRPP major ring, and specify the primary and secondary interfaces.

```
<S-switch-B> system-view
[S-switch-B] rrpp domain 1
[S-switch-B-rrpp-domain-region1] ring 1 node-mode transit primary-port
ethernet 0/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-B-rrpp-domain-region1] ring 1 enable
[S-switch-B-rrpp-domain-region1] quit
```

Configure S-switch-C as the transmit node on the RRPP major ring, and specify the primary and secondary interfaces.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 1
[S-switch-C-rrpp-domain-region1] ring 1 node-mode transit primary-port
ethernet 0/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-C-rrpp-domain-region1] ring 1 enable
[S-switch-C-rrpp-domain-region1] quit
```

Configure S-switch-D as the transmit node on the RRPP major ring, and specify the primary and secondary interfaces.

```
<S-switch-D> system-view
[S-switch-D] rrpp domain 1
[S-switch-D-rrpp-domain-region1] ring 1 node-mode transit primary-port
ethernet 0/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-D-rrpp-domain-region1] ring 1 enable
[S-switch-D-rrpp-domain-region1] quit
```

5. Enable RRPP.

After configuring the RRPP ring, you need to enable RRPP on each node on the ring. In this manner, the RRPP ring can be activated. The configuration procedure is as follows:

Enable RRPP on S-switch-A.

```
<S-switch-A> system-view
[S-switch-A] rrpp enable
```

Enable RRPP on S-switch-B.

```
<S-switch-B> system-view
[S-switch-B] rrpp enable
```

Enable RRPP on S-switch-C.

```
<S-switch-C> system-view
[S-switch-C] rrpp enable
```

Enable RRPP on S-switch-D.

```
<S-switch-D> system-view
[S-switch-D] rrpp enable
```

Configuration Files

- Configuration file of S-switch-A

```
#
rrpp domain 1
control-vlan 10
timer hello-timer 2 fail-timer 7
ring 1 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
#
interface ethernet0/0/1
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
interface ethernet0/0/2
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
rrpp enable
#
return
```

- Configuration file of S-switch-B

```
#
rrpp domain 1
control-vlan 10
timer hello-timer 2 fail-timer 7
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
Ethernet
0/0/2 level 0
ring 1 enable
#
interface ethernet0/0/1
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
interface ethernet0/0/2
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
rrpp enable
#
return
```

- Configuration file of S-switch-C

```
#
rrpp domain 1
control-vlan 10
timer hello-timer 2 fail-timer 7
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
#
interface ethernet0/0/1
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
interface ethernet0/0/2
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
rrpp enable
```

```
#
return
```

- Configuration file of S-switch-D

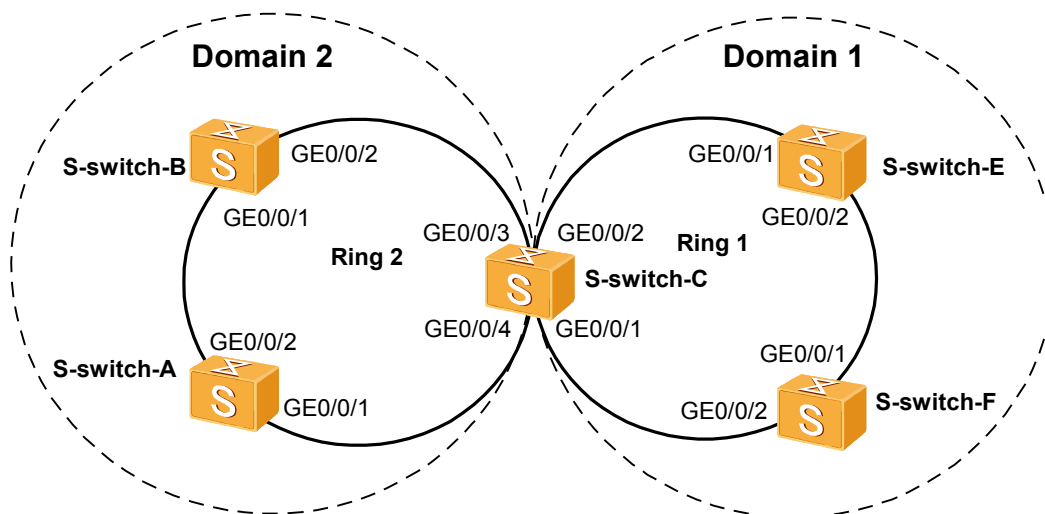

```
#
rrpp domain 1
control-vlan 10
timer hello-timer 2 fail-timer 7
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
#
interface ethernet0/0/1
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
interface ethernet0/0/2
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
rrpp enable
#
return
```

10.5.2 Example for Configuring Tangent RRPP Rings

Networking Requirements

As shown in [Figure 10-3](#), S-switch-A, S-switch-B, S-switch-C, S-switch-E, and S-switch-F support RRPP. Configure S-switch-A, S-switch-B, and S-switch-C as ring 2 of domain 2; configure S-switch-C, S-switch-E, and S-switch-F as ring 1 of domain 1. Ring 1 and ring 2 are tangent at S-switch-C.

Figure 10-3 Networking diagram for configuring RRPP



Configuration Roadmap

The configuration roadmap is as follows:

- Configure S-switch-A, S-switch-B, and S-switch-C as ring 2 in domain 2.
- Configure S-switch-C, S-switch-E, and S-switch-F as ring 1 in domain 1.
- Configure S-switch-A as the master node on ring 2; configure S-switch-B and S-switch-C as transit nodes on ring 2.
- Configure S-switch-E as the master node on ring 1; configure S-switch-C and S-switch-F as transit nodes on ring 1.

Data Preparation

To complete the configuration, you need the following data:

- Number of an RRPP interface
- IDs of the control VLANs of ring 1 and ring 2

Configuration Procedure

Do as follows on the devices that need to be configured to form RRPP rings.

1. Create RRPP domains and their control VLANs.

Do as follows on each S-switch in RRPP domains:

Configure the domain of S-switch-E, the master node on ring 1, to be domain 1, and the ID of the major control VLAN to be 10.

```
<S-switch-E> system-view
[S-switch-E] rrpp domain 1
[S-switch-E-rrpp-domain-region1] control-vlan 10
[S-switch-E-rrpp-domain-region1] quit
```

Configure the domain of S-switch-C, the transmit node on ring 1, to be domain 1, and the ID of the major control VLAN to be 10.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 1
[S-switch-C-rrpp-domain-region1] control-vlan 10
[S-switch-C-rrpp-domain-region1] quit
```

Configure the domain of S-switch-F, the transmit node on ring 1, to be domain 1, and the ID of the major control VLAN to be 10.

```
<S-switch-F> system-view
[S-switch-F] rrpp domain 1
[S-switch-F-rrpp-domain-region1] control-vlan 10
[S-switch-F-rrpp-domain-region1] quit
```

Configure the domain of S-switch-A, the transmit node on ring 2, to be domain 2, and the ID of the major control VLAN to be 20.

```
<S-switch-A> system-view
[S-switch-A] rrpp domain 2
[S-switch-A-rrpp-domain-region2] control-vlan 20
[S-switch-A-rrpp-domain-region2] quit
```

Configure the domain of S-switch-B, the transmit node on ring 2, to be domain 2, and the ID of the major control VLAN to be 20.

```
<S-switch-B> system-view
[S-switch-B] rrpp domain 2
[S-switch-B-rrpp-domain-region2] control-vlan 20
[S-switch-B-rrpp-domain-region2] quit
```

Configure the domain of S-switch-C, the transmit node on ring 2, to be domain 2, and the ID of the major control VLAN to be 20.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 2
[S-switch-C-rrpp-domain-region2] control-vlan 20
[S-switch-C-rrpp-domain-region2] quit
```

2. Set the values of timers in the RRPP domains.

 **NOTE**

You can configure two timers for tangent points because two tangent rings reside in different domains.

Do as follows on the master node and transmit nodes in RRPP domains:

Configure the timer of S-switch-E, the master node on ring 1.

```
<S-switch-E> system-view
[S-switch-E] rrpp domain 1
[S-switch-E-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

Configure the timer of S-switch-C, the transit node on ring 1.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 1
[S-switch-C-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

Configure the timer of S-switch-F, the transit node on ring 1.

```
<S-switch-F> system-view
[S-switch-F] rrpp domain 1
[S-switch-F-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

Configure the timer of S-switch-C, the transit node on ring 2.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 2
[S-switch-C-rrpp-domain-region2] timer hello-timer 3 fail-timer 10
```

Configure the timer of S-switch-A, the master node on ring 2.

```
<S-switch-A> system-view
[S-switch-A] rrpp domain 2
[S-switch-A-rrpp-domain-region2] timer hello-timer 3 fail-timer 10
```

Configure the timer of S-switch-B, the transit node on ring 2.

```
<S-switch-B> system-view
[S-switch-B] rrpp domain 2
[S-switch-B-rrpp-domain-region2] timer hello-timer 3 fail-timer 10
```

3. Disable the STP function of the interfaces to be added to an RRPP ring, and set the interfaces to trust the priorities carried in RRPP packets.

Do as follows on each S-switch in RRPP domains:

Disable the STP function on the interfaces to be added to the RRPP ring on S-switch-A.

```
<S-switch-A> system-view
[S-switch-A] interface ethernet0/0/1
[S-switch-A-GigabitEthernet0/0/1] trust 8021p
[S-switch-A-GigabitEthernet0/0/1] stp disable
[S-switch-A-GigabitEthernet0/0/1] quit
[S-switch-A] interface ethernet0/0/2
[S-switch-A-GigabitEthernet0/0/2] trust 8021p
[S-switch-A-GigabitEthernet0/0/2] stp disable
[S-switch-A-GigabitEthernet0/0/2] quit
```

Disable the STP function of the interfaces to be added to the RRPP ring on S-switch-B, and set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-B> system-view
[S-switch-B] interface ethernet0/0/1
[S-switch-B-GigabitEthernet0/0/1] trust 8021p
[S-switch-B-GigabitEthernet0/0/1] stp disable
[S-switch-B-GigabitEthernet0/0/1] quit
[S-switch-B] interface ethernet0/0/2
```

```
[S-switch-B-GigabitEthernet0/0/2] trust 8021p
[S-switch-B-GigabitEthernet0/0/2] stp disable
[S-switch-B-GigabitEthernet0/0/2] quit
```

Disable the STP function of the interfaces to be added to the RRPP ring on S-switch-C, and set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-C> system-view
[S-switch-C] interface ethernet0/0/3
[S-switch-C-GigabitEthernet0/0/3] trust 8021p
[S-switch-C-GigabitEthernet0/0/3] stp disable
[S-switch-C-GigabitEthernet0/0/3] quit
[S-switch-C] interface ethernet0/0/4
[S-switch-C-GigabitEthernet0/0/4] trust 8021p
[S-switch-C-GigabitEthernet0/0/4] stp disable
[S-switch-C-GigabitEthernet0/0/4] quit
[S-switch-C] interface ethernet0/0/1
[S-switch-C-GigabitEthernet0/0/1] trust 8021p
[S-switch-C-GigabitEthernet0/0/1] stp disable
[S-switch-C-GigabitEthernet0/0/1] quit
[S-switch-C] interface ethernet0/0/2
[S-switch-C-GigabitEthernet0/0/2] trust 8021p
[S-switch-C-GigabitEthernet0/0/2] stp disable
[S-switch-C-GigabitEthernet0/0/2] quit
```

Disable the STP function of the interfaces to be added to the RRPP ring on S-switch-E, and set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-E> system-view
[S-switch-E] interface ethernet0/0/1
[S-switch-E-GigabitEthernet0/0/1] trust 8021p
[S-switch-E-GigabitEthernet0/0/1] stp disable
[S-switch-E-GigabitEthernet0/0/1] quit
[S-switch-E] interface ethernet0/0/2
[S-switch-E-GigabitEthernet0/0/2] trust 8021p
[S-switch-E-GigabitEthernet0/0/2] stp disable
[S-switch-E-GigabitEthernet0/0/2] quit
```

Disable the STP function of the interfaces to be added to the RRPP ring on S-switch-F, and set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-F> system-view
[S-switch-F] interface ethernet0/0/1
[S-switch-F-GigabitEthernet0/0/1] trust 8021p
[S-switch-F-GigabitEthernet0/0/1] stp disable
[S-switch-F-GigabitEthernet0/0/1] quit
[S-switch-F] interface ethernet0/0/2
[S-switch-F-GigabitEthernet0/0/2] trust 8021p
[S-switch-F-GigabitEthernet0/0/2] stp disable
[S-switch-F-GigabitEthernet0/0/2] quit
```

4. Create RRPP rings.

Configure nodes on ring 2. The configuration procedure is as follows:

Configure S-switch-A as the master node on ring 2, and specify the primary and secondary interfaces.

```
<S-switch-A> system-view
[S-switch-A] rrpp domain 2
[S-switch-A-rrpp-domain-region2] ring 2 node-mode master primary-port ethernet
0/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-A-rrpp-domain-region2] ring 2 enable
[S-switch-A-rrpp-domain-region2] quit
```

Configure S-switch-B as the transmit node on RRPP major ring 2, and specify the primary and secondary interfaces.

```
<S-switch-B> system-view
[S-switch-B] rrpp domain 2
[S-switch-B-rrpp-domain-region2] ring 2 node-mode transit primary-port
ethernet 2/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-B-rrpp-domain-region2] ring 2 enable
```

```
[S-switch-B-rrpp-domain-region2] quit
```

Configure S-switch-C as the transmit node on RRPP ring 2, and specify the primary and secondary interfaces.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 2
[S-switch-C-rrpp-domain-region2] ring 2 node-mode transit primary-port
ethernet 0/0/3 secondary-port ethernet 0/0/4 level 0
[S-switch-C-rrpp-domain-region2] ring 2 enable
[S-switch-C-rrpp-domain-region2] quit
```

Configure nodes on ring 1. The configuration procedure is as follows:

Configure S-switch-E as the master node on RRPP major ring 1, and specify the primary and secondary interfaces.

```
<S-switch-E> system-view
[S-switch-E] rrpp domain 1
[S-switch-E-rrpp-domain-region1] ring 1 node-mode master primary-port ethernet
1/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-E-rrpp-domain-region1] ring 1 enable
[S-switch-E-rrpp-domain-region1] quit
```

Configure S-switch-C as the transmit node on RRPP ring 1, and specify the primary and secondary interfaces.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 1
[S-switch-C-rrpp-domain-region1] ring 1 node-mode transit primary-port
ethernet 1/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-C-rrpp-domain-region1] ring 1 enable
[S-switch-C-rrpp-domain-region1] quit
```

Configure S-switch-F as the transmit node on RRPP ring 1, and specify the primary and secondary interfaces.

```
<S-switch-F> system-view
[S-switch-F] rrpp domain 1
[S-switch-F-rrpp-domain-region1] ring 1 node-mode transit primary-port
ethernet 1/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-F-rrpp-domain-region1] ring 1 enable
[S-switch-F-rrpp-domain-region1] quit
```

5. Enable RRPP.

After configuring RRPP rings, you need to enable RRPP on each node on the rings. In this manner, the RRPP rings can be activated. The configuration procedure is as follows:

Enable RRPP on S-switch-A.

```
<S-switch-A> system-view
[S-switch-A] rrpp enable
```

Enable RRPP on S-switch-B.

```
<S-switch-B> system-view
[S-switch-B] rrpp enable
```

Enable RRPP on S-switch-C.

```
<S-switch-C> system-view
[S-switch-C] rrpp enable
```

Enable RRPP on S-switch-E.

```
<S-switch-E> system-view
[S-switch-E] rrpp enable
```

Enable RRPP on S-switch-F.

```
<S-switch-F> system-view
[S-switch-F] rrpp enable
```

Configuration Files

- Configuration file of S-switch-A

```
#
sysname S-switch-A
#
rrpp domain 2
control-vlan 20
timer hello-timer 3 fail-timer 10
ring 2 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 2 enable
#
interface ethernet0/0/1
port trunk allow-pass vlan 20 to 21
trust 8021p
stp disable
#
interface ethernet0/0/2
port trunk allow-pass vlan 20 to 21
trust 8021p
stp disable
#
rrpp enable
#
```

- Configuration file of S-switch-B

```
#
sysname S-switch-B
#
rrpp domain 2
control-vlan 20
timer hello-timer 3 fail-timer 10
ring 2 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 2 enable
#
interface ethernet0/0/1
port trunk allow-pass vlan 20 to 21
trust 8021p
stp disable
#
interface ethernet0/0/2
port trunk allow-pass vlan 20 to 21
trust 8021p
stp disable
#
rrpp enable
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
rrpp domain 1
control-vlan 10
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
timer hello-timer 2 fail-timer 7
#
rrpp domain 2
control-vlan 20
timer hello-timer 3 fail-timer 10
ring 2 node-mode transit primary-port GigabitEthernet 0/0/3 secondary-port
GigabitEthernet 0/0/4 level 0
ring 2 enable
#
```

```
interface ethernet0/0/1
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
interface ethernet0/0/2
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
interface ethernet0/0/1
port trunk allow-pass vlan 20 to 21
trust 8021p
stp disable
#
interface ethernet0/0/2
port trunk allow-pass vlan 20 to 21
trust 8021p
stp disable
#
rrpp enable
#
return
```

- Configuration file of S-switch-E

```
#
sysname S-switch-E
#
rrpp domain 1
control-vlan 10
timer hello-timer 2 fail-timer 7
ring 1 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
#
interface ethernet0/0/1
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
interface ethernet0/0/2
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
rrpp enable
#
return
```

- Configuration file of S-switch-F

```
#
sysname S-switch-F
#
rrpp domain 1
control-vlan 10
timer hello-timer 2 fail-timer 7
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
#
interface ethernet0/0/1
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
interface ethernet0/0/2
port trunk allow-pass vlan 10 to 11
trust 8021p
stp disable
#
```

```

rrpp enable
#
return

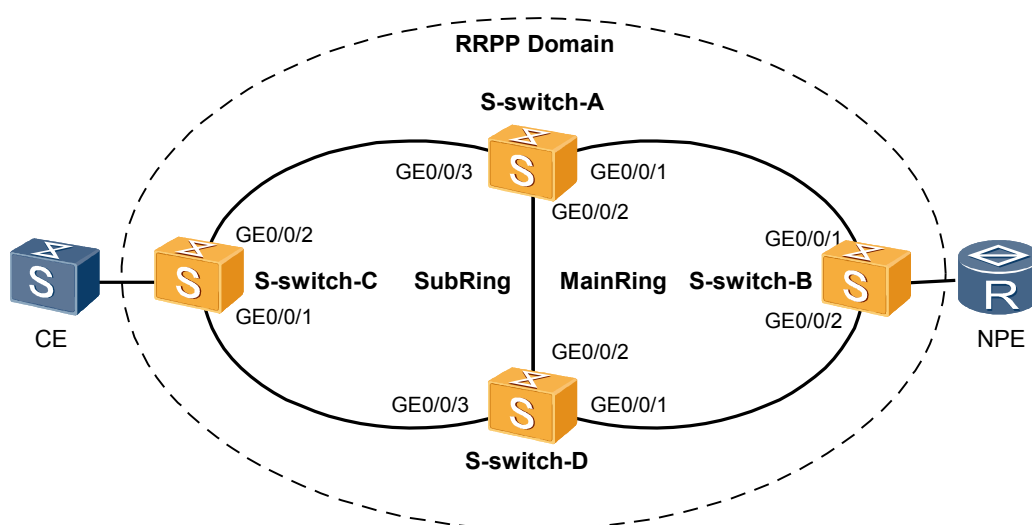
```

10.5.3 Example for Configuring Intersectant Rings in a Single RRPP Domain

Networking Requirements

As shown in [Figure 10-4](#), S-switch-A, S-switch-B, S-switch-C, and S-switch-D support the RRPP function. Configure S-switch-A, S-switch-B, and S-switch-D as major ring 1 in domain 1; configure S-switch-A, S-switch-C, and S-switch-D as sub-ring 2 in domain 1.

Figure 10-4 Networking diagram for configuring RRPP



Configuration Roadmap

The configuration roadmap is as follows:

- Configure S-switch-A, S-switch-B, and S-switch-D as major ring 1 in domain 1.
- Configure S-switch-A, S-switch-C, and S-switch-D as sub-ring 2 in domain 1.
- Configure S-switch-B as the master node on the major ring; configure S-switch-A and S-switch-D as transit nodes on the major ring.
- Configure S-switch-C as the master node on the sub-ring; configure S-switch-A as the edge node on the sub-ring; configure S-switch-D as the assistant edge node on the sub-ring.

Data Preparation

To complete the configuration, you need the following data:

- Number of an RRPP interface
- ID of the control VLAN

Configuration Procedure

Do as follows on the devices that need to be configured to form an RRPP ring.

1. Disable multiple sub-ring protection.

Do as follows on the device as the assistant edge node in an RRPP domain:

Disable multiple sub-ring protection.

```
<S-switch-D> system-view
[S-switch-D] rrpp domain 1
[S-switch-D-rrpp-domain-region1] undo rrpp multi-sub-ring protection enable
[S-switch-D-rrpp-domain-region1] quit
```

2. Create an RRPP domain and its control VLAN.

Do as follows on each S-switch in the RRPP domain:

Configure the domain of S-switch-B, the master node on the major ring, to be domain 1, and its major control VLAN to be VLAN 10.

```
<S-switch-B> system-view
[S-switch-B] rrpp domain 1
[S-switch-B-rrpp-domain-region1] control-vlan 10
[S-switch-B-rrpp-domain-region1] quit
```

Configure the domain of S-switch-A, the transit node on the major ring and the edge node on the sub-ring, to be domain 1, and its major control VLAN to be VLAN 10.

```
<S-switch-A> system-view
[S-switch-A] rrpp domain 1
[S-switch-A-rrpp-domain-region1] control-vlan 10
[S-switch-A-rrpp-domain-region1] quit
```

Configure the domain of S-switch-D, the transit node on the major ring and the assistant edge node on the sub-ring, to be domain 1, and its major control VLAN to be VLAN 10.

```
<S-switch-D> system-view
[S-switch-D] rrpp domain 1
[S-switch-D-rrpp-domain-region1] control-vlan 10
[S-switch-D-rrpp-domain-region1] quit
```

Configure the domain of S-switch-C, the master node on the sub-ring, to be domain 1, and its major control VLAN to be VLAN 10.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 1
[S-switch-C-rrpp-domain-region1] control-vlan 10
[S-switch-C-rrpp-domain-region1] quit
```

3. Set the values of timers in the RRPP domain.

Do as follows on the master nodes, edge node, and assistant edge node in the RRPP domain.

Configure the timer of S-switch-B, the master node on the major ring.

```
<S-switch-B> system-view
[S-switch-B] rrpp domain 1
[S-switch-B-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

Configure the timer of S-switch-C, the master node on the sub-ring.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 1
[S-switch-C-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

Configure the timer of S-switch-A, the edge node on the sub-ring.

```
<S-switch-A> system-view
[S-switch-A] rrpp domain 1
[S-switch-A-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

Configure the timer of S-switch-D, the assistant edge node on the sub-ring.

```
<S-switch-D> system-view
[S-switch-D] rrpp domain 1
```

```
[S-switch-D-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

4. Disable the STP function of the interfaces to be added to an RRPP ring. Set the interfaces to trust the priorities carried in RRPP packets. Do as follows on each S-switch in the RRPP domain:

Disable the STP function of the interfaces to be added to an RRPP ring on S-switch-B. Set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-B> system-view
[S-switch-B] interface ethernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] trust 8021p
[S-switch-B-GigabitEthernet0/0/1] stp disable
[S-switch-B-GigabitEthernet0/0/1] quit
[S-switch-B] interface ethernet 0/0/2
[S-switch-B-GigabitEthernet0/0/2] trust 8021p
[S-switch-B-GigabitEthernet0/0/2] stp disable
[S-switch-B-GigabitEthernet0/0/2] quit
```

Disable the STP function of the interfaces to be added to an RRPP ring on S-switch-A. Set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-A> system-view
[S-switch-A] interface ethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] trust 8021p
[S-switch-A-GigabitEthernet0/0/1] stp disable
[S-switch-A-GigabitEthernet0/0/1] quit
[S-switch-A] interface ethernet 0/0/2
[S-switch-A-GigabitEthernet0/0/2] trust 8021p
[S-switch-A-GigabitEthernet0/0/2] stp disable
[S-switch-A-GigabitEthernet0/0/2] quit
[S-switch-A] interface ethernet 0/0/3
[S-switch-A-GigabitEthernet0/0/3] trust 8021p
[S-switch-A-GigabitEthernet0/0/3] stp disable
[S-switch-A-GigabitEthernet0/0/3] quit
```

Disable the STP function of the interfaces to be added to an RRPP ring on S-switch-D. Set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-D> system-view
[S-switch-D] interface ethernet 0/0/1
[S-switch-D-GigabitEthernet0/0/1] trust 8021p
[S-switch-D-GigabitEthernet0/0/1] stp disable
[S-switch-D-GigabitEthernet0/0/1] quit
[S-switch-D] interface ethernet 0/0/2
[S-switch-D-GigabitEthernet0/0/2] trust 8021p
[S-switch-D-GigabitEthernet0/0/2] stp disable
[S-switch-D-GigabitEthernet0/0/2] quit
[S-switch-D] interface ethernet 0/0/3
[S-switch-D-GigabitEthernet0/0/3] trust 8021p
[S-switch-D-GigabitEthernet0/0/3] stp disable
[S-switch-D-GigabitEthernet0/0/3] quit
```

Disable the STP function of the interfaces to be added to an RRPP ring on S-switch-C. Set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-C> system-view
[S-switch-C] interface ethernet 0/0/1
[S-switch-C-GigabitEthernet0/0/1] trust 8021p
[S-switch-C-GigabitEthernet0/0/1] stp disable
[S-switch-C-GigabitEthernet0/0/1] quit
[S-switch-C] interface ethernet 0/0/2
[S-switch-C-GigabitEthernet0/0/2] trust 8021p
[S-switch-C-GigabitEthernet0/0/2] stp disable
[S-switch-C-GigabitEthernet0/0/2] quit
```

5. Create RRPP rings.

Configure S-switch-B as the master node on the RRPP major ring, and specify the primary and secondary interfaces.

```
<S-switch-B> system-view
[S-switch-B] rrpp domain 1
```

```
[S-switch-B-rrpp-domain-region1] ring 1 node-mode master primary-port ethernet
0/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-B-rrpp-domain-region1] ring 1 enable
[S-switch-B-rrpp-domain-region1] quit
```

Configure S-switch-C as the master node on the RRPP sub-ring, and specify the primary and secondary interfaces.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 1
[S-switch-C-rrpp-domain-region1] ring 2 node-mode master primary-port ethernet
0/0/1 secondary-port ethernet 0/0/2 level 1
[S-switch-C-rrpp-domain-region1] ring 2 enable
[S-switch-C-rrpp-domain-region1] quit
```

Configure S-switch-A as the transmit node on the RRPP major ring, and specify the primary and secondary interfaces.

```
<S-switch-A> system-view
[S-switch-A] rrpp domain 1
[S-switch-A-rrpp-domain-region1] ring 1 node-mode transit primary-port
ethernet 0/0/2 secondary-port ethernet 0/0/1 level 0
[S-switch-A-rrpp-domain-region1] ring 1 enable
[S-switch-A-rrpp-domain-region1] quit
```

Configure S-switch-A as the edge node on the RRPP sub-ring, and specify the common and edge interfaces.

```
[S-switch-A-rrpp-domain-region1] ring 2 node-mode edge common-port ethernet
0/0/2 edge-port ethernet 0/0/3
[S-switch-A-rrpp-domain-region1] ring 2 enable
[S-switch-A-rrpp-domain-region1] quit
```

Configure S-switch-D as the transmit node on the RRPP major ring, and specify the primary and secondary interfaces.

```
<S-switch-D> system-view
[S-switch-D] rrpp domain 1
[S-switch-D-rrpp-domain-region1] ring 1 node-mode transit primary-port
ethernet 0/0/2 secondary-port ethernet 0/0/1 level 0
[S-switch-D-rrpp-domain-region1] ring 1 enable
[S-switch-D-rrpp-domain-region1] quit
```

Configure S-switch-D as the assistant edge node on the RRPP sub-ring, and specify the common and edge interfaces.

```
[S-switch-D] rrpp domain 1
[S-switch-D-rrpp-domain-region1] ring 2 node-mode assistant-edge common-port
ethernet 0/0/2 edge-port ethernet 0/0/3
[S-switch-D-rrpp-domain-region1] ring 2 enable
[S-switch-D-rrpp-domain-region1] quit
```

6. Enable RRPP.

After configuring RRPP rings, you need to enable RRPP on each node on the rings. In this manner, the RRPP rings can be activated. The configuration procedure is as follows:

Enable RRPP on S-switch-B.

```
<S-switch-B> system-view [S-switch-B] rrpp enable
```

Enable RRPP on S-switch-C.

```
<S-switch-C> system-view [S-switch-C] rrpp enable
```

Enable RRPP on S-switch-A.

```
<S-switch-A> system-view [S-switch-A] rrpp enable
```

Enable RRPP on S-switch-D.

