

S Series Switch

SEP Technology White Paper

Issue 01

Date 2013-05-25

Copyright © Huawei Technologies Co., Ltd. 2012. 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 trademarks of Huawei Technologies Co., Ltd.

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

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

Contents

1 Feature Introduction	1
1.1 SEP Overview	1
1.2 References	2
2 Technology Description.....	3
2.1 Concepts.....	3
2.1.1 SEP Segment.....	3
2.1.2 Control VLAN	3
2.1.3 Node.....	3
2.1.4 Port Roles.....	3
2.1.5 Port Status	6
2.2 SEP Packet	7
2.3 SEP Implementation Mechanisms.....	14
2.3.1 Neighbor Negotiation.....	14
2.3.2 LSDB Synchronization and Topology Display	15
2.3.3 Primary Edge Port Election.....	18
2.3.4 Port Blocking Mechanism.....	19
2.3.5 Port Preemption	22
2.4 SEP Troubleshooting Mechanisms.....	26
2.4.1 Topology Change Notification and Suppression	26
2.4.2 Failover	31
2.4.3 Failback.....	35
2.5 SEP Load Balancing.....	39
3 Product Capabilities	43
3.1 Model Support.....	43
3.2 Specifications and Limitations	43
4 Application Scenarios	44
4.1 Example for Configuring SEP on a Closed Ring Network	44
4.1.1 Networking Requirements	44
4.1.2 Configuration Roadmap.....	45
4.1.3 Procedure	46
4.1.4 Configuration Files	48
4.2 Example for Configuring SEP on a Multi-Ring Network	51

4.2.1 Networking Requirements	51
4.2.2 Configuration Roadmap	52
4.2.3 Procedure	53
4.2.4 Configuration Files	58
4.3 Example for Configuring SEP Multi-Instance	64
4.3.1 Networking Requirements	64
4.3.2 Configuration Roadmap	65
4.3.3 Procedure	65
4.3.4 Configuration Files	68
4.4 Example for Configuring a Hybrid SEP+MSTP Network	71
4.4.1 Networking Requirements	71
4.4.2 Configuration Roadmap	73
4.4.3 Procedure	73
4.4.4 Configuration Files	77
4.5 Example for Configuring a Hybrid SEP+RRPP Network	80
4.5.1 Networking Requirements	80
4.5.2 Configuration Roadmap	82
4.5.3 Procedure	82
4.5.4 Configuration Files	89
4.6 Example for Configuring Association Between SEP and VPLS	93
4.6.1 Networking Requirements	93
4.6.2 Configuration Roadmap	95
4.6.3 Procedure	95
4.6.4 Configuration Files	102
5 Troubleshooting	108
5.1 Traffic Forwarding Fails After SEP Is Configured	108
6 FAQ	109
6.1 What Advantages Does SEP Have Compared with Other Ring Network Protocols?	109
A Acronyms and Abbreviations	110
B References	111

1 Feature Introduction

1.1 SEP Overview

Definition

The Smart Ethernet Protection (SEP) protocol is a ring network protocol specially used for the Ethernet link layer. SEP selectively blocks redundant links to eliminate Layer 2 loops, which effectively prevents ring faults such as broadcast storms and MAC address table flapping.

Purpose

As networks are spreading and network applications become diversified, reliability of basic networks is the focus of users. It is important to ensure non-interrupted service transmission.

Generally, redundant links are used on a network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms.

To solve the loop problem, Huawei datacom devices support many ring network protocols such as Spanning Tree Protocol (STP). STP is a standard protocol for eliminating loops on Ethernet networks. The network convergence time of STP is affected by the network topology. On a large network, convergence is slow, failing to meet transmission requirements of some real-time services.

Huawei developed SEP to overcome the disadvantages of other ring network protocols. SEP boasts fast convergence (less than 50 ms). Compared with STP, SEP meets transmission requirements of real-time services. When the network is complete, SEP selectively blocks redundant links to eliminate loops; when a link on the ring network fails, SEP immediately unblocks the blocked port and performs link switching, protecting user services on the network.

Benefits

SEP brings customers a new choice of the ring network protocol. Compared with traditional ring network protocols such as STP, SEP boasts fast convergence and applies to Layer 2 networks requiring short convergence time. In addition, SEP has the following advantages:

- Applies to diverse scenarios, and supports various network topologies and flexible configurations.
- Allows selective port blocking, which effectively implements traffic load balancing.

- Prevents traffic from being switched back after link recovery, which improves network stability.
- Displays the SEP network topology from any node, which facilitates management and improves network maintainability.

1.2 References

SEP is a Huawei proprietary protocol.

2 Technology Description

2.1 Concepts

2.1.1 SEP Segment

A SEP segment is the basic unit of SEP. A SEP segment consists of connected Layer 2 switches configured with the same SEP segment ID and control VLAN ID and links connecting the switches. Only two ports on each switch can be added to the same SEP segment.

A SEP segment includes:

- Control VLAN
- Node
- Edge port
- Common port

2.1.2 Control VLAN

In a SEP segment, the control VLAN is used to transmit only SEP packets. Different from the control VLAN, the data VLAN is used to transmit data packets.

Each SEP segment must have a control VLAN. All nodes in a SEP segment must be configured with the same control VLAN that has not been created or used by other protocols. Ports added to the SEP segment are automatically added to the control VLAN to ensure forwarding of SEP packets.

2.1.3 Node

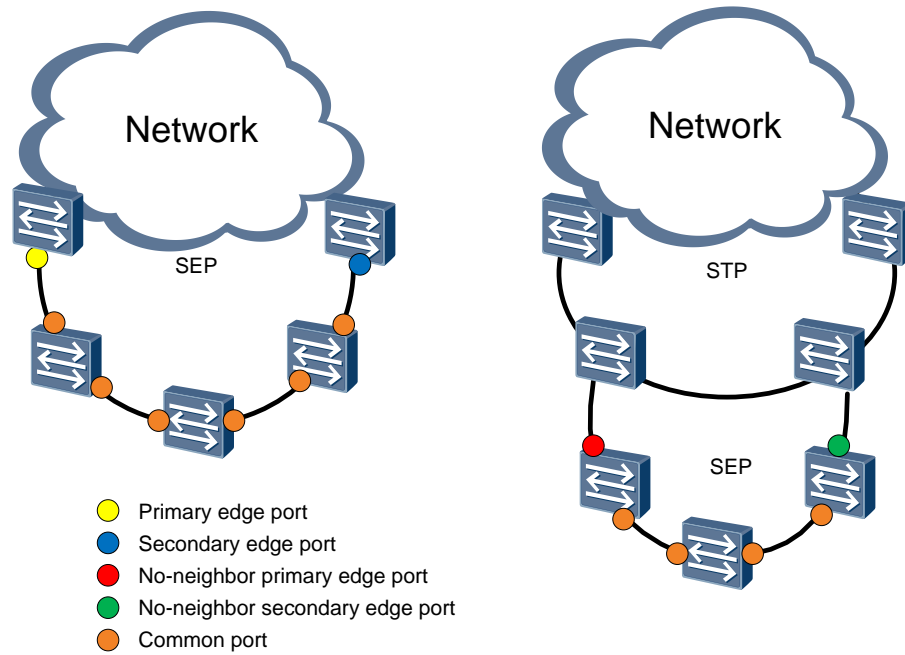
Each switch in a SEP segment is a node. Only two ports on each switch can be added to the same SEP segment.

2.1.4 Port Roles

As defined in SEP, ports are classified into common ports and edge ports.

Figure 2-1 shows port roles on an open ring network. An open ring network is a SEP segment where the primary and secondary edge ports are located on different nodes.

Figure 2-1 Port roles on an open ring network

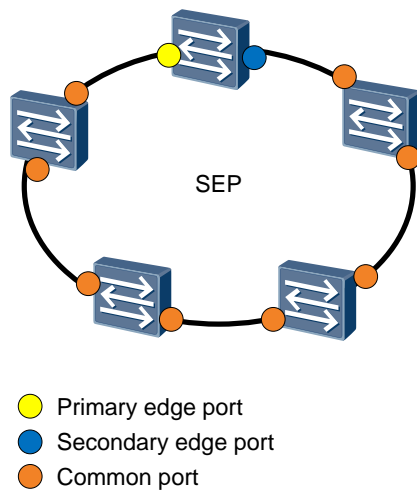


On an open ring network, port roles include:

- Common port
- Edge port
 - Primary edge port
 - Secondary edge port
 - No-neighbor primary edge port
 - No-neighbor secondary edge port

Figure 2-2 shows port roles on a closed ring network. A closed ring network is a SEP segment where the primary and secondary edge ports are located on the same node.

Figure 2-2 Port roles on a closed ring network




On a closed ring network, port roles include:

- Common port
- Edge port
 - Primary edge port
 - Secondary edge port

Table 2-1 describes port roles in details.

Table 2-1 Port roles

Port Role	Sub-role	Description
Edge port	Primary edge port	<p>A SEP segment has only one primary edge port, which is determined by the configuration and election.</p> <p>The primary edge port initiates blocked port preemption, terminates packets, and sends topology change notification messages to other networks.</p>
	Secondary edge port	<p>A SEP segment has only one secondary edge port, which is determined by the configuration and election.</p> <p>The secondary edge port terminates packets and sends topology change notification messages to other networks.</p>
	No-neighbor primary edge port	<p>A port on the edge of a SEP segment is a no-neighbor edge port, which is determined by the configuration.</p> <p>The no-neighbor primary edge port terminates packets and sends topology change notification messages to other networks.</p> <p>No-neighbor primary edge ports are used to connect Huawei devices and non-Huawei devices or devices that do not support SEP.</p> <p>A no-neighbor primary edge port initiates blocked port preemption based on whether the brother port of the no-neighbor primary edge port is a blocked port.</p> <p> NOTE</p> <p>Only two ports on each switch can be added to the same SEP segment. If one port is the no-neighbor primary edge port, the other port is the brother port of the no-neighbor primary edge port.</p> <ul style="list-style-type: none"> ● If the brother port is a blocked port, the no-neighbor primary edge port does not need to initiate blocked port preemption. ● If the brother port is not a blocked port, the brother port of the no-neighbor primary edge port initiates blocked port preemption.

Port Role	Sub-role	Description
	No-neighbor secondary edge port	<p>A SEP segment has only one no-neighbor secondary edge port, which is determined by the configuration and election.</p> <p>The no-neighbor secondary edge port terminates packets and sends topology change notification messages to other networks.</p> <p>No-neighbor secondary edge ports are used to connect Huawei devices and non-Huawei devices or devices that do not support SEP.</p>
Common port	-	<p>In a SEP segment, all ports except edge ports are common ports.</p> <p>A common port monitors the status of the directly connected SEP link. When the link status changes, the port sends a topology change notification message to notify its neighbors. Then the topology change notification message is flooded in the SEP segment until it finally reaches the primary edge port. The primary edge port determines how to process the link change.</p>

2.1.5 Port Status

In a SEP segment, a port can work in Forwarding state or Discarding state, as listed in Table 2-2.

Table 2-2 Port status in a SEP segment

Port Status	Description
Forwarding	A port in Forwarding state can forward service traffic while sending and receiving SEP packets.
Discarding	In a SEP segment, a port is blocked to prevent loops. The blocked port is in Discarding state. Any port in a SEP segment may be blocked if no port is explicitly specified to be blocked. A complete SEP segment has only one blocked port. A port in Discarding state can send and receive SEP packets and packets of other protocols but cannot forward service traffic.

Packets of some protocols besides SEP can pass a blocked port so that protocol exchange between two sides of the blocked port is not affected. Table 2-3 lists packets that can pass a port in Discarding state.

Table 2-3 Packets that can pass a port in Discarding state

Feature	Protocol Packet	Whether the Packet Can Pass the Port (Yes/No)
Eth-Trunk	Link Aggregation Control Protocol (LACP) packet	Yes
802.3ah	802.3ah protocol packet	Yes
	802.3ah test packet	Yes
Device Link Detection Protocol (DLDP)	DLDP packet	Yes
Link Layer Discovery Protocol (LLDP)	LLDP packet	Yes
	Cisco Discovery Protocol (CDP) packet	Yes
Flow control	Flow control packet	Yes
Bidirectional Forwarding Detection (BFD) for multicast	BFD packet in multicast mode	Yes
Huawei Group Management Protocol (HGMP)	HGMP Neighbor Discovery message (multicast)	Yes
	HGMP Neighbor Discovery message (broadcast)	No
802.1ag	Continuity check message (CCM)	Yes
	Loopback message (LBM), linktrace message (LTM), loopback reply (LBR) message, linktrace reply (LTR) message, MAC ping packet, and MAC trace packet	No

2.2 SEP Packet

Figure 2-3 shows the format of a SEP packet.

Figure 2-3 SEP packet format

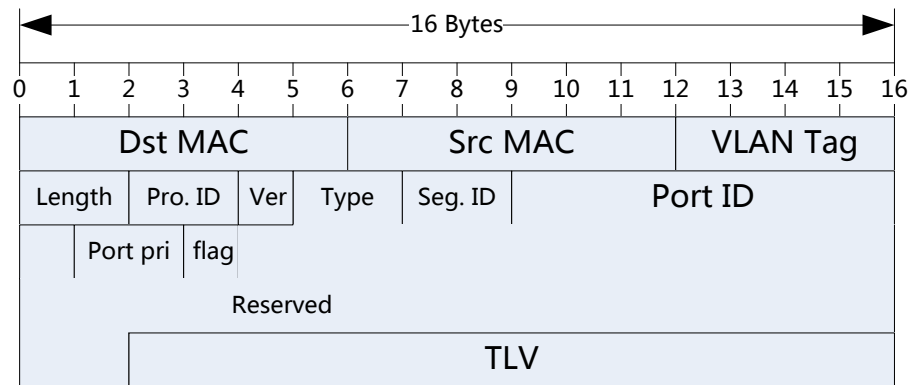


Table 2-4 lists the meanings of each field in a SEP packet.

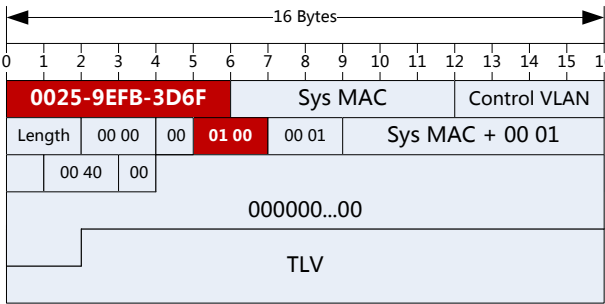
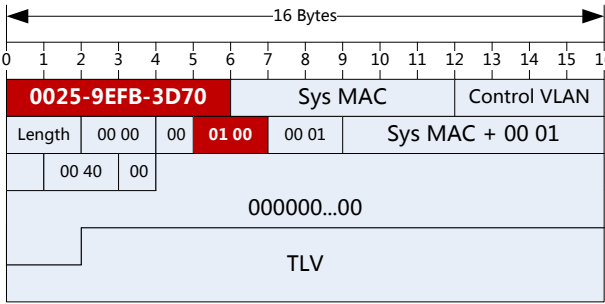
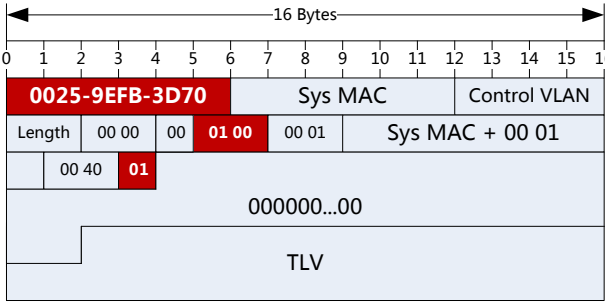
Table 2-4 Fields in a SEP packet

Field	Length (Byte)	Description
Dst MAC	6	Destination MAC address of a SEP packet, including 0025-9EFB-3D6F and 0025-9EFB-3D70. The MAC address 0025-9EFB-3D6F indicates a point-to-point (P2P) packet that is terminated at the next-hop port, and 0025-9EFB-3D70 indicates a point-to-multipoint (P2MP) packet that is terminated at an edge port. <ul style="list-style-type: none"> ● 0025-9EFB-3D6F: indicates a Hello packet, link-state advertisement (LSA) packet, or graceful restart (GR) packet. ● 0025-9EFB-3D70: indicates a preemption packet, edge port advertisement (EPA) packet for primary edge port election, blocked port advertisement (BPA) packet, or a topology change (TC) packet.
Src MAC	6	System MAC address.
VLAN Tag	4	VLAN tag of the SEP packet. The VLAN ID is the control VLAN ID of the SEP segment and the packet priority is 7.
Length	2	Length of the entire packet.
Pro. ID	2	SEP protocol ID, which is fixed as 00 00 and identifies a SEP packet.
Ver	1	SEP protocol version, which is 00 at present.
Type	2	Type and subtype of the SEP packet, each of which occupies 1 byte. For SEP packet types, see Table 2-5.
Seg. ID	2	SEP segment ID to which the SEP packet belongs.

Field	Length (Byte)	Description
Port ID	8	Port ID composed of the 6-byte system MAC address and 2-byte port index. The index of the first port added to the SEP segment is 00 00, and the index of the second port added to the SEP segment is 00 01.
Port Pri.	2	Port priority. The higher 8 bits of the port priority are defined by the system, and the lower 8 bits are set by the user. The default port priority is 64. For details, see SEP Port Priority in section 2.3.4 "Port Blocking Mechanism".
Flag	1	Whether the SEP packet contains TC information. <ul style="list-style-type: none"> 0: The SEP packet does not contain TC information. 1: The SEP packet contains TC information.
Reserved	30	Reserved field, which is filled with all 0s.
TLV	Not fixed	Type-length-value (TLV) combination based on the packet type. For the TLV definition, see Table 2-6.

Table 2-5 Type and subtype of a SEP packet

Type	Packet Function	Subtype	Description
00: Hello packet	After a port is added to a SEP segment, neighbor negotiation starts. The port and its neighbor exchange Hello packets to establish a neighbor relationship. After neighbor negotiation succeeds, the two ports continue to exchange Hello packets to detect their neighbor status. This packet is a P2P packet. The default transmission interval is 1s, and the default timeout period is 60s.	00: enabled	<p>Hello packet sent when the port is added to a SEP segment:</p>
		01: disabled	<p>Hello packet sent when the port is deleted from a SEP segment:</p>

Type	Packet Function	Subtype	Description
01: LSA packet	<p>LSA packets are used in the following scenarios:</p> <ul style="list-style-type: none"> Neighbor LSDB update. After a port has SEP enabled, the port periodically sends LSA packets to its neighbor. After the state machine of the neighbor goes Up, the two ports update their link state databases (LSDBs), that is, all topology information. This packet is a P2P packet, which is sent every 20s and aged out every 60s. When the local LSDB changes, the port immediately sends an LSA packet. Blocked node advertisement. The node where the blocked port resides sends a BPA packet to advertise the node's location to other nodes. This packet is a P2MP packet, which is sent every 1s. Topology change 	00: LSA Info packet	<p>LSA Info packet updating neighbor LSDBs</p>  <p>BPA packet</p>  <p>TC packet</p> 

Type	Packet Function	Subtype	Description
	advertisement. When the topology of the local SEP segment changes, the node sends a TC packet to notify other nodes in the SEP segment and upper-level and lower-level networks of the change. The other nodes and upper-level and lower-level networks then update their MAC address tables and ARP tables. This packet is a P2MP packet.	01: LSA ACK packet	<p>LSA ACK packet responding to an LSA Info packet</p>
02: Preemption packet	<p>A preemption packet is used to block the specified port.</p> <p>Preemption packets are sent by the elected primary edge port or the brother port of a no-neighbor primary edge port.</p> <p>This packet is a P2MP packet, which uses the request-ACK mechanism. If a port receives no response after sending five consecutive Preemption Request packets, the port considers preemption failed and records a log.</p>	00: Preemption Request packet	<p>Preemption Request packet</p>
		01: Preemption ACK packet	<p>Preemption ACK packet</p>

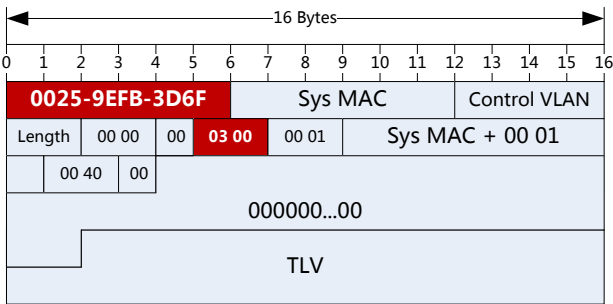
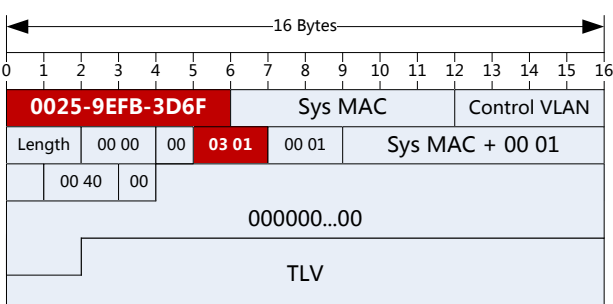
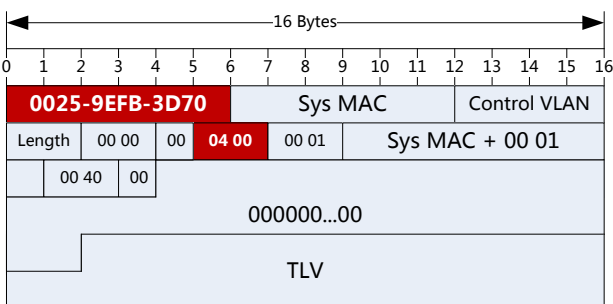
Type	Packet Function	Subtype	Description
03: GR packet	When a device performs an active/standby switchover, it sends a GR packet to instruct other nodes to prolong the aging time of the LSA packets received from the device. After the active/standby switchover is complete, the device needs to send another GR packet to instruct other nodes to restore the aging time of the LSA packets received from the device to the previous value. This packet is a P2P packet, which is triggered to be sent.	00: GR_START	GR and the active/standby switchover start. 
		01: GR_END	GR and the active/standby switchover are complete. 
04: EPA packet	After a port has SEP enabled, it periodically sends EPA packets without waiting for the success of neighbor negotiation, if it is qualified for the primary edge port election. This packet is a P2MP packet, which is sent every 1s and aged out every 60s by default.	-	An EPA packet contains the port role (primary edge port, secondary edge port, or common port), bridge MAC address of the port, port ID, and integrity of the topology database. 

Table 2-6 TLV fields

Packet	Type	Length	Value
Hello packet	0x01	00 08	Neighbor port ID. If the neighbor relationship is not established, the Hello packet does not contain the TLV.

Packet	Type	Length	Value
LSA Info packet or BPA packet	0x64	00 01	The followings are TLV fields in an LSA packet.
	0x01	00 08	Local port ID.
	0x02	Not fixed	Local system name.
	0x03	Not fixed	Local port name, in short form.
	0x04	00 02	SEP priority of the local port.
	0x05	00 01	Link status (0: down; 1: up).
	0x06	00 01	Neighbor status (0: down; 1: initial; 2: preup; 3: up, 4: conflict), in binary format.
	0x07	00 01	Port status (0: discarding; 1: forwarding).
	0x08	00 01	Management status role.
	0x09	00 01	Running status role.
	0x0a	00 08	Neighbor port ID.
	0x0b	00 08	Brother port ID.
	0x0c	00 02	Aging time of the local port.
	0x0d	00 04	Sequence number of the LSA packet.
	0x0e	00 01	Version number of the LSA packet, which is fixed as 0x01.
LSA ACK packet	0x64	00 01	Number of TLVs.
	0x01	00 08	Local port ID.
	0x0d	00 04	Sequence number of the LSA packet.
TC packet	0x65	00 01	On the basis of the TLV in an LSA Info packet, the following field is added. The followings are 5 TLVs in a TC packet.
	0x01	00 08	Port ID of link 1 where the TC occurs.
	0x02	00 08	Port ID of link 2 where the TC occurs.
	0x03	00 04	Sequence number of TC port 1, which is currently all 0s.
	0x04	00 04	Sequence number of TC port 2, which is currently all 0s.
	0x05	00 02	ID of the segment where the TC occurs.
Preemption Request packet	0x01	00 08	Blocked port ID.
Preemption ACK packet	0x01	00 08	Primary edge port ID.

Packet	Type	Length	Value
EPA packet	0x01	00 08	Local edge port ID.
	0x02	00 01	Timeout flag.
	0x03	00 01	Neighbor status (0: down; 1: initial; 2: preup; 3: up, 4: conflict), in binary format.
	0x04	00 01	Management status role.
	0x05	00 01	Running status role.

2.3 SEP Implementation Mechanisms

2.3.1 Neighbor Negotiation

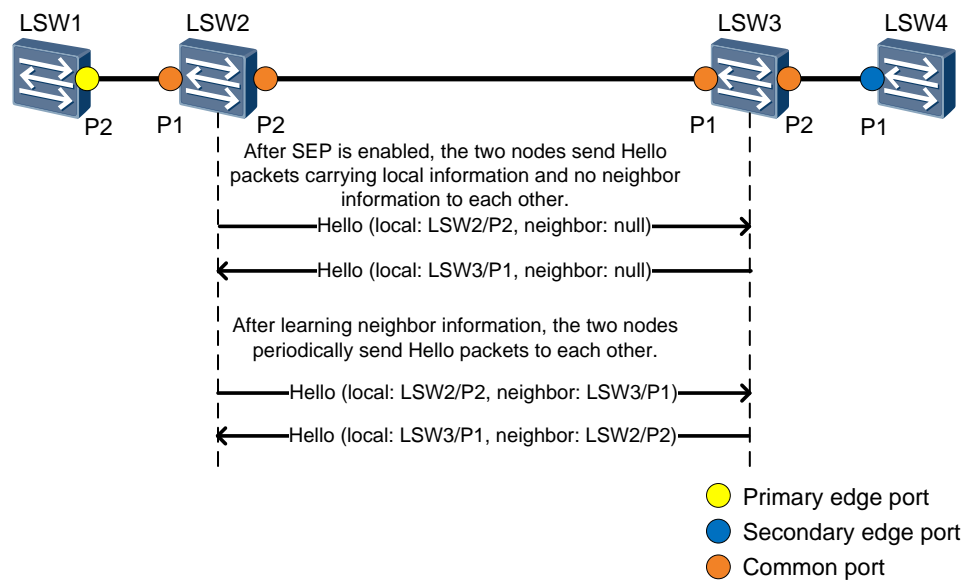
After a port is added to a SEP segment, neighbor negotiation starts. The port and its neighbor exchange Hello packets to establish a neighbor relationship. After neighbor negotiation succeeds, the two ports continue to exchange Hello packets to detect their neighbor status.

The neighbor negotiation mechanism prevents unidirectional links because neighbor negotiation is bidirectional. Ports on both ends of a link must send Hello packets to each other, as a means of status confirmation. If a port does not receive a Hello packet from the peer port within the timeout period, the port considers the peer port to be Down.

Each two neighbors in a SEP segment perform neighbor negotiation by sending P2P SEP packets. When receiving a Hello packet from the neighbor, the port sends the packet to the CPU for processing but does not forward the packet in the SEP segment.

Neighbor negotiation provides information required to obtain the SEP segment topology. After neighbor relationships are established between ports using neighbor negotiation, the links can be connected to form a complete SEP segment. This helps display the complete topology of the SEP segment.

Figure 2-4 Neighbor negotiation



Links in a SEP segment go to the link status synchronization phase. In Table 2-7, devices form LSDBs after establishing neighbor relationships.

Table 2-7 LSDBs

Device	Link Status Data		
	Name	Port	Directly Connected Neighbor Information <Device Name, Port>
LSW1	LSW1	P2	<LSW2, P1>
LSW2	LSW2	P1	<LSW1, P2>
	LSW2	P2	<LSW3, P1>
LSW3	LSW3	P1	<LSW2, P2>
	LSW3	P2	<LSW4, P1>
LSW4	LSW4	P1	<LSW3, P2>

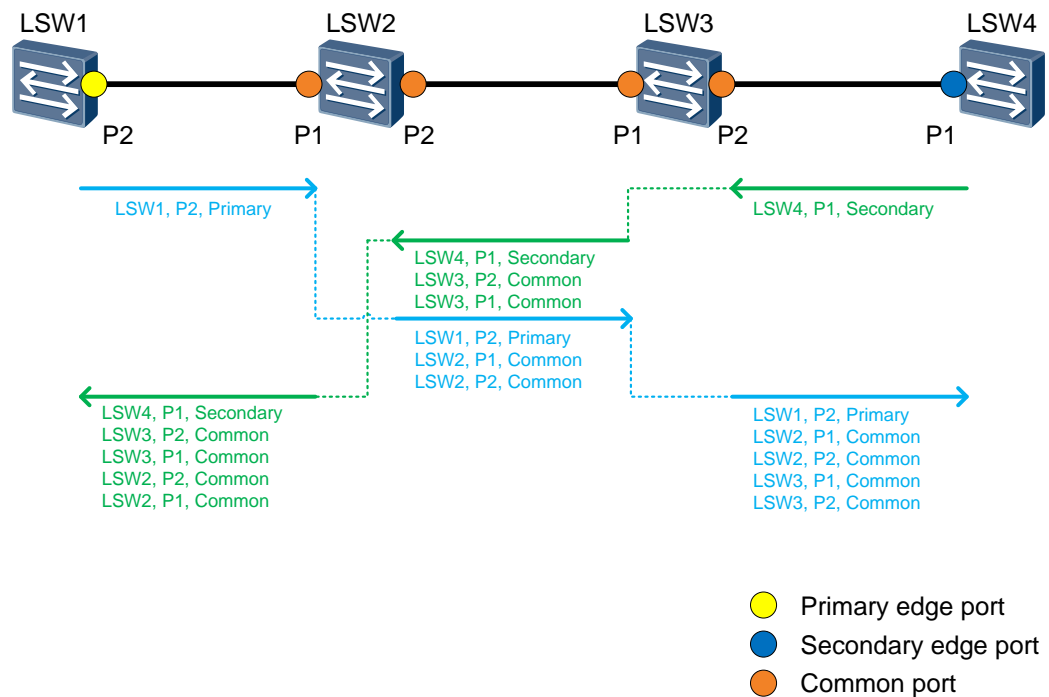
2.3.2 LSDB Synchronization and Topology Display

LSDB Synchronization

After neighbor relationships are established, all nodes in a SEP segment periodically send LSA packets. After a node receives LSA packets from other nodes on a port, the node updates its LSDB and advertises the updated LSDB from another port.