```
<S-switch-D> system-view [S-switch-D] rrpp enable
```

7. Verify the configuration.

After the previous configurations are complete, run the following commands to verify the configuration:

- Run the **display rrpp brief** command on S-switch-B. The configuration results are as follows:

```
<S-switch-B> display rrpp brief Abbreviations for Switch Node Mode : M -
Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable Number of RRPP Domains: 1

Domain Index : 1 Control VLAN : major 10 sub 11 Hello Timer : 2 sec
(default is 1 sec) Fail Timer : 7 sec(default is 6 sec) Ring Ring
Node Primary/Common Secondary/Edge Is ID Level
Mode Port Port Enabled
-----
1 0 M GigabitEthernet0/0/1
GigabitEthernet0/0/2 Yes
```

The output information shows that RRPP is enabled on S-switch-B, with major control VLAN 10 and sub control VLAN 11. S-switch-B is the master node on the major ring, with the primary interface Ethernet 0/0/1 and the secondary interface GigabitEthernet 0/0/2.

- Run the **display rrpp verbose domain 1** command on S-switch-B. The configuration results are as follows:

```
<S-switch-B> display rrpp verbose domain 1 Domain Index : 1 Control VLAN :
major 10 sub 11 Hello Timer : 2 sec(default is 1 sec) Fail Timer : 7
sec(default is 6 sec) RRPP Ring : 1 Ring Level : 0 Node Mode :
Master Ring State : Compeltd Is Enabled : Enable Is Activd : Yes
Primary port : GigabitEthernet0/0/1 Port status: UP Secondary port:
GigabitEthernet0/0/2 Port status: BLOCKED
```

You can view that the ring is in the Complete state and the secondary interface of the master node is blocked.

- Run the **display rrpp brief** command on S-switch-C. The configuration results are as follows:

```
<S-switch-C> display rrpp brief Abbreviations for Switch Node Mode : M -
Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable Number of RRPP Domains: 1

Domain Index : 1 Control VLAN : major 10 sub 11 Hello Timer : 2 sec
(default is 1 sec) Fail Timer : 7 sec(default is 6 sec) Ring Ring
Node Primary/Common Secondary/Edge Is ID Level
Mode Port Port Enabled
-----
2 1 M GigabitEthernet0/0/1
GigabitEthernet0/0/2 Yes
```

The output information shows that RRPP is enabled on S-switch-C, with major control VLAN 10 and sub control VLAN 11. S-switch-C is the master node on the sub-ring, with the primary interface Ethernet 0/0/1 and the secondary interface GigabitEthernet 0/0/2.

- Run the **display rrpp verbose domain 1** command on S-switch-C. The configuration results are as follows:

```
<S-switch-C> display rrpp verbose domain 1 Domain Index : 1 Control VLAN :
major 10 sub 11 Hello Timer : 2 sec(default is 1 sec) Fail Timer : 7
sec(default is 6 sec) RRPP Ring : 2 Ring Level : 1 Node Mode :
Master Ring State : Compeltd Is Enabled : Enable Is Activd : Yes
Primary port : GigabitEthernet0/0/1 Port status: UP Secondary port:
GigabitEthernet0/0/2 Port status: BLOCKED
```

You can view that the sub-ring is in the Complete state and the secondary interface of the master node on the sub-ring is blocked.

- Run the **display rrpp brief** command on S-switch-A. The configuration results are as follows:

```
<S-switch-A> display rrpp brief Abbreviations for Switch Node Mode : M -
Master , T - Transit , E - Edge , A - Assistant-Edge
```

```
RRPP Protocol Status: Enable Number of RRPP Domains: 1
```

```
Domain Index : 1 Control VLAN : major 10 sub 11 Hello Timer : 2 sec
(default is 1 sec) Fail Timer : 7 sec(default is 6 sec) Ring Ring
Node Primary/Common Secondary/Edge Is ID Level
Mode Port Port Enabled
-----
1 0 T GigabitEthernet0/0/2 GigabitEthernet0/0/1
Yes 2 1 E GigabitEthernet0/0/2
GigabitEthernet0/0/3 Yes
```

The output information shows that RRPP is enabled on S-switch-A, with major control VLAN 10 and sub control VLAN 11. S-switch-A functions as the transit node on major ring 1, with the primary interface Ethernet 0/0/2 and the secondary interface GigabitEthernet 0/0/1.

In addition, S-switch-A is the edge node on sub-ring 2, with the common interface Ethernet 0/0/2 and the edge interface GigabitEthernet 0/0/3.

- Run the **display rrpp verbose domain 1** command on S-switch-A. The configuration results are as follows:

```
<S-switch-A> display rrpp verbose domain 1 Domain Index : 1 Control VLAN :
major 10 sub 11 Hello Timer : 2 sec(default is 1 sec) Fail Timer : 7
sec(default is 6 sec) RRPP Ring : 1 Ring Level : 0 Node Mode :
Transit Ring State : Linkup Is Enabled : Enable Is Activated : Yes
Primary port : GigabitEthernet0/0/2 Port status: UP Secondary port:
GigabitEthernet0/0/1 Port status: UP
```

```
RRPP Ring : 2 Ring Level : 1 Node Mode : Edge Ring State :
Linkup Is Enabled : Enable Is Activated : Yes Common port :
GigabitEthernet0/0/2 Port status: UP Edge port :
GigabitEthernet0/0/3 Port status: UP
```

- Run the **display rrpp brief** command on S-switch-D. The configuration results are as follows:

```
<S-switch-D> display rrpp brief Abbreviations for Switch Node Mode : M -
Master , T - Transit , E - Edge , A - Assistant-Edge
```

```
RRPP Protocol Status: Enable Number of RRPP Domains: 1
```

```
Domain Index : 1 Control VLAN : major 10 sub 11 Hello Timer : 2 sec
(default is 1 sec) Fail Timer : 7 sec(default is 6 sec) Ring Ring
Node Primary/Common Secondary/Edge Is ID Level
Mode Port Port Enabled
-----
1 0 T GigabitEthernet0/0/2 GigabitEthernet0/0/1
Yes 2 1 A GigabitEthernet0/0/2
GigabitEthernet0/0/3 Yes
```

The output information shows that RRPP is enabled on S-switch-D, with major control VLAN 10 and sub control VLAN 11. S-switch-D functions as the transit node on major ring 1, with the primary interface Ethernet 0/0/2 and the secondary interface GigabitEthernet 0/0/1. In addition, S-switch-D functions as the assistant edge node on sub-ring 2, with the common interface GigabitEthernet 0/0/2 and the edge interface GigabitEthernet 0/0/3.

- Run the **display rrpp verbose domain 1** command on S-switch-D. The configuration results are as follows:

```
<S-switch-D> display rrpp verbose domain 1 Domain Index : 1 Control VLAN :
major 10 sub 11 Hello Timer : 2 sec(default is 1 sec) Fail Timer : 7
sec(default is 6 sec) RRPP Ring : 1 Ring Level : 0 Node Mode :
Transit Ring State : Linkup Is Enabled : Enable Is Activated : Yes
Primary port : GigabitEthernet0/0/2 Port status: UP Secondary port:
GigabitEthernet0/0/1 Port status: UP
```

```

RRPP Ring      : 2 Ring Level      : 1 Node Mode      : Assistant-Edge Ring
State          : Linkup Is Enabled  : Enable        Is Activated : Yes Common port   :
GigabitEthernet0/0/2      Port status: UP Edge port      :
GigabitEthernet0/0/3      Port status: UP

```

Configuration Files

- Configuration file of S-switch-A

```

# sysname S-switch-A # rrpp domain 1 control-vlan 10 timer hello-timer 2 fail-
timer 7 ring 1 node-mode transit primary-port ethernet 0/0/2 secondary-port
ethernet 0/0/1 level 0 ring 1 enable ring 2 node-mode edge common-port ethernet
0/0/2 edge-port ethernet 0/0/3 ring 2 enable # interface ethernet0/0/1 port
trunk allow-pass vlan 10 to 11 trust 8021p stp disable # interface
ethernet0/0/2 port trunk allow-pass vlan 10 to 11 trust 8021p stp disable #
interface ethernet0/0/3 port trunk allow-pass vlan 11 trust 8021p stp disable
# rrpp enable # return

```

- Configuration file of S-switch-B

```

sysname S-switch-B # rrpp enable # rrpp domain 1 control-vlan 10 ring 1 node-
mode master primary-port GigabitEthernet0/0/1 secondary-port
GigabitEthernet0/0/2 level 0 ring 1 enable timer hello-timer 2 fail-timer 7 #
interface GigabitEthernet0/0/1 port trunk allow-pass vlan 10 to 11 trust 8021p
stp disable # interface GigabitEthernet0/0/2 port trunk allow-pass vlan 10 to
11 trust 8021p stp disable # return

```

- Configuration file of S-switch-C

```

# sysname S-switch-C # rrpp enable # rrpp domain 1 control-vlan 10 ring 2 node-
mode master primary-port GigabitEthernet0/0/1 secondary-port
GigabitEthernet0/0/2 level 1 ring 2 enable timer hello-timer 2 fail-timer 7 #
interface GigabitEthernet0/0/1 port trunk allow-pass vlan 11 trust 8021p stp
disable # interface GigabitEthernet0/0/2 port trunk allow-pass vlan 11 trust
8021p stp disable # return

```

- Configuration file of S-switch-D

```

# sysname S-switch-D # rrpp enable # rrpp domain 1 undo rrpp multi-sub-ring
protection enable control-vlan 10 ring 1 node-mode transit primary-port
GigabitEthernet0/0/2 secondary-port GigabitEthernet0/0/1 level 0 ring 1 enable
ring 2 node-mode assistant-edge common-port GigabitEthernet0/0/2 edge-port
GigabitEthernet0/0/3 ring 2 enable timer hello-timer 2 fail-timer 7 # interface
GigabitEthernet0/0/1 port trunk allow-pass vlan 10 to 11 trust 8021p stp
disable # interface GigabitEthernet0/0/2 port trunk allow-pass vlan 10 to 11
trust 8021p stp disable # interface GigabitEthernet0/0/3 port trunk allow-pass
vlan 11 trust 8021p stp disable #
return

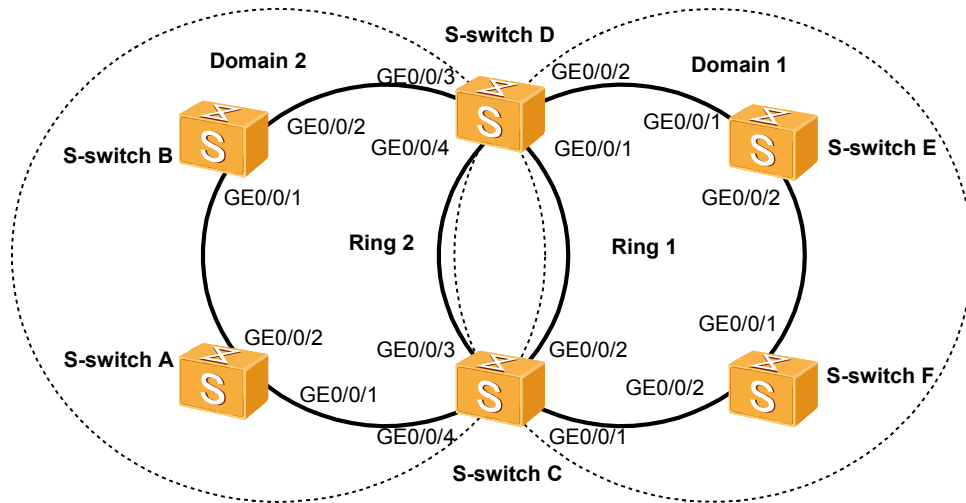
```

10.5.4 Example for Configuring Intersectant Rings in Multiple RRPP Domains

Networking Requirements

As shown in [Figure 10-5](#), S-switch-A, S-switch-B, S-switch-C, S-switch-D, S-switch-E, and S-switch-F support RRPP. Configure S-switch-A, S-switch-B, S-switch-C, and S-switch-D as ring 2 of domain 2; configure S-switch-C, S-switch-D, S-switch-E, and S-switch-F as ring 1 of domain 1. Ring 1 intersects ring 2 at S-switch-C and S-switch-D.

Figure 10-5 Networking diagram for configuring intersectant rings in multiple RRPP domains



Configuration Roadmap

The configuration roadmap is as follows:

- Configure S-switch-A, S-switch-B, S-switch-C, and S-switch-D as ring 2 in domain 2.
- Configure S-switch-C, S-switch-D, S-switch-E, and S-switch-F as ring 1 in domain 1.
- Configure S-switch-A as the master node on ring 2; configure S-switch-B, S-switch-C, and S-switch-D as transit nodes on ring 2.
- Configure S-switch-E as the master node on ring 1; configure S-switch-C, S-switch-D, and S-switch-E as transit nodes on ring 1.

Data Preparation

To complete the configuration, you need the following data:

- Number of an RRPP interface
- IDs of control VLANs of ring 1 and ring 2

Configuration Procedure

Do as follows on the devices on which an RRPP ring needs to be configured.

1. Create an RRPP domain and its control VLAN.

Do as follows on each S-switch in the RRPP domain:

Configure the domain of S-switch-E, the master node on ring 1, to be domain 1, and the ID of the major control VLAN to be 10.

```
<S-switch-E> system-view
[S-switch-E] rrpp domain 1
[S-switch-E-rrpp-domain-region1] control-vlan 10
[S-switch-E-rrpp-domain-region1] quit
```

Configure the domain of S-switch-C, the transmit node on ring 1, to be domain 1, and the ID of the major control VLAN to be 10.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 1
[S-switch-C-rrpp-domain-region1] control-vlan 10
[S-switch-C-rrpp-domain-region1] quit
```

Configure the domain of S-switch-D, the transmit node on ring 1, to be domain 1, and the ID of the major control VLAN to be 10.

```
<S-switch-D> system-view
[S-switch-D] rrpp domain 1
[S-switch-D-rrpp-domain-region1] control-vlan 10
[S-switch-D-rrpp-domain-region1] quit
```

Configure the domain of S-switch-F, the transmit node on ring 1, to be domain 1, and the ID of the major control VLAN to be 10.

```
<S-switch-F> system-view
[S-switch-F] rrpp domain 1
[S-switch-F-rrpp-domain-region1] control-vlan 10
[S-switch-F-rrpp-domain-region1] quit
```

Configure the domain of S-switch-A, the master node on ring 2, to be domain 2, and the ID of the major control VLAN to be 20.

```
<S-switch-A> system-view
[S-switch-A] rrpp domain 2
[S-switch-A-rrpp-domain-region1] control-vlan 20
[S-switch-A-rrpp-domain-region1] quit
```

Configure the domain of S-switch-B, the transmit node on ring 2, to be domain 2, and the ID of the major control VLAN to be 20.

```
<S-switch-B> system-view
[S-switch-B] rrpp domain 2
[S-switch-B-rrpp-domain-region1] control-vlan 20
[S-switch-B-rrpp-domain-region1] quit
```

Configure the domain of S-switch-C, the transmit node on ring 2, to be domain 2, and the ID of the major control VLAN to be 20.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 2
[S-switch-C-rrpp-domain-region1] control-vlan 20
[S-switch-C-rrpp-domain-region1] quit
```

Configure the domain of S-switch-D, the transmit node on ring 2, to be domain 2, and the ID of the major control VLAN to be 20.

```
<S-switch-D> system-view
[S-switch-D] rrpp domain 2
[S-switch-D-rrpp-domain-region1] control-vlan 20
[S-switch-D-rrpp-domain-region1] quit
```

2. Set the values of timers in RRPP domains.

NOTE

You can configure two timers for intersectant points because two intersectant rings reside in different domains.

Do as follows on the master nodes, edge nodes, and assistant edge nodes in RRPP domains.

Configure the timer of S-switch-E, the master node on ring 1.

```
<S-switch-E> system-view
[S-switch-E] rrpp domain 1
[S-switch-E-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

Configure the timer of S-switch-C, the transit node on ring 1.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 1
[S-switch-C-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

Configure the timer of S-switch-D, the transit node on ring 1.

```
<S-switch-D> system-view
```

- ```
[S-switch-D] rrpp domain 1
[S-switch-D-rrpp-domain-region1] timer hello-timer 2 fail-timer 7

Configure the timer of S-switch-F, the transit node on ring 1.

<S-switch-F> system-view
[S-switch-F] rrpp domain 1
[S-switch-F-rrpp-domain-region1] timer hello-timer 2 fail-timer 7

Configure the timer of S-switch-A, the master node on ring 2.

<S-switch-A> system-view
[S-switch-A] rrpp domain 2
[S-switch-A-rrpp-domain-region1] timer hello-timer 3 fail-timer 10

Configure the timer of S-switch-B, the transit node on ring 2.

<S-switch-B> system-view
[S-switch-B] rrpp domain 2
[S-switch-B-rrpp-domain-region1] timer hello-timer 3 fail-timer 10

Configure the timer of S-switch-C, the transit node on ring 2.

<S-switch-C> system-view
[S-switch-C] rrpp domain 2
[S-switch-C-rrpp-domain-region1] timer hello-timer 3 fail-timer 10

Configure the timer of S-switch-D, the transit node on ring 2.

<S-switch-D> system-view
[S-switch-D] rrpp domain 2
[S-switch-D-rrpp-domain-region1] timer hello-timer 3 fail-timer 10
```
3. # Disable the STP function of the interfaces to be added to an RRPP ring, and set the interfaces to trust the priorities carried in RRPP packets.
- Do as follows on each S-switch in RRPP domains:
- # Disable the STP function on the interfaces to be added to an RRPP ring on S-switch-A.
- ```
<S-switch-A> system-view
[S-switch-A] interface ethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] trust 8021p
[S-switch-A-GigabitEthernet0/0/1] stp disable
[S-switch-A-GigabitEthernet0/0/1] quit
[S-switch-A] interface ethernet 0/0/2
[S-switch-A-GigabitEthernet0/0/2] trust 8021p
[S-switch-A-GigabitEthernet0/0/2] stp disable
[S-switch-A-GigabitEthernet0/0/2] quit
```
- # Disable the STP function of the interfaces to be added to an RRPP ring on S-switch-B, and set the interfaces to trust the priorities carried in RRPP packets.
- ```
<S-switch-B> system-view
[S-switch-B] interface ethernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] trust 8021p
[S-switch-B-GigabitEthernet0/0/1] stp disable
[S-switch-B-GigabitEthernet0/0/1] quit
[S-switch-B] interface ethernet 0/0/2
[S-switch-B-GigabitEthernet0/0/2] trust 8021p
[S-switch-B-GigabitEthernet0/0/2] stp disable
[S-switch-B-GigabitEthernet0/0/2] quit
```
- # Disable the STP function of the interfaces to be added to an RRPP ring on S-switch-C, and set the interfaces to trust the priorities carried in RRPP packets.
- ```
<S-switch-C> system-view
[S-switch-C] interface ethernet 0/0/3
[S-switch-C-GigabitEthernet0/0/3] trust 8021p
[S-switch-C-GigabitEthernet0/0/3] stp disable
[S-switch-C-GigabitEthernet0/0/3] quit
[S-switch-C] interface ethernet 0/0/4
[S-switch-C-GigabitEthernet0/0/4] trust 8021p
[S-switch-C-GigabitEthernet0/0/4] stp disable
[S-switch-C-GigabitEthernet0/0/4] quit
[S-switch-C] interface ethernet 0/0/1
```

```
[S-switch-C-GigabitEthernet0/0/1] trust 8021p
[S-switch-C-GigabitEthernet0/0/1] stp disable
[S-switch-C-GigabitEthernet0/0/1] quit
[S-switch-C] interface ethernet 0/0/2
[S-switch-C-GigabitEthernet0/0/2] trust 8021p
[S-switch-C-GigabitEthernet0/0/2] stp disable
[S-switch-C-GigabitEthernet0/0/2] quit
```

Disable the STP function of the interfaces to be added to an RRPP ring on S-switch-D, and set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-D> system-view
[S-switch-D] interface ethernet 0/0/3
[S-switch-D-GigabitEthernet0/0/3] trust 8021p
[S-switch-D-GigabitEthernet0/0/3] stp disable
[S-switch-D-GigabitEthernet0/0/3] quit
[S-switch-D] interface ethernet 0/0/4
[S-switch-D-GigabitEthernet0/0/4] trust 8021p
[S-switch-D-GigabitEthernet0/0/4] stp disable
[S-switch-D-GigabitEthernet0/0/4] quit
[S-switch-D] interface ethernet 0/0/1
[S-switch-D-GigabitEthernet0/0/1] trust 8021p
[S-switch-D-GigabitEthernet0/0/1] stp disable
[S-switch-D-GigabitEthernet0/0/1] quit
[S-switch-D] interface ethernet 0/0/2
[S-switch-D-GigabitEthernet0/0/2] trust 8021p
[S-switch-D-GigabitEthernet0/0/2] stp disable
[S-switch-D-GigabitEthernet0/0/2] quit
```

Disable the STP function of the interfaces to be added to an RRPP ring on S-switch-E, and set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-E> system-view
[S-switch-E] interface ethernet 0/0/1
[S-switch-E-GigabitEthernet0/0/1] trust 8021p
[S-switch-E-GigabitEthernet0/0/1] stp disable
[S-switch-E-GigabitEthernet0/0/1] quit
[S-switch-E] interface ethernet 0/0/2
[S-switch-E-GigabitEthernet0/0/2] trust 8021p
[S-switch-E-GigabitEthernet0/0/2] stp disable
[S-switch-E-GigabitEthernet0/0/2] quit
```

Disable the STP function of the interfaces to be added to an RRPP ring on S-switch-F, and set the interfaces to trust the priorities carried in RRPP packets.

```
<S-switch-F> system-view
[S-switch-F] interface ethernet 0/0/1 [S-switch-F-GigabitEthernet0/0/1] trust
8021p [S-switch-F-GigabitEthernet0/0/1] stp disable [S-switch-F-
GigabitEthernet0/0/1] quit [S-switch-F] interface ethernet 0/0/2 [S-switch-F-
GigabitEthernet0/0/2] trust 8021p [S-switch-F-GigabitEthernet0/0/2] stp
disable [S-switch-F-GigabitEthernet0/0/2] quit
```

4. Create RRPP rings.

Configure nodes on ring 2. The configuration procedure is as follows:

Configure S-switch-A as the master node on ring 2, and specify the primary and secondary interfaces.

```
<S-switch-A> system-view
[S-switch-A] rrpp domain 1
[S-switch-A-rrpp-domain-region2] ring 2 node-mode master primary-port ethernet
0/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-A-rrpp-domain-region2] ring 2 enable
[S-switch-A-rrpp-domain-region2] quit
```

Configure S-switch-B as the transmit node on ring 2, and specify the primary and secondary interfaces.

```
<S-switch-B> system-view
[S-switch-B] rrpp domain 2
[S-switch-B-rrpp-domain-region2] ring 2 node-mode master primary-port ethernet
0/0/1 secondary-port ethernet 0/0/2 level 0
```

```
[S-switch-B-rrpp-domain-region2] ring 2 enable
[S-switch-B-rrpp-domain-region2] quit
```

Configure S-switch-C as the transmit node on ring 2, and specify the primary and secondary interfaces.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 2
[S-switch-C-rrpp-domain-region2] ring 2 node-mode master primary-port ethernet
0/0/3 secondary-port ethernet 0/0/4 level 0
[S-switch-C-rrpp-domain-region2] ring 2 enable
[S-switch-C-rrpp-domain-region2] quit
```

Configure S-switch-D as the transmit node on ring 2, and specify the primary and secondary interfaces.

```
<S-switch-D> system-view
[S-switch-D] rrpp domain 2
[S-switch-D-rrpp-domain-region2] ring 2 node-mode master primary-port ethernet
0/0/3 secondary-port ethernet 0/0/4 level 0
[S-switch-D-rrpp-domain-region2] ring 2 enable
[S-switch-D-rrpp-domain-region2] quit
```

Configure nodes on ring 1. The configuration procedure is as follows:

Configure S-switch-E as the master node on ring 1, and specify the primary and secondary interfaces.

```
<S-switch-E> system-view
[S-switch-E] rrpp domain 1
[S-switch-E-rrpp-domain-region1] ring 1 node-mode master primary-port ethernet
0/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-E-rrpp-domain-region1] ring 1 enable
[S-switch-E-rrpp-domain-region1] quit
```

Configure S-switch-C as the transmit node on ring 1, and specify the primary and secondary interfaces.

```
<S-switch-C> system-view
[S-switch-C] rrpp domain 1
[S-switch-C-rrpp-domain-region1] ring 1 node-mode master primary-port ethernet
0/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-C-rrpp-domain-region1] ring 1 enable
[S-switch-C-rrpp-domain-region1] quit
```

Configure S-switch-D as the transmit node on ring 1, and specify the primary and secondary interfaces.

```
<S-switch-D> system-view
[S-switch-D] rrpp domain 1
[S-switch-D-rrpp-domain-region1] ring 1 node-mode transit primary-port
ethernet 0/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-D-rrpp-domain-region1] ring 1 enable
[S-switch-D-rrpp-domain-region1] quit
```

Configure S-switch-F as the transmit node on ring 1, and specify the primary and secondary interfaces.

```
<S-switch-F> system-view
[S-switch-F] rrpp domain 1
[S-switch-F-rrpp-domain-region1] ring 1 node-mode transit primary-port
ethernet 0/0/1 secondary-port ethernet 0/0/2 level 0
[S-switch-F-rrpp-domain-region1] ring 1 enable
[S-switch-F-rrpp-domain-region1] quit
```

5. Enable RRPP.

After configuring RRPP rings, you need to enable RRPP on each node on the rings. In this manner, the RRPP rings can be activated. The configuration procedure is as follows:

Enable RRPP on S-switch-A.

```
<S-switch-A> system-view
[S-switch-A] rrpp enable
```

Enable RRPP on S-switch-B.

```
<S-switch-B> system-view
[S-switch-B] rrpp enable
```

Enable RRPP on S-switch-C.

```
<S-switch-C> system-view
[S-switch-C] rrpp enable
```

Enable RRPP on S-switch-D.

```
<S-switch-D> system-view
[S-switch-D] rrpp enable
```

Enable RRPP on S-switch-E.

```
<S-switch-E> system-view
[S-switch-E] rrpp enable
```

Enable RRPP on S-switch-F.