The LSDB uses the system MAC address as the unique index of the system.

Figure 2-5 LSDB synchronization process



To ensure consistent LSDBs on all nodes in a SEP segment, SEP uses the info-ACK mechanism.

1. If a node does not receive an LSA ACK packet, the node considers a failure in sending LSA Info packets and starts the retransmit timer. When the retransmit timer expires, the node retransmits LSA Info packets until it receives the LSA ACK packets.
2. After receiving an LSA ACK packet, the node starts the keepalive timer. When the timer expires, the node retransmits LSA Info packets in the same process as step 1.
3. After receiving an LSA Info packet, the node starts the lifetime timer. After the timer expires, the node deletes the local LSA. When receiving an update LSA, the node resets the lifetime timer.

Delays may exist on a network. To ensure that nodes update their LSDBs according to the latest LSA information, SEP adopts the sequence number mechanism. Each node in a SEP segment maintains LSDB sequence numbers. The initial LSDB sequence number is 1. Every time when the neighbor relationship changes or node attributes change, the sequence number increases by 1. When receiving an LSA packet with a larger sequence number, a node uses the new LSA packet to advertise its LSDB status; when receiving an LSA packet with a smaller sequence number, the node discards the packet. The sequence number field is 4 bytes long. The sequence numbers are used up after 136 years even if the sequence number increases every 1s. Therefore, it is considered that the sequence numbers cannot be used up. If the sequence number of the local node is reversed after being used up, the node enters the sleeping state for a period longer than the lifetime. A sleeping device does not send LSA packets. After other nodes in the SEP segment age out LSDB status of the local node, the node re-establishes neighbor relationships and sends LSA packets.

When a faulty node in the SEP segment recovers, the node needs to immediately obtain topology information about all nodes in the SEP segment. The node sends LSA Info packets.

After receiving the LSA Info packets, neighboring ports respond with LSA ACK packets to notify the node of their latest LSDB status.

SEP Topology Display

The topology display function allows you to view the topology with the highest network connectivity on any node in a SEP segment.

After link status synchronization, all nodes display the same topology. To ensure the consistent topology display on all nodes in a SEP segment, perform the following operations:

- Select the initial node for the topology display.
- Select the direction of the topology display, that is, the port from which the topology is displayed.

Figure 2-6 shows the topology display rules of a SEP segment on an open ring network.

Figure 2-6 Topology display on an open ring network

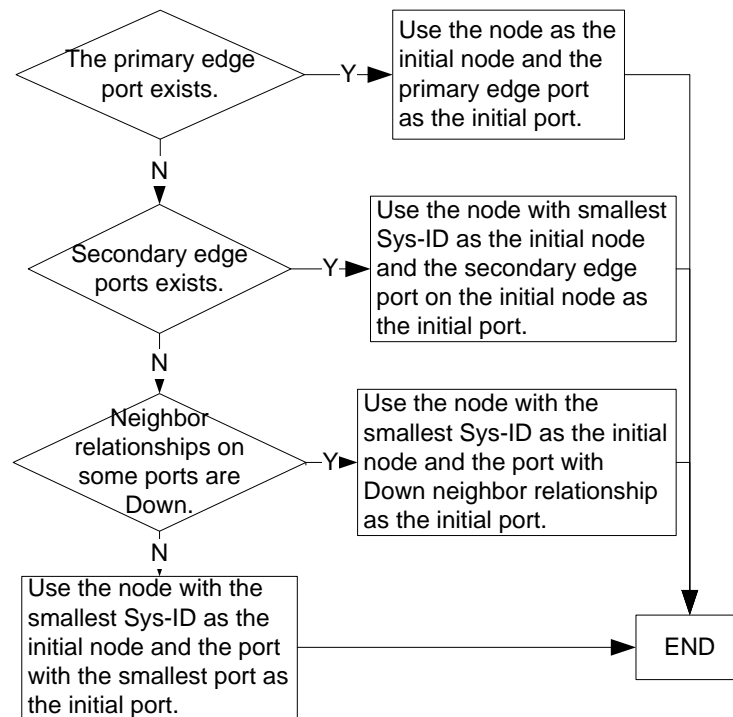
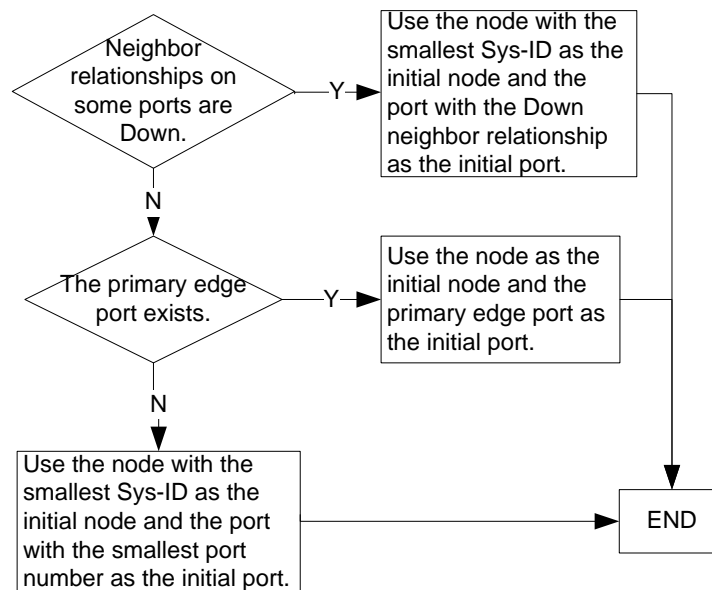


Figure 2-7 shows the topology display rules of a SEP segment on a closed ring network.

Figure 2-7 Topology display on a closed ring network



2.3.3 Primary Edge Port Election

Only ports that are configured as no-neighbor edge ports, primary edge ports, and secondary edge ports can participate in primary edge port election. If only one port on a node has SEP enabled, you must set the role of the port to edge so that the port can function as an edge port.

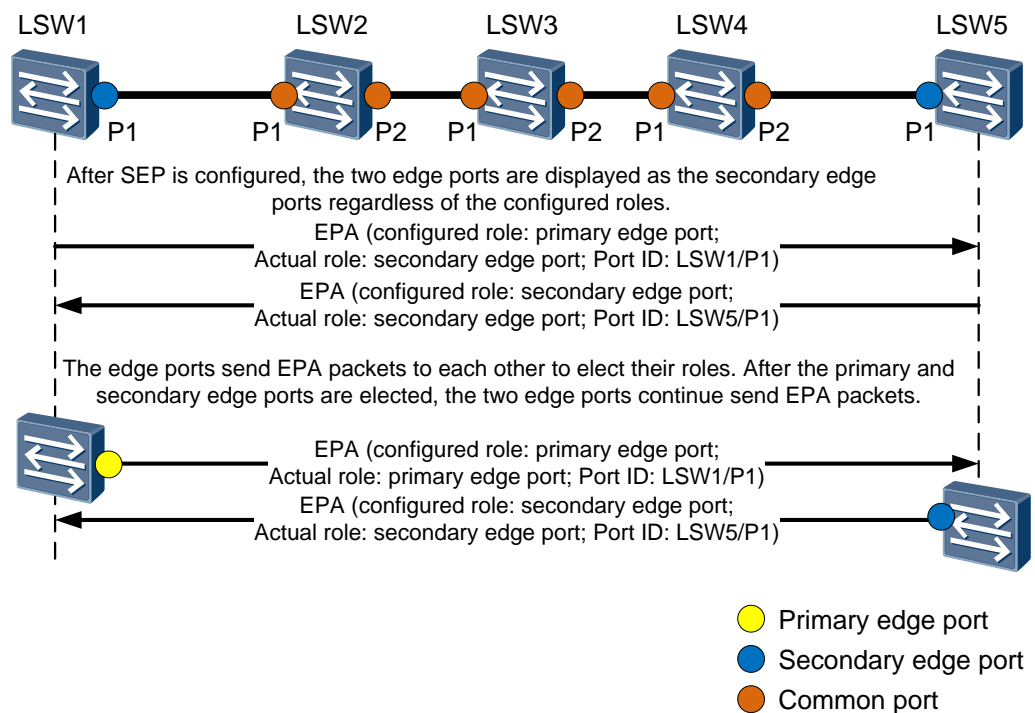
In a SEP segment, only the primary edge port can initiate blocked port preemption.

As shown in Figure 2-8, if no link is faulty on the network and SEP is enabled on the ports, the following situations occur:

- Common ports do not participate in primary edge port election. Only P1 on LSW1 and LSW5 participate in primary edge port election.
- Election order and basis:
 - If P1 on LSW1 and P1 on LSW5 have different roles, the primary edge port is elected based on the port role.
 - If P1 on LSW1 and P1 on LSW5 have the same role, P1 with a larger port ID is elected as the primary edge port.

After the primary edge port is elected, it periodically sends primary edge port election packets without waiting for the success of neighbor negotiation. A primary edge port election packet contains the port role (primary edge port or secondary edge port), bridge MAC address of the port, and port ID.

Figure 2-8 Primary edge port election process



If a link fault occurs in the SEP segment, P1 on LSW1 and P1 on LSW5 receive fault notification packets or P1 on LSW5 does not receive primary edge port election packets within a specified period. P1 on LSW1 then becomes the secondary edge port. Consequently, two secondary edge ports exist in the SEP segment

and periodically send primary edge port election packets. When all link faults in the SEP segment are rectified, the two secondary edge ports can receive primary edge port election packets and elect a new primary edge port within a configured interval (1s by default).

2.3.4 Port Blocking Mechanism

SEP Port Priority

Each SEP port has a priority that determines the election of the blocked port. A higher port priority indicates a higher possibility of becoming the blocked port. The priority value of a port contains 16 bits. The higher 8 bits are defined by the system, and the lower 8 bits are set by the user.

A blocked port is determined based on the management priority and user priority (64 by default).

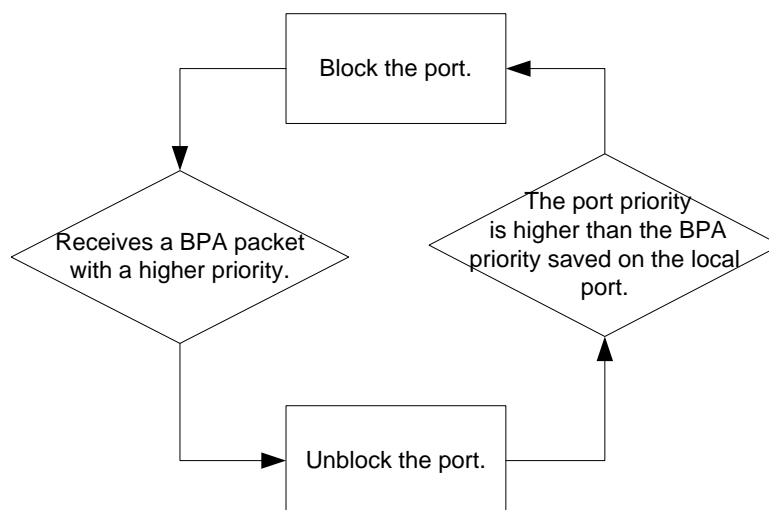
Table 2-8 System priority description

Condition or Event	Priority	Description
The local port is Down.		0xA0 40, the port priority when the SEP port is Down. In this case, the port has the highest priority and preempts the original blocked port in the SEP segment, generating an active/standby switchover.
The neighbor port is Down.		0x20 40, the port priority when the SEP neighbor port is Down. The Down state of the neighbor port here refers to the protocol status, for example, when the neighbor port is not configured with SEP.
Blocked port preemption is specified.		0x08 40, the port priority when the SEP port is specified as the blocked port.

Port Blocking

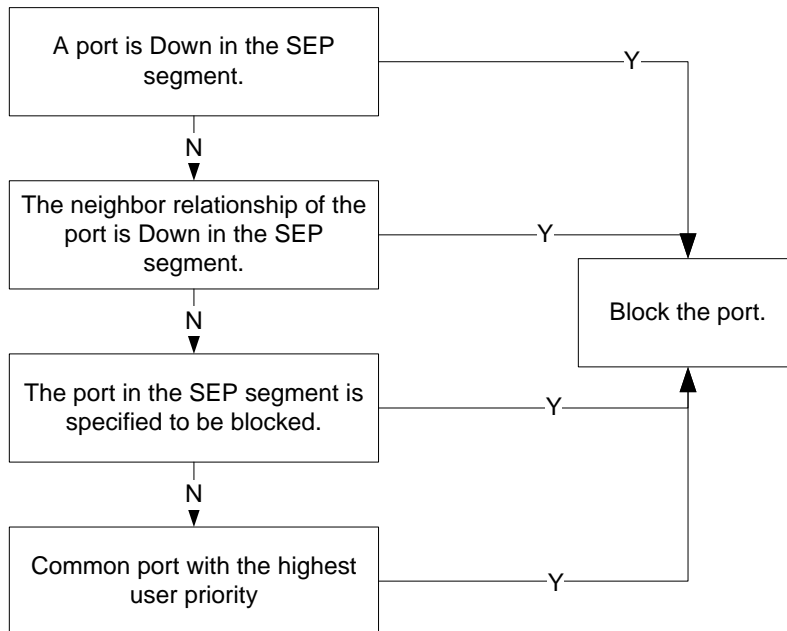
In Rapid Ring Protection Protocol (RRPP) and Ethernet ring protection switching (ERPS), the primary node or ring protection link (RPL) owner determines the blocked port and whether to perform an active/standby switchover. Different from RRPP and ERPS, each SEP node compares their port priorities with each other in the SEP segment to determine whether to block the local port, as shown in Figure 2-9.

Figure 2-9 Port blocking process



Based on the SEP port priority and port blocking mechanism, a port in a SEP segment enters the Discarding state in the order as shown in Figure 2-10.

Figure 2-10 Blocking a port



On a complete link without a specified blocked port, any port in the SEP segment can be a blocked port, which may not be the blocked port expected by users. To meet user requirements for flexibly specifying the blocked port, SEP provides multiple port blocking modes, as listed in Table 2-9.