```
<S-switch-F> system-view
[S-switch-F] rrpp enable
```

Configuration Files

- Configuration file of S-switch-A

```
# sysname S-switch-A # rrpp domain 2 control-vlan 20 timer hello-timer 3 fail-
timer 10 ring 2 node-mode master primary-port GigabitEthernet 0/0/1 secondary-
port GigabitEthernet 0/0/2 level 0 ring 2 enable # interface ethernet0/0/1 port
trunk allow-pass vlan 20 to 21 trust 8021p stp disable # interface
ethernet0/0/2 port trunk allow-pass vlan 20 to 21 trust 8021p stp disable #
rrpp enable # return #
```

- Configuration file of S-switch-B

```
# sysname S-switch-B # rrpp domain 2 control-vlan 20 timer hello-timer 3 fail-
timer 10 ring 2 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-
port GigabitEthernet 0/0/2 level 0 ring 2 enable # interface ethernet0/0/1 port
trunk allow-pass vlan 20 to 21 trust 8021p stp disable # interface
ethernet0/0/2 port trunk allow-pass vlan 20 to 21 trust 8021p stp disable #
rrpp enable # return #
```

- Configuration file of S-switch-C

```
# sysname S-switch-C # rrpp domain 1 control-vlan 10 ring 1 node-mode transit
primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level
0 ring 1 enable timer hello-timer 2 fail-timer 7 # rrpp domain 2 control-vlan
20 timer hello-timer 3 fail-timer 10 ring 2 node-mode transit primary-port
GigabitEthernet 0/0/3 secondary-port GigabitEthernet 0/0/4 level 0 ring 2
enable # interface ethernet0/0/1 port trunk allow-pass vlan 10 to 11 trust
8021p stp disable # interface ethernet0/0/2 port trunk allow-pass vlan 10 to
11 trust 8021p stp disable # interface ethernet0/0/3 port trunk allow-pass vlan
20 to 21 trust 8021p stp disable # interface ethernet0/0/4 port trunk allow-
pass vlan 20 to 21 trust 8021p stp disable # rrpp enable # return
```

- Configuration file of S-switch-D

```
# sysname S-switch-D # rrpp domain 1 control-vlan 10 ring 1 node-mode transit
primary-port GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level
0 ring 1 enable timer hello-timer 2 fail-timer 7 # rrpp domain 2 control-vlan
20 timer hello-timer 3 fail-timer 10 ring 2 node-mode transit primary-port
GigabitEthernet 0/0/3 secondary-port GigabitEthernet 0/0/4 level 0 ring 2
enable # interface ethernet0/0/1 port trunk allow-pass vlan 10 to 11 trust
8021p stp disable # interface ethernet0/0/2 port trunk allow-pass vlan 10 to
11 trust 8021p stp disable # interface ethernet0/0/3 port trunk allow-pass vlan
20 to 21 trust 8021p stp disable # interface ethernet0/0/4 port trunk allow-
pass vlan 20 to 21 trust 8021p stp disable # rrpp enable # return
```

- Configuration file of S-switch-E

```
# sysname S-switch-E # rrpp domain 1 control-vlan 10 timer hello-timer 2 fail-
timer 7 ring 1 node-mode master primary-port GigabitEthernet 0/0/1 secondary-
port GigabitEthernet 0/0/2 level 0 ring 1 enable # interface ethernet0/0/1 port
trunk allow-pass vlan 10 to 11 trust 8021p stp disable # interface
```

```
ethernet0/0/2 port trunk allow-pass vlan 10 to 11 trust 8021p stp disable #
rrpp enable # return
```

- Configuration file of S-switch-F

```
# sysname S-switch-F # rrpp domain 1 control-vlan 10 timer hello-timer 2 fail-
timer 7 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-
port GigabitEthernet 0/0/2 level 0 ring 1 enable # interface ethernet0/0/1 port
trunk allow-pass vlan 10 to 11 trust 8021p stp disable # interface
ethernet0/0/2 port trunk allow-pass vlan 10 to 11 trust 8021p stp disable #
rrpp enable # return
```

10.5.5 Example for Configuring Single RRPP Ring of Multi-Instance

Networking Requirements

As shown in [Figure 10-6](#), a single RRPP ring of multi-instance is composed of UPE A, UPE B, UPE C, and a PE-AGG.

Two RRPP rings, namely, ring 1 in domain 1 and ring 1 in domain 2, are existent.

The VLANs that access CEs ranges from VLAN 100 to VLAN 300. Traffic from these VLANs is transmitted to and then balanced between domain 1 and domain 2. Domain 1 is responsible to transmit the packets from VLANs 100 to 200; domain 2 is responsible to transmit the packets from VLANs 201 to 300.

For details of the protected VLANs in domain 1 and domain 2, and the instances to which these protected VLANs belong, refer to [Table 10-1](#).

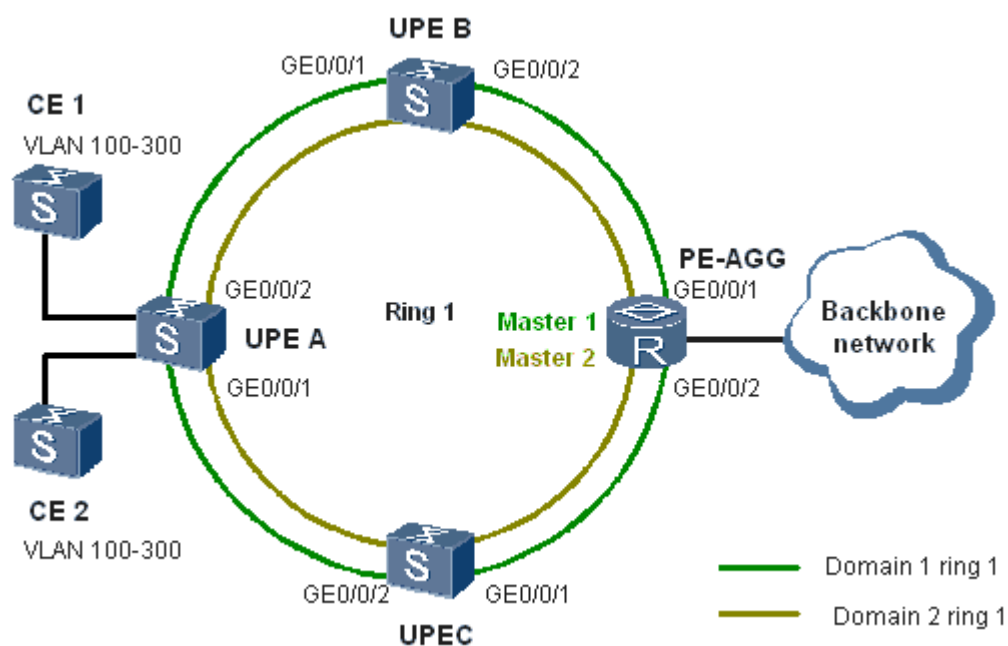
Table 10-1 Mapping between protected VLAN and instance

Domain ID	Control VLAN ID	Instance ID of Control VLAN	Data VLAN ID	Instance ID of Data VLAN
Domain 1	VLAN 1, VLAN 2	Instance 1	VLANs 100 to 200	Instance 1
Domain 2	VLAN 10, VLAN 11	Instance 2	VLANs 201 to 300	Instance 2

For details of the master nodes in two rings, refer to [Table 10-2](#).

Table 10-2 Information table of master nodes

Ring ID	Master Node	Primary Port	Secondary Port
Ring 1 in domain 1	PE-AGG	GE 0/0/1	GE 0/0/2
Ring 1 in domain 2	PE-AGG	GE 0/0/2	GE 0/0/1

Figure 10-6 Networking diagram of single RRPP ring of multi-instance

Configuration Roadmap

The configuration roadmap is as follows:

1. Map VLANs 100 to 200 to instance 1. Map VLANs 201 to 300 to instance 2.
2. Establish ring 1 in domain 1 by configuring UPE A, UPE B, UPE C, and a PE-AGG.
3. Establish ring 1 in domain 2 by configuring UPE A, UPE B, UPE C, and a PE-AGG.
4. Configure protected VLANs in domain 1 and domain 2.
5. Configure control VLANs in domain 1 and domain 2.
6. In ring 1 of domain 1, configure the PE-AGG as the master node; configure UPE A, UPE B, and UPE C as transit nodes.
7. In ring 1 of domain 2, configure the PE-AGG as the master node; configure UPE A, UPE B, and UPE C as transit nodes.

Data Preparation

To complete the configuration, you need the following data:

- Instance ID
- Range of protected VLANs
- ID of the control VLAN
- Number of the RRPP interface

Procedure

Step 1 Create instances.

- Configure UPE A.
 - # Create data VLANs 100 to 300 on UPE A.
 - ```
<UPEA> system-view
[UPEA] vlan batch 100 to 300
```
  - # Create instance 1. Then in domain 1, map the data VLANs 100 to 200 and the control VLAN 1 to 2 to the instance.
  - ```
[UPEA] stp region-configuration
[UPEA-mst-region] instance 1 vlan 1 2 100 to 200
```
 - # Create instance 2. Then in domain 2, map the data VLANs 201 to 300 and the control VLAN 10 to 11 to the instance.
 - ```
[UPEA-mst-region] instance 2 vlan 10 11 201 to 300
```
  - # Activate the configuration.
  - ```
[UPEA-mst-region] active region-configuration
```
- Configure UPE B.
 - # Create data VLANs 100 to 300 on UPE B.
 - ```
<UPEB> system-view
[UPEB] vlan batch 100 to 300
```
  - # Create instance 1. Then in domain 1, map data VLANs 100 to 200 and the control VLAN 1 to 2 to the instance.
  - ```
[UPEB] stp region-configuration
[UPEB-mst-region] instance 1 vlan 1 2 100 to 200
```
 - # Create instance 2. Then in domain 2, map the data VLANs 201 to 300 and the control VLAN 10 to 11 to the instance.
 - ```
[UPEB-mst-region] instance 2 vlan 10 11 201 to 300
```
  - # Activate the configuration.
  - ```
[UPEB-mst-region] active region-configuration
```
- Configure UPE C.
 - # Create data VLANs 100 to 300 on UPE C.
 - ```
<UPEC> system-view
[UPEC] vlan batch 100 to 300
```
  - # Create instance 1. Then in domain 1, map the data VLANs 100 to 200 and the control VLAN 1 to 2 to the instance.
  - ```
[UPEC] stp region-configuration
[UPEC-mst-region] instance 1 vlan 1 2 100 to 200
```
 - # Create instance 2. Then in domain 2, map the data VLANs 201 to 300 and the control VLAN 10 to 11 to the instance.
 - ```
[UPEC-mst-region] instance 2 vlan 10 11 201 to 300
```
  - # Activate the configuration.
  - ```
[UPEC-mst-region] active region-configuration
```
- Configure PE-AGG.
 - # Create data VLANs 100 to 300 on the PE-AGG.
 - ```
<PE-AGG> system-view
[PE-AGG] vlan batch 100 to 300
```
  - # Create instance 1. Then in domain 1, map the data VLANs 100 to 200 and the control VLAN 1 to 2 to the instance.
  - ```
[PE-AGG] stp region-configuration
[PE-AGG-mst-region] instance 1 vlan 1 2 100 to 200
```
 - # Create instance 2. Then in domain 2, map the data VLANs 201 to 300 and the control VLAN 10 to 11 to the instance.

```
[PE-AGG-mst-region] instance 2 vlan 10 11 201 to 300
```

Activate the configuration.

```
[PE-AGG-mst-region] active region-configuration
```

- Verify the configuration.

After the configuration, perform the following procedures to verify the previous configuration. Take the display of UPEA as an example.

```
<UPEA> display stp region-configuration
Oper configuration
Format selector      :0
Region name          :00e0cd568d00
Revision level       :0

Instance  Vlan Mapped
0         3 to 9, 12 to 99, 301 to 4094
1         1 to 2, 100 to 200
2         10 to 11, 201 to 300
```

Step 2 Configure the port that joins in the RRPP ring.

- # Configure UPE-A.

Disable the STP function on the port that is ready to join in the RRPP ring. Then configure the port to allow the packets from VLANs 100 to 300 to pass.

```
<UPEA> system-view
[UPEA] interface GigabitEthernet 0/0/1
[UPEA-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/1] stp disable
[UPEA-GigabitEthernet0/0/1] quit
[UPEA] interface GigabitEthernet 0/0/2
[UPEA-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/2] stp disable
[UPEA-GigabitEthernet0/0/2] quit
```

- Configure UPE-B.

Disable the STP function on the port that is ready to join in the RRPP ring. Then configure the port to allow the packets from VLANs 100 to 300 to pass.

```
<UPEB> system-view
[UPEB] interface GigabitEthernet 0/0/1
[UPEB-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/1] stp disable
[UPEB-GigabitEthernet0/0/1] quit
[UPEB] interface GigabitEthernet 0/0/2
[UPEB-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/2] stp disable
[UPEB-GigabitEthernet0/0/2] quit
```

- Configure UPE C.

Disable the STP function on the port that is ready to join in the RRPP ring. Then configure the port to allow the packets from VLANs 100 to 300 to pass.

```
<UPEC> system-view
[UPEC] interface GigabitEthernet 0/0/1
[UPEC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/1] stp disable
[UPEC-GigabitEthernet0/0/1] quit
[UPEC] interface GigabitEthernet 0/0/2
[UPEC-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/2] stp disable
[UPEC-GigabitEthernet0/0/2] quit
```

- Configure PE-AGG.

Disable the STP function on the port that is ready to join in the RRPP ring. Then configure the port to allow the packets from VLANs 100 to 300 to pass.

```
<PE-AGG> system-view
[PE-AGG] interface GigabitEthernet 0/0/1
[PE-AGG-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[PE-AGG-GigabitEthernet0/0/1] stp disable
[PE-AGG-GigabitEthernet0/0/1] quit
[PE-AGG] interface GigabitEthernet 0/0/2
[PE-AGG-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[PE-AGG-GigabitEthernet0/0/2] stp disable
[PE-AGG-GigabitEthernet0/0/2] quit
```

Step 3 Create RRPP domains, and configure the protected VLANs and control VLANs.

- Configure UPE A.

In domain 1, configure protected VLANs as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<UPEA> system-view
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEA-rrpp-domain-region1] control-vlan 1
[UPEA-rrpp-domain-region1] quit
```

In domain 2, configure protected VLANs as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<UPEA> system-view
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEA-rrpp-domain-region2] control-vlan 10
[UPEA-rrpp-domain-region2] quit
```

- Configure UPE B.

In domain 1, configure protected VLANs as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<UPEB> system-view
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEB-rrpp-domain-region1] control-vlan 1
[UPEB-rrpp-domain-region1] quit
```

In domain 2, configure protected VLANs as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<UPEB> system-view
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEB-rrpp-domain-region2] control-vlan 10
[UPEB-rrpp-domain-region2] quit
```

- Configure UPE C.

In domain 1, configure protected VLANs as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<UPEC> system-view
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEC-rrpp-domain-region1] control-vlan 1
[UPEC-rrpp-domain-region1] quit
```

In domain 2, configure protected VLANs as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<UPEC> system-view
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEC-rrpp-domain-region2] control-vlan 10
[UPEC-rrpp-domain-region2] quit
```

- Configure PE-AGG.

In domain 1, configure protected VLANs as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<PE-AGG> system-view
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] protected-vlan reference-instance 1
[PE-AGG-rrpp-domain-region1] control-vlan 1
[PE-AGG-rrpp-domain-region1] quit
```

In domain 2, configure protected VLANs as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<PE-AGG> system-view
[PE-AGG] rrpp domain 2
[PE-AGG-rrpp-domain-region2] protected-vlan reference-instance 2
[PE-AGG-rrpp-domain-region2] control-vlan 10
[PE-AGG-rrpp-domain-region2] quit
```

Step 4 Create RRPP rings.

- Configure UPE A.

Configure UPE A as a transit node of ring 1 in domain 1, and then specify primary and secondary ports.

```
<UPEA> system-view
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEA-rrpp-domain-region1] ring 1 enable
[UPEA-rrpp-domain-region1] quit
```

Configure UPE A as a transit node of ring 1 in domain 2, and then specify primary and secondary ports.

```
<UPEA> system-view
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEA-rrpp-domain-region2] ring 1 enable
[UPEA-rrpp-domain-region2] quit
```

- Configure UPE B.

Configure UPE B as a transit node of ring 1 in domain 1, and then specify primary and secondary ports.

```
<UPEB> system-view
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEB-rrpp-domain-region1] ring 1 enable
[UPEB-rrpp-domain-region1] quit
```

Configure UPE B as a transit node of ring 1 in domain 2, and then specify primary and secondary ports.

```
<UPEB> system-view
[[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEB-rrpp-domain-region2] ring 1 enable
[UPEB-rrpp-domain-region2] quit
```

- Configure UPE C.

Configure UPE C as a transit node of ring 1 in domain 1, and then specify primary and secondary ports.

```
<UPEC> system-view
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
```

```
[UPEC-rrpp-domain-region1] ring 1 enable
[UPEC-rrpp-domain-region1] quit
```

Configure UPE C as a transit node of ring 1 in domain 2, and then specify primary and secondary ports.

```
<UPEC> system-view
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEC-rrpp-domain-region2] ring 1 enable
[UPEC-rrpp-domain-region2] quit
```

- Configure PE-AGG.

Configure the PE-AGG as the master node of ring 1 in domain 1, and then specify GE 0/0/1 as the primary port and GE 0/0/2 as the secondary port.

```
<PE-AGG> system-view
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] ring 1 node-mode master primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[PE-AGG-rrpp-domain-region1] ring 1 enable
[PE-AGG-rrpp-domain-region1] quit
```

Configure the PE-AGG as the master node of ring 1 in domain 2, and then specify GE 0/0/2 as the primary port and GE 0/0/1 as the secondary port.

```
<PE-AGG> system-view
[PE-AGG] rrpp domain 2
[PE-AGG-rrpp-domain-region2] ring 1 node-mode master primary-port
GigabitEthernet 0/0/2 secondary-port GigabitEthernet 0/0/1 level 0
[PE-AGG-rrpp-domain-region2] ring 1 enable
[PE-AGG-rrpp-domain-region2] quit
```

Step 5 Enable RRPP.

After configuring an RRPP ring, enable RRPP on each node in the ring. In this manner, the RRPP ring can be activated. The configuration procedure is as follows:

- Configure UPE A.

Enable RRPP.

```
<UPEA> system-view
[UPEA] rrpp enable
```

- Configure UPE B.

Enable RRPP.

```
<UPEB> system-view
[UPEB] rrpp enable
```

- Configure UPE C.

Enable RRPP.

```
<UPEC> system-view
[UPEC] rrpp enable
```

- Configure PE-AGG.

Enable RRPP.

```
<PE-AGG> system-view
[PE-AGG] rrpp enable
```

Step 6 Verify the configuration.

After the previous configuration, run the following commands to verify the configuration. Take the display on UPE A and the PE-AGG as an example.

- Run the **display rrpp brief** command on UPE A. The following results are displayed:

```

<UPEA> display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
RRPP Linkup Delay Timer: 0 sec(default is 0 sec)
Number of RRPP Domains: 2

Domain Index : 1
Control VLAN : major 1 sub 2
Protected VLAN : Reference Instance 1
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)
  Ring Ring Node Primary/Common Secondary/Edge Is
  ID Level Mode Port Port
Enabled

-----
-
  1      0      T      GigabitEthernet0/0/1      GigabitEthernet0/0/2      Yes

Domain Index : 2
Control VLAN : major 10 sub 11
Protected VLAN: Reference Instance 2
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)
  Ring Ring Node Primary/Common Secondary/Edge Is
  ID Level Mode Port Port
Enabled

-----
-
  1      0      T      GigabitEthernet0/0/1      GigabitEthernet0/0/2      Yes

```

You can view that RRPP is enabled on UPE B.

In domain 1, the major control VLAN is VLAN 1, the protected VLAN is the VLAN mapped to instance 1, and the transit node of ring 1 is UPE A. The primary port is GE 0/0/1, and the secondary port is GE 0/0/2.

In domain 2, the ID of the major control VLAN is 10, the protected VLAN is instance 2, and the transit node of ring 1 is UPE A. The primary port is GE 0/0/1, and the secondary port is GE 0/0/2.

- Run the **display rrpp brief** command on the PE-AGG. The following results are displayed:

```

<PE-AGG> display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
RRPP Linkup Delay Timer: 0 sec(default is 0 sec)
Number of RRPP Domains: 2

Domain Index : 1
Control VLAN : major 1 sub 2Protected VLAN : Reference Instance 1
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)
  Ring Ring Node Primary/Common Secondary/Edge Is
  ID Level Mode Port Port
Enabled

-----
-
  1      0      M      GigabitEthernet0/0/1      GigabitEthernet0/0/2      Yes

Domain Index : 2
Control VLAN : major 10 sub 11Protected VLAN: Reference Instance 2
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)
  Ring Ring Node Primary/Common Secondary/Edge Is
  ID Level Mode Port Port
Enabled

```

```
-----
-
1      0      M      GigabitEthernet0/0/2      GigabitEthernet0/0/1      Yes
```

You can view that RRPP is enabled on the PE-AGG.

In domain 1, the ID of the major control VLAN is 1, the protected VLAN is instance 1, and the master node of ring 1 is the PE-AGG. The primary port is GE 0/0/1, and the secondary port is GE 0/0/2.

In domain 2, the ID of the major control VLAN is 10, the protected VLAN is instance 2, and the master node of ring 1 is the PE-AGG. The primary port is GE 0/0/2, and the secondary port is GE 0/0/1.

- On UPE A, run the **display rrpp verbose domain** command. The following results are displayed.

View detailed information about UPE A in domain 1.

```
<UPEA> display rrpp verbose domain 1
Domain Index : 1
Control VLAN : major 1 sub 2
Protected VLAN: Reference Instance 1
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)

RRPP Ring : 1
Ring Level : 0
Node Mode : Transit
Ring State : LinkUp
Is Enabled : Enable Is Activated : Yes
Primary port : GigabitEthernet0/0/1 Port status: UP
Secondary port: GigabitEthernet0/0/2 Port status: UP
```

In domain 1, the control VLAN is VLAN 1, and the protected VLAN is the VLAN mapped to instance 1. UPE A is the transit node, and the node status is LinkUp.

View detailed information about UPE A in domain 2.

```
<UPEA> display rrpp verbose domain 2
Domain Index : 2
Control VLAN : major 10 sub 11
Protected VLAN: Reference Instance 2
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)

RRPP Ring : 1
Ring Level : 0
Node Mode : Transit
Ring State : LinkUp
Is Enabled : Enable Is Activated : Yes
Primary port : GigabitEthernet0/0/1 Port status: UP
Secondary port: GigabitEthernet0/0/2 Port status: UP
```

In domain 2, the control VLAN is VLAN 10, and the protected VLAN is the VLAN mapped to instance 2. The transit node is UPE A, and the node status is LinkUp.

- Run the **display rrpp verbose domain** command on the PE-AGG. The following results are displayed:

View detailed information about the PE-AGG in domain 1.

```
<PE-AGG> display rrpp verbose domain 1
Domain Index : 1
Control VLAN : major 1 sub 2
Protected VLAN: Reference Instance 1
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)

RRPP Ring : 1
Ring Level : 0
Node Mode : Master
Ring State : Complete
Is Enabled : Enable Is Activated : Yes
Primary port : GigabitEthernet0/0/1 Port status: UP
Secondary port: GigabitEthernet0/0/2 Port status: BLOCKED
```

In domain 1, the control VLAN is VLAN 1, and the protected VLAN is the VLAN mapped to instance 1.

The master node is the PE-AGG, and the node status is Complete.

The primary port is GE 0/0/1, and the secondary port is GE 0/0/2.

View detailed information about the PE-AGG in domain 2.

```
<PE-AGG> display rrpp verbose domain 2
Domain Index : 2
Control VLAN : major 10      sub 11Protected VLAN: Reference Instance 2
Hello Timer  : 1 sec(default is 1 sec)  Fail Timer : 3 sec(default is 3 sec)

RRPP Ring    : 1
Ring Level   : 0
Node Mode    : Master
Ring State   : Complete
Is Enabled   : Enable      Is Activated : Yes
Primary port : GigabitEthernet0/0/2      Port status: UP
Secondary port: GigabitEthernet0/0/1      Port status: BLOCKED
```

In domain 2, the control VLAN is VLAN 10, and the protected VLAN is the VLAN mapped to instance 2.

The master node is the PE-AGG, and the node status is Complete.

The primary port is GE 0/0/2, and the secondary port is GE 0/0/1.

----End

Configuration Files

- Configuration file of UPE A

```
#
sysname UPEA
#
vlan batch 1 to 2 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
instance 1 vlan 1 2 100 to 200
instance 2 vlan 10 11 201 to 300
active region-configuration
#
rrpp domain 1
control-vlan 1
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
rrpp domain 2
control-vlan 10
protected-vlan reference-instance 2
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
return
```

- Configuration file of UPE B

```
#
sysname UPEB
#
```

```

vlan batch 1 to 2 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
instance 1 vlan 1 2 100 to 200
instance 2 vlan 10 11 201 to 300
active region-configuration
#
rrpp domain 1
control-vlan 1
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
rrpp domain 2
control-vlan 10
protected-vlan reference-instance 2
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
return

```

- Configuration file of UPE C

```

#
sysname UPEC
#
vlan batch 1 to 2 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
instance 1 vlan 1 2 100 to 200
instance 2 vlan 10 11 201 to 300
active region-configuration
#
rrpp domain 1
control-vlan 1
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
rrpp domain 2
control-vlan 10
protected-vlan reference-instance 2
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
Return

```

- Configuration file of PE-AGG

```
#
sysname PE-AGG
#
vlan batch 1 to 2 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
instance 1 vlan 1 2 100 to 200
instance 2 vlan 10 11 201 to 300
active region-configuration
#
rrpp domain 1
control-vlan 1
protected-vlan reference-instance 1
ring 1 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
rrpp domain 2
control-vlan 10
protected-vlan reference-instance 2
ring 1 node-mode master primary-port GigabitEthernet 0/0/2 secondary-port
GigabitEthernet 0/0/1 level 0
ring 1 enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
return
```

10.5.6 Example for Configuring the Crossed RRPP Ring of Multi-Instance

Networking Requirements

As shown in [Figure 10-7](#), the RRPP major rings of multi-instance, that is, ring 1 in domain 1 and ring 1 in domain 2, are constructed by UPE A, UPE B, UPE C, UPE D, and a PE-AGG.

The RRPP sub-rings of multi-instance, that is, ring 2 in domain 1 and ring 2 in domain 2, are constructed by CE1, UPE B, and UPE C. The sub-ring on which CE1 resides and the major rings are crossed on the GE 0/0/3 interfaces of UPE B and UPE C. UPE B is the edge node, and the UPE C is the assistant edge node.

The RRPP sub-rings of multi-instance, that is, ring 3 in domain 1 and ring 3 in domain 2, are constructed by CE2, UPE B, and UPE C. CE2 and the major rings are crossed on the GE 0/0/4 interfaces of UPE B and UPE C. UPE B is the edge node, and the UPE C is the assistant edge node.

The VLANs that access the major rings through CEs range from VLAN 100 to VLAN 300. Domain 1 and domain 2 perform load balancing for the packets from these VLANs. Domain 1 transmits the packets from VLANs 100 to 200; domain 2 transmits the packets from VLANs 201 to 300.

For details of the protected VLANs in domain 1 and domain 2, and the instance to which these protected VLANs belong, refer to [Table 10-3](#).

Table 10-3 Mapping between the protected VLAN and instance

Domain ID	Control VLAN ID	Instance ID of Control VLAN	Data VLAN ID	Instance ID of Data VLAN
Domain 1	VLAN 1, VLAN 2	Instance 1	VLANs 100 to 200	Instance 1
Domain 2	VLAN 10, VLAN 11	Instance 2	VLANs 201 to 300	Instance 2

For details of the master nodes in the six rings, refer to [Table 10-4](#).

Table 10-4 Information table of master nodes

Ring ID	Master Node	Primary Port	Secondary Port	Ring Type
Ring 1 in domain 1	PE-AGG	GE 0/0/1	GE 0/0/2	Major ring
Ring 1 in domain 2	PE-AGG	GE 0/0/2	GE 0/0/1	Major ring
Ring 2 in domain 1	CE1	GE 0/0/1	GE 0/0/2	Sub ring
Ring 2 in domain 2	CE1	GE 0/0/2	GE 0/0/1	Sub ring
Ring 3 in domain 1	CE2	GE 0/0/1	GE 0/0/2	Sub ring
Ring 3 in domain 2	CE2	GE 0/0/2	GE 0/0/1	Sub ring

Information about edge nodes, assistant edge nodes, common ports, and edge ports of four sub-rings is shown in [Table 10-5](#).

Table 10-5 Information table of nodes and ports

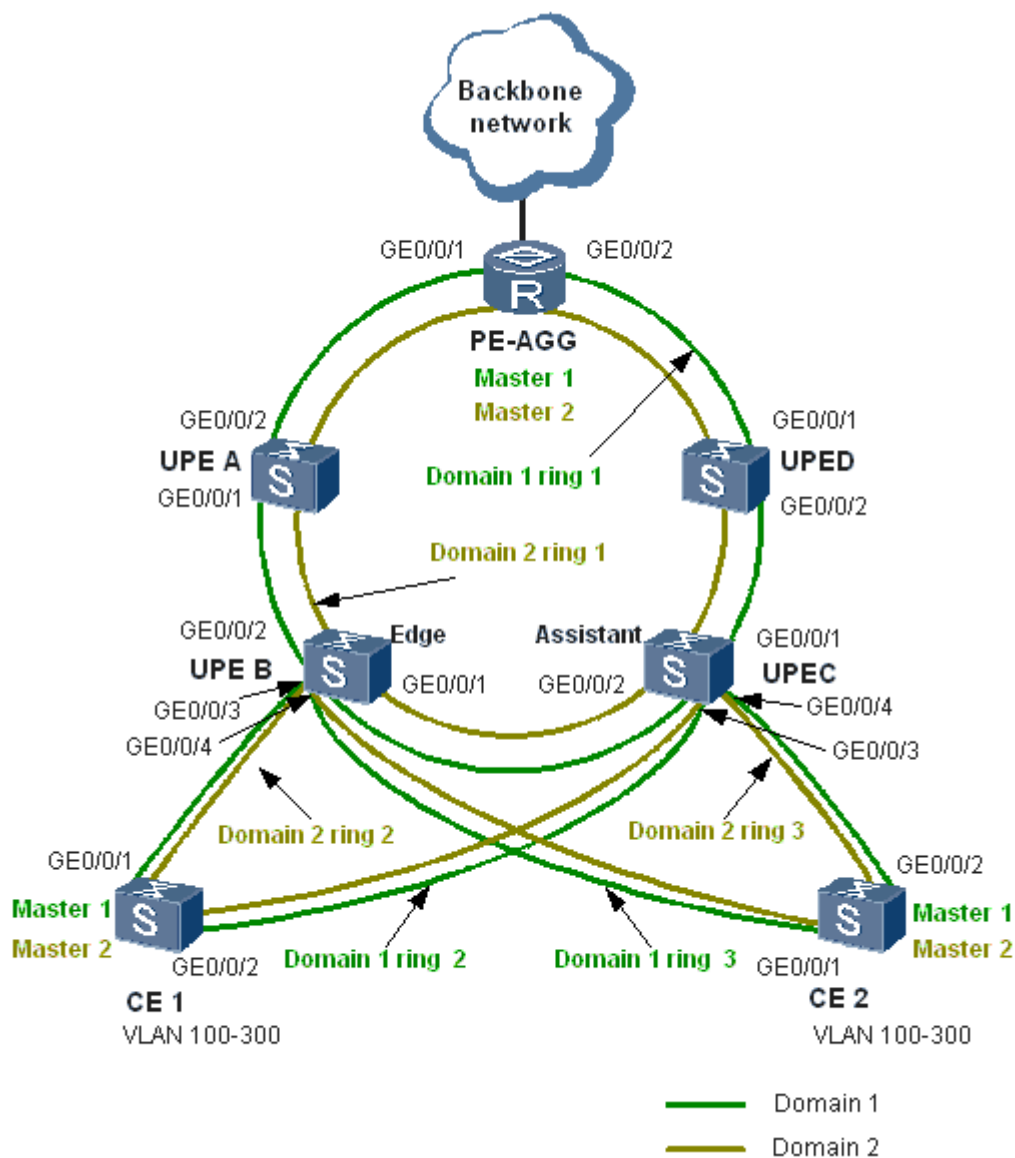
Ring ID	Edge Node	Common Port	Edge Port	Edge-Assistant Node	Common Port	Edge Port
Ring 2 in domain 1	UPE B	GE 0/0/1	GE 0/0/3	UPE C	GE 0/0/2	GE 0/0/3

Ring ID	Edge Node	Common Port	Edge Port	Edge-Assistant Node	Common Port	Edge Port
Ring 3 in domain 1	UPE B	GE 0/0/1	GE 0/0/4	UPE C	GE 0/0/2	GE 0/0/4
Ring 2 in domain 2	UPE B	GE 0/0/1	GE 0/0/3	UPE C	GE 0/0/2	GE 0/0/3
Ring 3 in domain 2	UPE B	GE 0/0/1	GE 0/0/4	UPE C	GE 0/0/2	GE 0/0/4

To reduce the number of Edge-Hello packets sent from four sub-rings and transmitted on major rings, add all sub-rings into a ring group. In this manner, the bandwidth resources of the major rings can be saved.

To avoid topology flapping, configure a timer on the master node to define the delay for the link to go Up.

Figure 10-7 Networking diagram of crossed RRPP ring of multi-instance



Configuration Roadmap

The configuration roadmap is as follows:

1. Map VLANs 100 to 200 to instance 1. Map VLANs 201 to 300 to instance 2.
2. Construct ring 1 in domain 1 and ring 1 in domain 2 by UPE A, UPE B, UPE C, UPE D, and a PE-AGG.
3. Construct ring 2 in domain 1 and ring 2 in domain 2 by CE1, UPE B, and UPE C.
4. Construct ring 3 in domain 1 and ring 3 in domain 2 by CE2, UPE B, and UPE C.
5. Configure protected VLANs for domain 1 and domain 2.
6. Configure control VLANs for domain 1 and domain 2.

7. In ring 1 of domain 1 and ring 1 of domain 2, configure the PE-AGG as the master node; configure UPE A, UPE B, and UPE C as transit nodes.
8. In ring 2 of domain 1 and ring 2 of domain 2, configure CE1 as the master node, UPE B as the edge node, and UPE C as the assistant edge node.
9. In ring 3 of domain 1 and ring 3 of domain 2, configure CE2 as the master node, UPE B as the edge node, and UPE C as the assistant edge node.
10. Configure a ring group.
11. Initiate the timer that defines the delay for the link to go Up.

Data Preparation

To complete the configuration, you need the following data:

- Instance IDs
- Range of protected VLANs
- Control VLAN IDs
- Number of the RRPP port
- ID of the ring group
- Value of the timer that defines the delay for the link to go Up

Procedure

Step 1 Create instances.

- Configure CE1.
 - # Create data VLANs 100 to 300 on CE1.
 - ```
<CE1> system-view
[CE1] vlan batch 100 to 300
```
  - # Create instance 1. Then in domain 1, map data VLANs 100 to 200 and the control VLAN 1 to 2 to the instance.
  - ```
[CE1] stp region-configuration
[CE1-mst-region] instance 1 vlan 1 2 100 to 200
```
 - # Create instance 2. Then in domain 2, map the data VLANs 201 to 300 and the control VLAN 10 to 11 to the instance.
 - ```
[CE1-mst-region] instance 2 vlan 10 11 201 to 300
```
  - # Activate the configuration.
  - ```
[CE1-mst-region] active region-configuration
```
- Configure CE2.
 - # Create data VLANs 100 to 300 on CE 2.
 - ```
<CE2> system-view
[CE2] vlan batch 100 to 300
```
  - # Create instance 1. Then in domain 1, map the data VLANs 100 to 200 and the control VLAN 1 to 2 to the instance.
  - ```
[CE2] stp region-configuration
[CE2-mst-region] instance 1 vlan 1 2 100 to 200
```
 - # Create instance 2. Then in domain 2, map the data VLANs 201 to 300 and the control VLAN 10 to 11 to the instance.
 - ```
[CE2-mst-region] instance 2 vlan 10 11 201 to 300
```
  - # Activate the configuration.