Table 2-9 Port blocking modes

Port Blocking Mode	Description
Specify the port with the highest priority as the blocked port.	SEP compares port priorities as follows: Compares configured port priority values. A larger value indicates a higher priority. Compares bridge MAC addresses of ports with the same priority value. A smaller bridge MAC address indicates a higher priority. Compares port numbers if their bridge MAC addresses are the same. A smaller port number indicates a higher priority.
Specify the port in the middle of a SEP segment as the blocked port.	If an even number of ports exist in the SEP segment, the port closest to the primary edge port is blocked.
Specify the blocked port based on the configured hop count.	SEP sets the hop count of the primary edge port to 1 and the hop count of the neighbor port of the primary edge port to 2. Hop counts of other ports increase by steps of 1 in the downstream direction of the primary edge port.

Port Blocking Mode	Description
Specify a blocked port based on the device name and port name.	<p>After SEP is enabled, a port is blocked based on the device name and the port name. Before specifying a port to be blocked, you can run the display command to view details about the current ring topology and all the ports in the topology, and then specify the device name and port name of the port to be blocked.</p> <p>If multiple devices share the same device name and port name on the ring network, SEP searches these devices from the primary edge port and blocks the first searched device with the specified device name and interface name.</p> <p>If you change the device name or port name of a port that is specified as the blocked port, the port cannot preempt to be the blocked port.</p>

Table 2-10 compares scenarios when the blocked port is specified and not specified.

Table 2-10 Comparing scenarios when the blocked port is specified and not specified

Item	Blocked Port Not Specified	Blocked Port Specified
Blocked port selection	Compares priorities of ports on both ends of the last link that succeeds in neighbor negotiation or recovers from a fault.	Specifies a port to be blocked.
Manageability	Low. The blocked port may be located in any position of a SEP segment.	High. The blocked port location is fixed.

If no blocked port is specified, uncertainty may affect service forwarding. You are advised to specify a port to be blocked according to the actual situation.


The specified blocked port takes effects only after the preemption mode is configured and takes effect.

2.3.5 Port Preemption

Preemption Mode Selection

After the port blocking mode is specified or the link fault is rectified, whether a specified port will be blocked is determined by the preemption mode. Table 2-11 lists the preemption modes.

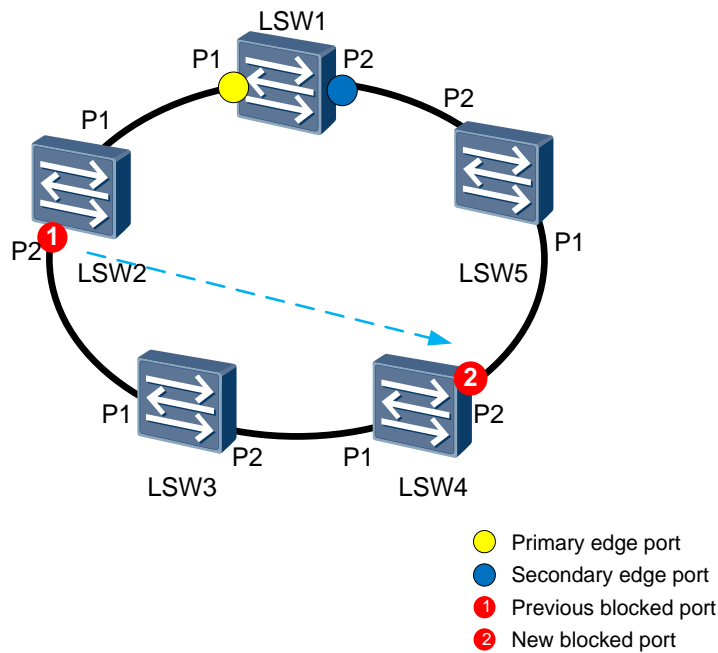
Table 2-11 Preemption modes

Preemption Mode	Description	Recommended Scenario
No preemption	When all link faults are rectified or the last two ports enabled with SPE complete neighbor negotiation, the ports send blocking status packets to each other. The port with the highest priority is then blocked, and the other ports enter the Forwarding state.	High-reliability network that is sensitive to switchover times and has sufficient bandwidth, regardless of service payloads.
Preemption mode (delayed preemption and manual preemption)	<p>Delayed preemption</p> <p>After all the faulty ports recover, the edge ports no longer receive fault notification packets. If the primary edge port does not receive any fault notification packet within 3 seconds, the port starts the delay timer. After the delay timer expires, nodes in the SEP segment start blocked port preemption.</p>	Scenarios with high requirements for network service planning. Delayed preemption can adjust the delay based on network stability, reducing network flapping.
	<p>Manual preemption</p> <p>When the LSDBs of the primary and secondary edge ports are complete, the primary edge port or the brother port of the no-neighbor primary edge port sends preemption packets to block the specified port. The specified port sends a packet to advertise its status immediately after being blocked to instruct the previously blocked port to enter the Forwarding state.</p> <p> NOTE</p> <p>Only two ports on a device can be added to the same SEP segment. If one port is the no-neighbor primary edge port, the other port is the brother port of the no-neighbor primary edge port.</p>	Scenarios such as link maintenance and network commissioning. Manual preemption is a triggered operation.

Preemption Process

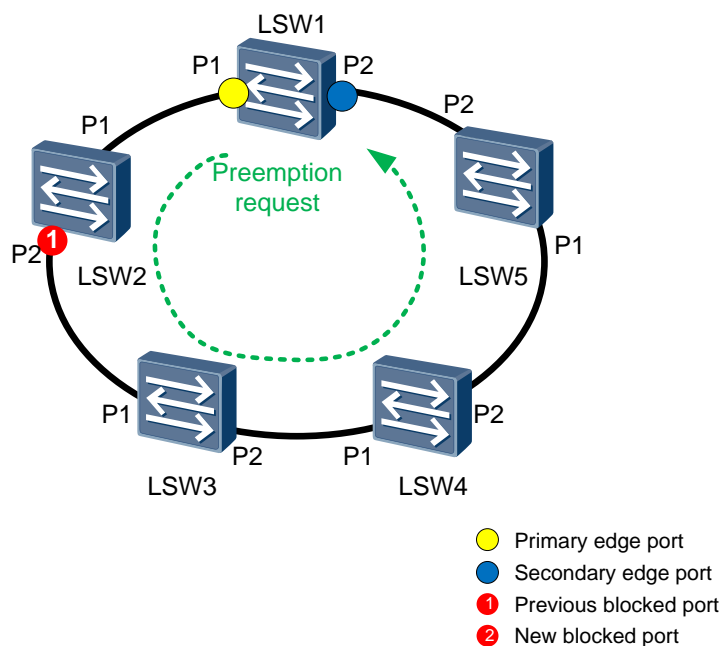
The following describes the preemption process. As shown in Figure 2-11, LSW1 through LSW5 form a SEP segment. P1 on LSW1 is the primary edge port, and P2 on LSW1 is the secondary edge port. The previous blocked port is P2 on LSW2. The following describes how P2 on LSW4 is specified as the blocked port using commands.

Figure 2-11 SEP preemption process (A)



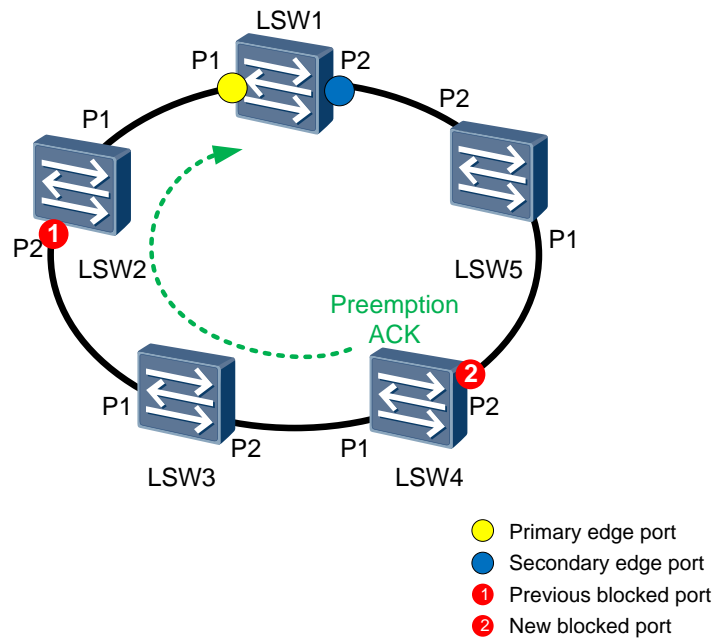
The blocked port and preemption mode specified using command lines take effect only when being delivered by the node where the primary edge port resides. LSW1 specifies P2 on LSW4 as the blocked port based on the device name and port name and sets the preemption mode to manual mode. LSW1 sends a Preemption Request packet carrying the destination device name and port name from the primary edge port.

Figure 2-12 SEP preemption process (B)



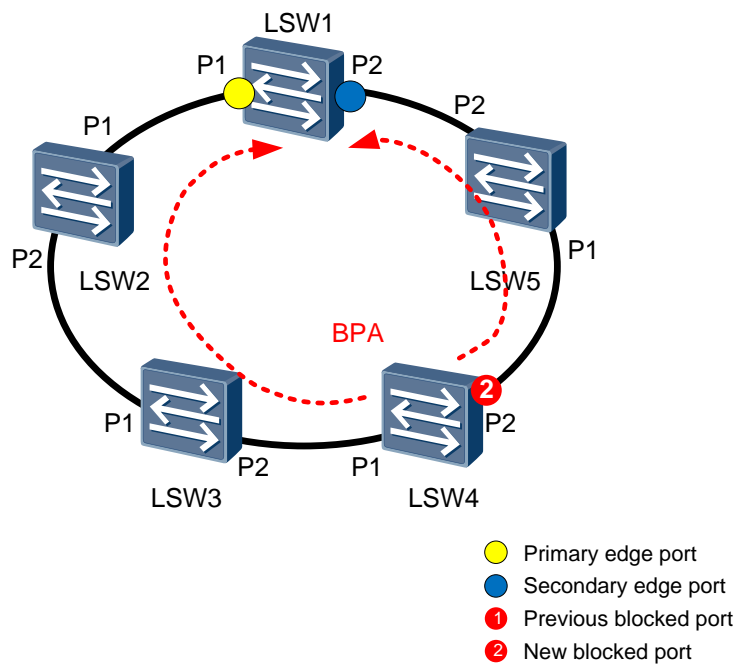
Upon receiving the Preemption Request packet, LSW4 finds that the new specified blocked port resides on the local node. LSW4 then sends a preemption ACK packet from the port receiving the Preemption Request packet, as shown in Figure 2-13. If LSW1 receives no preemption ACK packet after sending Preemption Request packets for five consecutive times, LSW1 considers preemption failed and records a log. The preemption process is complete. Meantime, P2 on LSW4 changes from the Forwarding state to the Discarding state.

Figure 2-13 SEP preemption process (C)



As shown in Figure 2-14, LSW4 sends BPA packets from P1 and P2. According to SEP packet types listed in Table 2-5, the packets are P2MP LSA Info packets whose destination MAC address is 0025-9EFB-3D70 and source MAC address is the system MAC address of LSW4. The SEP port priority carried in the BPA packets is 2112. The priority of P2 (previous blocked port) on LSW2 is 64 by default, which is lower than the priority of the new blocked port. LSW2 changes P2 to the Forwarding state and stops sending BPA packets.

Figure 2-14 SEP preemption process (D)



LSW4 sends five BPA packets with port priority 2112, sets P2 priority to 64, and continuously sends common port advertisement packets until the preemption process is complete. The blocked node is changed successfully. After the blocked port is changed, the traffic path is changed and forwarding entries are updated, which are described in XXX (2.4.1).

2.4 SEP Troubleshooting Mechanisms

2.4.1 Topology Change Notification and Suppression

SEP Topology Change Notification

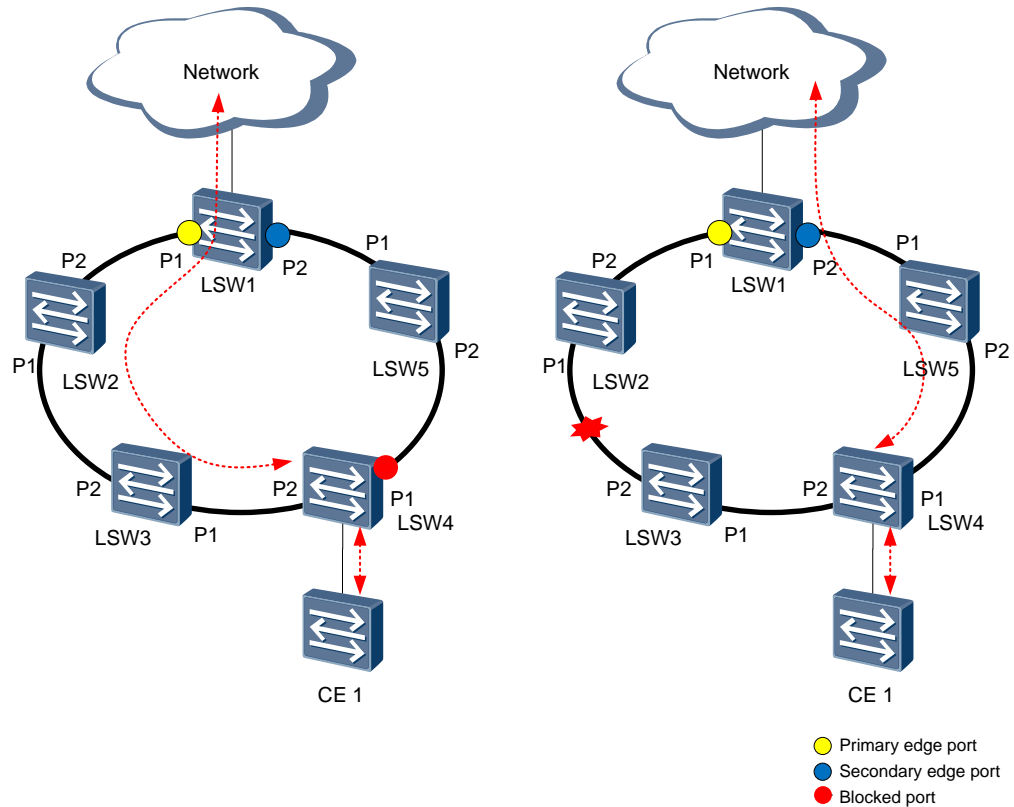
When a fault occurs or a fault is recovered in a SEP segment, the SEP topology change is sent to instruct other nodes in the SEP segment to update their forwarding entries. Table 2-12 lists the topology changes.

Table 2-12 SEP topology change notification

SEP Topology Change Notification	Description
A port fault occurs.	If a port in a complete SEP segment fails, the topology of the SEP segment changes. A port fault can be a link fault or the incorrect neighbor status on the port.
Faults are rectified and the preemption takes effect.	When all faulty ports recover, the blocked port is preempted and the topology is considered changed.

When the SEP topology changes, the traffic path changes. If original forwarding entries are not deleted, traffic fails to be forwarded. In Figure 2-15, P1 on LSW4 is the blocked port, and traffic from users connected to CE1 is forwarded along path LSW4-LSW3-LSW2-LSW1-LSW5. MAC addresses of the users connected to CE1 are then learned on P1 ports of LSW3, LSW2, LSW1, and LSW5.

Figure 2-15 SEP traffic path change



If the link between LSW2 and LSW3 fails, SEP unblocks the blocked port and traffic from users connected to CE1 is forwarded along path LSW4-LSW5-LSW1-LSW2-LSW3. If old forwarding entries are not deleted, network-side traffic destined for LSW1 is forwarded to LSW2 and fails to reach the destination connected to CE1.

After SEP is enabled, a node advertises TC packets in the SEP segment to instruct ports on the ring network to update their MAC address entries. Different from other ring protection protocol, the MAC address entries are updated only on the port receiving the packet.

When a port on a node changes from the Forwarding state to the Discarding state, the two ports of the node send TC packets. The port changing to the Discarding state is called the new blocked port (NBP).

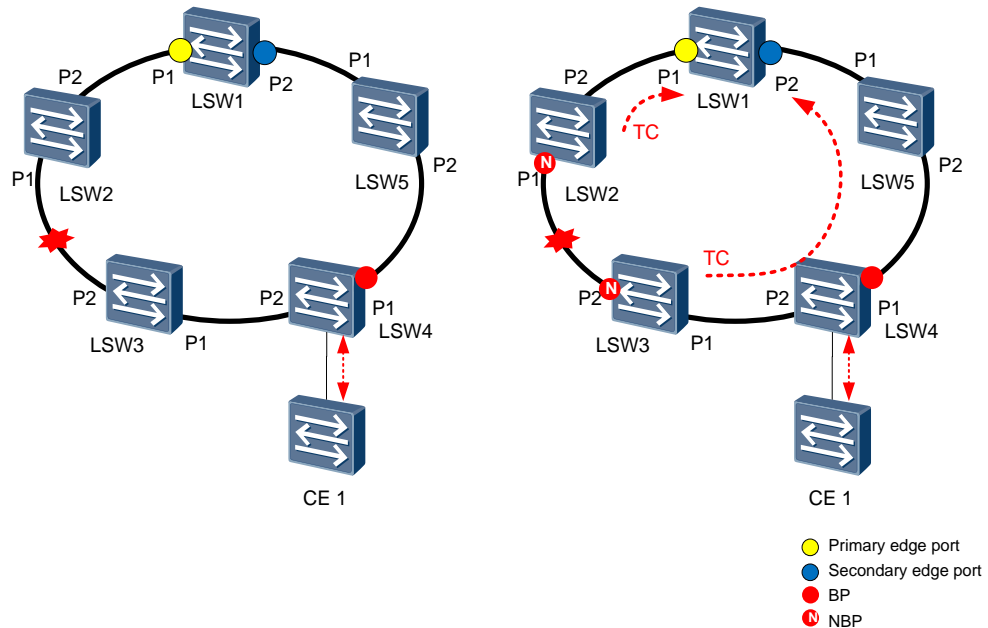
MAC address entries on a port are updated as follows:

- The port that changes from the Forwarding state to the Discarding state deletes the MAC address entries on the local port.
- Based on LSA information, the port sending or receiving TC packets searches for the NBP from the neighbor port hop by hop and checks whether the previous blocked port

(BP) resides between the local port and NBP. If yes, the port deletes the MAC address entry of the brother port; if not, the port deletes the MAC address entry on the local port.

As shown in Figure 2-16, P1 on LSW4 is the BP. When the link between LSW2 and LSW3 fails, the ports on both ends of the faulty link enter the Discarding state. P1 on LSW4 changes from the Discarding to Forwarding state.

Figure 2-16 Topology update



According to the MAC address entry update mechanism, P1 on LSW2 and P2 on LSW3 changes from the Forwarding state to the Discarding state. LSW2 and LSW3 send TC packets from their ports in the SEP segment. The two ports on LSW2 and LSW3 are both NBPs and delete their MAC address entries on the local port. For example, after receiving a TC packet, P1 on LSW1 searches for the NBP in the direction of P1 on LSW1 to P2 on LSW2. When finding that BP P1 on LSW4 is not located between P1 on LSW1 and P1 on LSW2, LSW1 needs to update the MAC address entry of P1 on LSW1. The preceding process is repeated. P1 on LSW1, P1 on LSW5, P2 on LSW4, P2 on LSW3, and P1 on LSW2 need to update their MAC address entries.

Network Topology Change Notification

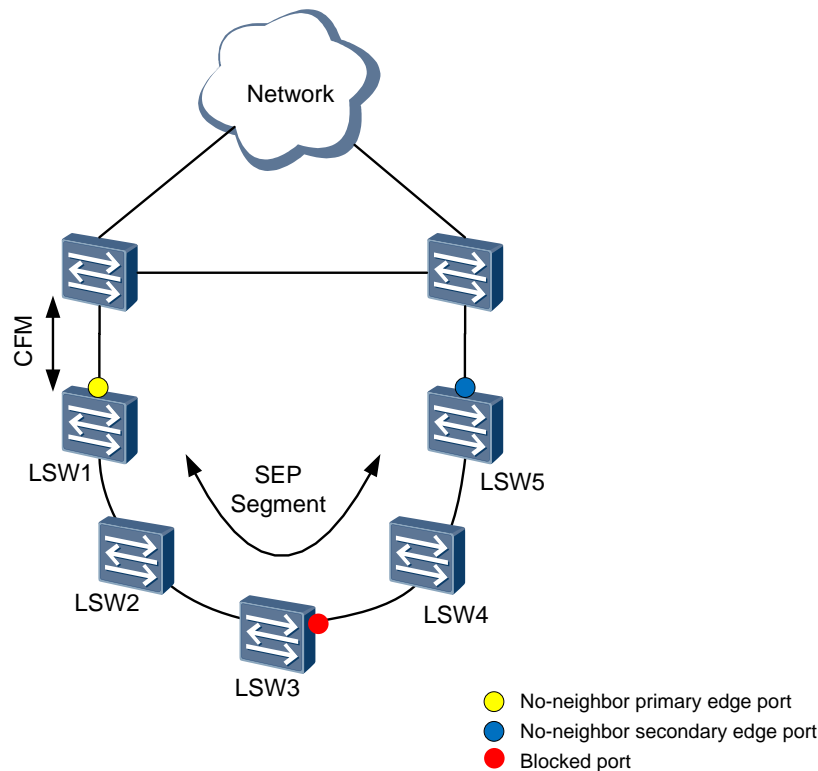
Network topology change notification is configured on a device between networks so that when the topology of a network changes, the device can notify the other network of the change. Table 2-13 describes network topology change notification

Table 2-13 Network topology change notification

Network Topology Change Notification	Scenario	Description	Solution
Topology change notification from a lower-layer network to an upper-layer network	A SEP network is connected to an upper-layer network running other features such as SEP, STP, and RRPP.	<p>If the blocked port in a SEP segment on a lower-layer network is manually changed, the topology of the SEP segment changes. The upper-layer network cannot detect the topology change, leading to traffic interruption.</p> <p>If a port in a SEP segment on a lower-layer network becomes faulty, the topology of the SEP segment changes but the upper-layer network cannot detect the change. As a result, traffic is interrupted.</p>	Configure the SEP topology change notification function.
	A device is connected to a SEP network using Smart Link.	<p>During an active/standby switchover, the device sends a Smart Link Flush packet to notify connected devices in the SEP segment of the switchover.</p> <p>If the connected devices cannot identify the Smart Link Flush packet, that is, the connected devices cannot detect topology changes of the lower-layer network, traffic is interrupted.</p>	Enable devices in the SEP segment to process Smart Link Flush packets.
Topology change notification from an upper-layer network to a lower-layer network	A SEP network is connected to an upper-layer network where connectivity fault management (CFM) is configured.	If a fault occurs on the upper-layer network, the network topology changes but the lower-layer network cannot detect the change. As a result, traffic is interrupted.	Configure association between SEP and CFM.

The following uses association between SEP and CFM as an example to briefly describe network topology notification. As shown in Figure 2-17, association between SEP and CFM is configured on LSW1. If CFM detects a fault on the upper-layer network, LSW1 sends a CFM packet to notify the operation, administration, and maintenance (OAM) module of the fault. The SEP status of the port associated with CFM then changes to Down.

Figure 2-17 Association between SEP and CFM



After the port associated with CFM on LSW1 is Down, LSW2 connected to LSW1 sends a TC packet to notify other nodes in the SEP segment of the topology change. After LSW3 receives the TC packet, the blocked port on LSW3 is unblocked and enters the Forwarding state. This port sends a TC packet to instruct other nodes in the SEP segment to update their MAC address tables and ARP tables. In this manner, the lower-layer network can detect faults on the upper-layer network, ensuring reliable service transmission.

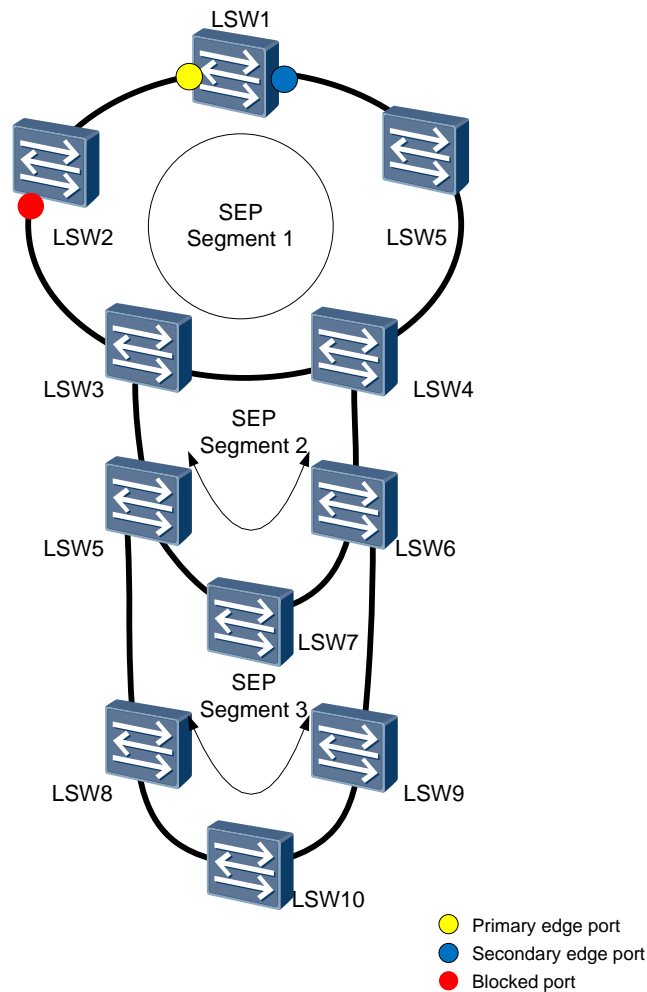
Suppression of SEP Topology Change Notification

Topology changes of a SEP segment are advertised to other segments or the upper-layer network. However, a large number of TC packets are generated in the following cases:

- A link becomes disconnected intermittently.
- A SEP segment is attacked by invalid TC packets.
- Multiple SEP ring networks exist.

In the previous two cases, a large number of TC packets are generated because frequent topology changes or attacks. Figure 2-18 shows a three-level SEP networking. If the topology of SEP segment 3 changes, LSW5 or LSW6 sends TC packets from the two ports in SEP segment 2. The SEP blocked port does not block SEP packets, so the number of ports in SEP segment 2 doubles and SEP segment 2 is flooded with these packets. Each time TC packets pass through a SEP segment, the number of TC packets doubles.

Figure 2-18 Multiple SEP ring networks



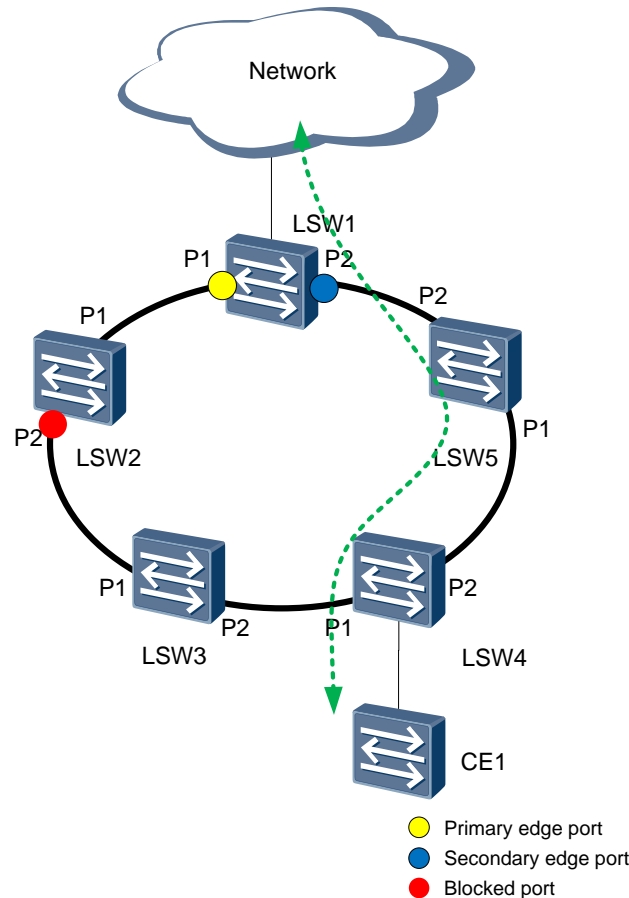
A large number of TC packets lower the CPU processing capability and make devices in SEP segments frequently send and receive TC packets, occupying bandwidth. To solve such problems, the following measures can be taken to suppress TC packets:

- Configure a device to process only one of the TC packets carrying the same source address.
- Configure a device to process a specified number of TC packets within a specified period. By default, a device can process TC packets with three different sources within 2s.
- Avoid the networking scenario with more than three SEP ring networks.

2.4.2 Failover

As shown in Figure 2-19, LSW1, LSW2, LSW3, LSW4, and LSW5 form a closed ring network. P1 and P2 on LSW1 are the primary and secondary edge ports respectively. When the link is complete, P2 on LSW2 is the blocked port, and service traffic from CE1 reaches the network through LSW4, LSW5, and LSW1.

Figure 2-19 SEP packet exchange when the link is complete



SEP packets are exchanged as follows when the link is complete:

- P1 and P2 on LSW1 send EPA packets that reach P2 and P1 after passing through the entire SEP segment. The primary edge port is still P1 and is not changed. The interval for sending EPA packets is 1s.
- All SEP ports send Hello packets to maintain neighbor relationships with neighbor ports. The interval for sending Hello packets is 1s.
- All SEP ports send LSA packets to periodically maintain and update the SEP topology on the local device. The interval for sending LSA packets is 20s.
- P1 and P2 on the blocked node LSW2 send BPA packets to notify other nodes of the blocked node location and blocked port priority. The BPA packets pass through the SEP segment and are terminated on the primary and secondary edge ports. The interval for sending BPA packets is 1s.

If the link between LSW4 and LSW5 fails, SEP packets are exchanged as follows:

- LSW4 and LSW5 set management priorities of Down ports to higher than the port priority of P2 on LSW2. P2 on LSW4 and P1 on LSW5 are blocked and send BPA packets to all nodes in the SEP segment. The BPA packets are terminated on the primary and secondary edge ports, as shown in Figure 2-20. The interval for sending BPA packets is 1s.