```
[CE2-mst-region] active region-configuration
```

- Configure UPE A.

# Create data VLANs 100 to 300 on UPE A.

```
<UPEA> system-view
[UPEA] vlan batch 100 to 300
```

# Create instance 1. Then in domain 1, map the data VLANs 100 to 200 and the control VLAN 1 to 2 to the instance.

```
[UPEA] stp region-configuration
[UPEA-mst-region] instance 1 vlan 1 2 100 to 200
```

# Create instance 2. Then in domain 2, map the data VLANs 201 to 300 and the control VLAN 10 to 11 to the instance.

```
[UPEA-mst-region] instance 2 vlan 10 11 201 to 300
```

# Activate the configuration.

```
[UPEA-mst-region] active region-configuration
```

- Configure UPE B.

# Create data VLANs 100 to 300 on UPE B.

```
<UPEB> system-view
[UPEB] vlan batch 100 to 300
```

# Create instance 1. Then in domain 1, map the data VLANs 100 to 200 and the control VLAN 1 to 2 to the instance.

```
[UPEB] stp region-configuration
[UPEB-mst-region] instance 1 vlan 1 2 100 to 200
```

# Create instance 2. Then in domain 2, map the data VLANs 201 to 300 and the control VLAN 10 to 11 to the instance.

```
[UPEB-mst-region] instance 2 vlan 10 11 201 to 300
```

# Activate the configuration.

```
[UPEB-mst-region] active region-configuration
```

- Configure UPE C.

# Create data VLANs 100 to 300 on UPE C.

```
<UPEC> system-view
[UPEC] vlan batch 100 to 300
```

# Create instance 1. Then in domain 1, map the data VLANs 100 to 200 and the control VLAN 1 to 2 to the instance.

```
[UPEC] stp region-configuration
[UPEC-mst-region] instance 1 vlan 1 2 100 to 200
```

# Create instance 2. Then in domain 2, map the data VLANs 201 to 300 and the control VLAN 10 to 11 to the instance.

```
[UPEC-mst-region] instance 2 vlan 10 11 201 to 300
```

# Activate the configuration.

```
[UPEC-mst-region] active region-configuration
```

- Configure UPE D.

# Create data VLANs 100 to 300 on UPE D.

```
<UPED> system-view
[UPED] vlan batch 100 to 300
```

# Create instance 1. Then in domain 1, map the data VLANs 100 to 200 and the control VLAN 1 to 2 to the instance.

```
[UPED] stp region-configuration
[UPED-mst-region] instance 1 vlan 1 2 100 to 200
```

# Create instance 2. Then in domain 2, map the data VLANs 201 to 300 and the control VLAN 10 to 11 to the instance.

```
[UPED-mst-region] instance 2 vlan 10 11 201 to 300
```

# Activate the configuration.

```
[UPED-mst-region] active region-configuration
```

- Configure PE-AGG.

# Create data VLANs 100 to 300 on the PE-AGG.

```
<PE-AGG> system-view
[PE-AGG] vlan batch 100 to 300
```

# Create instance 1. Then in domain 1, map the data VLANs 100 to 200 and the control VLAN 1 to 2 to the instance.

```
[PE-AGG] stp region-configuration
[PE-AGG-mst-region] instance 1 vlan 1 2 100 to 200
```

# Create instance 2. Then in domain 2, map the data VLANs 201 to 300 and the control VLAN 10 to 11 to the instance.

```
[PE-AGG-mst-region] instance 2 vlan 10 11 201 to 300
```

# Activate the configuration.

```
[PE-AGG-mst-region] active region-configuration
```

- Verify the configuration.

After the configuration, perform the following procedures to verify the previous configuration. Take the display of UPE A as an example.

```
<UPEA> display stp region-configuration
Oper configuration
 Format selector :0
 Region name :00e0cd568d00
 Revision level :0

 Instance Vlans Mapped
 0 3 to 9, 12 to 99, 301 to 4094
 1 1 to 2, 100 to 200
 2 10 to 11, 201 to 300
```

## Step 2 Configure the port to be added into the RRPP ring.

- Configure CE1.

# On CE 1, disable the STP function on the port that is ready to join in the RRPP ring. Then configure the port to allow the packets from VLANs 100 to 300 to pass.

```
<CE1> system-view
[CE1] interface GigabitEthernet 0/0/1
[CE1-GigabitEthernet0/0/1] undo shutdown
[CE1-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[CE1-GigabitEthernet0/0/1] stp disable
[CE1-GigabitEthernet0/0/1] quit
[CE1] interface GigabitEthernet 0/0/2
[CE1-GigabitEthernet0/0/2] undo shutdown
[CE1-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[CE1-GigabitEthernet0/0/2] stp disable
[CE1-GigabitEthernet0/0/2] quit
```

- Configure CE2.

# On CE2, disable the STP function on the port that is ready to join in the RRPP ring. Then configure the port to allow the packets from VLANs 100 to 300 to pass.

```
<CE2> system-view
[CE2] interface GigabitEthernet 0/0/1
[CE2-GigabitEthernet0/0/1] undo shutdown
[CE2-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[CE2-GigabitEthernet0/0/1] stp disable
```

```
[CE2-GigabitEthernet0/0/1] quit
[CE2] interface GigabitEthernet 0/0/2
[CE2-GigabitEthernet0/0/2] undo shutdown
[CE2-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[CE2-GigabitEthernet0/0/2] stp disable
[CE2-GigabitEthernet0/0/2] quit
```

- Configure UPE A.

# On UPE A, disable the STP function on the port that is ready to join in the RRPP ring. Then configure the port to allow the packets from VLANs 100 to 300 to pass.

```
<UPEA> system-view
[UPEA] interface GigabitEthernet 0/0/1
[UPEA-GigabitEthernet0/0/1] undo shutdown
[UPEA-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/1] stp disable
[UPEA-GigabitEthernet0/0/1] quit
[UPEA] interface GigabitEthernet 0/0/2
[UPEA-GigabitEthernet0/0/2] undo shutdown
[UPEA-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/2] stp disable
[UPEA-GigabitEthernet0/0/2] quit
```

- Configure UPE B.

# On UPE B, disable the STP function on the port that is ready to join in the RRPP ring. Then configure the port to allow the packets from VLANs 100 to 300 to pass.

```
<UPEB> system-view
[UPEB] interface GigabitEthernet 0/0/1
[UPEB-GigabitEthernet0/0/1] undo shutdown
[UPEB-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/1] stp disable
[UPEB-GigabitEthernet0/0/1] quit
[UPEB] interface GigabitEthernet 0/0/2
[UPEB-GigabitEthernet0/0/2] undo shutdown
[UPEB-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/2] stp disable
[UPEB-GigabitEthernet0/0/2] quit
[UPEB] interface GigabitEthernet 0/0/3
[UPEB-GigabitEthernet0/0/3] undo shutdown
[UPEB-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/3] stp disable
[UPEB-GigabitEthernet0/0/3] quit
[UPEB] interface GigabitEthernet 0/0/4
[UPEB-GigabitEthernet0/0/4] undo shutdown
[UPEB-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/4] stp disable
[UPEB-GigabitEthernet0/0/4] quit
```

- Configure UPE C.

# On UPE C, disable the STP function on the port that is ready to join in the RRPP ring. Then configure the port to allow the packets from VLANs 100 to 300 to pass.

```
<UPEC> system-view
[UPEC] interface GigabitEthernet 0/0/1
[UPEC-GigabitEthernet0/0/1] undo shutdown
[UPEC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/1] stp disable
[UPEC-GigabitEthernet0/0/1] quit
[UPEC] interface GigabitEthernet 0/0/2
[UPEC-GigabitEthernet0/0/2] undo shutdown
[UPEC-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/2] stp disable
[UPEC-GigabitEthernet0/0/2] quit
[UPEC] interface GigabitEthernet 0/0/3
[UPEC-GigabitEthernet0/0/3] undo shutdown
[UPEC-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/3] stp disable
[UPEC-GigabitEthernet0/0/3] quit
```

```
[UPEC] interface GigabitEthernet 0/0/4
[UPEC-GigabitEthernet0/0/4] undo shutdown
[UPEC-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/4] stp disable
[UPEC-GigabitEthernet0/0/4] quit
```

- Configure UPE D.

# On UPE D, disable the STP function on the port that is ready to join in the RRPP ring. Then configure the port to allow the packets from VLANs 100 to 300 to pass.

```
<UPED> system-view
[UPED] interface GigabitEthernet 0/0/1
[UPED-GigabitEthernet0/0/1] undo shutdown
[UPED-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPED-GigabitEthernet0/0/1] stp disable
[UPED-GigabitEthernet0/0/1] quit
[UPED] interface GigabitEthernet 0/0/2
[UPED-GigabitEthernet0/0/2] undo shutdown
[UPED-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPED-GigabitEthernet0/0/2] stp disable
[UPED-GigabitEthernet0/0/2] quit
```

- Configure PE-AGG.

# On the PE-AGG, disable the STP function on the port that is ready to join in the RRPP ring. Then configure the port to allow the packets from VLANs 100 to 300 to pass.

```
<PE-AGG> system-view
[PE-AGG] interface GigabitEthernet 0/0/1
[PE-AGG-GigabitEthernet0/0/1] undo shutdown
[PE-AGG-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[PE-AGG-GigabitEthernet0/0/1] stp disable
[PE-AGG-GigabitEthernet0/0/1] quit
[PE-AGG] interface GigabitEthernet 0/0/2
[PE-AGG-GigabitEthernet0/0/2] undo shutdown
[PE-AGG-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[PE-AGG-GigabitEthernet0/0/2] stp disable
[PE-AGG-GigabitEthernet0/0/2] quit
```

### Step 3 Create RRPP domains, and configure protected VLANs and control VLANs.

- Configure CE1.

# In domain 1, configure protected VLANs as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<CE1> system-view
[CE1] rrpp domain 1
[CE1-rrpp-domain-region1] protected-vlan reference-instance 1
[CE1-rrpp-domain-region1] control-vlan 1
[CE1-rrpp-domain-region1] quit
```

# In domain 2, configure protected VLANs as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<CE1> system-view
[CE1] rrpp domain 2
[CE1-rrpp-domain-region2] protected-vlan reference-instance 2
[CE1-rrpp-domain-region2] control-vlan 10
[CE1-rrpp-domain-region2] quit
```

- Configure CE2.

# In domain 1, configure protected VLANs as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<CE2> system-view
[CE2] rrpp domain 1
[CE2-rrpp-domain-region1] protected-vlan reference-instance 1
[CE2-rrpp-domain-region1] control-vlan 1
[CE2-rrpp-domain-region1] quit
```

# In domain 2, configure protected VLANs as VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<CE1> system-view
[CE2] rrpp domain 2
[CE2-rrpp-domain-region2] protected-vlan reference-instance 2
[CE2-rrpp-domain-region2] control-vlan 10
[CE2-rrpp-domain-region2] quit
```

- Configure UPE A.

# In domain 1, configure protected VLANs as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<UPEA> system-view
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEA-rrpp-domain-region1] control-vlan 1
[UPEA-rrpp-domain-region1] quit
```

# In domain 2, configure protected VLANs as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<UPEA> system-view
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEA-rrpp-domain-region2] control-vlan 10
[UPEA-rrpp-domain-region2] quit
```

- Configure UPE B.

# In domain 1, configure protected VLANs as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<UPEB> system-view
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEB-rrpp-domain-region1] control-vlan 1
[UPEB-rrpp-domain-region1] quit
```

# In domain 2, configure protected VLANs as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<UPEB> system-view
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEB-rrpp-domain-region2] control-vlan 10
[UPEB-rrpp-domain-region2] quit
```

- Configure UPE C.

# In domain 1, configure protected VLANs as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<UPEC> system-view
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEC-rrpp-domain-region1] control-vlan 1
[UPEC-rrpp-domain-region1] quit
```

# In domain 2, configure protected VLANs as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<UPEC> system-view
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEC-rrpp-domain-region2] control-vlan 10
[UPEC-rrpp-domain-region2] quit
```

- Configure UPE D.

# In domain 1, configure protected VLANs as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<UPED> system-view
[UPED] rrpp domain 1
```

```
[UPED-rrpp-domain-region1] protected-vlan reference-instance 1
[UPED-rrpp-domain-region1] control-vlan 1
[UPED-rrpp-domain-region1] quit
```

# In domain 2, configure protected VLANs as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<UPED> system-view
[UPED] rrpp domain 2
[UPED-rrpp-domain-region2] protected-vlan reference-instance 2
[UPED-rrpp-domain-region2] control-vlan 10
[UPED-rrpp-domain-region2] quit
```

- Configure PE-AGG.

# In domain 1, configure protected VLANs as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<PE-AGG> system-view
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] protected-vlan reference-instance 1
[PE-AGG-rrpp-domain-region1] control-vlan 1
[PE-AGG-rrpp-domain-region1] quit
```

# In domain 2, configure protected VLANs as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<PE-AGG> system-view
[PE-AGG] rrpp domain 2
[PE-AGG-rrpp-domain-region2] protected-vlan reference-instance 2
[PE-AGG-rrpp-domain-region2] control-vlan 10
[PE-AGG-rrpp-domain-region2] quit
```

#### Step 4 Create RRPP rings.

- Configure CE1.

# In ring 2 of domain 1, configure CE1 as the master node, and then specify GE 0/0/1 as the primary port and GE 0/0/2 as the secondary port .

```
<CE1> system-view
[CE1] rrpp domain 1
[CE1-rrpp-domain-region1] ring 2 node-mode master primary-port GigabitEthernet
0/0/1 secondary-port GigabitEthernet 0/0/2 level 1
[CE1-rrpp-domain-region1] ring 2 enable
[CE1-rrpp-domain-region1] quit
```

# In ring 2 of domain 2, configure CE1 as the master node, and then specify GE 0/0/2 as the primary port and GE 0/0/1 as the secondary port.

```
<CE1> system-view
[CE1] rrpp domain 2
[CE1-rrpp-domain-region2] ring 2 node-mode master primary-port GigabitEthernet
0/0/2 secondary-port GigabitEthernet 0/0/1 level 1
[CE1-rrpp-domain-region2] ring 2 enable
[CE1-rrpp-domain-region2] quit
```

- Configure CE2.

# In ring 3 of domain 1, configure CE2 as the master node, and then specify GE 0/0/1 as the primary port and GE 0/0/2 as the secondary port.

```
<CE2> system-view
[CE2] rrpp domain 1
[CE2-rrpp-domain-region1] ring 3 node-mode master primary-port GigabitEthernet
0/0/1 secondary-port GigabitEthernet 0/0/2 level 1
[CE2-rrpp-domain-region1] ring 3 enable
[CE2-rrpp-domain-region1] quit
```

# In ring 3 of domain 2, configure CE2 as the master node, and then specify GE 0/0/2 as the primary port and GE 0/0/1 as the secondary port.

```
<CE2> system-view
[CE2] rrpp domain 2
```

```
[CE2-rrpp-domain-region2] ring 3 node-mode master primary-port GigabitEthernet
0/0/2 secondary-port GigabitEthernet 0/0/1 level 1
[CE2-rrpp-domain-region2] ring 3 enable
[CE2-rrpp-domain-region2] quit
```

- Configure UPE A.

# In ring 1 of domain 1, configure UPE A as the transit node, and then specify primary and secondary ports.

```
<UPEA> system-view
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEA-rrpp-domain-region1] ring 1 enable
[UPEA-rrpp-domain-region1] quit
```

# In ring 1 of domain 2, configure UPE A as the transit node, and then specify primary and secondary ports.

```
<UPEA> system-view
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEA-rrpp-domain-region2] ring 1 enable
[UPEA-rrpp-domain-region2] quit
```

- Configure UPE B.

# In ring 1 of domain 1, configure UPE B as the transit node, and then specify primary and secondary ports.

```
<UPEB> system-view
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEB-rrpp-domain-region1] ring 1 enable
[UPEB-rrpp-domain-region1] quit
```

# In ring 1 of domain 2, configure UPE B as the transit node, and then specify primary and secondary ports.

```
<UPEB> system-view
[[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEB-rrpp-domain-region2] ring 1 enable
[UPEB-rrpp-domain-region2] quit
```

# In ring 2 of domain 1, configure UPE B as the edge node, GE 0/0/1 as the common port, and GE 0/0/3 as the edge port.

```
<UPEB> system-view
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] ring 2 node-mode edge common-port GigabitEthernet
0/0/1 edge-port GigabitEthernet 0/0/3
[UPEB-rrpp-domain-region1] ring 2 enable
[UPEB-rrpp-domain-region1] quit
```

# In ring 2 of domain 2, configure UPE B as the edge node, GE 0/0/1 as the common port, and GE 0/0/3 as the edge port.

```
<UPEB> system-view
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] ring 2 node-mode edge common-port GigabitEthernet
0/0/1 edge-port GigabitEthernet 0/0/3
[UPEB-rrpp-domain-region2] ring 2 enable
[UPEB-rrpp-domain-region2] quit
```

# In ring 3 of domain 1, configure UPE B as the edge node, GE 0/0/1 as the common port, and GE 0/0/4 as the edge port.

```
<UPEB> system-view
[UPEB] rrpp domain 1
```

```
[UPEB-rrpp-domain-region1] ring 3 node-mode edge common-port GigabitEthernet
0/0/1 edge-port GigabitEthernet 0/0/4
[UPEB-rrpp-domain-region1] ring 3 enable
[UPEB-rrpp-domain-region1] quit
```

# In ring 3 of domain 2, configure UPE B as the edge node, GE 0/0/1 as the common port, and GE 0/0/4 as the edge port.

```
<UPEB> system-view
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] ring 3 node-mode edge common-port GigabitEthernet
0/0/1 edge-port GigabitEthernet 0/0/4
[UPEB-rrpp-domain-region2] ring 3 enable
[UPEB-rrpp-domain-region2] quit
```

- Configure UPE C.

# In ring 1 of domain 1, configure UPE C as the transit node, and then specify primary and secondary ports.

```
<UPEC> system-view
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEC-rrpp-domain-region1] ring 1 enable
[UPEC-rrpp-domain-region1] quit
```

# In ring 1 of domain 2, configure UPE C as the transit node, and then specify primary and secondary ports.

```
<UPEC> system-view
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEC-rrpp-domain-region2] ring 1 enable
[UPEC-rrpp-domain-region2] quit
```

# In ring 2 of domain 1, configure UPE C as the assistant edge node, GE 0/0/2 as the common port, and GE 0/0/3 as the edge port.

```
<UPEC> system-view
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 2 node-mode assistant-edge common-port
GigabitEthernet 0/0/2 edge-port GigabitEthernet 0/0/3
[UPEC-rrpp-domain-region1] ring 2 enable
[UPEC-rrpp-domain-region1] quit
```

# In ring 2 of domain 2, configure UPE C as the assistant edge node, GE 0/0/2 as the common port, and GE 0/0/3 as the edge port.

```
<UPEC> system-view
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 2 node-mode assistant-edge common-port
GigabitEthernet 0/0/2 edge-port GigabitEthernet 0/0/3
[UPEC-rrpp-domain-region2] ring 2 enable
[UPEC-rrpp-domain-region2] quit
```

# In ring 3 of domain 1, configure UPE C as the assistant edge node, GE 0/0/1 as the common port, and GE 0/0/4 as the edge port.

```
<UPEC> system-view
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 3 node-mode assistant-edge common-port
GigabitEthernet 0/0/2 edge-port GigabitEthernet 0/0/4
[UPEC-rrpp-domain-region1] ring 3 enable
[UPEC-rrpp-domain-region1] quit
```

# In ring 3 of domain 2, configure UPE C as the assistant edge node, GE 0/0/2 as the common port, and GE 0/0/4 as the edge port.

```
<UPEC> system-view
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 3 node-mode assistant-edge common-port
GigabitEthernet 0/0/2 edge-port GigabitEthernet 0/0/4
```

```
[UPEC-rrpp-domain-region2] ring 3 enable
[UPEC-rrpp-domain-region2] quit
```

- Configure UPE D.

# In ring 1 of domain 1, configure UPE D as a transit node, and then specify primary and secondary ports.

```
<UPED> system-view
[UPED] rrpp domain 1
[UPED-rrpp-domain-region1] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPED-rrpp-domain-region1] ring 1 enable
[UPED-rrpp-domain-region1] quit
```

# In ring 1 of domain 2, configure UPE D as a transit node, and then specify primary and secondary ports.

```
<UPED> system-view
[UPED] rrpp domain 2
[UPED-rrpp-domain-region2] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPED-rrpp-domain-region2] ring 1 enable
[UPED-rrpp-domain-region2] quit
```

- Configure PE-AGG.

# In ring 1 of domain 1, configure the PE-AGG as the master node, and specify GE 0/0/1 as the primary port and GE 0/0/2 as the secondary port.

```
<PE-AGG> system-view
[PE-AGG] rrpp domain 1
[PE-AGG-rrpp-domain-region1] ring 1 node-mode master primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[PE-AGG-rrpp-domain-region1] ring 1 enable
[PE-AGG-rrpp-domain-region1] quit
```

# In ring 1 of domain 2, configure the PE-AGG as the master node, and specify GE 0/0/2 as the primary port and specify GE 0/0/1 as the secondary port.

```
<PE-AGG> system-view
[PE-AGG] rrpp domain 2
[PE-AGG-rrpp-domain-region2] ring 1 node-mode master primary-port
GigabitEthernet 0/0/2 secondary-port GigabitEthernet 0/0/1 level 0
[PE-AGG-rrpp-domain-region2] ring 1 enable
[PE-AGG-rrpp-domain-region2] quit
```

## Step 5 Enable RRPP.

After configuring an RRPP ring, enable RRPP on each node on the ring. In this manner, the RRPP ring can be activated. The configuration procedure is as follows:

- Configure CE1.

# Enable RRPP.

```
<CE1> system-view
[CE1] rrpp enable
```

- Configure CE2.

# Enable RRPP.

```
<CE2> system-view
[CE2] rrpp enable
```

- Configure UPE A.

# Enable RRPP.

```
<UPEA> system-view
[UPEA] rrpp enable
```

- Configure UPE B.

# Enable RRPP.

```
<UPEB> system-view
[UPEB] rrpp enable
```

- Configure UPE C.

# Enable RRPP.

```
<UPEC> system-view
[UPEC] rrpp enable
```

- Configure UPE D.

# Enable RRPP.

```
<UPED> system-view
[UPED] rrpp enable
```

- Configure PE-AGG.

# Enable RRPP.

```
<PE-AGG> system-view
[PE-AGG] rrpp enable
```

#### Step 6 Configure ring groups.

- Configure UPE B (edge node).

# Create ring group 1, which includes four sub-rings, namely, ring 2 in domain 1, ring 3 in domain 1, ring 2 in domain 2, and ring 3 in domain 2.

```
<UPEB> system-view
[UPEB] rrpp ring-group 1
[UPEB-rrpp-ring-group1] domain 1 ring 2 to 3
[UPEB-rrpp-ring-group1] domain 2 ring 2 to 3
[UPEB-rrpp-ring-group1] quit
```

- Configure UPE C (assistant edge node)

# Create ring group 1, which includes four sub-rings, namely, ring 2 in domain 1, ring 3 in domain 1, ring 2 in domain 2, and ring 3 in domain 2.

```
<UPEC> system-view
[UPEC] rrpp ring-group 1
[UPEC-rrpp-ring-group1] domain 1 ring 2 to 3
[UPEC-rrpp-ring-group1] domain 2 ring 2 to 3
[UPEC-rrpp-ring-group1] quit
```

#### Step 7 Configure the timer that defines the delay for the link to go Up.

- Configure CE1.

# Set the delay for RRPP link restoration to 2 seconds.

```
<CE1> rrpp linkup-delay-timer 2
```

- Configure CE2.

# Set the delay for RRPP link restoration to 2 seconds.

```
<CE2> rrpp linkup-delay-timer 2
```

- Configure PE-AGG.

# Set the delay for RRPP link restoration to 2 seconds.

```
<PE-AGG> rrpp linkup-delay-timer 2
```

#### Step 8 Verify the configuration.

After the previous configuration, run the following commands to verify the configuration. Take the display on UPE B and the PE-AGG as an example.

- Run the **display rrpp brief** command on UPE B. The following results are displayed:

```
<UPEB> display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge
```

```
RRPP Protocol Status: Enable
RRPP Linkup Delay Timer: 0 sec(default is 0 sec)
Number of RRPP Domains: 2

Domain Index : 1
Control VLAN : major 1 sub 2
Protected VLAN : Reference Instance 1
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)
 Ring Ring Node Primary/Common Secondary/Edge Is
 ID Level Mode Port Port
Enabled

--
 1 0 T GigabitEthernet0/0/1 GigabitEthernet0/0/2 Yes
 2 1 E GigabitEthernet0/0/1 GigabitEthernet0/0/3 Yes
 3 1 E GigabitEthernet0/0/1 GigabitEthernet0/0/4 Yes

Domain Index : 2
Control VLAN : major 10 sub 11
Protected VLAN: Reference Instance 2
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)
 Ring Ring Node Primary/Common Secondary/Edge Is
 ID Level Mode Port Port
Enabled

--
 1 0 T GigabitEthernet0/0/1 GigabitEthernet0/0/2 Yes
 2 1 E GigabitEthernet0/0/1 GigabitEthernet0/0/3 Yes
 3 1 E GigabitEthernet0/0/1 GigabitEthernet0/0/4 Yes
```

You can view that RRPP is enabled on UPE A.

In domain 1:

The major control VLAN is VLAN 1, and the protected VLAN is the VLAN mapped to instance 1.

In ring 1 of domain 1, the transit node is UPE B, the primary port is GE 0/0/1, and the secondary port is GE 0/0/2.

In ring 2 of domain 1, the edge node is UPE B, the common port is GE 0/0/1, and the edge port is GE 0/0/3.

In ring 3 of domain 1, the edge node is UPE B, the common port is GE 0/0/1, and the edge port is GE 0/0/4.

In domain 2:

The major control VLAN is VLAN 10, and the protected VLAN is the VLAN mapped to instance 2.

In ring 1 of domain 2, the transit node is UPE B, the primary port is GE 0/0/1, and the secondary port is GE 0/0/2.

In ring 2 of domain 2, the edge node is UPE B, the common port is GE 0/0/1, and the edge port is GE 0/0/3.

In ring 3 of domain 2, the edge node is UPE B, the common port is GE 0/0/1, and the edge port is GE 0/0/4.

- Run the **display rrpp brief** command on the PE-AGG. The following results are displayed:

```
<PE-AGG> display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
RRPP Linkup Delay Timer: 2 sec(default is 0 sec)
```

**Number of RRPP Domains: 2**

```

Domain Index : 1
Control VLAN : major 1 sub 2
Protected VLAN: Reference Instance 1
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)
 Ring Ring Node Primary/Common Secondary/Edge Is
 ID Level Mode Port Port
Enabled

```

```

--
1 0 M GigabitEthernet0/0/1 GigabitEthernet0/0/2 Yes

```

```

Domain Index : 2
Control VLAN : major 10 sub 11
Protected VLAN: Reference Instance 2
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)
 Ring Ring Node Primary/Common Secondary/Edge Is
 ID Level Mode Port Port
Enabled

```

```

--
1 0 M GigabitEthernet0/0/2 GigabitEthernet0/0/1 Yes

```

You can view that RRPP is enabled on UPE B, and the delay for the link to go Up is set to two seconds.

In domain 1, the major control VLAN is VLAN 1, the protected VLAN is the VLAN mapped to instance 1, and the transit node of ring 1 is the PE-AGG. In addition, the primary port is GE 0/0/1, and the secondary port is GE 0/0/2.

In domain 2, the major control VLAN is VLAN 10, the protected VLAN is the VLAN mapped to instance 2, and the master node of ring 1 is the PE-AGG. In addition, the primary port is GE 0/0/2, and the secondary port is GE 0/0/1.

- On UPE B, run the **display rrpp verbose domain** command. The following results are displayed.

# View detailed information about UPE B in domain 1.

```

<UPEB> display rrpp verbose domain 1
Domain Index : 1
Control VLAN : major 1 sub 2
Protected VLAN: Reference Instance 1
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)

RRPP Ring : 1
Ring Level : 0
Node Mode : TransitRing State : LinkUp
Is Enabled : Enable Is Activated : Yes
Primary port : GigabitEthernet0/0/1 Port status: UP
Secondary port: GigabitEthernet0/0/2 Port status: UP

RRPP Ring : 2
Ring Level : 1
Node Mode : EdgeRing State : LinkUp
Is Enabled : Enable Is Activated : Yes
Common port : GigabitEthernet0/0/1 Port status: UP
Edge port : GigabitEthernet0/0/3 Port status: UP

RRPP Ring : 3
Ring Level : 1
Node Mode : Edge
Ring State : LinkUp
Is Enabled : Enable Is Activated : Yes
Common port : GigabitEthernet0/0/1 Port status: UP
Edge port : GigabitEthernet0/0/4 Port status: UP

```

In domain 1, the control VLAN is VLAN 1, and the protected VLAN is the VLAN mapped to instance 1.

In ring 1 of domain 1, the transit node is UPE B, and the node status is LinkUp.

In ring 2 of domain 1, the edge node is UPE B, and the node status is LinkUp. The common port is GE 0/0/1, and the edge port is GE 0/0/3.

In ring 3 of domain 1, the edge node is UPE B, and the node status is LinkUp. The common port is GE 0/0/1, and the edge port is GE 0/0/4.

# View detailed information about UPE B in domain 2.

```
<UPEB> display rrpp verbose domain 2
Domain Index : 2
Control VLAN : major 10 sub 11
Protected VLAN: Reference Instance 2
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)

RRPP Ring : 1
Ring Level : 0
Node Mode : Transit
Ring State : LinkUp
Is Enabled : Enable Is Activated : Yes
Primary port : GigabitEthernet0/0/1 Port status: UP
Secondary port : GigabitEthernet0/0/2 Port status: UP

RRPP Ring : 2
Ring Level : 1
Node Mode : Edge
Ring State : LinkUp
Is Enabled : Enable Is Activated : Yes
Common port : GigabitEthernet0/0/1 Port status: UP
Edge port : GigabitEthernet0/0/3 Port status: UP

RRPP Ring : 3
Ring Level : 1
Node Mode : Edge
Ring State : LinkUp
Is Enabled : Enable Is Activated : Yes
Common port : GigabitEthernet0/0/1 Port status: UP
Edge port : GigabitEthernet0/0/4 Port status: UP
```

In domain 2, the control VLAN is VLAN 10, and the protected VLAN is the VLAN mapped to instance 2.

In ring 1 of domain 2, the transit node is UPE B, and the node status is LinkUp.

In ring 2 of domain 2, the edge node is UPE B, and the node status is LinkUp. The common port is GE 0/0/1, and the edge port is GE 0/0/3.

In ring 3 of domain 2, the edge node is UPE B, and the node status is LinkUp. The common port is GE 0/0/1, and the edge port is GE 0/0/4.

- Run the **display rrpp verbose domain** command on the PE-AGG. The following results are displayed:

# View detailed information about the PE-AGG in domain 1.

```
<PE-AGG> display rrpp verbose domain 1
Domain Index : 1
Control VLAN : major 1 sub 2
Protected VLAN: Reference Instance 1
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)

RRPP Ring : 1
Ring Level : 0
Node Mode : Master
Ring State : Complete
Is Enabled : Enable Is Activated : Yes
Primary port : GigabitEthernet0/0/1 Port status: UP
Secondary port : GigabitEthernet0/0/2 Port status: BLOCKED
```

In domain 1, the control VLAN is VLAN 1, and the protected VLAN is the VLAN mapped to instance 1.

The master node is the PE-AGG, and the node status is Complete.

The primary port is GE 0/0/1, and the secondary port is GE 0/0/2.

# View detailed information about the PE-AGG in domain 2.

```
<PE-AGG> display rrpp verbose domain 2
Domain Index : 2
Control VLAN : major 10 sub 11
Protected VLAN: Reference Instance 2
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)

RRPP Ring : 1
Ring Level : 0
Node Mode : Master
Ring State : Complete
Is Enabled : Enable Is Activated : Yes
Primary port : GigabitEthernet0/0/2 Port status: UP
Secondary port : GigabitEthernet0/0/1 Port status: BLOCKED
```

In domain 2, the control VLAN is VLAN 10, and the protected VLAN is the VLAN mapped to instance 2.

The master node is the PE-AGG, and the node status is Complete.

The primary port is GE 0/0/2, and the secondary port is GE 0/0/1.

- Run the **display rrpp ring-group** command on UPE B. The configuration of the ring group is displayed as follows:

# Display information about ring group 1.

```
<UPEB> display rrpp ring-group 1
Ring Group 1:
```

```
domain 1 ring 2 to 3
domain 2 ring 2 to 3
```

----End

## Configuration Files

- Configuration file of CE1

```
#
sysname CE1
#
vlan batch 1 to 2 10 to 11 100 to 300
#
rrpp enable
rrpp linkup-delay-timer 2
#
stp region-configuration
instance 1 vlan 1 to 2 100 to 200
instance 2 vlan 10 to 11 201 to 300
active region-configuration
#
rrpp domain 1
control-vlan 1
protected-vlan reference-instance 1
ring 2 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 1
ring 2 enable
rrpp domain 2
```

```

control-vlan 10
protected-vlan reference-instance 2
ring 2 node-mode master primary-port GigabitEthernet 0/0/2 secondary-port
GigabitEthernet 0/0/1 level 1
ring 2 enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 2 11 100 to 300
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 2 11 100 to 300
stp disable
#
return

```

- Configuration file of CE2

```

#
sysname CE2
#
vlan batch 1 to 2 10 to 11 100 to 300
#
rrpp enable
rrpp linkup-delay-timer 2
#
stp region-configuration
instance 1 vlan 1 to 2 100 to 200
instance 2 vlan 10 to 11 201 to 300
active region-configuration
#
rrpp domain 1
control-vlan 1
protected-vlan reference-instance 1
ring 3 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 1
ring 3 enable
rrpp domain 2
control-vlan 10
protected-vlan reference-instance 2
ring 3 node-mode master primary-port GigabitEthernet 0/0/2 secondary-port
GigabitEthernet 0/0/1 level 1
ring 3 enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 2 11 100 to 300
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 2 11 100 to 300
stp disable
#
Return

```

- Configuration file of UPE A

```

#
sysname UPEA
#
vlan batch 1 to 2 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
instance 1 vlan 1 to 2 100 to 200
instance 2 vlan 10 to 11 201 to 300
active region-configuration
#
rrpp domain 1
control-vlan 1
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port

```

```
GigabitEthernet 0/0/2 level 0
 ring 1 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
 stp disable
#
return
```

- Configuration file of UPE B

```
#
sysname UPEB
#
vlan batch 1 to 2 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 1 to 2 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 1
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
 ring 1 enable
 ring 2 node-mode edge common-port GigabitEthernet 0/0/1 edge-port
GigabitEthernet 0/0/3
 ring 2 enable
 ring 3 node-mode edge common-port GigabitEthernet 0/0/1 edge-port
GigabitEthernet 0/0/4
 ring 3 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
 ring 1 enable
 ring 2 node-mode edge common-port GigabitEthernet 0/0/1 edge-port
GigabitEthernet 0/0/3
 ring 2 enable
 ring 3 node-mode edge common-port GigabitEthernet 0/0/1 edge-port
GigabitEthernet 0/0/4
 ring 3 enable
#
rrpp ring group 1
 domain 1 ring 2 to 3
 domain 2 ring 2 to 3
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/3
```

```

 port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/4
 port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
 stp disable
#
return

```

- Configuration file of UPE C

```

#
sysname UPEC
#
vlan batch 1 to 2 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 1 to 2 100 to 200
 instance 2 vlan 10 to 11 201 to 300
 active region-configuration
#
rrpp domain 1
 control-vlan 1
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge common-port GigabitEthernet 0/0/2 edge-port
GigabitEthernet 0/0/3
 ring 2 enable
 ring 3 node-mode assistant-edge common-port GigabitEthernet 0/0/2 edge-port
GigabitEthernet 0/0/4
 ring 3 enable
rrpp domain 2
 control-vlan 10
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge common-port GigabitEthernet 0/0/2 edge-port
GigabitEthernet 0/0/3
 ring 2 enable
 ring 3 node-mode assistant-edge common-port GigabitEthernet 0/0/2 edge-port
GigabitEthernet 0/0/4
 ring 3 enable
#
rrpp ring group 1
 domain 1 ring 2 to 3
 domain 2 ring 2 to 3
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/3
 port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
 stp disable
#
interface GigabitEthernet0/0/4
 port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
 stp disable
#
Return

```

- Configuration file of UPE D

```
#
sysname UPED
#
vlan batch 1 to 2 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
instance 1 vlan 1 to 2 100 to 200
instance 2 vlan 10 to 11 201 to 300
active region-configuration
#
rrpp domain 1
control-vlan 1
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
rrpp domain 2
control-vlan 10
protected-vlan reference-instance 2
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
return
```

- Configuration file of PE-AGG

```
#
sysname PE-AGG
#
vlan batch 1 to 2 10 to 11 100 to 300
#
rrpp enable
rrpp linkup-delay-timer 2
#
stp region-configuration
instance 1 vlan 1 to 2 100 to 200
instance 2 vlan 10 to 11 201 to 300
active region-configuration
#
rrpp domain 1
control-vlan 1
protected-vlan reference-instance 1
ring 1 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
rrpp domain 2
control-vlan 10
protected-vlan reference-instance 2
ring 1 node-mode master primary-port GigabitEthernet 0/0/2 secondary-port
GigabitEthernet 0/0/1 level 0
ring 1 enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
```

```

return
```

## 10.5.7 Example for Configuring the Tangent RRPP Ring of Multi-Instance

### Networking Requirements

As shown in [Figure 10-8](#), UPE A, UPE B, UPE C, and UPE D form an RRPP multi-instance ring that includes ring 1 in domain 1 and ring 1 in domain 2. UPE D, UPE E, UPE F, and UPE G form RRPP ring 1 in domain 3. The packets of data VLANs are sent from CEs to the two tangent rings, and then sent to the backbone network by UPE F.

UPE D is the tangent point of the two physical rings.

The VLANs accessing the tangent rings through CEs range from VLAN 100 to VLAN 300. The packets of VLANs 100 to 300 are balanced in domain 1 and domain 2. The packets of VLANs 100 to 200 and VLANs 201 to 300 are processed in domain 1 and domain 2 respectively.

For details of the protected VLANs and the instance to which protected VLANs are mapped in domain 1, domain 2, and domain 3, refer to [Table 10-6](#).

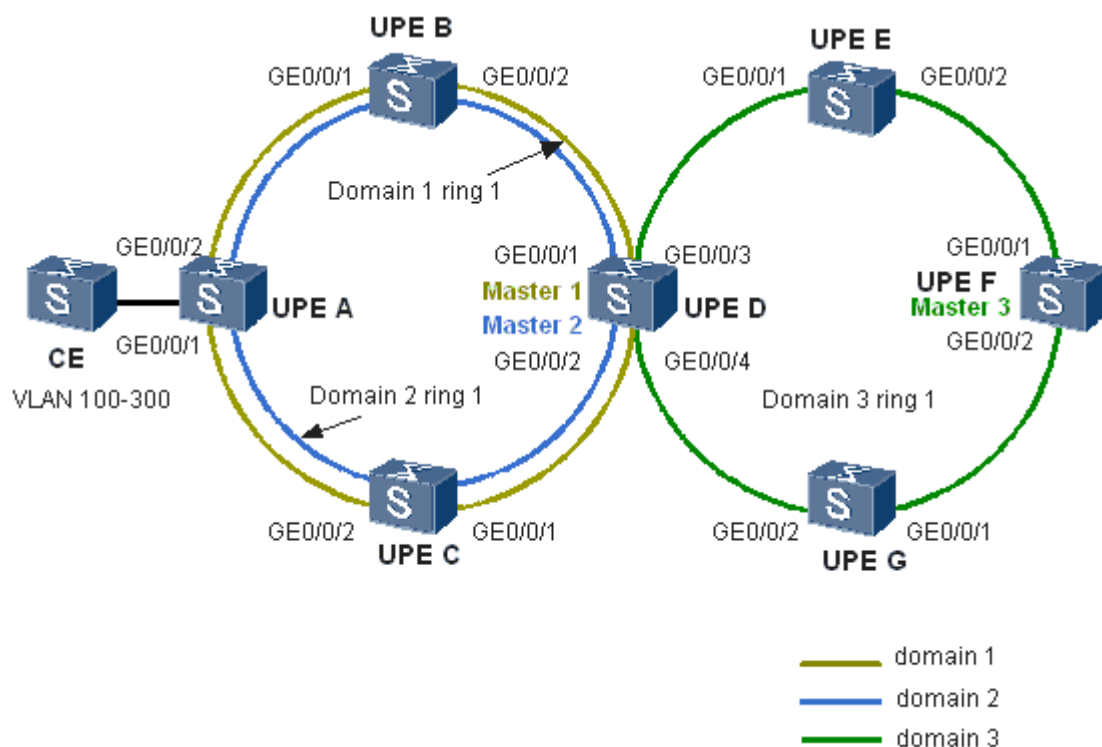
**Table 10-6** Mapping between protected VLANs and instances

| Domain ID        | Control VLAN ID | Instance ID of Control VLAN | Data VLAN ID    | Instance ID of Data VLAN  |
|------------------|-----------------|-----------------------------|-----------------|---------------------------|
| Domain 1         | VLAN 1 to 2     | Instance 1                  | VLAN 100 to 200 | Instance 1                |
| Domain 2         | VLAN 10 to 11   | Instance 2                  | VLAN 201 to 300 | Instance 2                |
| Domain 3 (UPE D) | VLAN 20 to 21   | Instance 3                  | VLAN 100 to 300 | Instance 1 and instance 2 |
| Domain 3         | VLAN 20 to 21   | Instance 1                  | VLAN 100 to 300 | Instance 1                |

For details of the master node and primary and secondary ports on the master node in the three rings, refer to [Table 10-7](#).

**Table 10-7** Information about the master node, primary port, and secondary port

| Ring ID            | Master Node | Primary Port | Secondary Port |
|--------------------|-------------|--------------|----------------|
| Ring 1 in domain 1 | UPE D       | GE 0/0/1     | GE 0/0/2       |
| Ring 1 in domain 2 | UPE D       | GE 0/0/2     | GE 0/0/1       |
| Ring 1 in domain 3 | UPE F       | GE 0/0/1     | GE 0/0/2       |

**Figure 10-8** Networking diagram of configuring the tangent RRPP ring of multi-instance

## Configuration Roadmap

The configuration roadmap is as follows:

1. Map VLANs 100 to 200 to instance 1 and VLANs 201 to 300 to instance 2.
2. Deploy UPE A, UPE B, UPE C, and UPE D in ring 1 of domain 1 and ring 1 of domain 2.
3. Deploy UPE D, UPE E, UPE F, and UPE G in ring 1 of domain 3.
4. Configure protected VLANs for domain 1 and domain 2.
5. Configure control VLANs for domain 1 and domain 2.
6. Configure control VLANs for domain 3.
7. Configure UPE D as the master node and UPE A, UPE B, and UPE C as transit nodes in ring 1 of domain 1 and ring 1 of domain 2.
8. Configure UPE F as the master node and UPE D, UPE E, and UPE G as transit nodes in ring 1 of domain 3.

## Data Preparation

To complete the configuration, you need the following data:

- IDs of instances
- Range of protected VLANs
- IDs of control VLANs
- Number of the RRPP interface

## Procedure

### Step 1 Create instances.

- Configure UPE A.
  - # Create data VLANs 100 to 300 on UPE A.

```
<UPEA> system-view
[UPEA] vlan batch 100 to 300
```
  - # Create instance 1, and map data VLANs 100 to 200 and the control VLAN 1 to 2 in domain 1 to instance 1.

```
[UPEA] stp region-configuration
[UPEA-mst-region] instance 1 vlan 1 2 100 to 200
```
  - # Create instance 2, and map data VLANs 201 to 300 and the control VLAN 10 to 11 in domain 2 to instance 2.

```
[UPEA-mst-region] instance 2 vlan 10 11 201 to 300
```
  - # Activate the configurations.

```
[UPEA-mst-region] active region-configuration
```
- Configure UPE B.
  - # Create data VLANs 100 to 300 on UPE B.

```
<UPEB> system-view
[UPEB] vlan batch 100 to 300
```
  - # Create instance 1, and map data VLANs 100 to 200 and the control VLAN 1 to 2 in domain 1 to instance 1.

```
[UPEB] stp region-configuration
[UPEB-mst-region] instance 1 vlan 1 2 100 to 200
```
  - # Create instance 2, and map data VLANs 201 to 300 and the control VLAN 10 to 11 in domain 2 to instance 2.

```
[UPEB-mst-region] instance 2 vlan 10 11 201 to 300
```
  - # Activate the configurations.

```
[UPEB-mst-region] active region-configuration
```
- Configure UPE C.
  - # Create data VLANs 100 to 300 on UPE C.

```
<UPEC> system-view
[UPEC] vlan batch 100 to 300
```
  - # Create instance 1, and map data VLANs 100 to 200 and the control VLAN 1 to 2 in domain 1 to instance 1.

```
[UPEC] stp region-configuration
[UPEC-mst-region] instance 1 vlan 1 2 100 to 200
```
  - # Create instance 2, and map data VLANs 201 to 300 and the control VLAN 10 to 11 in domain 2 to instance 2.

```
[UPEC-mst-region] instance 2 vlan 10 11 201 to 300
```
  - # Activate the configurations.

```
[UPEC-mst-region] active region-configuration
```
- # Configure UPE D.
  - # Create data VLANs 100 to 300 on UPE D.

```
<UPED> system-view
[UPED] vlan batch 100 to 300
```
  - # Create instance 1, and map data VLANs 100 to 200 and the control VLAN 1 to 2 in domain 1 to instance 1.

```
[UPED] stp region-configuration
[UPED-mst-region] instance 1 vlan 1 2 100 to 200

Create instance 2, and map data VLANs 201 to 300 and the control VLAN 10 to 11 in
domain 2 to instance 2.
[UPED-mst-region] instance 2 vlan 10 11 201 to 300

Create instance 3, and map the control VLAN 20 to 21 in domain 3 to instance 3.
[UPED-mst-region] instance 3 vlan 20 to 21

Activate the configurations.
[UPED-mst-region] active region-configuration
```

- # Configure UPE E.
 

```
Create data VLANs 100 to 300 on UPE E.
<UPEE> system-view
[UPEE] vlan batch 100 to 300

Create instance 1, and map data VLANs 100 to 300 and the control VLAN 20 to 21 in
domain 3 to instance 1.
[UPEE] stp region-configuration
[UPEE-mst-region] instance 1 vlan 20 to 21 100 to 300

Activate the configurations.
[PE-AGG-mst-region] active region-configuration
```
- # Configure UPE F.
 

```
Create data VLANs 100 to 300 on UPE F.
<UPEF> system-view
[UPEF] vlan batch 100 to 300

Create instance 1, and map data VLANs 100 to 300 and the control VLAN 20 to 21 in
domain 3 to instance 1.
[UPEF] stp region-configuration
[UPEF-mst-region] instance 1 vlan 20 to 21 100 to 300

Activate the configurations.
[UPEF-mst-region] active region-configuration
```
- # Configure UPE G.
 

```
Create data VLANs 100 to 300 on UPE G.
<UPEG> system-view
[UPEG] vlan batch 100 to 300

Create instance 1, and map data VLANs 100 to 300 and the control VLAN 20 to 21 in
domain 3 to instance 1.
[UPEG] stp region-configuration
[UPEG-mst-region] instance 1 vlan 20 to 21 100 to 300

Activate the configurations.
[UPEG-mst-region] active region-configuration
```
- Verify the configuration.
 

After the configurations, perform the following procedures to check the mapping between instances and VLANs. Take the display on UPE A as an example.

```
<UPEA> display stp region-configuration
Oper configuration
Format selector :0
Region name :00e0cd568d00
Revision level :0

Instance Vlans Mapped
0 3 to 9, 12 to 99, 301 to 4094
```

```

1 1 to 2, 100 to 200
2 10 to 11, 201 to 300

```

## Step 2 Configure the port to be added into the RRPP ring.

- Configure UPE A.

# On UPE A, disable the STP function on the interface to be added into the RRPP ring.  
Configure the port to allow packets of VLANs 100 to 300 to pass.

```

<UPEA> system-view
[UPEA] interface GigabitEthernet 0/0/1
[UPEA-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/1] stp disable
[UPEA-GigabitEthernet0/0/1] quit
[UPEA] interface GigabitEthernet 0/0/2
[UPEA-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEA-GigabitEthernet0/0/2] stp disable
[UPEA-GigabitEthernet0/0/2] quit

```

- Configure UPE B.

# On UPE B, disable the STP function on the interface to be added into in the RRPP ring.  
Configure the port to allow packets of VLANs 100 to 300 to pass.

```

<UPEB> system-view
[UPEB] interface GigabitEthernet 0/0/1
[UPEB-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/1] stp disable
[UPEB-GigabitEthernet0/0/1] quit
[UPEB] interface GigabitEthernet 0/0/2
[UPEB-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEB-GigabitEthernet0/0/2] stp disable
[UPEB-GigabitEthernet0/0/2] quit

```

- Configure UPE C.

# On UPE C, disable the STP function on the interface to be added into the RRPP ring.  
Configure the port to allow packets of VLANs 100 to 300 to pass.

```

<UPEC> system-view
[UPEC] interface GigabitEthernet 0/0/1
[UPEC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/1] stp disable
[UPEC-GigabitEthernet0/0/1] quit
[UPEC] interface GigabitEthernet 0/0/2
[UPEC-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEC-GigabitEthernet0/0/2] stp disable
[UPEC-GigabitEthernet0/0/2] quit

```

- # Configure UPE D.

# On UPE D, disable the STP function on the interface to be added into the RRPP ring.  
Configure the port to allow packets of VLANs 100 to 300 to pass.

```

<UPED> system-view
[UPED] interface GigabitEthernet 0/0/1
[UPED-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPED-GigabitEthernet0/0/1] stp disable
[UPED-GigabitEthernet0/0/1] quit
[UPED] interface GigabitEthernet 0/0/2
[UPED-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPED-GigabitEthernet0/0/2] stp disable
[UPED-GigabitEthernet0/0/2] quit
[UPED] interface GigabitEthernet 0/0/3
[UPED-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 to 300
[UPED-GigabitEthernet0/0/3] stp disable
[UPED-GigabitEthernet0/0/3] quit
[UPED] interface GigabitEthernet 0/0/4
[UPED-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 300
[UPED-GigabitEthernet0/0/4] stp disable
[UPED-GigabitEthernet0/0/4] quit

```

- # Configure UPE E.

# On UPE E, disable the STP function on the interface to be added into the RRPP ring.  
Configure the port to allow packets of VLANs 100 to 300 to pass.

```
<UPEE> system-view
[UPEE] interface GigabitEthernet 0/0/1
[UPEE-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEE-GigabitEthernet0/0/1] stp disable
[UPEE-GigabitEthernet0/0/1] quit
[UPEE] interface GigabitEthernet 0/0/2
[UPEE-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEE-GigabitEthernet0/0/2] stp disable
[UPEE-GigabitEthernet0/0/2] quit
```

- # Configure UPE F.

# On UPE F, disable the STP function on the interface to be added into the RRPP ring.  
Configure the port to allow packets of VLANs 100 to 300 to pass.

```
<UPEF> system-view
[UPEF] interface GigabitEthernet 0/0/1
[UPEF-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEF-GigabitEthernet0/0/1] stp disable
[UPEF-GigabitEthernet0/0/1] quit
[UPEF] interface GigabitEthernet 0/0/2
[UPEF-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEF-GigabitEthernet0/0/2] stp disable
[UPEF-GigabitEthernet0/0/2] quit
```

- # Configure UPE G.

# On UPE G, disable the STP function on the interface to be added into in the RRPP ring.  
Configure the port to allow packets of VLANs 100 to 300 to pass.

```
<UPEG> system-view
[UPEG] interface GigabitEthernet 0/0/1
[UPEG-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 300
[UPEG-GigabitEthernet0/0/1] stp disable
[UPEG-GigabitEthernet0/0/1] quit
[UPEG] interface GigabitEthernet 0/0/2
[UPEG-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 300
[UPEG-GigabitEthernet0/0/2] stp disable
[UPEG-GigabitEthernet0/0/2] quit
```

### Step 3 Create an RRPP domain, and configure protected VLANs and control VLANs.

- Configure UPE A.

# Configure the protected VLANs of domain 1 as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<UPEA> system-view
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEA-rrpp-domain-region1] control-vlan 1
[UPEA-rrpp-domain-region1] quit
```

# Configure the protected VLANs of domain 2 as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<UPEA> system-view
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEA-rrpp-domain-region2] control-vlan 10
[UPEA-rrpp-domain-region2] quit
```

- Configure UPE B.

# Configure the protected VLANs of domain 1 as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<UPEB> system-view
[UPEB] rrpp domain 1
```

```
[UPEB-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEB-rrpp-domain-region1] control-vlan 1
[UPEB-rrpp-domain-region1] quit
```

# Configure the protected VLANs of domain 2 as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<UPEB> system-view
[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEB-rrpp-domain-region2] control-vlan 10
[UPEB-rrpp-domain-region2] quit
```

- Configure UPE C.

# Configure the protected VLANs of domain 1 as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<UPEC> system-view
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] protected-vlan reference-instance 1
[UPEC-rrpp-domain-region1] control-vlan 1
[UPEC-rrpp-domain-region1] quit
```

# Configure the protected VLANs of domain 2 as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<UPEC> system-view
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] protected-vlan reference-instance 2
[UPEC-rrpp-domain-region2] control-vlan 10
[UPEC-rrpp-domain-region2] quit
```

- # Configure UPE D.

# Configure the protected VLANs of domain 1 as the VLANs mapped to instance 1, and the control VLAN as VLAN 1.

```
<UPED> system-view
[UPED] rrpp domain 1
[UPED-rrpp-domain-region1] protected-vlan reference-instance 1
[UPED-rrpp-domain-region1] control-vlan 1
[UPED-rrpp-domain-region1] quit
```

# Configure the protected VLANs of domain 2 as the VLANs mapped to instance 2, and the control VLAN as VLAN 10.

```
<UPED> system-view
[UPED] rrpp domain 2
[UPED-rrpp-domain-region2] protected-vlan reference-instance 2
[UPED-rrpp-domain-region2] control-vlan 10
[UPED-rrpp-domain-region2] quit
```

# Configure the protected VLANs of domain 3 as the VLANs mapped to instance 1 to instance 3, and the control VLAN as VLAN 20.

```
<UPED> system-view
[UPED] rrpp domain 3
[UPED-rrpp-domain-region3] protected-vlan reference-instance 1 2 3
[UPED-rrpp-domain-region3] control-vlan 20
[UPED-rrpp-domain-region3] quit
```

- # Configure UPE E.

# Configure VLAN 20 as the control VLAN of domain 3.

```
<UPEE> system-view
[UPEE] rrpp domain 3
[UPEE-rrpp-domain-region3] protected-vlan reference-instance 1
[UPEE-rrpp-domain-region3] control-vlan 20
[UPEE-rrpp-domain-region3] quit
```

- # Configure UPE F.

# Configure VLAN 20 as the control VLAN of domain 3.

```

<UPEF> system-view
[UPEF] rrpp domain 3
[UPEF-rrpp-domain-region3] protected-vlan reference-instance 1
[UPEF-rrpp-domain-region3] control-vlan 20
[UPEF-rrpp-domain-region3] quit

```

- # Configure UPE G.

# Configure VLAN 20 as the control VLAN of domain 3.

```

<UPEG> system-view
[UPEG] rrpp domain 3
[UPEG-rrpp-domain-region3] protected-vlan reference-instance 1
[UPEG-rrpp-domain-region3] control-vlan 20
[UPEG-rrpp-domain-region3] quit

```

#### Step 4 Create RRPP rings.

- Configure UPE A.

# In ring 1 of domain 1, configure UPE A as a transit node and specify primary and secondary ports.

```

<UPEA> system-view
[UPEA] rrpp domain 1
[UPEA-rrpp-domain-region1] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEA-rrpp-domain-region1] ring 1 enable
[UPEA-rrpp-domain-region1] quit

```

# In ring 1 of domain 2, configure UPE A as a transit node and specify primary and secondary ports.

```

<UPEA> system-view
[UPEA] rrpp domain 2
[UPEA-rrpp-domain-region2] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEA-rrpp-domain-region2] ring 1 enable
[UPEA-rrpp-domain-region2] quit

```

- Configure UPE B.

# In ring 1 of domain 1, configure UPE B as a transit node and specify primary and secondary ports.

```

<UPEB> system-view
[UPEB] rrpp domain 1
[UPEB-rrpp-domain-region1] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEB-rrpp-domain-region1] ring 1 enable
[UPEB-rrpp-domain-region1] quit

```

# In ring 1 of domain 2, configure UPE B as a transit node and specify primary and secondary ports.

```

<UPEB> system-view
[[UPEB] rrpp domain 2
[UPEB-rrpp-domain-region2] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEB-rrpp-domain-region2] ring 1 enable
[UPEB-rrpp-domain-region2] quit

```

- Configure UPE C.

# In ring 1 of domain 1, configure UPE C as a transit node and specify primary and secondary ports.