- After receiving a BPA packet, LSW2 finds that the priority in the packet is higher than the port priority on P2 and unblocks P2.
- P2 on LSW4 and P1 on LSW5 enter the Discarding state and delete their MAC address entries that have actually been deleted when the ports go Down. The two blocked ports then send TC packets to instruct other nodes to update their MAC address entries, as shown in Figure 2-21. The LSDB status carried in TC packets has been updated, so other nodes in the SEP segment update their local LSDB status when receiving the TC packet.
- P1 and P2 on LSW1 cannot receive EPA packets from each other. When receiving EPA packets times out, P1 becomes the secondary edge port.

Figure 2-20 Sending BPA packets

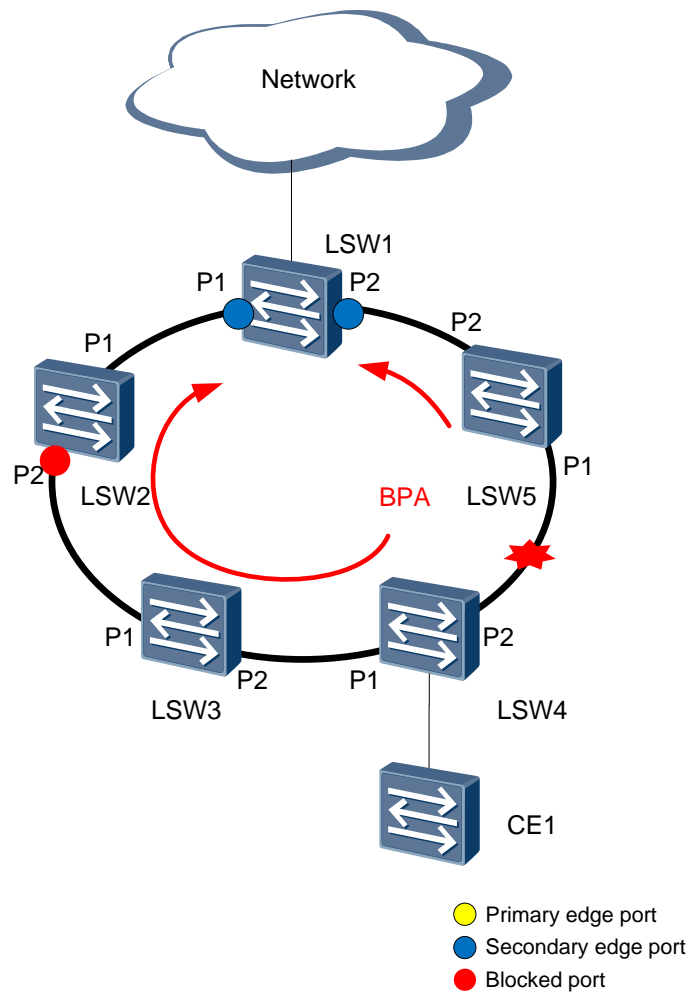
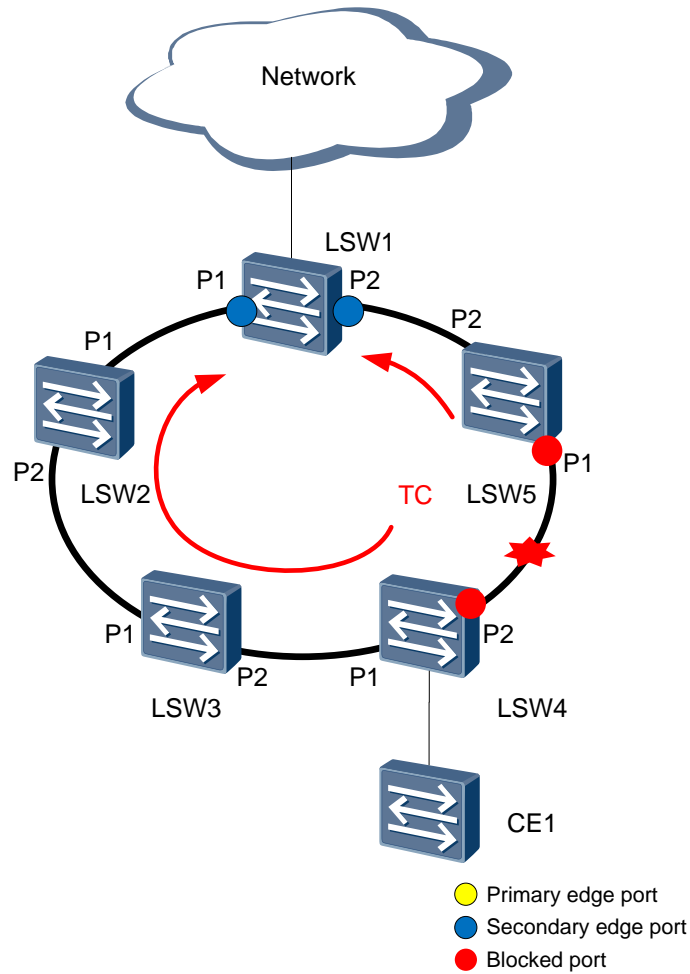
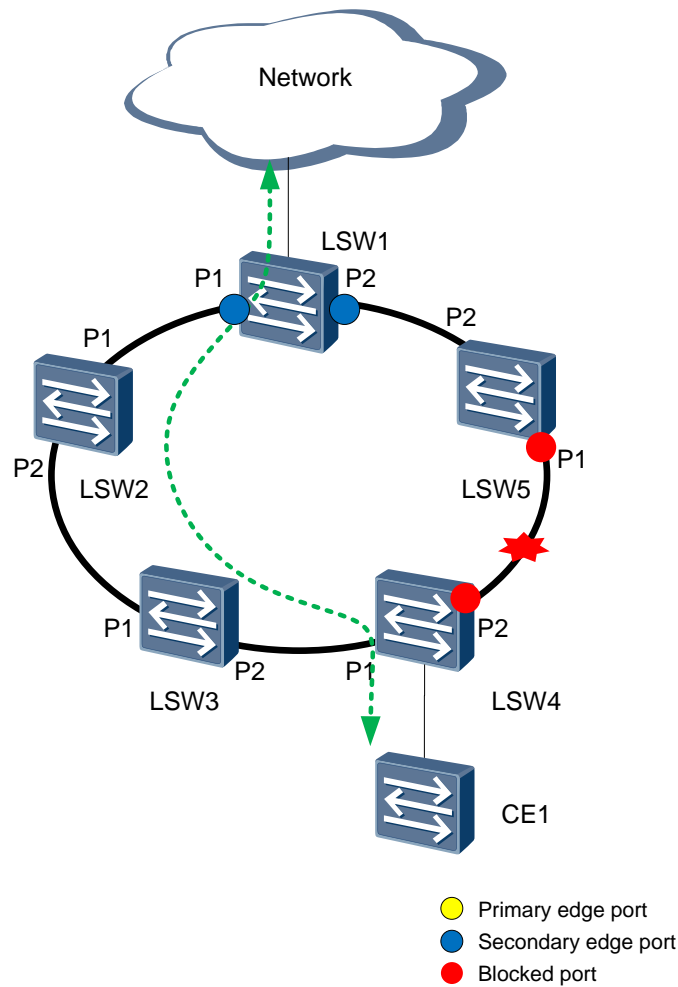


Figure 2-21 Sending TC packets



After the packet exchanges, in the SEP segment unblocks the original blocked port, correctly updates MAC address entries on ports, and changes the traffic path to CE1-LSW4-LSW3-LSW2-LSW1, as shown in Figure 2-22.

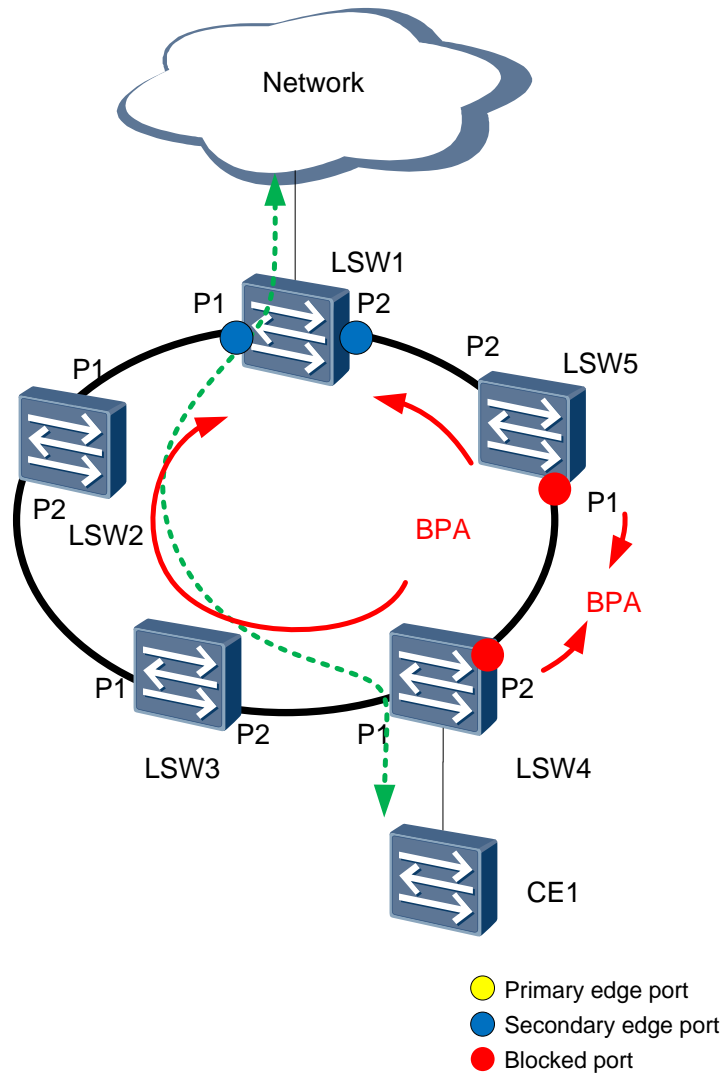
Figure 2-22 Traffic path



2.4.3 Failback

As shown in Figure 2-23, a link in a SEP segment fails, and traffic is transmitted along path CE1-LSW4-LSW3-LSW2-LSW1. When the faulty link between LSW4 and LSW5 recovers, the SEP segment can switch the traffic path back to the original one only after the automatic failback function is configured; if automatic switchback is not configured, the SEP segment blocks the recovered link.

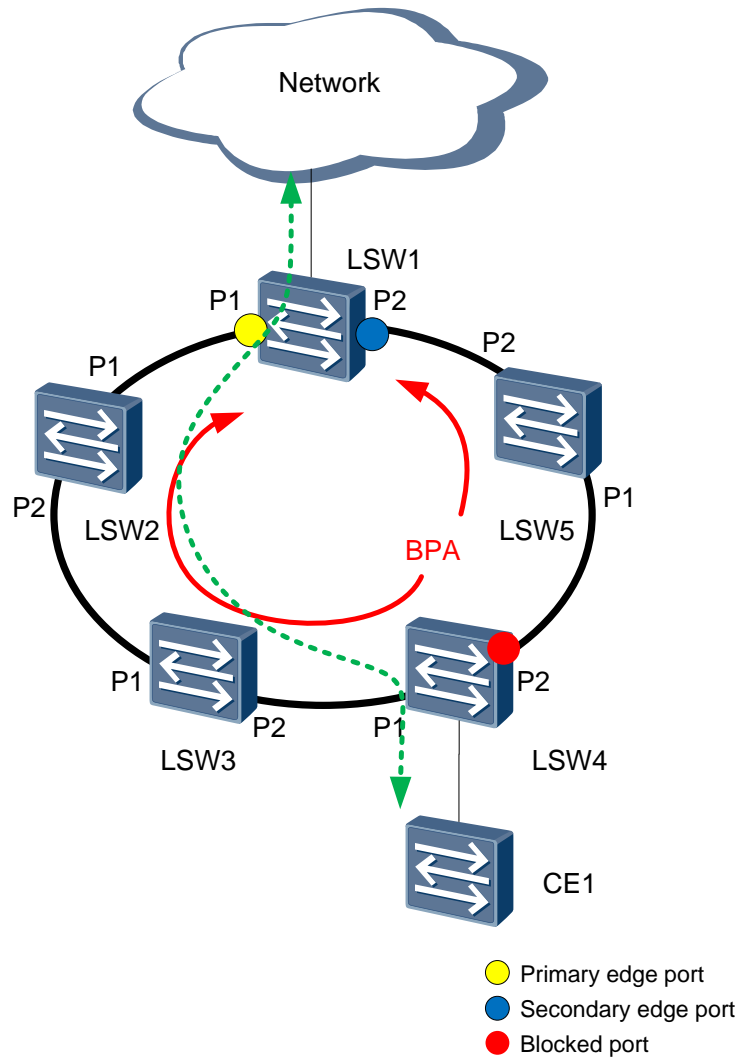
Figure 2-23 Switchback process (A)



When the faulty link recovers, P2 on LSW4 and P1 on LSW5 go Up. SEP packets are exchanged as follows:

- P2 on LSW4 and P1 on LSW5 send Hello packets to each other to set the neighbor relationship.
- Due to the topology change, LSW4 and LSW5 send their local LSDB status to each other and update the peer LSDB status.
- P2 on LSW4 and P1 on LSW5 send BPA packets that carry the default port priority. After receiving the packets, the two ports compare the port priority, bridge MAC address, and port ID and elect a blocked port. Assuming that P2 on LSW4 has a higher priority, P2 on LSW4 is blocked and P1 on LSW5 is unblocked, as shown in Figure 2-24. LSW4 sends BPA packets from P1 and P2, with the default interval of 1s.
- P1 and P2 on LSW1 can send EPA packets along the recovered link and elect the primary edge port. P1 on LSW1 is elected as the primary edge port.