```

<UPEC> system-view
[UPEC] rrpp domain 1
[UPEC-rrpp-domain-region1] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEC-rrpp-domain-region1] ring 1 enable
[UPEC-rrpp-domain-region1] quit

```

# In ring 1 of domain 2, configure UPE C as a transit node of and specify primary and secondary ports.

```
<UPEC> system-view
[UPEC] rrpp domain 2
[UPEC-rrpp-domain-region2] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEC-rrpp-domain-region2] ring 1 enable
[UPEC-rrpp-domain-region2] quit
```

- Configure UPE D.

# In ring 1 of domain 1, configure UPE D as a transit node and specify primary and secondary ports.

```
<UPED> system-view
[UPED] rrpp domain 1
[UPED-rrpp-domain-region1] ring 1 node-mode master primary-port GigabitEthernet
0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPED-rrpp-domain-region1] ring 1 enable
[UPED-rrpp-domain-region1] quit
```

# In ring 1 of domain 2, configure UPE D as a transit node and specify primary and secondary ports.

```
<UPED> system-view
[UPED] rrpp domain 2
[UPED-rrpp-domain-region2] ring 1 node-mode master primary-port GigabitEthernet
0/0/2 secondary-port GigabitEthernet 0/0/1 level 0
[UPED-rrpp-domain-region2] ring 1 enable
[UPED-rrpp-domain-region2] quit
```

# In ring 1 of domain 3, configure UPE D as a transit node and specify primary and secondary ports.

```
<UPED> system-view
[UPED] rrpp domain 3
[UPED-rrpp-domain-region3] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/3 secondary-port GigabitEthernet 0/0/4 level 0
[UPED-rrpp-domain-region3] ring 1 enable
[UPED-rrpp-domain-region3] quit
```

- Configure UPE E.

# In ring 1 of domain 3, configure UPE E as a transit node and specify primary and secondary ports.

```
<UPEE> system-view
[UPEE] rrpp domain 3
[UPEE-rrpp-domain-region3] ring 1 node-mode transit primary-port
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEE-rrpp-domain-region3] ring 1 enable
[UPEE-rrpp-domain-region3] quit
```

- Configure UPE F.

# In ring 1 of domain 3, configure UPE F as a transit node and specify primary and secondary ports.

```
<UPEF> system-view
[UPEF] rrpp domain 3
[UPEF-rrpp-domain-region3] ring 1 node-mode master primary-port GigabitEthernet
0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEF-rrpp-domain-region3] ring 1 enable
[UPEF-rrpp-domain-region3] quit
```

- Configure UPE G.

# In ring 1 of domain 3, configure UPE G as a transit node and specify primary and secondary ports.

```
<UPEG> system-view
[UPEG] rrpp domain 3
[UPEG-rrpp-domain-region3] ring 1 node-mode transit primary-port
```

```
GigabitEthernet 0/0/1 secondary-port GigabitEthernet 0/0/2 level 0
[UPEG-rrpp-domain-region3] ring 1 enable
[UPEG-rrpp-domain-region3] quit
```

**Step 5** Enable RRPP.

After configuring an RRPP ring, enable RRPP on each node in the ring. In this manner, the RRPP ring can be activated. The configuration procedure is as follows:

- Configure UPE A.  
# Enable RRPP.  

```
<UPEA> system-view
[UPEA] rrpp enable
```
- Configure UPE B.  
# Enable RRPP.  

```
<UPEB> system-view
[UPEB] rrpp enable
```
- Configure UPE C.  
# Enable RRPP.  

```
<UPEC> system-view
[UPEC] rrpp enable
```
- Configure UPE D.  
# Enable RRPP.  

```
<UPED> system-view
[UPED] rrpp enable
```
- Configure UPE E.  
# Enable RRPP.  

```
<UPEE> system-view
[UPEE] rrpp enable
```
- Configure UPE F.  
# Enable RRPP.  

```
<UPEF> system-view
[UPEF] rrpp enable
```
- Configure UPE G.  
# Enable RRPP.  

```
<UPEG> system-view
[UPEG] rrpp enable
```

**Step 6** Verify the configuration.

After the previous configurations are performed and the network converges, run the following commands to verify the configuration. Take the display on UPE D for example:

- Run the **display rrpp brief** command on UPE D. The following results are displayed:  

```
<UPED> display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
RRPP Linkup Delay Timer: 0 sec(default is 0 sec)
Number of RRPP Domains: 3
Domain Index : 1
Control VLAN : major 1 sub 2
Protected VLAN : Reference Instance 1
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)
Ring Ring Node Primary/Common Secondary/Edge Is
```

```

ID Level Mode Port
Enabled

--
1 0 M GigabitEthernet0/0/1 GigabitEthernet0/0/2 Yes

Domain Index : 2
Control VLAN : major 10 sub 11
Protected VLAN: Reference Instance 2
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)
Ring Ring Node Primary/Common Secondary/Edge Is
ID Level Mode Port Port
Enabled

--
1 0 M GigabitEthernet0/0/2 GigabitEthernet0/0/1 Yes

Domain Index : 3
Control VLAN : major 20 sub 21
Protected VLAN: Reference Instance 0
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)
Ring Ring Node Primary/Common Secondary/Edge Is
ID Level Mode Port Port Enabled

--
1 0 T GigabitEthernet0/0/3 GigabitEthernet0/0/4 Yes

```

You can view that RRPP is enabled on UPE D.

In domain 1:

In the major ring, the control VLAN is VLAN 1 and the protected VLANs are the VLANs mapped to instance 1.

UPE D is the master node of ring 1, and the primary port and secondary port are GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 respectively.

In domain 2:

The control VLAN of the major ring is VLAN 10, and the protected VLANs are the VLANs mapped to instance 2.

UPE D is the master node of ring 1, and the primary port and secondary port are GigabitEthernet 0/0/2 and GigabitEthernet 0/0/1 respectively.

In domain 3:

The control VLAN of the major ring is VLAN 20, and the protected VLANs are the VLANs mapped to instance 0.

UPE D is the transit node of ring 1, and the primary port and secondary port are Gigabit Ethernet 1/0/1 and Gigabit Ethernet 2/0/1 respectively.

- Run the **display rrpp verbose domain** command on UPE D. The following results are displayed:

# View detailed information about UPE D in domain 1.

```

<UPED> display rrpp verbose domain 1
Domain Index : 1
Control VLAN : major 1 sub 2
Protected VLAN: Reference Instance 1
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)

RRPP Ring : 1
Ring Level : 0
Node Mode : Master
Ring State : Complete
Is Enabled : Enable Is Activated : Yes

```

```

Primary port : GigabitEthernet0/0/1 Port status: UP
Secondary port: GigabitEthernet0/0/2 Port status: BLOCKED

```

The control VLAN of domain 1 is VLAN 1, and the protected VLANs are the VLANs mapped to instance 1.

UPE D is the master node in domain 1, and the node status is Complete.

The primary port and secondary port are GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 respectively.

# View detailed information about UPE D in domain 2.

```

<UPED> display rrpp verbose domain 2
Domain Index : 2
Control VLAN : major 10 sub 11
Protected VLAN: Reference Instance 2
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)

RRPP Ring : 1
Ring Level : 0
Node Mode : Master
Ring State : Complete
Is Enabled : Enable Is Activated : Yes
Primary port : GigabitEthernet0/0/2 Port status: UP
Secondary port: GigabitEthernet0/0/1 Port status: BLOCKED

```

In domain 2, the control VLAN is VLAN 10 and the protected VLANs are the VLANs mapped to instance 2.

The master node in domain 2, and the node status is Complete.

The primary port and secondary port are GigabitEthernet 0/0/2 and GigabitEthernet 0/0/1 respectively.

# View detailed information about UPE D in domain 3.

```

<UPED> display rrpp verbose domain 3
Domain Index : 3
Control VLAN : major 20 sub 21
Protected VLAN: Reference Instance 0
Hello Timer : 1 sec(default is 1 sec) Fail Timer : 3 sec(default is 3 sec)

RRPP Ring : 1
Ring Level : 0
Node Mode : Transit
Ring State : LinkUp
Is Enabled : Enable Is Activated : Yes
Primary port : GigabitEthernet0/0/2 Port status: UP
Secondary port: GigabitEthernet0/0/1 Port status: UP

```

The control VLAN of domain 3 is VLAN 20, and the protected VLANs are the VLANs mapped to 0.

UPE D is the transit node in domain 3, and the node status is LinkUp.

The primary port and secondary port are GigabitEthernet 0/0/2 and GigabitEthernet 0/0/1 respectively.

----End

## Configuration Files

- Configuration file of UPE A

```

#
sysname UPEA
#
vlan batch 1 to 2 10 to 11 100 to 300
#
rrpp enable
#

```

```

stp region-configuration
instance 1 vlan 1 to 2 100 to 200
instance 2 vlan 10 to 11 201 to 300
active region-configuration
#
rrpp domain 1
control-vlan 1
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
rrpp domain 2
control-vlan 10
protected-vlan reference-instance 2
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
return

```

- Configuration file of UPE B

```

#
sysname UPEB
#
vlan batch 1 to 2 10 to 11 100 to 300
#
rrpp enable
#
stp region-configuration
instance 1 vlan 1 to 2 100 to 200
instance 2 vlan 10 to 11 201 to 300
active region-configuration
#
rrpp domain 1
control-vlan 1
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
rrpp domain 2
control-vlan 10
protected-vlan reference-instance 2
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
return

```

- Configuration file of UPE C

```

#
sysname UPEC
#
vlan batch 1 to 2 10 to 11 100 to 300
#

```

```

rrpp enable
#
stp region-configuration
instance 1 vlan 1 to 2 100 to 200
instance 2 vlan 10 to 11 201 to 300
active region-configuration
#
rrpp domain 1
control-vlan 1
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
rrpp domain 2
control-vlan 10
protected-vlan reference-instance 2
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
Return

```

- Configuration file of UPE D

```

#
sysname UPED
#
vlan batch 1 to 2 10 to 11 20 to 21 100 to 300
#
rrpp enable
#
stp region-configuration
instance 1 vlan 1 to 2 100 to 200
instance 2 vlan 10 to 11 201 to 300
instance 3 vlan 20 to 21
active region-configuration
#
rrpp domain 1
control-vlan 1
protected-vlan reference-instance 1
ring 1 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
rrpp domain 2
control-vlan 10
protected-vlan reference-instance 2
ring 1 node-mode master primary-port GigabitEthernet 0/0/2 secondary-port
GigabitEthernet 0/0/1 level 0
ring 1 enable
rrpp domain 3
control-vlan 20
protected-vlan reference-instance 1 2 3
ring 1 node-mode transit primary-port GigabitEthernet 0/0/3 secondary-port
GigabitEthernet 0/0/4 level 0
ring 1 enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 1 to 2 10 to 11 100 to 300
stp disable

```

```
#
interface GigabitEthernet0/0/3
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface GigabitEthernet0/0/4
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
```

- Configuration file of UPE E

```
#
sysname UPEE
#
vlan batch 20 to 21 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 20 to 21 100 to 300
 active region-configuration
#
rrpp domain 3
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
```

- Configuration file of UPE F

```
#
sysname UPEF
#
vlan batch 20 to 21 100 to 300
#
rrpp enable
#
stp region-configuration
 instance 1 vlan 20 to 21 100 to 300
 active region-configuration
#
rrpp domain 3
 control-vlan 20
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
 ring 1 enable
#
interface GigabitEthernet0/0/1
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
interface GigabitEthernet0/0/2
 port trunk allow-pass vlan 20 to 21 100 to 300
 stp disable
#
return
```

- Configuration file of UPE G

```
#
sysname UPEG
#
vlan batch 20 to 21 100 to 300
#
rrpp enable
#
stp region-configuration
instance 1 vlan 20 to 21 100 to 300
active region-configuration
#
rrpp domain 3
control-vlan 20
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet 0/0/1 secondary-port
GigabitEthernet 0/0/2 level 0
ring 1 enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 20 to 21 100 to 300
stp disable
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 20 to 21 100 to 300
stp disable
#
return
```

# 11 BPDU Tunneling and Partitioned STP Configuration

---

## About This Chapter

This chapter describes the basics, methods, and examples for configuring Bridge Protocol Data Unit (BPDU) tunneling and partitioned Spanning Tree Protocol (STP).

### [11.1 Introduction](#)

This section describes basic concepts of BPDU tunneling and partitioned STP.

### [11.2 Configuring Interface-based Transparent Transmission of BPDUs from the Same Customer Network](#)

This section describes the procedure for configuring interface-based transparent transmission of BPDUs from the same customer network.

### [11.3 Configuring Interface-based Transparent Transmission of BPDUs from Different Customer Networks](#)

This section describes the procedure for configuring interface-based transparent transmission of BPDUs from different customer networks.

### [11.4 Configuring VLAN-based BPDU Tunneling](#)

This section describes the procedure for configuring VLAN-based BPDU tunneling.

### [11.5 Configuring QinQ-based BPDU Tunneling](#)

This section describes the procedure for configuring QinQ-based BPDU tunneling.

### [11.6 Configuring Partitioned STP](#)

This section describes the procedure for configuring partitioned STP.

### [11.7 Configuration Examples](#)

This section provides examples for configuring the Multiple Spanning Tree Protocol (MSTP), BPDU tunneling, and partitioned STP.

## 11.1 Introduction

This section describes basic concepts of BPDU tunneling and partitioned STP.

### 11.1.1 BPDU Tunneling

#### 11.1.2 Partitioned STP

#### 11.1.3 Logic Relationships Between Configuration Tasks

### 11.1.1 BPDU Tunneling

The S-switch can forward tagged BPDUs as common Layer 2 data frames in the VLAN to which the BPDUs belong without sending them to the local STP module for processing. This technology is known as BPDU tunneling.

To transparently transmit BPDUs across a provider network, the following conditions must be met:

- Every branch of a customer network must be able to receive the BPDUs sent by the customer network.
- The BPDUs of a customer network should not be processed by the central processing unit (CPU) of the provider network.
- BPDUs of different customer networks are isolated and do not affect each other.

### 11.1.2 Partitioned STP

With the partitioned STP technology, users of the same customer network but in different areas can transparently transmit BPDUs across the provider network, and spanning trees can be calculated uniformly in the customer network. In addition, the spanning tree of the customer network and that of the provider network are irrelevant to each other.

The partitioned STP technology is the extension of the BPDU tunneling technology, which brings the following advantages:

- Link switching is implemented locally. A link change affects only the local node.
- Service switching speeds up. When services are switched between the links of the local node, other nodes are informed to update the related entries. In this manner, services can be quickly recovered.

### 11.1.3 Logic Relationships Between Configuration Tasks

The features of partitioned STP, with the convergence function added and link switching speeded up, are the extensions and improvements of the BPDU tunneling technology. Therefore, BPDU tunneling must be enabled before the configuration of partitioned STP.

## 11.2 Configuring Interface-based Transparent Transmission of BPDUs from the Same Customer Network

This section describes the procedure for configuring interface-based transparent transmission of BPDUs from the same customer network.

### 11.2.1 Establishing the Configuration Task

#### 11.2.2 Enabling STP on CEs

#### 11.2.3 Configuring the Provider Mode for UPEs

#### 11.2.4 Enabling UPEs to Process BPDUs

#### 11.2.5 Checking the Configuration

### 11.2.1 Establishing the Configuration Task

#### Applicable Environment

Each branch of a customer network has the STP function enabled and is connected to a Underlayer Provider Edge (UPE) which connects no other customer networks. BPDUs from the customer network need to be transparently transmitted over the provider network.

You need to specify the Customer Edges (CEs) and the UPEs so that BPDUs from the customer network can be transparently transmitted across the provider network without being sent to the CPUs of the UPEs for processing. BPDUs from the customer network are processed by the CPUs on the CEs and then forwarded across the provider network.

#### NOTE

If the provider network across which BPDUs are transparently transmitted is simple in structure and all devices on the middle link are S-switches, you can enable all these devices to process BPDUs.

#### Pre-configuration Tasks

Before configuring interface-based transparent transmission of BPDUs from the same customer network, complete the following task:

- Configuring the basic functions of the customer network and the provider network

#### Data Preparation

To configure interface-based transparent transmission of BPDUs from the same customer network, you need the following data.

| No. | Data                                                         |
|-----|--------------------------------------------------------------|
| 1   | Numbers of the UPE interfaces to be enabled to process BPDUs |

### 11.2.2 Enabling STP on CEs

## Context

Do as follows on the CEs.

## Procedure

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

**Step 2** Run the **stp enable** command to enable STP.

----End

## 11.2.3 Configuring the Provider Mode for UPEs

### Context

Do as follows on the UPEs.

### Procedure

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

**Step 2** Run the **bpdu-tunnel stp bridge role provider** command to configure the provider mode.



#### NOTE

The destination MAC address of BPDUs is fixed and does not vary with devices.

When a UPE runs in provider mode, it transmits only STP BPDUs with MAC address 01-80-c2-00-00-08.

When a UPE runs in customer mode, it transmits only STP BPDUs with MAC address 01-80-c2-00-00-00.  
By default, a UPE is in customer mode.

----End

## 11.2.4 Enabling UPEs to Process BPDUs

### Context



#### CAUTION

Enable the UPE to process BPDUs before configuring BPDU tunneling; otherwise, BPDUs are discarded on the UPE interfaces.

Do as follows on the UPEs.

### 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 **budu enable** command to enable S-switch to process BPDUs.

----End

## 11.2.5 Checking the Configuration

Run the following command to check the previous configuration.

| Action                                            | Command                                  |
|---------------------------------------------------|------------------------------------------|
| Check the global configuration of BPDU tunneling. | <b>display bpdu-tunnel global config</b> |

### NOTE

The **display bpdu-tunnel global config** command is valid only in the system view.

Run the **display bpdu-tunnel global config** command on a UPE, and you can view the location of the UPE and the multicast MAC address of STP BPDUs.

## 11.3 Configuring Interface-based Transparent Transmission of BPDUs from Different Customer Networks

This section describes the procedure for configuring interface-based transparent transmission of BPDUs from different customer networks.

### [11.3.1 Establishing the Configuration Task](#)

### [11.3.2 Enabling UPE Interfaces to Process BPDUs](#)

### [11.3.3 Adding UPE Interfaces to Specified VLANs in Untagged Mode](#)

### [11.3.4 Replacing the MAC Address of BPDUs with a Reserved Multicast MAC Address](#)

### [11.3.5 Enabling BPDU Tunneling](#)

### [11.3.6 Checking the Configuration](#)

## 11.3.1 Establishing the Configuration Task

### Applicable Environment

A UPE interface at the CE side is connected to only one customer network. BPDUs from customer networks are untagged. You need to configure interface-based BPDU tunneling to transparently transmit BPDUs from different customer networks across a provider network of Layer 2 to the destinations. In this manner, the STP function can be implemented.

### NOTE

If the provider network across which BPDUs are transparently transmitted is complicated in structure, configure a multicast MAC address for BPDUs on the UPEs. Then, the provider network can automatically support the traversing of BPDUs from the customer networks.

## Pre-configuration Tasks

Before configuring interface-based transparent transmission of BPDUs from different customer networks, complete the following tasks:

- Configuring the basic functions of the customer networks and the provider network
- Enabling STP in the customer networks

## Data Preparation

To configure interface-based transparent transmission of BPDUs from different customer networks, you need the following data.

| No. | Data                                                            |
|-----|-----------------------------------------------------------------|
| 1   | Numbers of the UPE interfaces to be enabled with BPDU tunneling |
| 2   | VLAN IDs of the UPE interfaces connected to the CEs             |

### 11.3.2 Enabling UPE Interfaces to Process BPDUs

#### Context

Do as follows on the UPE interfaces connected to the CEs.

#### 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 **bpdu enable** command to enable S-switch to process BPDUs.
- End

### 11.3.3 Adding UPE Interfaces to Specified VLANs in Untagged Mode

#### Context

Do as follows on the UPE interfaces connected to the CEs.

#### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **vlan** *vlan-id* command to create a VLAN and enter the VLAN view.
- Step 3** Run the **port** *interface-type { interface-number1 [ to interface-number2 ] }* **&<1-10>** command to add the interface to the VLAN.

 **NOTE**

You can also run the **port default vlan *vlanid*** command on the UPE interfaces connected to the CEs to add the interfaces to the specified VLANs in untagged mode.

----End

## 11.3.4 Replacing the MAC Address of BPDUs with a Reserved Multicast MAC Address

### Context

Do as follows on the UPE interfaces connected to the CEs.

### Procedure

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

**Step 2** Run the **bpdu-tunnel stp group-mac *group-mac*** command to replace the MAC address of BPDUs with a multicast MAC address.

----End

## 11.3.5 Enabling BPDU Tunneling

### Context

Do as follows on the UPE interfaces connected to the CEs.

### 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 **bpdu-tunnel enable** command to enable BPDU tunneling.

----End

## 11.3.6 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                                           | Command                                     |
|------------------------------------------------------------------|---------------------------------------------|
| Check the configuration of BPDU tunneling in the interface view. | <b>display bpdu-tunnel interface config</b> |
| Check the global configuration of BPDU tunneling.                | <b>display bpdu-tunnel global config</b>    |

 **NOTE**

The **display bpd-tunnel global config** command is valid only in the system view.

The **display bpd-tunnel interface config** command is valid only in the interface view.

Run the **display bpd-tunnel global config** command on a UPE, and you can view the location of the UPE and the multicast MAC address of STP BPDUs.

Run the **display bpd-tunnel interface config** command, and you can view the BPDU configuration on the UPE interface including:

- Whether BPDUs sent from the interface are tagged
- Whether interface-based BPDU tunneling is configured
- Whether the interface allows tagged BPDUs to pass through
- Ethernet encapsulation type value of the outer tag
- Tag value of BPDUs sent from the interface
- Tag value of the BPDUs that the interface allows to pass through

## 11.4 Configuring VLAN-based BPDU Tunneling

This section describes the procedure for configuring VLAN-based BPDU tunneling.

### [11.4.1 Establishing the Configuration Task](#)

### [11.4.2 Setting VLAN IDs of the BPDUs that CE Interfaces Allow to Pass Through](#)

### [11.4.3 Tagging BPDUs](#)

### [11.4.4 \(Optional\) Replacing the MAC Address of BPDUs with a Multicast MAC Address](#)

### [11.4.5 Configuring UPEs to Transmit Tagged BPDUs Through BPDU Tunnels](#)

### [11.4.6 Checking the Configuration](#)

## 11.4.1 Establishing the Configuration Task

### Applicable Environment

When a UPE interface is connected to multiple customer networks, BPDUs from the CEs must be tagged to identify different users.

To transparently transmit BPDUs from the customer networks across the provider network, you need to configure BPDU tunneling and replace the destination MAC address of BPDUs with a multicast MAC address on the UPEs.

### Pre-configuration Tasks

Before configuring VLAN-based BPDU tunneling, complete the following tasks:

- Configuring the basic functions of the customer networks and the provider network
- Enabling STP in the customer networks

## Data Preparation

To configure VLAN-based BPDU tunneling, you need the following data.

| No. | Data                                                                   |
|-----|------------------------------------------------------------------------|
| 1   | VLAN IDs of the BPDUs that the CE interfaces allow to pass through     |
| 2   | Multicast MAC address used to replace the MAC address of BPDUs         |
| 3   | Tag values of the BPDUs that can be transmitted by the CEs to the UPEs |

### 11.4.2 Setting VLAN IDs of the BPDUs that CE Interfaces Allow to Pass Trough

#### Context

Do as follows on the CE interfaces connected to the UPEs.

#### 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 **port trunk allow-pass vlan { { vlan-id1 [ to vlan-id2 ] } & <1-10> | all }** command to set the VLAN ID of the BPDUs that the interface allows to pass through.

The VLAN ID belongs to a customer network. Only BPDUs with the specified VLAN ID can be sent to the UPE through the CE interface.

----End

### 11.4.3 Tagging BPDUs

#### Context

Do as follows on the CE interfaces connected to the UPEs.

#### 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 **stp bpdu vlan vlan-id** command to set the tag value of the BPDUs to be sent to the UPE.

This VLAN ID is the port VLAN ID (PVID) of the CE interface connected to the UPE. The value ranges from 1 to 4094. It is irrelative with VLAN IDs of the customer networks.

----End

## 11.4.4 (Optional) Replacing the MAC Address of BPDUs with a Multicast MAC Address

### Context

Do as follows on the UPE interfaces connected to the CEs.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bpdu-tunnel stp group-mac group-mac** command to replace the MAC address of BPDUs with a multicast MAC address.

----End

## 11.4.5 Configuring UPEs to Transmit Tagged BPDUs Through BPDU Tunnels

### Context

Do as follows on the inbound UPE interfaces connected to the CEs.

### 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 **port trunk allow-pass vlan { { vlan-id1 [ to vlan-id2 ] } & <1-10> | all }** command to set the VLAN ID of the BPDUs that the interface allows to pass through.
- Step 4** Run the **bpdu-tunnel stp vlan vlan-id1 [ to vlan-id2 ]** command to configure the UPE to transmit BPDUs with the specified tag value.

The VLAN ID is the tag value set for BPDUs on the CE connected to the UPE. Only BPDUs with the specified tag value can pass the UPE and travel through the BPDU tunnel.

----End

## 11.4.6 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                                           | Command                                     |
|------------------------------------------------------------------|---------------------------------------------|
| Check the configuration of BPDU tunneling in the interface view. | <b>display bpdu-tunnel interface config</b> |
| Check the global configuration of BPDU tunneling.                | <b>display bpdu-tunnel global config</b>    |



**NOTE**

The **display bpdu-tunnel global config** command is valid only in the system view.

The **display bpdu-tunnel interface config** command is valid only in the interface view.

Run the **display bpdu-tunnel global config** command on a UPE, and you can view the location of the UPE and the multicast MAC address of BPDUs.

Run the **display bpdu-tunnel interface config** command, and you can view the BPDU configuration on the interface including:

- Whether the BPDUs sent from the interface are tagged
- Whether interface-based BPDU tunneling is configured
- Whether the interface allows tagged BPDUs to pass through
- Ethernet encapsulation type of the outer tag
- Tag value of the BPDUs sent from the interface
- Tag value of the BPDUs that the interface allows to pass through

## 11.5 Configuring QinQ-based BPDU Tunneling

This section describes the procedure for configuring QinQ-based BPDU tunneling.

### [11.5.1 Establishing the Configuration Task](#)

### [11.5.2 Setting VLAN IDs of the BPDUs that CE Interfaces Allow to Pass Through](#)

### [11.5.3 Tagging BPDUs](#)

### [11.5.4 Tagging and Untagging the Tagged BPDUs](#)

### [11.5.5 Replacing the MAC Address of BPDUs with a Reserved Multicast MAC Address](#)

### [11.5.6 Configuring BPDU Tunneling](#)

### [11.5.7 Checking the Configuration](#)

## 11.5.1 Establishing the Configuration Task

### Applicable Environment

When a UPE interface connects multiple user VLANs, BPDUs from the CEs must be tagged to identify different users.

To save VLAN IDs of the provider network, you need to add outer tags to the tagged BPDUs from the CEs. Thus, BPDUs of different VLANs are transmitted across the provider network to corresponding destinations through different BPDU tunnels.

### Pre-configuration Tasks

Before configuring QinQ-based BPDU tunneling, complete the following tasks:

- Configuring the basic functions of the customer networks and the provider network
- Enabling STP in the customer network

## Data Preparation

To configure QinQ-based BPDU tunneling, you need the following data.

| No. | Data                                                               |
|-----|--------------------------------------------------------------------|
| 1   | Names of the CE interfaces to be enabled with STP                  |
| 2   | VLAN IDs of the BPDUs that the CE interfaces allow to pass through |
| 3   | Inner tag values of the BPDUs sent from the CEs to the UPEs        |
| 4   | Outer tag values of the BPDUs sent from the CEs on the UPEs        |

### 11.5.2 Setting VLAN IDs of the BPDUs that CE Interfaces Allow to Pass Through

#### Context

Do as follows on the CE interfaces connected to the UPEs.

#### 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 **port trunk allow-pass vlan { { vlan-id1 [ to vlan-id2 ] } & <1-10> | all }** command to set the VLAN ID of the BPDUs that the CE allows to pass through.

The VLAN ID belongs to a customer network. Only BPDUs from the specified VLAN can be sent to the UPE through the CE interface connected to the UPE.

----End

### 11.5.3 Tagging BPDUs

#### Context

Do as follows on the CE interfaces connected to the UPEs.

#### 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 **stp bpdu vlan vlan-id** command to set the VLAN ID of BPDUs to be sent to the UPE.

This VLAN ID is the default VLAN ID of the CE interface connected to the UPE. The value ranges from 1 to 4094.

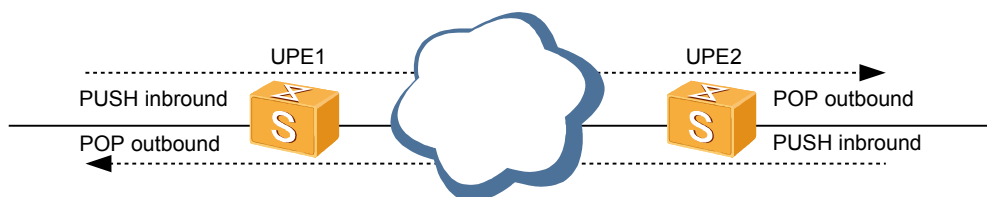
----End

## 11.5.4 Tagging and Untagging the Tagged BPDUs

### Context

As shown in [Figure 11-1](#), the BPDUs tagged on the CEs need be tagged again with outer tags on the inbound interfaces of the UPEs before being transmitted through the provider network. When leaving the provider network, the outer tags are removed on the outbound interfaces on the opposite UPEs.

**Figure 11-1** Tagging and Untagging the Tagged BPDUs



### 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 **qinq vlan-translation enable** command to remove the outer tags from the BPDUs of the customer networks.
- Step 4** Run the **port vlan-stacking vlan vlan-id1 [ to vlan-id2 ] push vlan vlan-id3 {remark-8021p priority-id | priority-inherit } inbound** command to add different outer tags in the BPDUs of different users.

----End

## 11.5.5 Replacing the MAC Address of BPDUs with a Reserved Multicast MAC Address

### Context

Do as follows on the UPEs.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **bpdu-tunnel stp group-mac group-mac** command to replace the MAC address of BPDUs with a multicast MAC address.

----End

## 11.5.6 Configuring BPDU Tunneling

### Context

Do as follows on the inbound UPE interfaces connected to the CEs:

### 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 **port trunk allow-pass vlan { { vlan-id1 [ to vlan-id2 ] } & <1-10> | all }** command to set the VLAN ID of the BPDUs that the UPE allows to pass through.
- Step 4** Run the **bpdu-tunnel stp vlan vlan-id1 [ to vlan-id2 ]** command to enable the UPE to transmit BPDUs with the specified VLAN ID.

----End

## 11.5.7 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                                           | Command                                     |
|------------------------------------------------------------------|---------------------------------------------|
| Check the configuration of BPDU tunneling in the interface view. | <b>display bpdu-tunnel interface config</b> |
| Check the global configuration of BPDU tunneling.                | <b>display bpdu-tunnel global config</b>    |

### NOTE

The **display bpdu tunnel global config** command is valid only in the system view.

The **display bpdu tunnel interface config** command is valid only in the interface view.

Run the **display bpdu-tunnel global config** command on a UPE, and you can display the location of the UPE and the multicast MAC address of BPDUs. For example:

```
<Quidway> system-view
[Quidway] display bpdu-tunnel global config
BridgeRole customer
GroupMac 0100-0ccf-ffff
```

Run the **display bpdu-tunnel interface config** command on a CE, and you can view the tag value of the BPDUs sent from the CE. The UPE connected to the CE transmits only BPDUs with the specified tag value. For example:

```
<Quidway> system-view
[Quidway] interface ethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] display bpdu-tunnel interface config
BpduDot1qStatus enable
BpduOneQStatus disable
BpduTwoQStatus disable
EtherType 8100
Dot1qVlan 10
TwoQList
```

## 11.6 Configuring Partitioned STP

This section describes the procedure for configuring partitioned STP.

### 11.6.1 Establishing the Configuration Task

#### 11.6.2 Enabling STP

#### 11.6.3 Enabling Interfaces Connected to the MAN to Tag BPDU

#### 11.6.4 Setting VLAN IDs for Inbound Interfaces

#### 11.6.5 Configuring BPDU Tunneling

#### 11.6.6 Enabling STP Snooping

#### 11.6.7 Checking the Configuration

## 11.6.1 Establishing the Configuration Task

### Applicable Environment

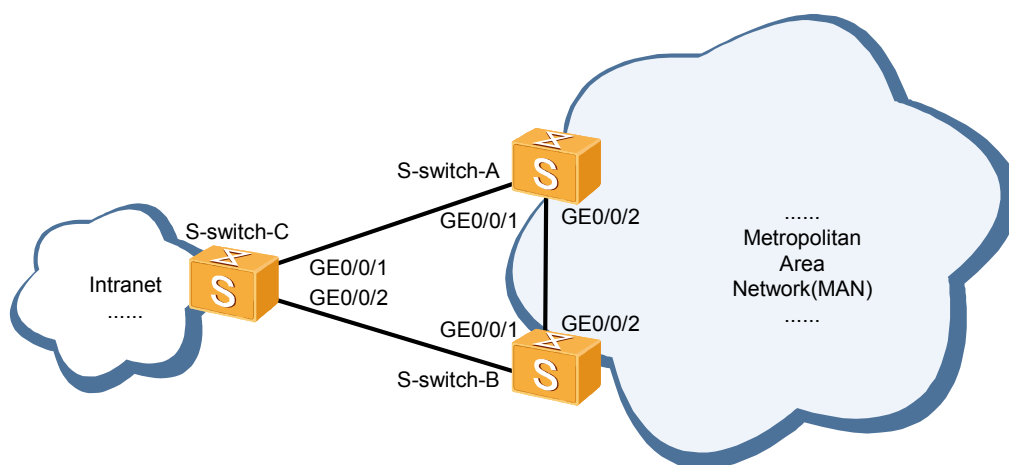
When devices access a Metropolitan Area Network (MAN) in dual-homed mode, partitioned STP helps in avoiding loops, limiting the size of the STP network, and speeding up the convergence of the STP network.

#### NOTE

In this configuration task, unless otherwise stated:

- "S-switchs outside the MAN" refer to the devices that access the MAN in dual-homed mode, for example, S-switch-C shown in [Figure 11-2](#).
- "S-switchs at the edge of the MAN" refer to the devices through which the outside devices access the MAN in dual-homing mode, for example, S-switch-A and S-switch-B shown in [Figure 11-2](#).

**Figure 11-2** Networking of partitioned STP



## Pre-configuration Tasks

None

## Data Preparation

To configure partitioned STP, you need the following data.

| No. | Data                                        |
|-----|---------------------------------------------|
| 1   | VLAN ID used in the partitioned STP network |

## 11.6.2 Enabling STP

### Context

Do as follows on the S-switch outside the MAN.

### Procedure

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

**Step 2** Run the **stp enable** command to enable MSTP.

By default, the MSTP function is disabled.

When the MSTP function is enabled, the MSTP function is enabled on all interfaces by default.

----End

## 11.6.3 Enabling Interfaces Connected to the MAN to Tag BPDUs

### Context

Do as follows on the S-switch outside the MAN.

*vlan-id*, that is, the VLAN ID used in the partitioned STP network, in [Step 2](#) and [Step 5](#) should be the same.

Perform [Step 4](#) to [Step 6](#) on the two interfaces connected to the MAN respectively to enable them to tag BPDUs.

### Procedure

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

**Step 2** Run the **vlan *vlan-id*** command to create a VLAN and enter the VLAN view.

**Step 3** Run the **quit** command to quit the VLAN view.

**Step 4** Run the **interface *interface-type interface-number*** or **interface *eth-trunk trunk-id*** command to enter the view of the interface connected to the MAN.

**Step 5** Run the **stp bpdu vlan** *vlan-id* command to enable the interface to tag BPDUs.

By default, an interface does not tag BPDUs.

**Step 6** Run the **bpdu enable** command to enable the interface to process BPDUs.

By default, an interface does not process BPDUs.

----End

## 11.6.4 Setting VLAN IDs for Inbound Interfaces

### Context

Do as follows on the two S-switches at the edge of the MAN so that the two interfaces connected to the S-switch outside the MAN can tag incoming BPDUs.

### 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 **port trunk allow-pass vlan** { { *vlan-id1* [ *to vlan-id2* ] } &<1-10> | **all** } command to configure the VLAN ID for the inbound interface.

The values of *vlan-id1* and *vlan-id2* are the VLAN IDs used in the partitioned STP network.

----End

## 11.6.5 Configuring BPDU Tunneling

### Context

Do as follows on the two S-switches at the edge of the MAN.

#### NOTE

BPDUs can be transparently transmitted only based on their destination MAC address. Whether this MAC address is a multicast MAC address cannot be identified. Therefore this MAC address must be dedicated to this special use.

Do not use the **port hybrid untagged vlan** command to add the interfaces to the VLAN used for transparent transmission of BPDUs. Otherwise, BPDU tunneling configured on the interfaces will be affected.

**Step 2**, **Step 3**, and **Step 9** are optional. If you have taken the steps in **11.6.4 Setting VLAN IDs for Inbound Interfaces**, you can skip these three steps; otherwise, they are mandatory. **Step 8** is optional, without which the destination MAC address of BPDUs will be replaced with multicast MAC address 0100-0ccd-cdd0.

### Procedure

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

**Step 2** Run the **vlan** *vlan-id* command to create a VLAN and enter the VLAN view.

The value of *vlan-id* is the VLAN ID used in the partitioned STP network.

- Step 3** Run the **quit** command to quit the VLAN view.
- Step 4** Run the **interface** *interface-type interface-number* or **interface eth-trunk** *trunk-id* command to enter the view of the interface connected to the S-switch outside the MAN.
- Step 5** Run the **quit** command to quit the interface view.
- Step 6** Run the **bpdu enable** command to enable the interface to process BPDUs.
- By default, an interface does not process BPDUs.
- Step 7** Run the **bpdu enable stp vlan** *vlan-id1* [ **to** *vlan-id2* ] command to enable BPDU tunneling on the inbound interface.
- By default, BPDU tunneling is disabled.
- Step 8** Run the **bpdu-tunnel stp group-mac** *group-mac* command to replace the destination MAC address of BPDUs with a multicast MAC address.
- Step 9** Run the **port trunk allow-pass vlan** *vlan-id* command to add the interface to the VLAN.
- Step 10** Run the **quit** command to quit the interface view.
- Step 11** Run the **interface** *interface-type interface-number* or **interface eth-trunk** *trunk-id* command to enter the view of the interface connected to the other S-switch at the edge of the MAN.
- Step 12** Run the **port trunk allow-pass vlan** *vlan-id* command to add the interface connected to the other S-switch at the edge of the MAN to the VLAN.

----End

## 11.6.6 Enabling STP Snooping

### Context

Do as follows on the two S-switchs at the edge of the MAN.

### Procedure

- Step 1** Run the **system-view** command to enter the system view.
- Step 2** Run the **stp-snooping enable** command to enable STP snooping.

By default, STP snooping is disabled.

----End

## 11.6.7 Checking the Configuration

Run the following commands to check the previous configuration.

| Action                                                   | Command                                                   |
|----------------------------------------------------------|-----------------------------------------------------------|
| Check the configuration of the S-switch outside the MAN. | <b>display current-configuration configuration system</b> |

| Action                                                                                                       | Command                                                                               |
|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Check the configurations of the interfaces connected to the MAN on the S-switch outside the MAN.             | <b>display current-configuration interface</b> <i>interface-type interface-number</i> |
| Check the configurations of the inbound interfaces on the S-switchs at the edge of the MAN.                  | <b>display current-configuration interface</b> <i>interface-type interface-number</i> |
| Check the configurations of the interfaces through which the S-switchs at the edge of the MAN are connected. | <b>display current-configuration interface</b> <i>interface-type interface-number</i> |
| Check the configurations of the S-switchs at the edge of the MAN.                                            | <b>display current-configuration configuration system</b>                             |

If the configurations succeed, you can view the following information by running the preceding commands:

- MSTP is enabled on the S-switch outside the MAN.
- BPDUs are tagged correctly on the interfaces connected to the MAN on the S-switch outside the MAN.
- The VLAN ID and BPDU tunneling are configured correctly on the inbound interfaces on the S-switchs at the edge of the MAN.
- The VLAN ID is set correctly on the interfaces through which the S-switchs at the edge of the MAN are connected.
- STP snooping is enabled on the S-switchs at the edge of the MAN.

## 11.7 Configuration Examples

This section provides examples for configuring the Multiple Spanning Tree Protocol (MSTP), BPDU tunneling, and partitioned STP.

[11.7.1 Example for Configuring Interface-based BPDU Tunnel of the Same Customer](#)

[11.7.2 Example for Configuring Interface-based BPDU Tunnel of Different Customer](#)

[11.7.3 Example for Configuring VLAN-based BPDU Tunneling](#)

[11.7.4 Example for Configuring QinQ-based BPDU Tunneling](#)

[11.7.5 Example for Configuring Partitioned STP](#)

### 11.7.1 Example for Configuring Interface-based BPDU Tunnel of the Same Customer

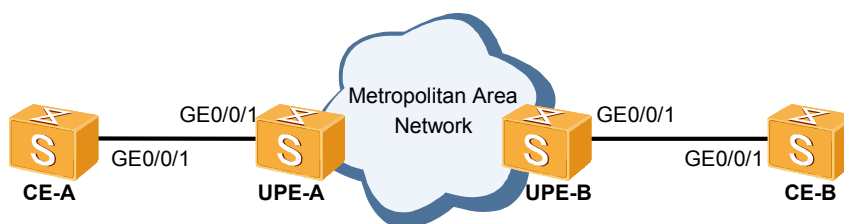
#### Networking Requirements

As shown in [Figure 11-3](#), the CEs are connected to the provider network through the UPEs. The UPEs are in provider mode. All devices on the link between the two UPEs are the S-switchs that

can process BPDUs. In this scenario, the devices on the link for transparent transmission of BPDUs do not use BPDUs for STP calculation. Instead, they directly transmit BPDUs to the opposite UPE.

The UPEs broadcast BPDUs from the CEs to the entire provider network. In this manner, the provider network automatically supports the traversing of BPDUs from the customer network.

**Figure 11-3** Networking for configuring interface-based transparent transmission of BPDUs from the same customer network



## Configuration Roadmap

The configuration roadmap is as follows:

- Enable STP on the CEs.
- Set the provider mode for UPE-A and UPE-B.
- Enable the GigabitEthernet 0/0/1 interfaces on UPE-A and UPE-B to process BPDUs.
- Assume that the interfaces on the link between the two UPEs are enabled to process BPDUs.

## Data Preparation

To complete the configuration, you need the following data:

- Names of the interfaces on the CEs enabled with STP
- Names of the UPE interfaces connected to the CEs
- Names of the interfaces on the link between the two UPEs

## Configuration Procedure

1. Enable STP on the CEs.

# Configure CE-A.

```
<Quidway> system-view
[Quidway] sysname CE-A
[CE-A] stp enable
```

# Configure CE-B.

```
<Quidway> system-view
[Quidway] sysname CE-B
[CE-B] stp enable
```

2. Set the provider mode for the UPEs.

# Configure UPE-A.

```
<Quidway> system-view
```

- ```
[Quidway] sysname UPE-A
[UPE-A] bpdu-tunnel stp bridge role provider

# Configure UPE-B.

<Quidway> system-view
[Quidway] sysname UPE-B
[UPE-B] bpdu-tunnel stp bridge role provider
```
3. Enable the UPEs to process BPDUs.
- ```
Configure UPE-A.

<UPE-A> system-view
[UPE-A] interface ethernet 0/0/1
[UPE-A-GigabitEthernet0/0/1] bpdu enable

Configure UPE-B.

<UPE-B> system-view
[UPE-B] interface ethernet 0/0/1
[UPE-B-GigabitEthernet0/0/1] bpdu enable
```
4. Verify the configuration.
- ```
# Check the global BPDU configuration.

[UPE-A] display bpdu-tunnel global config
BridgeRole      provider
GroupMac        0100-0ccd-cdd0

# Check the STP configuration on CE-A and CE-B to check that BPDU tunneling is
configured successfully.
```
- | [CE-A] display stp brief | | | | | |
|--------------------------|----------------------|------|------------|------------|--|
| MSTID | Port | Role | STP State | Protection | |
| 0 | GigabitEthernet0/0/1 | ROOT | FORWARDING | NONE | |
-
- | [CE-B] display stp brief | | | | | |
|--------------------------|----------------------|------|------------|------------|--|
| MSTID | Port | Role | STP State | Protection | |
| 0 | GigabitEthernet0/0/1 | DESI | FORWARDING | NONE | |

Configuration Files

- Configuration file of CE-A


```
#
sysname CE-A
#
stp enable
#
return
```
- Configuration file of CE-B


```
#
sysname CE-B
#
stp enable
#
return
```
- Configuration file of UPE-A


```
#
sysname UPE-A
#
bpdu-tunnel stp bridge role provider
#
interface GigabitEthernet0/0/1
bpdu enable
#
return
```
- Configuration file of UPE-B


```
#
```

```

sysname UPE-B
#
bpdu-tunnel stp bridge role provider
#
interface GigabitEthernet0/0/1
  bpdu enable
#
return

```

11.7.2 Example for Configuring Interface-based BPDU Tunnel of Different Customer

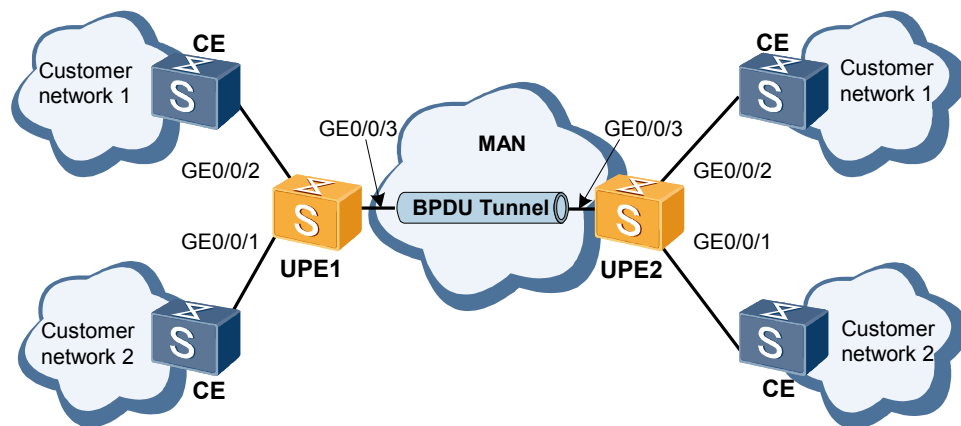
Networking Requirements

As shown in [Figure 11-4](#), Customer network 1 has STP enabled and connects the GigabitEthernet 0/0/2 interfaces on UPE1 and UPE2; Customer network 2 also has STP enabled and connects the GigabitEthernet 0/0/1 interfaces on UPE1 and UPE2.

By configuring interface-based transparent transmission of BPDUs from different customer networks, you can obtain the following results:

- All the devices that belong to Customer network 1 work together to form a spanning tree.
- All the devices that belong to Customer network 2 work together to form a spanning tree.

Figure 11-4 Networking for configuring interface-based transparent transmission of BPDUs from different customer networks



Configuration Roadmap

The configuration roadmap is as follows:

- Add the GigabitEthernet 0/0/2 interfaces connected to Customer network 1 on the UPEs to VLAN 100 in untagged mode.
- Add the GigabitEthernet 0/0/1 interfaces connected to Customer network 2 on the UPEs to VLAN 200 in untagged mode.
- Allow BPDUs from VLAN 100 and VLAN 200 to pass the Ethernet 0/0/3 interfaces on the UPEs.

- Replace the destination MAC address of BPDUs with a multicast MAC address.
- Enable BPDU tunneling on the GigabitEthernet 0/0/2 and Ethernet 0/0/1 interfaces on the UPEs.

Data Preparation

To complete the configuration, you need the following data:

- IDs of the VLANs to which the UPEs connected with Customer network 1 and Customer network 2 belong
- Multicast MAC address to be used to replace the destination MAC address of BPDUs

Configuration Procedure

1. On the UPEs, enable the interfaces connected to the CEs to process BPDUs.

Configure UPE1.

```
<Quidway> system-view
[Quidway] sysname UPE1
[UPE1] interface ethernet 0/0/2
[UPE1-GigabitEthernet0/0/2] bpdu enable
[UPE1-GigabitEthernet0/0/2] quit
[UPE1] interface ethernet 0/0/1
[UPE1-GigabitEthernet0/0/1] bpdu enable
```

Configure UPE2.

```
<Quidway> system-view
[Quidway] sysname UPE2
[UPE2] interface ethernet 0/0/2
[UPE2-GigabitEthernet0/0/2] bpdu enable
[UPE2-GigabitEthernet0/0/2] quit
[UPE2] interface ethernet 0/0/1
[UPE2-GigabitEthernet0/0/1] bpdu enable
```

2. On the UPEs, add the GigabitEthernet 0/0/2 interfaces to VLAN 100 in untagged mode.

Configure UPE1.

```
[UPE1] vlan batch 100
[UPE1] interface ethernet 0/0/2
[UPE1-GigabitEthernet0/0/2] port default vlan 100
[UPE1-GigabitEthernet0/0/2] quit
```

Configure UPE2.

```
[UPE2] vlan batch 100
[UPE2] interface ethernet 0/0/2
[UPE2-GigabitEthernet0/0/2] port default vlan 100
[UPE2-GigabitEthernet0/0/2] quit
```

3. On the UPEs, add the GigabitEthernet 0/0/1 interfaces to VLAN 200 in untagged mode.

Configure UPE1.

```
[UPE1] vlan batch 200
[UPE1] interface ethernet 0/0/1
[UPE1-GigabitEthernet0/0/1] port default vlan 200
[UPE1-GigabitEthernet0/0/1] quit
```

Configure UPE2.

```
[UPE2] vlan batch 200
[UPE2] interface ethernet 0/0/1
[UPE2-GigabitEthernet0/0/1] port default vlan 200
[UPE2-GigabitEthernet0/0/1] quit
```

4. On the UPEs, allow BPDUs from VLAN 100 and VLAN 200 to pass the GigabitEthernet 0/0/3 interfaces.

Configure UPE1.

```
[UPE1] interface ethernet 0/0/3
[UPE1-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 200
```

Configure UPE2.

```
[UPE2] interface ethernet 0/0/3
[UPE2-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 200
```

5. Replace the destination MAC address of BPDUs with a multicast MAC address.

Configure UPE1.

```
[UPE1] bpdu-tunnel stp group-mac 0100-5e00-0011
```

Configure UPE2.

```
[UPE2] bpdu-tunnel stp group-mac 0100-5e00-0011
```

6. On the UPEs, enable BPDU tunneling on the GigabitEthernet 0/0/1 and Ethernet 0/0/2 interfaces.

Configure UPE1.

```
[UPE1] interface ethernet 0/0/2
[UPE1-GigabitEthernet0/0/2] bpdu-tunnel enable
[UPE1-GigabitEthernet0/0/2] quit
[UPE1] interface ethernet 0/0/1
[UPE1-GigabitEthernet0/0/1] bpdu-tunnel enable
[UPE1-GigabitEthernet0/0/1] quit
```

Configure UPE2.

```
[UPE2] interface ethernet 0/0/2
[UPE2-GigabitEthernet0/0/2] bpdu-tunnel enable
[UPE2-GigabitEthernet0/0/2] quit
[UPE2] interface ethernet 0/0/1
[UPE2-GigabitEthernet0/0/1] bpdu-tunnel enable
[UPE2-GigabitEthernet0/0/1] quit
```

7. Verify the configuration.

Check the configuration of UPE1.

```
[UPE1] interface ethernet 0/0/1
[UPE1-GigabitEthernet0/0/1] display bpdu-tunnel interface config
BpduDot1qStatus  disable
BpduOneQStatus   enable
BpduTwoQStatus   disable
EtherType        8100
Dot1qVlan
TwoQList
[UPE1] interface ethernet 0/0/2
[UPE1-GigabitEthernet0/0/2] display bpdu-tunnel interface config
BpduDot1qStatus  disable
BpduOneQStatus   enable
BpduTwoQStatus   disable
EtherType        8100
Dot1qVlan
TwoQList
```

Check the configuration of UPE2.

Omitted. The verification on UPE2 is same as that on UPE1 and is not mentioned here.

If the UPEs are correctly configured, BPDUs sent from CEs can reach the peer CEs to realize the STP calculation, and interfaces obtain corresponding roles correctly.

Configuration Files

- Configuration file of UPE1

```
#
sysname UPE1
#
```

```

vlan batch 100 200
#
bpdu-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/2
bpdu enable
port default vlan 100
bpdu-tunnel enable
#
interface GigabitEthernet0/0/1
bpdu enable
port default vlan 200
bpdu-tunnel enable
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 100 200
#
return

```

- Configuration file of UPE2

```

#
sysname UPE2
#
vlan batch 100 200
#
bpdu-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/2
bpdu enable
port default vlan 100
bpdu-tunnel enable
#
interface GigabitEthernet0/0/1
bpdu enable
port default vlan 200
bpdu-tunnel enable
#
interface GigabitEthernet0/0/3
port trunk allow-pass vlan 100 200
#
#
return

```

11.7.3 Example for Configuring VLAN-based BPDU Tunneling

Networking Requirements

As shown in [Figure 11-5](#), Customer network 1 belongs to VLAN 10 and connects the GigabitEthernet 0/0/1 interfaces on UPE1 and UPE2 through CE1 and CE2; Customer network 2 belongs to VLAN 20 and connects the GigabitEthernet 0/0/2 interfaces on UPE1 and UPE2 through CE3 and CE4.

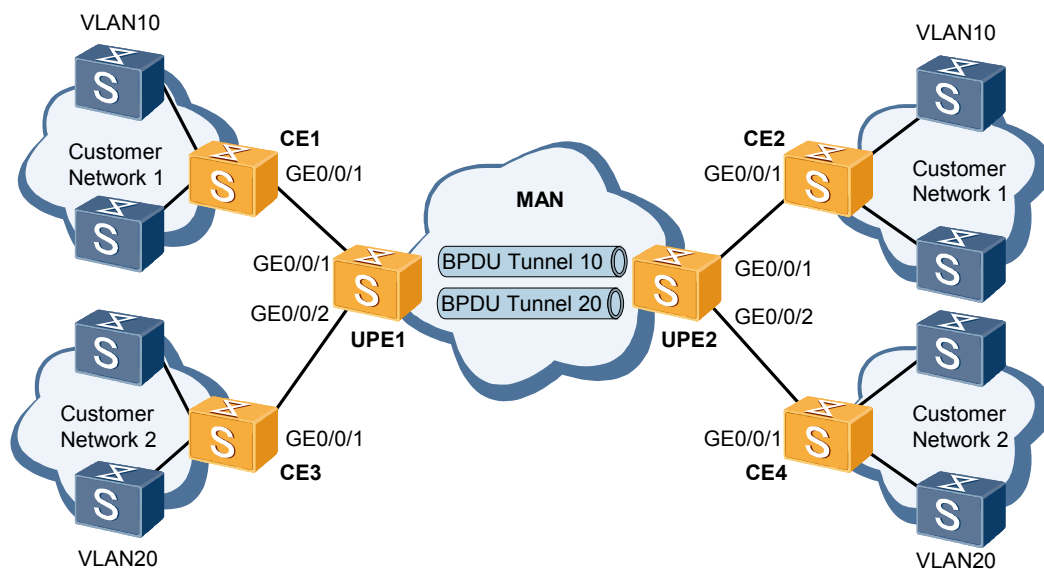
By configuring VLAN-based BPDU tunneling, you can obtain the following results:

- The GigabitEthernet 0/0/1 interfaces on CE1 and CE2 allow BPDUs from VLAN 10 to pass and tag the BPDUs to the UPEs with VLAN ID 10.
- The GigabitEthernet 0/0/1 interfaces on CE3 and CE4 allow BPDUs from VLAN 20 to pass and tag the BPDUs to the UPEs with VLAN ID 20.
- All the devices that belong to VLAN 10 work together to form a spanning tree.
- All the devices that belong to VLAN 20 work together to form a spanning tree.

The UPE interfaces connected to the CEs converge multiple user VLANs. Therefore, BPDUs from CEs must be tagged to identify different users.

To transmit BPDUs transparently across the provider network, you should enable BPDU tunneling and replace the destination MAC address of the BPDUs on the UPEs.

Figure 11-5 Networking for configuring VLAN-based BPDU tunneling



Configuration Roadmap

The configuration roadmap is as follows:

- Tag the BPDUs sent from the CEs to the UPEs.
- Allow the tagged BPDUs to pass the UPE interfaces connected to the CEs.
- Configure the UPEs to replace the destination MAC address of BPDUs with a multicast MAC address.
- Configure the UPEs to set up the BPDU tunnel according to the tag value in BPDUs and enable BPDU tunneling.
- Unify the configurations on the UPEs and the CEs at the two ends of the BPDU tunnel.

Data Preparation

To complete the configuration, you need the following data:

- BPDUs from CE1 and CE2 to the UPEs belonging to VLAN 10
- BPDUs from CE3 and CE4 to the UPEs belonging to VLAN 20
- Numbers of the UPE interfaces connected to the CEs
- Multicast MAC address 0100-5e00-0011 to be used to replace the destination MAC address of BPDUs

Configuration Procedure

1. Configure CEs to allow BPDUs from the specified VLANs to pass the GigabitEthernet 0/0/1 interfaces.

Configure CE1.

```
<Quidway> system-view
[Quidway] sysname CE1
[CE1] interface ethernet 0/0/1
[CE1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[CE1-GigabitEthernet0/0/1] quit
```

Configure CE2.

```
<Quidway> system-view
[Quidway] sysname CE2
[CE2] interface ethernet 0/0/1
[CE2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[CE2-GigabitEthernet0/0/1] quit
```

Configure CE3.

```
<Quidway> system-view
[Quidway] sysname CE3
[CE3] interface ethernet 0/0/1
[CE3-GigabitEthernet0/0/1] port trunk allow-pass vlan 20
[CE3-GigabitEthernet0/0/1] quit
```

Configure CE4.

```
<Quidway> system-view
[Quidway] sysname CE4
[CE4] interface ethernet 0/0/1
[CE4-GigabitEthernet0/0/1] port trunk allow-pass vlan 20
[CE4-GigabitEthernet0/0/1] quit
```

2. Configure CE1 and CE2 to tag BPDUs to be sent to the UPEs with VLAN ID 10.

```
<CE1> system-view
[CE1] vlan 10
[CE1-vlan10] port ethernet 0/0/1
[CE1-vlan10] quit
[CE1] interface ethernet 0/0/1
[CE1-GigabitEthernet0/0/1] bpdu enable
[CE1-GigabitEthernet0/0/1] stp bpdu vlan 10
[CE1-GigabitEthernet0/0/1] quit
```

Configure CE2.

```
<CE2> system-view
[CE2] vlan 10
[CE2-vlan10] port ethernet 0/0/1
[CE2-vlan10] quit
[CE2] interface ethernet 0/0/1
[CE2-GigabitEthernet0/0/1] bpdu enable
[CE2-GigabitEthernet0/0/1] stp bpdu vlan 10
[CE2-GigabitEthernet0/0/1] quit
```

3. Configure CE3 and CE4 to tag BPDUs to be sent to the UPEs with VLAN ID 20.

Configure CE3.

```
<CE3> system-view
[CE3] vlan 20
[CE3-vlan20] port ethernet 0/0/1
[CE3-vlan20] quit
[CE3] interface ethernet 0/0/1
[CE3-GigabitEthernet0/0/1] bpdu enable
[CE3-GigabitEthernet0/0/1] stp bpdu vlan 20
[CE3-GigabitEthernet0/0/1] quit
```

Configure CE4.