Figure 2-24 Switchback process (B)

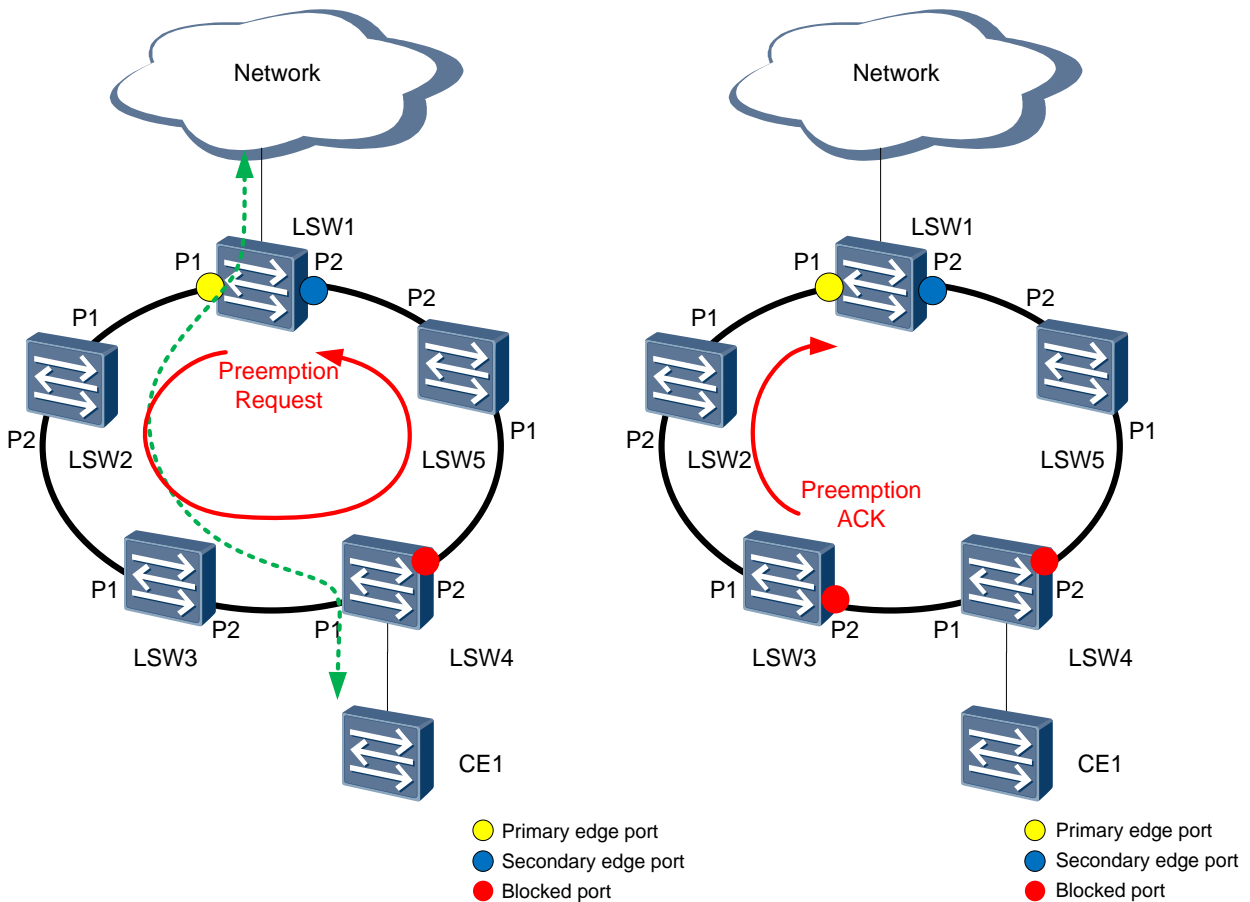


If the SEP segment is not configured with the port blocking mode or delayed preemption, the link switchback is complete, and P2 on LSW4 becomes the new blocked port (NBP).

If the port blocking mode and preemption are configured for the SEP segment, the primary node starts the delay timer when all faulty links recover. Assuming that P2 on LSW3 is blocked and the preemption delay duration is 30s, SEP packets are exchanged as follows:

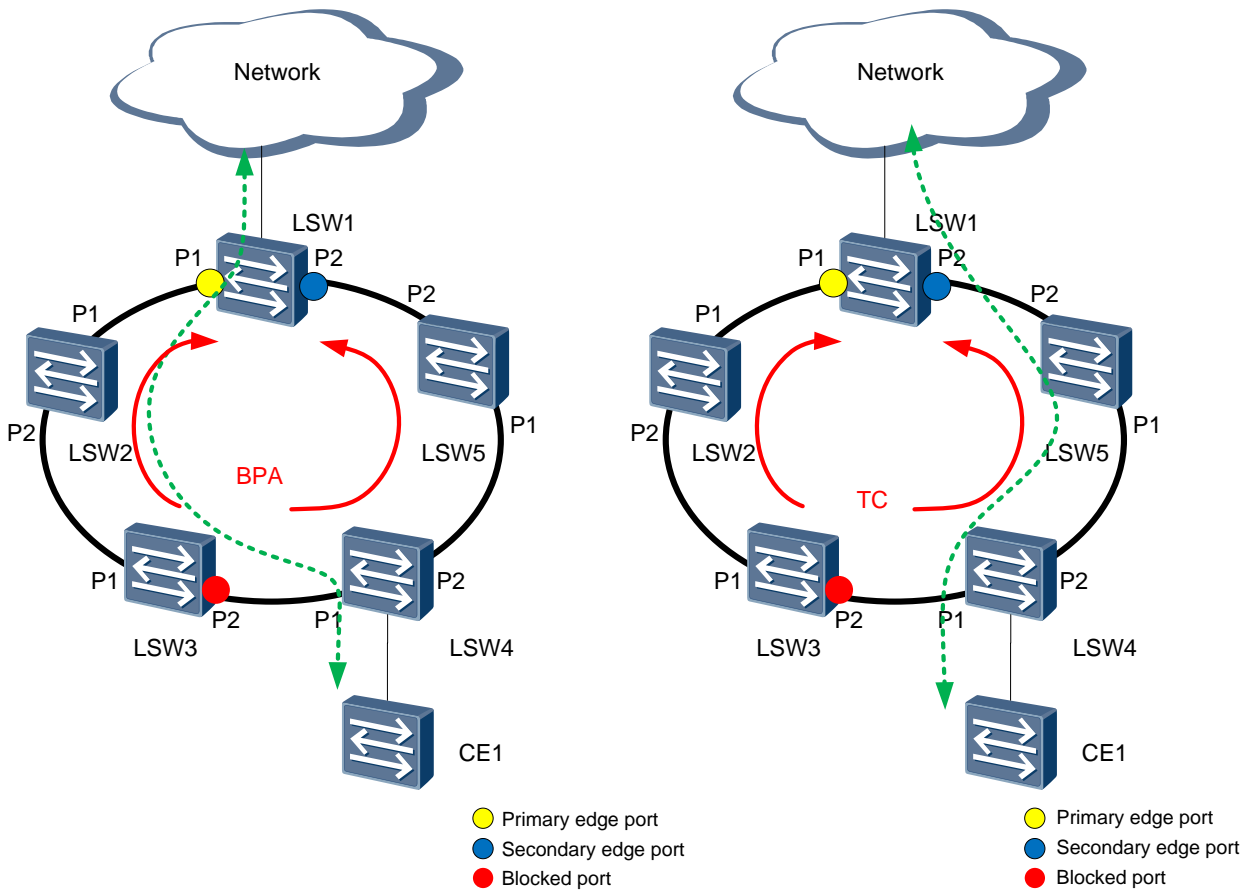
- After all faulty links recover, LSW1 starts the delay timer. When the timer expires, LSW1 sends a Preemption Request packet from the primary edge port P1, as shown in Figure 2-25. The Preemption Request packet carries the bridge MAC address and port ID of the specified blocked port and is terminated on the secondary edge port after 1s. Regardless of the blocking mode, the node where the primary edge port resides searches the local neighbor database for the port to be blocked and adds the bridge MAC address and port ID of this port to the TLV field in the Preemption Request packet.
- After receiving the Preemption Request packet, LSW3 finds that the specified blocked port is the local P2 and sends a Preemption ACK packet to the primary edge port, as shown in Figure 2-25.

Figure 2-25 Switchback process (C)



- LSW3 blocks P2 and sends BPA packets from P1 and P2 every 1s. The priority carried in the packets is the preemption priority. The BPA packets are terminated on the primary and secondary edge ports, as shown in Figure 2-26.
- After receiving a BPA packet, LSW4 finds that the priority in the packet is higher than the port priority on P2 and unblocks P2.
- LSW3 blocks P2, deletes the MAC address entries on P2, and sends TC packets from P1 and P2 to instruct other nodes to update their MAC address entries, as shown in Figure 2-26. Traffic from CE1 is forwarded along path LSW1-LSW5-LSW4.

Figure 2-26 Switchback process (D)

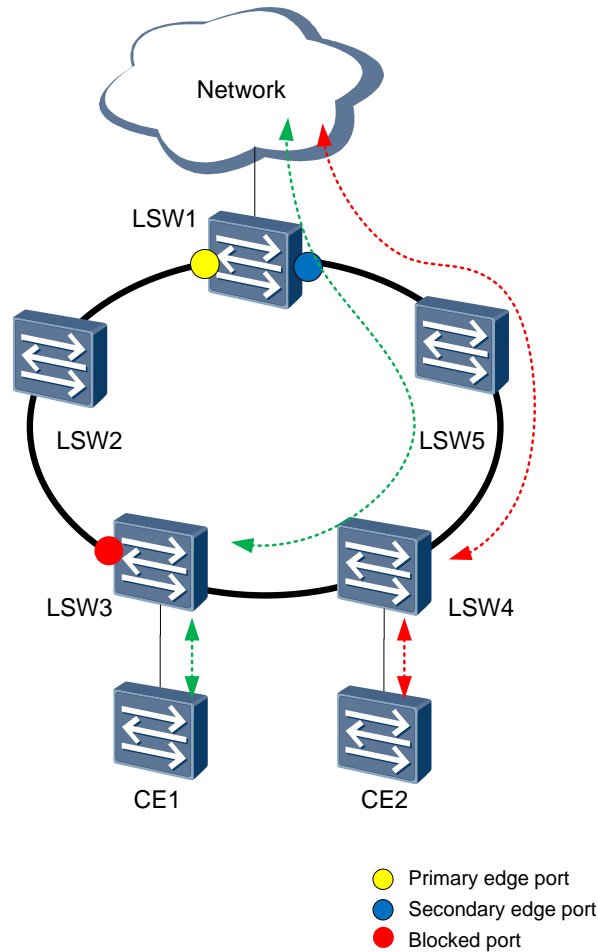


2.5 SEP Load Balancing

As shown in Figure 2-27, on a common SEP network, a physical ring network can be configured with only one SEP segment in which only one port can be blocked.

If a port in a complete SEP segment is blocked, all user data is transmitted along the path where the primary edge port resides. The path where the secondary edge port resides remains idle, wasting bandwidth.

Figure 2-27 SEP single instance

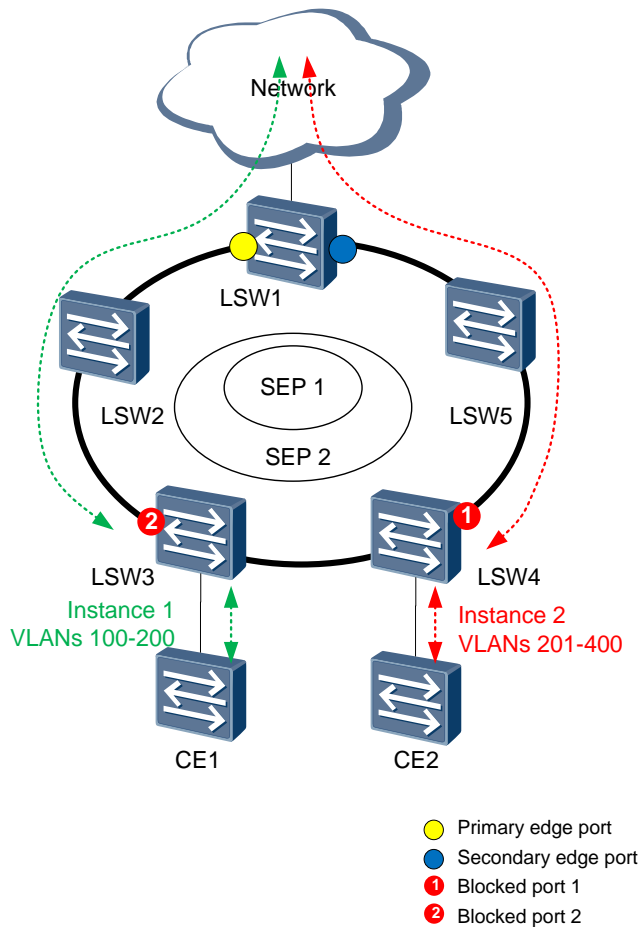


SEP multi-instance allows two SEP segments to be configured on a physical ring network. All devices, port roles, and control VLAN in each SEP segment complies with basic SEP rules. A physical ring network can have two ports blocked. Each blocked port independently detects the completeness of the physical ring network and then blocks or unblocks the port without affecting each other.

A physical ring network may contain one or more SEP segments. Multiple SEP segments can be granted management rights based on VLANs. Each SEP segment needs to be configured with a protected instance that indicates a VLAN range. The topology calculated by a SEP segment is only valid for this SEP segment, without affect on other SEP segments. Blocked ports in a SEP segment discards packets only in the VLAN range bound to this SEP segment and forwards data packets from other VLANs.

After different protected instances are configured for SEP segments, blocked ports discard packets only in the protected VLAN ranges bound to their local SEP segments. Data packets in different VLANs are transmitted along different paths, implementing traffic load balancing and link backup.

Figure 2-28 SEP multi-instance



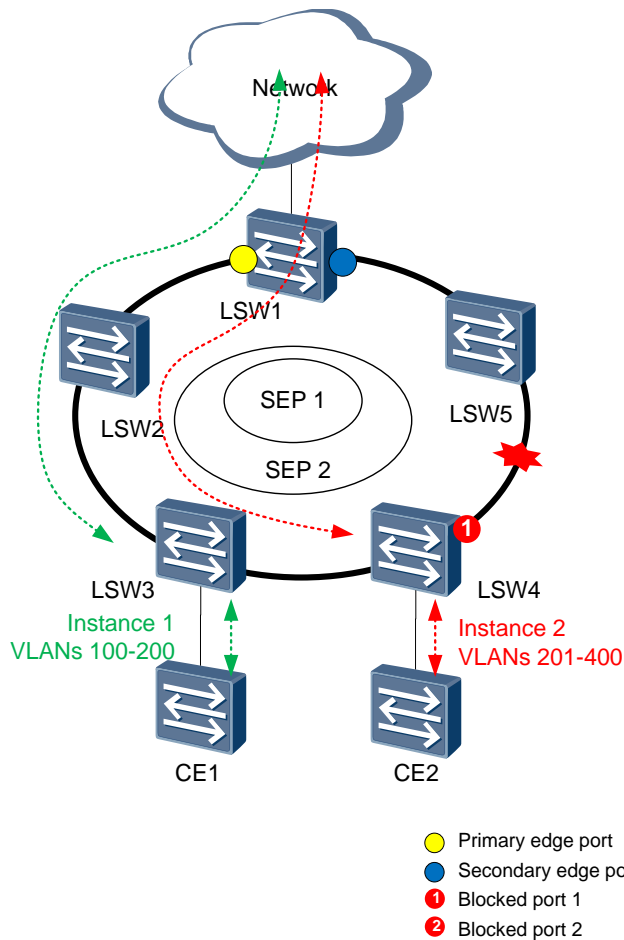
As shown in Figure 2-28, the SEP multi-instance ring network that consists of LSW1 to LSW5 has two SEP segments. P1 is the blocked port in SEP segment 1, and P2 is the blocked port in SEP segment 2.

- Protected instance 1 is configured in SEP segment 1 to protect the data from VLAN 100 through VLAN 200. The data is transmitted along path LSW4-LSW3-LSW2-LSW1-LSW5. As the blocked port in SEP segment 2, P2 blocks only the data from VLAN 201 through VLAN 400.
- Protected instance 2 is configured in SEP segment 2 to protect the data from VLAN 201 through VLAN 400. The data is transmitted along path LSW3-LSW4-LSW5-LSW1-LSW2. As the blocked port in SEP segment 1, P1 blocks only the data from VLAN 100 through VLAN 200.