```
<CE4> system-view
[CE4] vlan 20
[CE4-vlan20] port ethernet 0/0/1
[CE4-vlan20] quit
[CE4] interface ethernet 0/0/1
[CE4-GigabitEthernet0/0/1] bpdu enable
[CE4-GigabitEthernet0/0/1] stp bpdu vlan 20
```

```
[CE4-GigabitEthernet0/0/1] quit
```

4. Enable the UPEs to process BPDUs.

Configure UPE1.

```
<Quidway> system-view
[Quidway] sysname UPE1
[UPE1] interface ethernet 0/0/1
[UPE1-GigabitEthernet0/0/1] bpdu enable
[UPE1] interface ethernet 0/0/2
[UPE1-GigabitEthernet0/0/2] bpdu enable
```

Configure UPE2.

```
<Quidway> system-view
[Quidway] sysname UPE2
[UPE2] interface ethernet 0/0/1
[UPE2-GigabitEthernet0/0/1] bpdu enable
[UPE2] interface ethernet 0/0/2
[UPE2-GigabitEthernet0/0/2] bpdu enable
```

5. Configure the UPEs to replace the destination MAC address of BPDUs with a multicast MAC address.

Configure UPE1.

```
[UPE1] bpdu-tunnel stp group-mac 0100-5e00-0011
```

Configure UPE2.

```
[UPE2] bpdu-tunnel stp group-mac 0100-5e00-0011
```

NOTE

The multicast MAC address can vary on UPE1 and UPE2. You are recommended to set the same multicast MAC address on the UPEs.

6. Configure the UPEs to transmit the BPDUs from VLAN 10 and VLAN 20 through the BPDU tunnel.

Configure UPE1.

```
[UPE1] interface ethernet 0/0/1
[UPE1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[UPE1-GigabitEthernet0/0/1] bpdu-tunnel stp vlan 10
[UPE1-GigabitEthernet0/0/1] quit
[UPE1] interface ethernet 0/0/2
[UPE1-GigabitEthernet0/0/2] bpdu-tunnel stp vlan 20
[UPE1-GigabitEthernet0/0/2] port trunk allow-pass vlan 20
[UPE1-GigabitEthernet0/0/2] quit
```

Configure UPE2.

```
[UPE2] interface ethernet 0/0/1
[UPE2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[UPE2-GigabitEthernet0/0/1] bpdu-tunnel stp vlan 10
[UPE2-GigabitEthernet0/0/1] quit
[UPE2] interface ethernet 0/0/2
[UPE2-GigabitEthernet0/0/2] port trunk allow-pass vlan 20
[UPE2-GigabitEthernet0/0/2] bpdu-tunnel stp vlan 20
[UPE2-GigabitEthernet0/0/2] quit
```

7. Verify the configuration.

Run the **display bpdu-tunnel interface config** command and you can view VLAN IDs and TPIDs configured on the interfaces.

Take CE1 as an example.

```
[CE1-GigabitEthernet0/0/1] display bpdu-tunnel interface config
BpduDot1qStatus   enable
BpduOneQStatus    disable
BpduTwoQStatus    disable
EtherType         8100
Dot1qVlan         10
TwoQList
```

```
# Take UPE1 as an example.
[UPE1-GigabitEthernet0/0/1] display bpdu-tunnel interface config
BpduDot1qStatus  disable
BpduOneQStatus   disable
BpduTwoQStatus   enable
EtherType        8100
Dot1qVlan
TwoQList         10

# Run the display stp brief command to check the STP calculation result on the CEs.

[CE1] display stp brief
MSTID    Port                Role    STP State    Protection
0        GigabitEthernet0/0/1  ROOT    FORWARDING   NONE

[CE2] display stp brief
MSTID    Port                Role    STP State    Protection
0        GigabitEthernet0/0/1  DESI    FORWARDING   NONE
```

Configuration Files

- Configuration file of CE1


```
#
sysname CE1
#
vlan batch 10
#
stp enable
#
interface ethernet 0/0/1
port trunk allow-pass vlan 10
bpdu enable
stp bpdu vlan 10
#
return
```
- Configuration file of CE2, the same as that of CE1
- Configuration file of CE3


```
#
sysname CE3
#
vlan batch 20
#
stp enable
#
interface ethernet 0/0/1
port trunk allow-pass vlan 20
stp bpdu vlan 20
bpdu enable
#
return
```
- Configuration file of CE4, the same as that of CE3
- Configuration file of UPE1


```
#
sysname UPE1
#
vlan batch 10 20
#
bpdu-tunnel stp group-mac 0100-5e00-0011
#
interface ethernet 0/0/1
port trunk allow-pass vlan 10
bpdu-tunnel stp vlan 10
bpdu enable
#
interface ethernet 0/0/2
port trunk allow-pass vlan 2
```

```

    bpdutunnel stp vlan 20
    bpdutunnel enable
    #
    return

```

- Configuration file of UPE2, the same as that of UPE1

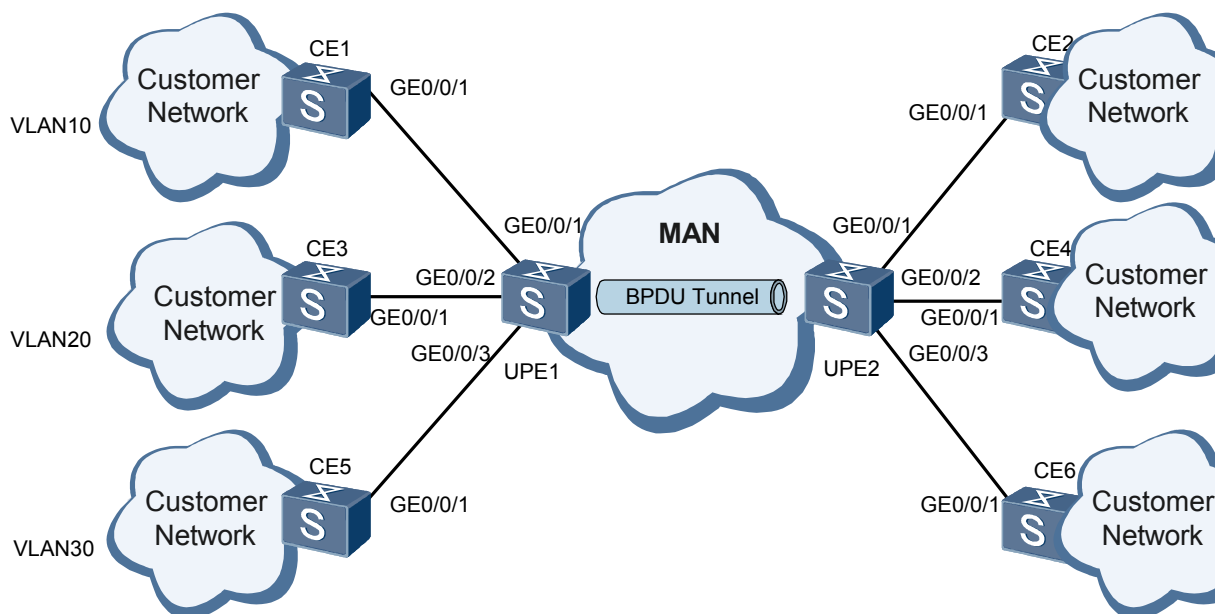
11.7.4 Example for Configuring QinQ-based BPDU Tunneling

Networking Requirements

As shown in [Figure 11-6](#), Customer network 1 connects the GigabitEthernet 0/0/1 interfaces on UPE1 and UPE2 through CE1 and CE2; Customer network 2 connects the Ethernet 0/0/2 interfaces on UPE1 and UPE2 through CE3 and CE4; Customer network 3 connects the GigabitEthernet 0/0/3 interfaces on UPE1 and UPE2 through CE5 and CE6.

It is required that BPDUs from the customer networks with STP enabled be transparently transmitted through the MAN to the peer customer networks so that the spanning tree calculation of each customer network can be complete.

Figure 11-6 Networking for configuring QinQ-based BPDU tunneling



Configuration Roadmap

The configuration roadmap is as follows:

- Tag BPDUs to be sent to the UPEs on the CEs.
- Allow the tagged BPDUs to pass the interfaces connected to the CEs on the UPEs.
- Tag the tagged BPDUs on the UPEs according to the inner tags of the BPDUs sent from the CEs.

- Replace the destination MAC address of BPDUs with a multicast MAC address on the UPEs.
- Set up the BPDU tunnel according to the tag values in BPDUs on the UPEs and enable BPDU tunneling.
- Unify the configurations on the UPEs and the CEs at the two ends of the BPDU tunnel.
- Remove the outer tags from BPDUs on the opposite UPE and send the BPDUs to the destination CEs.

Data Preparation

To complete the configuration, you need the following data:

- BPDUs from CE1 and CE2 to the UPEs belonging to VLAN 10
- BPDUs from CE3 and CE4 to the UPEs belonging to VLAN 20
- BPDUs from CE5 and CE6 to the UPEs belonging to VLAN 30
- Numbers of the user-side interfaces and that of the network-side interfaces on the UPEs
- Multicast MAC address to be used to replace the MAC address of BPDUs

Configuration Procedure

1. Configure the CEs to allow BPDUs from the specified VLANs to pass the GigabitEthernet 0/0/1 interfaces.

Configure CE1.

```
<Quidway> system-view
[Quidway] sysname CE1
[CE1] stp enable
[CE1] interface ethernet 0/0/1
[CE1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[CE1-GigabitEthernet0/0/1] quit
```

Configure CE2.

```
<Quidway> system-view
[Quidway] sysname CE2
[CE2] stp enable
[CE2] interface ethernet 0/0/1
[CE2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[CE2-GigabitEthernet0/0/1] quit
```

Configure CE3.

```
<Quidway> system-view
[Quidway] sysname CE3
[CE3] stp enable
[CE3] interface ethernet 0/0/1
[CE3-GigabitEthernet0/0/1] port trunk allow-pass vlan 20
[CE3-GigabitEthernet0/0/1] quit
```

Configure CE4.

```
<Quidway> system-view
[Quidway] sysname CE4
[CE4] stp enable
[CE4] interface ethernet 0/0/1
[CE4-GigabitEthernet0/0/1] port trunk allow-pass vlan 20
[CE4-GigabitEthernet0/0/1] quit
```

Configure CE5.

```
<Quidway> system-view
[Quidway] sysname CE5
[CE5] stp enable
```

```
[CE5] interface ethernet 0/0/1
[CE5-GigabitEthernet0/0/1] port trunk allow-pass vlan 30
[CE5-GigabitEthernet0/0/1] quit
```

Configure CE6.

```
<Quidway> system-view
[Quidway] sysname CE6
[CE6] stp enable
[CE6] interface ethernet 0/0/1
[CE6-GigabitEthernet0/0/1] port trunk allow-pass vlan 30
[CE6-GigabitEthernet0/0/1] quit
```

2. Configure the CEs to tag BPDUs to be sent to the UPEs.

Configure CE1.

```
<CE1> system-view
[CE1] vlan 10
[CE1-vlan10] port ethernet 0/0/1
[CE1-vlan10] quit
[CE1] interface ethernet 0/0/1
[CE1-GigabitEthernet0/0/1] bpdu enable
[CE1-GigabitEthernet0/0/1] stp bpdu vlan 10
[CE1-GigabitEthernet0/0/1] quit
```

Configure CE2.

```
<CE2> system-view
[CE2] vlan 10
[CE2-vlan10] port ethernet 0/0/1
[CE2-vlan10] quit
[CE2] interface ethernet 0/0/1
[CE2-GigabitEthernet0/0/1] bpdu enable
[CE2-GigabitEthernet0/0/1] stp bpdu vlan 10
[CE2-GigabitEthernet0/0/1] quit
```

Configure CE3.

```
<CE3> system-view
[CE3] vlan 20
[CE3-vlan20] port ethernet 0/0/1
[CE3-vlan20] quit
[CE3] interface ethernet 0/0/1
[CE3-GigabitEthernet0/0/1] bpdu enable
[CE3-GigabitEthernet0/0/1] stp bpdu vlan 20
[CE3-GigabitEthernet0/0/1] quit
```

Configure CE4.

```
<CE4> system-view
[CE4] vlan 20
[CE4-vlan20] port ethernet 0/0/1
[CE4-vlan20] quit
[CE4] interface ethernet 0/0/1
[CE4-GigabitEthernet0/0/1] bpdu enable
[CE4-GigabitEthernet0/0/1] stp bpdu vlan 20
[CE4-GigabitEthernet0/0/1] quit
```

Configure CE5.

```
<CE5> system-view
[CE5] vlan 30
[CE5-vlan30] port ethernet 0/0/1
[CE5-vlan30] quit
[CE5] interface ethernet 0/0/1
[CE5-GigabitEthernet0/0/1] bpdu enable
[CE5-GigabitEthernet0/0/1] stp bpdu vlan 30
[CE5-GigabitEthernet0/0/1] quit
```

Configure CE6.

```
<CE6> system-view
[CE6] vlan 30
[CE6-vlan30] port ethernet 0/0/1
[CE6-vlan30] quit
```

```
[CE6] interface ethernet 0/0/1
[CE6-GigabitEthernet0/0/1] bpdu enable
[CE6-GigabitEthernet0/0/1] stp bpdu vlan 30
[CE6-GigabitEthernet0/0/1] quit
```

3. Configure the UPEs to replace the destination MAC address of BPDUs with a multicast MAC address.

Configure UPE1.

```
<Quidway> system-view
[Quidway] sysname UPE1
[UPE1] bpdu-tunnel stp group-mac 0100-5e00-0011
```

Configure UPE2.

```
<Quidway> system-view
[Quidway] sysname UPE2
[UPE2] bpdu-tunnel stp group-mac 0100-5e00-0011
```

NOTE

The multicast MAC address can vary on UPE1 and UPE2. You are recommended to set the same multicast MAC address on the UPEs.

4. Configure the UPEs to tag BPDUs from the CEs and remove the outer tags from BPDUs to the CEs.

Configure UPE1.

```
<UPE1> system-view
[UPE1] vlan 100
[UPE1-vlan100] quit
[UPE1] interface ethernet 0/0/1
[UPE1-GigabitEthernet0/0/1] port default vlan 3
[UPE1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[UPE1-GigabitEthernet0/0/1] qinq vlan-traslation enable
[UPE1-GigabitEthernet0/0/1] qinq vlan-traslation port vlan-stacking vlan 10
priority-inherit inbound
[UPE1-GigabitEthernet0/0/1] quit
[UPE1] interface ethernet 0/0/3
[UPE1-GigabitEthernet0/0/3] port default vlan 3
[UPE1-GigabitEthernet0/0/3] port trunk allow-pass vlan 30
[UPE1-GigabitEthernet0/0/3] qinq vlan-traslation enable
[UPE1-GigabitEthernet0/0/3] qinq vlan-traslation vlan 30 push vlan 100
priority-inherit inbound
[UPE1-GigabitEthernet0/0/3] quit
```

Configure UPE2.

```
<UPE2> system-view
[UPE2] vlan 100
[UPE2-vlan100] quit
[UPE2] interface ethernet 0/0/1
[UPE2-GigabitEthernet0/0/1] port default vlan 3
[UPE2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[UPE2-GigabitEthernet0/0/1] qinq vlan-traslation enable
[UPE2-GigabitEthernet0/0/1] qinq vlan-traslation vlan 10 push vlan 100
priority-inherit inbound [UPE2-GigabitEthernet0/0/1] quit
[UPE2] interface ethernet 0/0/2
[UPE2-GigabitEthernet0/0/2] port default vlan 3
[UPE2-GigabitEthernet0/0/2] port trunk allow-pass vlan 20
[UPE2-GigabitEthernet0/0/2] qinq vlan-traslation enable
[UPE2-GigabitEthernet0/0/2] qinq vlan-traslation vlan 20 push vlan 100
priority-inherit inbound [UPE2-GigabitEthernet0/0/2] quit
[UPE2] interface ethernet 0/0/3
[UPE2-GigabitEthernet0/0/3] port default vlan 3
[UPE2-GigabitEthernet0/0/3] port trunk allow-pass vlan 30
[UPE2-GigabitEthernet0/0/3] qinq vlan-traslation enable
[UPE2-GigabitEthernet0/0/3] qinq vlan-traslation vlan 30 push vlan 100
priority-inherit inbound [UPE2-GigabitEthernet0/0/3] quit
```

5. Configure the PEs to transmit BPDUs from the specified VLANs through the BPDU tunnel.

Configure UPE1.

```

<UPE1> system-view
[UPE1] interface ethernet 0/0/1
[UPE1-GigabitEthernet0/0/1] bpdu-tunnel stp vlan 100
[UPE1-GigabitEthernet0/0/1] quit
[UPE1] interface ethernet 0/0/2
[UPE1-GigabitEthernet0/0/2] bpdu enable
[UPE1-GigabitEthernet0/0/2] bpdu-tunnel stp vlan 100
[UPE1-GigabitEthernet0/0/2] quit
[UPE1] interface ethernet 0/0/3
[UPE1-GigabitEthernet0/0/3] bpdu enable
[UPE1-GigabitEthernet0/0/3] bpdu-tunnel stp vlan 100
[UPE1-GigabitEthernet0/0/3] quit
[UPE1] interface ethernet 0/0/4
[UPE1-GigabitEthernet0/0/4] port trunk allow-pass vlan 100
[UPE1-GigabitEthernet0/0/4] quit

```

Configure UPE2.

```

<UPE2> system-view
[UPE2] interface ethernet 0/0/1
[UPE2-GigabitEthernet0/0/1] bpdu enable
[UPE2-GigabitEthernet0/0/1] bpdu-tunnel stp vlan 100
[UPE2-GigabitEthernet0/0/1] quit
[UPE2] interface ethernet 0/0/2
[UPE2-GigabitEthernet0/0/2] bpdu enable
[UPE2-GigabitEthernet0/0/2] bpdu-tunnel stp vlan 100
[UPE2-GigabitEthernet0/0/2] quit
[UPE2] interface ethernet 0/0/3
[UPE2-GigabitEthernet0/0/3] bpdu enable
[UPE2-GigabitEthernet0/0/3] bpdu-tunnel stp vlan 100
[UPE2-GigabitEthernet0/0/3] quit
[UPE2] interface ethernet 0/0/4
[UPE2-GigabitEthernet0/0/4] port trunk allow-pass vlan 100
[UPE2-GigabitEthernet0/0/4] quit

```

6. Verify the configuration.

Run the **display bpdu-tunnel interface config** command, and you can view the inner tag, outer tag, and TPID configured on an interface.

Take CE1 as an example.

```

[CE1-GigabitEthernet0/0/1] display bpdu-tunnel interface config
BpduDot1qStatus  enable
BpduOneQStatus   disable
BpduTwoQStatus   disable
EtherType        8100
Dot1qVlan        10
TwoQList

```

Take UPE1 as an example.

```

[UPE1-GigabitEthernet0/0/1] display bpdu-tunnel interface config
BpduDot1qStatus  disable
BpduOneQStatus   disable
BpduTwoQStatus   enable
EtherType        8100
Dot1qVlan        100
TwoQList

```

Configuration Files

- Configuration file of CE1

```

#
sysname CE1
#
stp enable
#
interface ethernet 0/0/1
port trunk allow-pass vlan 10
stp bpdu vlan 10

```

```
    bpdu enable
#
    vlan batch 10
#
return
```

- Configuration file of CE2

```
#
sysname CE2
#
    stp enable
#
interface GigabitEthernet0/0/1
    port trunk allow-pass vlan 10
    stp bpdu vlan 10
    bpdu enable
#
vlan batch 10
#
return
```

- Configuration file of CE3

```
#
sysname CE3
#
    stp enable
#
interface GigabitEthernet0/0/1
    port trunk allow-pass vlan 20
    stp bpdu vlan 20
    bpdu enable
#
vlan batch 20
#
return
```

- Configuration file of CE4

```
#
sysname CE4
#
    stp enable
#
interface GigabitEthernet0/0/1
    port trunk allow-pass vlan 20
    bpdu enable
    stp bpdu vlan 20
#
vlan batch 20
#
return
```

- Configuration file of CE5

```
#
sysname CE5
#
    stp enable
#
interface GigabitEthernet0/0/1
    port trunk allow-pass vlan 30
    stp bpdu vlan 30
    bpdu enable
#
vlan batch 30
#
return
```

- Configuration file of CE6

```
#
sysname CE6
```

```
#
stp enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 30
stp bpdu vlan 30
bpdu enable
#
vlan batch 30
#
return
```

- Configuration file of UPE1

```
#
sysname UPE1
#
bpdu-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/1
port default vlan 3
port trunk allow-pass vlan 10
port vlan-stacking enable
port vlan-stacking vlan 10 push vlan 100 priority-inherit inbound
bpdu-tunnel stp vlan 10
bpdu enable
#
interface GigabitEthernet0/0/2
port default vlan 3
port trunk allow-pass vlan 20
port vlan-stacking enable
port vlan-stacking vlan 20 push vlan 100 priority-inherit inbound
bpdu-tunnel stp vlan 20
#
interface GigabitEthernet0/0/3
port default vlan 3
port trunk allow-pass vlan 30
port vlan-stacking enable
port vlan-stacking vlan 30 push vlan 100 priority-inherit inbound
bpdu-tunnel stp vlan 30
bpdu enable
interface GigabitEthernet0/0/4
port trunk allow-pass vlan 100
#
return
```

- Configuration file of UPE2

```
#
sysname UPE2
#
bpdu-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/1 port default vlan 3
port trunk allow-pass vlan 10
port vlan-stacking enable
port vlan-stacking vlan 10 push vlan 100 priority-inherit inbound
bpdu-tunnel stp vlan 10 bpdu enable
#
interface Ethernet0/0/2
port default vlan 3
port trunk allow-pass vlan 20
port vlan-stacking enable
port vlan-stacking vlan 20 push vlan 100 priority-inherit inbound
bpdu-tunnel stp vlan 20 bpdu enable
#
interface Ethernet0/0/3
port default vlan 3
port trunk allow-pass vlan 30
port vlan-stacking enable
port vlan-stacking vlan 30 push vlan 100 priority-inherit inbound
bpdu-tunnel stp vlan 30 bpdu enable
```

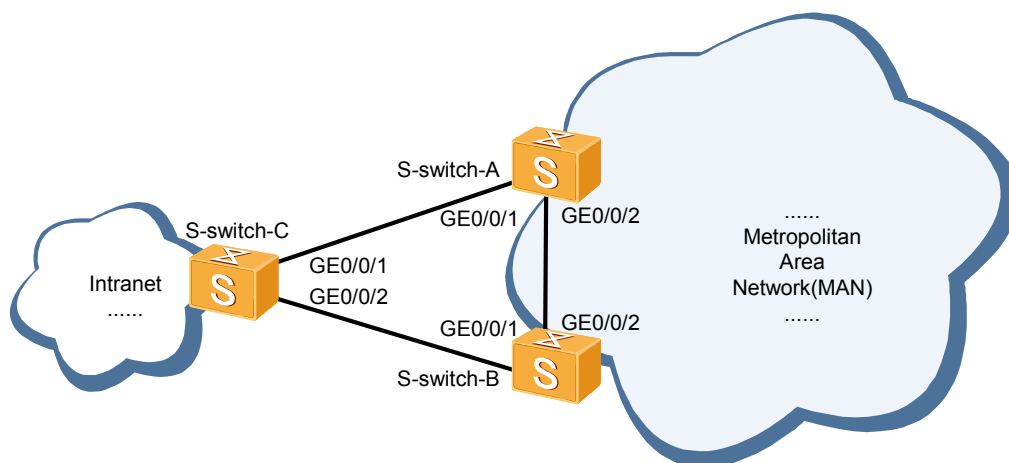
```
#
interface Ethernet0/0/4
 port trunk allow-pass vlan 100
#
return
```

11.7.5 Example for Configuring Partitioned STP

Networking Requirements

As shown in [Figure 11-7](#), the intranet accesses the MAN through two Ethernet interfaces on the S-switch which connects two S-switchs in the MAN for the sake of high availability. It is required that no loop occur between the intranet and the MAN when partitioned STP is enabled.

Figure 11-7 Networking for configuring partitioned STP



Configuration Roadmap

The configuration roadmap is as follows:

- Enable MSTP on S-switch-C.
- Create VLAN 10 on S-switch-C. Enable the GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 interfaces to tag and process BPDUs.
- Create VLAN 10 on S-switch-A. Enable the processing of BPDUs and BPDU tunneling on GigabitEthernet 0/0/1. Allow BPDUs from VLAN 10 to pass GigabitEthernet 0/0/2.
- Create VLAN 10 on S-switch-B. Enable the processing of BPDUs and BPDU tunneling on GigabitEthernet 0/0/1. Allow BPDUs from VLAN 10 to pass GigabitEthernet 0/0/2.
- Enable STP snooping on S-switch-A and S-switch-B.

Data Preparation

To complete the configuration, you need the following data:

- VLAN ID 10 to be used in the partitioned STP network

- Numbers of the interfaces through which the S-switchs are directly connected

Configuration Procedure

1. Enable MSTP on S-switch-C.

```
[S-switch-C] stp enable
```

2. On S-switch-C, configure the interfaces to tag BPDUs.

Create VLAN 10.

```
[S-switch-C] vlan 10
[S-switch-C-vlan10] quit
```

Configure GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 to tag and process BPDUs.

```
[S-switch-C] interface ethernet 0/0/1
[S-switch-C-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[S-switch-C-GigabitEthernet0/0/1] stp bpdu vlan 10
[S-switch-C-GigabitEthernet0/0/1] bpdu enable
[S-switch-C-GigabitEthernet0/0/1] quit
[S-switch-C] interface ethernet 0/0/2
[S-switch-C-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[S-switch-C-GigabitEthernet0/0/2] stp bpdu vlan 10
[S-switch-C-GigabitEthernet0/0/2] bpdu enable
```

3. Enable BPDU tunneling on S-switch-A.

Create VLAN 10.

```
[S-switch-A] vlan 10
[S-switch-A-vlan10] quit
```

Enable BPDU tunneling on GigabitEthernet 0/0/1.

```
[S-switch-A] interface gigabitethernet 0/0/1
[S-switch-A-GigabitEthernet0/0/1] bpdu-tunnel stp vlan 10
```

Replace the MAC address of BPDUs.

```
[S-switch-A] bpdu-tunnel stp group-mac 0100-5e00-0011
```

Configure Ethernet 0/0/1 to process BPDUs.

```
[S-switch-A-GigabitEthernet0/0/1] bpdu enable
```

Allow BPDUs from VLAN 10 to pass Ethernet 0/0/1.

```
[S-switch-A-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[S-switch-A-GigabitEthernet0/0/1] quit
```

Allow BPDUs from VLAN 10 to pass GigabitEthernet 0/0/2.

```
[S-switch-A] interface ethernet 0/0/2
[S-switch-A-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
```

4. Enable BPDU tunneling on S-switch-B.

Create VLAN 10.

```
[S-switch-B] vlan 10
[S-switch-B-vlan10] quit
```

Enable BPDU tunneling on GigabitEthernet 0/0/1.

```
[S-switch-B] interface ethernet 0/0/1
[S-switch-B-GigabitEthernet0/0/1] bpdu-tunnel stp vlan 10
```

Replace the MAC address of BPDUs.

```
[S-switch-B] bpdu-tunnel stp group-mac 0100-5e00-0011
```

Configure Ethernet 0/0/1 to process BPDUs.

```
[S-switch-B-GigabitEthernet0/0/1] bpdu enable
```

Allow BPDUs from VLAN 10 to pass Ethernet 0/0/1.

```
[S-switch-B-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
```

- ```
[S-switch-B-GigabitEthernet0/0/1] quit
```
- # Allow BPDUs from VLAN 10 to pass GigabitEthernet 0/0/2.
- ```
[S-switch-B] interface ethernet 0/0/2
[S-switch-B-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
```
5. Enable STP snooping on S-switch-A and S-switch-B.

Enable STP snooping on S-switch-A.

```
[S-switch-A] stp-snooping enable
```

Enable STP snooping on S-switch-B.

```
[S-switch-B] stp-snooping enable
```
 6. Verify the configuration.

Check the configuration of S-switch-C.

```
<S-switch-C> display stp brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/1	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/2	BACK	DISCARDING	NONE

You can view that the STP calculation on S-switch-C is correct, Ethernet 0/0/2 is in the Discarding state, and no loop is formed between S-switch-C, S-switch-A, and S-switch-B.

Check the configuration of S-switch-A.

```
[S-switch-A] interface ethernet0/0/1
[S-switch-A-GigabitEthernet0/0/1] display bpdu-tunnel interface config
```

```
BpduDot1qStatus  disable
BpduOneQStatus   disable
BpduTwoQStatus   enable
EtherType        8100
Dot1qVlan
TwoQList         10
```

The "BpduTwoQStatus enable" field indicates that Ethernet 0/0/1 allows the tagged BPDUs to pass.

Configuration Files

- Configuration file of S-switch-A


```
#
sysname S-switch-A
#
vlan batch 10
#
stp-snooping enable
#
bpdu-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
bpdu enable
bpdu-tunnel stp vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 10
#
return
```
- Configuration file of S-switch-B


```
#
sysname S-switch-B
#
vlan batch 10
#
stp-snooping enable
#
```

```
bpdu-tunnel stp group-mac 0100-5e00-0011
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
bpdu enable
bpdu-tunnel stp vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 10
#
return
```

- Configuration file of S-switch-C

```
#
sysname S-switch-C
#
vlan batch 10
#
stp enable
#
interface GigabitEthernet0/0/1
port trunk allow-pass vlan 10
bpdu enable
stp bpdu vlan 10
#
interface GigabitEthernet0/0/2
port trunk allow-pass vlan 10
stp bpdu vlan 10
bpdu enable
#
return
```