When a node or a link fails, each SEP segment calculates the topology independently and updates the LSDB on each node.

As shown in Figure 2-29, a fault occurs on the link between LSW4 and LSW5. The link fault does not affect the transmission path for the data from VLAN 100 through VLAN 200 in SEP segment 1, but blocks the transmission path for the data from VLAN 201 through VLAN 400 in SEP segment 2.

Figure 2-29 Link fault on a SEP multi-instance network



After the link between LSW4 and LSW5 fails, LSW3 in SEP segment 2 starts to send LSA packets to instruct the other devices in SEP segment 2 to update their LSDBs, and the blocked port enters the Forwarding state. After the topology of SEP segment 2 is recalculated, the data from VLAN 201 through VLAN 400 is transmitted along path LSW3-LSW2-LSW1-LSW5.

After the link between LSW3 and LSW4 recovers, the devices in SEP segment 2 perform delayed preemption. After the preemption delay expires, P2 becomes the blocked port again, and sends LSA packets to instruct the other devices in SEP segment 2 to update their LSDBs. After the topology of SEP segment 2 is recalculated, the data from VLAN 201 through VLAN 400 is transmitted along path LSW3-LSW4-LSW5-LSW1-LSW2.

3 Product Capabilities



NOTE

Information in this chapter is subject to changes without notices. To obtain product capabilities, see the specification list.

3.1 Model Support

Table 3-1 describes models supporting SEP.

Table 3-1 SEP support (switches of V200R003 as an example)

Model	S2750	S5700	S6700	S7700	S9700
Whether SEP is supported (Yes/No)	Yes	Yes	Yes	Yes	Yes
Maximum number of SEP segments	16	16	16	256	256

3.2 Specifications and Limitations

Pay attention to the following when using SEP:

- A port can be added to a maximum of two SEP segments.
- Each segment supports a maximum of 128 ports, that is, 64 nodes.
- SEP ports do not support VLAN stacking.

4 Application Scenarios

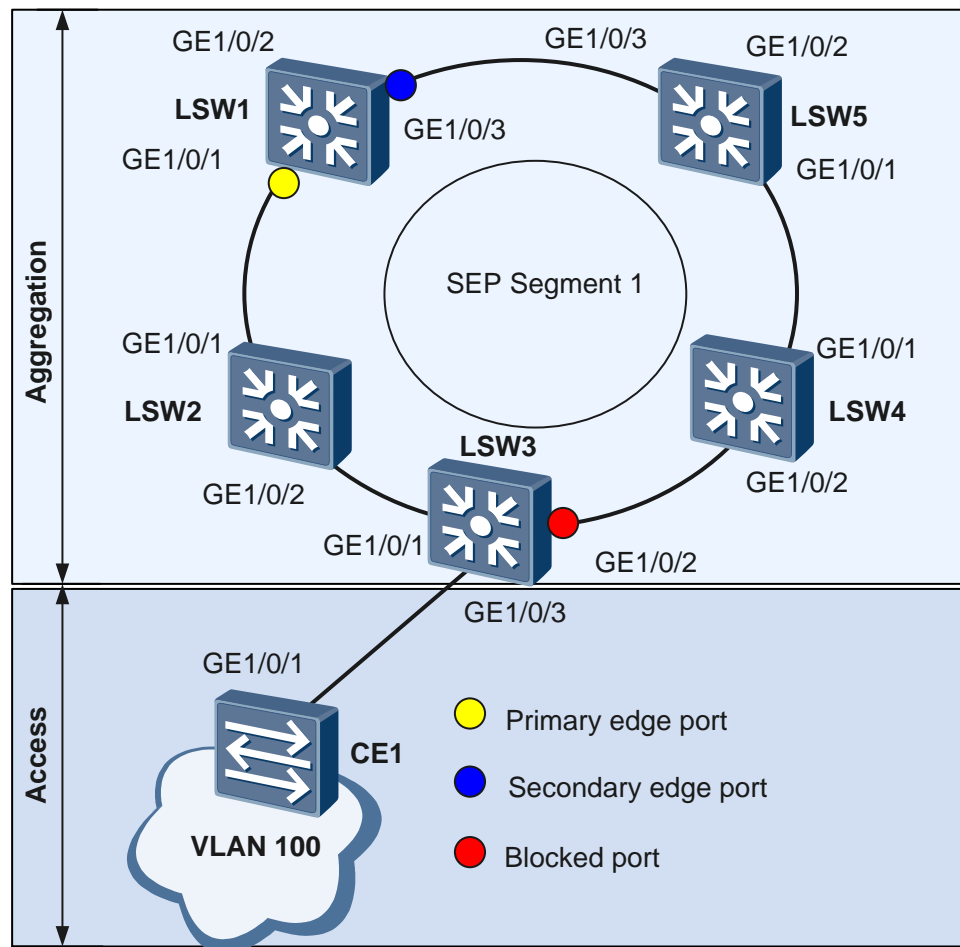
4.1 Example for Configuring SEP on a Closed Ring Network

4.1.1 Networking Requirements

To implement link backup and enhance network reliability, users access an upper-layer network through redundant links. The use of redundant links, however, may produce loops. The loops cause broadcast storms and make the MAC address table unstable. As a result, communication quality deteriorates, and communication services may even be interrupted. SEP can be deployed on the ring network to eliminate loops and restore communication if a link fails.

In the closed ring networking, CE1 is dual-homed to an upper-layer network. The two edge devices on the upper-layer network are directly connected. The closed ring network is deployed at the aggregation layer to transparently transmit Layer 2 unicast and multicast services. SEP runs at the aggregation layer to implement link redundancy.

Figure 4-1 Closed ring SEP networking



As shown in Figure 4-1, Layer 2 switching devices LSW1 to LSW5 form a ring network.

SEP runs at the aggregation layer.

- When no faulty link exists on the ring network, SEP can eliminate loops on the network.
- When a link on the ring network fails, SEP can rapidly restore communication between nodes on the ring network.

4.1.2 Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic SEP functions.
 - Configure SEP segment 1 on LSW1 to LSW5 and configure VLAN 10 as the control VLAN of SEP segment 1.
 - Add all the devices on the ring network to SEP segment 1 and configure the roles of GE1/0/1 and GE1/0/3 on LSW1.
 - On the device where the primary edge port resides, specify the port with the highest priority to be blocked.
 - Set priorities of the ports in the SEP segment.

Set the highest priority for GE1/0/2 on LSW3 and retain the default priority of the other ports so that GE1/0/2 on LSW3 will be blocked.

- Configure delayed preemption on the device where the primary edge port resides.
2. Configure the Layer 2 forwarding function on CE1 and LSW1 to LSW5.

4.1.3 Procedure

Step 1 Configure basic SEP functions.

1. Configure SEP segment 1 on LSW1 to LSW5 and configure VLAN 10 as the control VLAN of SEP segment 1.

Configure LSW1.

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] protected-instance all
[LSW1-sep-segment1] quit
```

Configure LSW2.

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment 1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] protected-instance all
[LSW2-sep-segment1] quit
```

Configure LSW3.

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
[LSW3-sep-segment1] protected-instance all
[LSW3-sep-segment1] quit
```

Configure LSW4.

```
<Quidway> system-view
[Quidway] sysname LSW4
[LSW4] sep segment 1
[LSW4-sep-segment1] control-vlan 10
[LSW4-sep-segment1] protected-instance all
[LSW4-sep-segment1] quit
```

Configure LSW5.

```
<Quidway> system-view
[Quidway] sysname LSW5
[LSW5] sep segment 1
[LSW5-sep-segment1] control-vlan 10
[LSW5-sep-segment1] protected-instance all
[LSW5-sep-segment1] quit
```



NOTE

- The control VLAN must be a VLAN that has not been created or used, and the configuration file automatically displays the command for creating common VLANs.
- Each SEP segment must be configured with a control VLAN. After a port is added to the SEP segment configured with a control VLAN, the port is automatically added to the control VLAN.

2. Add all the devices on the ring network to SEP segment 1 and configure port roles on the devices.



NOTE

If STP is enabled on a port, disable STP on the port before adding the port to a SEP segment.

On LSW1, configure GE1/0/1 as the primary edge port and GE1/0/3 as the secondary edge port.

```
[LSW1] interface gigabitethernet 1/0/1
[LSW1-GigabitEthernet1/0/1] stp disable
[LSW1-GigabitEthernet1/0/1] sep segment 1 edge primary
[LSW1-GigabitEthernet1/0/1] quit
[LSW1] interface gigabitethernet 1/0/3
[LSW1-GigabitEthernet1/0/3] stp disable
[LSW1-GigabitEthernet1/0/3] sep segment 1 edge secondary
[LSW1-GigabitEthernet1/0/3] quit
```

Configure LSW2.

```
[LSW2] interface gigabitethernet 1/0/1
[LSW2-GigabitEthernet1/0/1] stp disable
[LSW2-GigabitEthernet1/0/1] sep segment 1
[LSW2-GigabitEthernet1/0/1] quit
[LSW2] interface gigabitethernet 1/0/2
[LSW2-GigabitEthernet1/0/2] stp disable
[LSW2-GigabitEthernet1/0/2] sep segment 1
[LSW2-GigabitEthernet1/0/2] quit
```

Configure LSW3.

```
[LSW3] interface gigabitethernet 1/0/1
[LSW3-GigabitEthernet1/0/1] stp disable
[LSW3-GigabitEthernet1/0/1] sep segment 1
[LSW3-GigabitEthernet1/0/1] quit
[LSW3] interface gigabitethernet 1/0/2
[LSW3-GigabitEthernet1/0/2] stp disable
[LSW3-GigabitEthernet1/0/2] sep segment 1
[LSW3-GigabitEthernet1/0/2] quit
```

Configure LSW4.

```
[LSW4] interface gigabitethernet 1/0/1
[LSW4-GigabitEthernet1/0/1] stp disable
[LSW4-GigabitEthernet1/0/1] sep segment 1
[LSW4-GigabitEthernet1/0/1] quit
[LSW4] interface gigabitethernet 1/0/2
[LSW4-GigabitEthernet1/0/2] stp disable
[LSW4-GigabitEthernet1/0/2] sep segment 1
[LSW4-GigabitEthernet1/0/2] quit
```

Configure LSW5.

```
[LSW5] interface gigabitethernet 1/0/1
[LSW5-GigabitEthernet1/0/1] stp disable
[LSW5-GigabitEthernet1/0/1] sep segment 1
[LSW5-GigabitEthernet1/0/1] quit
```

```
[LSW5] interface gigabitethernet 1/0/3
[LSW5-GigabitEthernet1/0/3] stp disable
[LSW5-GigabitEthernet1/0/3] sep segment 1
[LSW5-GigabitEthernet1/0/3] quit
```

3. Specify a port to be blocked.

On LSW1 where the primary edge port resides, specify the port with the highest priority to be blocked.

```
[LSW1] sep segment 1
[LSW1-sep-segment1] block port optimal
```

4. Set the priority of GE1/0/2 on LSW3.

```
[LSW3] interface gigabitethernet 1/0/2
[LSW3-GigabitEthernet1/0/2] sep segment 1 priority 128
[LSW3-GigabitEthernet1/0/2] quit
```

5. Configure the preemption mode.

Configure delayed preemption on LSW1.

```
[LSW1-sep-segment1] preempt delay 30
[LSW1-sep-segment1] quit
```



NOTE

- You must set the preemption delay when delayed preemption is used because no default preemption delay time is available.
- After all the faulty ports recover, the edge ports no longer receive fault notification packets. If the primary edge port does not receive any fault notification packet within 3 seconds, the port starts the delay timer. After the delay timer expires, nodes in the SEP segment start blocked port preemption. To implement delayed preemption in this example, simulate a port fault and then rectify the fault. For example, run the **shutdown** command on GE1/0/2 on LSW2 to simulate a port fault, and then run the **undo shutdown** command on GE1/0/1 to rectify the fault.

Step 2 Configure the Layer 2 forwarding function on CE1 and LSW1 to LSW5.

For details about the configurations, see the configuration files.

Step 3 Verify the configuration.

Run the **shutdown** command on GE1/0/1 of LSW3 to simulate a port fault, and then run the **display sep interface** command on LSW3 to check whether GE1/0/2 on LSW3 has switched from the Discarding state to the Forwarding state.

```
<LSW3> display sep interface gigabitethernet 1/0/2
SEP segment 1
-----
Interface          Port Role   Neighbor Status   Port Status
-----
GE1/0/2            common    up                 forwarding
```

----End

4.1.4 Configuration Files

Configuration file of LSW1

```
#
 sysname LSW1
#
 vlan batch 10 100 200
```

```
#
sep segment 1
  control-vlan 10
  block port optimal
  preempt delay 30
  protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
  port hybrid tagged vlan 10 100
  stp disable
  sep segment 1 edge primary
#
interface GigabitEthernet1/0/2
  port hybrid pvid vlan 200
  port hybrid tagged vlan 100
  port hybrid untagged vlan 200
#
interface GigabitEthernet1/0/3
  port hybrid tagged vlan 10 100 200
  stp disable
  sep segment 1 edge secondary
#
return
```

Configuration file of LSW2

```
#
sysname LSW2
#
vlan batch 10 100
#
sep segment 1
  control-vlan 10
  protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
  port hybrid tagged vlan 10 100
  stp disable
  sep segment 1
#
interface GigabitEthernet1/0/2
  port hybrid tagged vlan 10 100
  stp disable
  sep segment 1
#
return
```

Configuration file of LSW2

```
#
sysname LSW3
#
vlan batch 10 100
#
sep segment 1
  control-vlan 10
  protected-instance 0 to 48
```

```
#
interface GigabitEthernet1/0/1
  port hybrid tagged vlan 10 100
  stp disable
  sep segment 1
#
interface GigabitEthernet1/0/2
  port hybrid tagged vlan 10 100
  stp disable
  sep segment 1
  sep segment 1 priority 128
#
interface GigabitEthernet1/0/3
  port hybrid tagged vlan 100
#
return
```

Configuration file of LSW4

```
#
sysname LSW4
#
vlan batch 10 100
#
sep segment 1
  control-vlan 10
  protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
  port hybrid tagged vlan 10 100
  stp disable
  sep segment 1
#
interface GigabitEthernet1/0/2
  port hybrid tagged vlan 10 100
  stp disable
  sep segment 1
#
return
```

Configuration file of LSW5

```
#
sysname LSW5
#
vlan batch 10 100 200
#
sep segment 1
  control-vlan 10
  protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
  port hybrid tagged vlan 10 100
  stp disable
  sep segment 1
#
interface GigabitEthernet1/0/2
```

```
port hybrid pvid vlan 200
port hybrid tagged vlan 100
port hybrid untagged vlan 200
#
interface GigabitEthernet1/0/3
port hybrid tagged vlan 10 100 200
stp disable
sep segment 1
#
return
```

Configuration file of CE1

```
#
sysname CE1
#
vlan batch 100
#
interface GigabitEthernet1/0/1
port hybrid tagged vlan 100
#
return
```

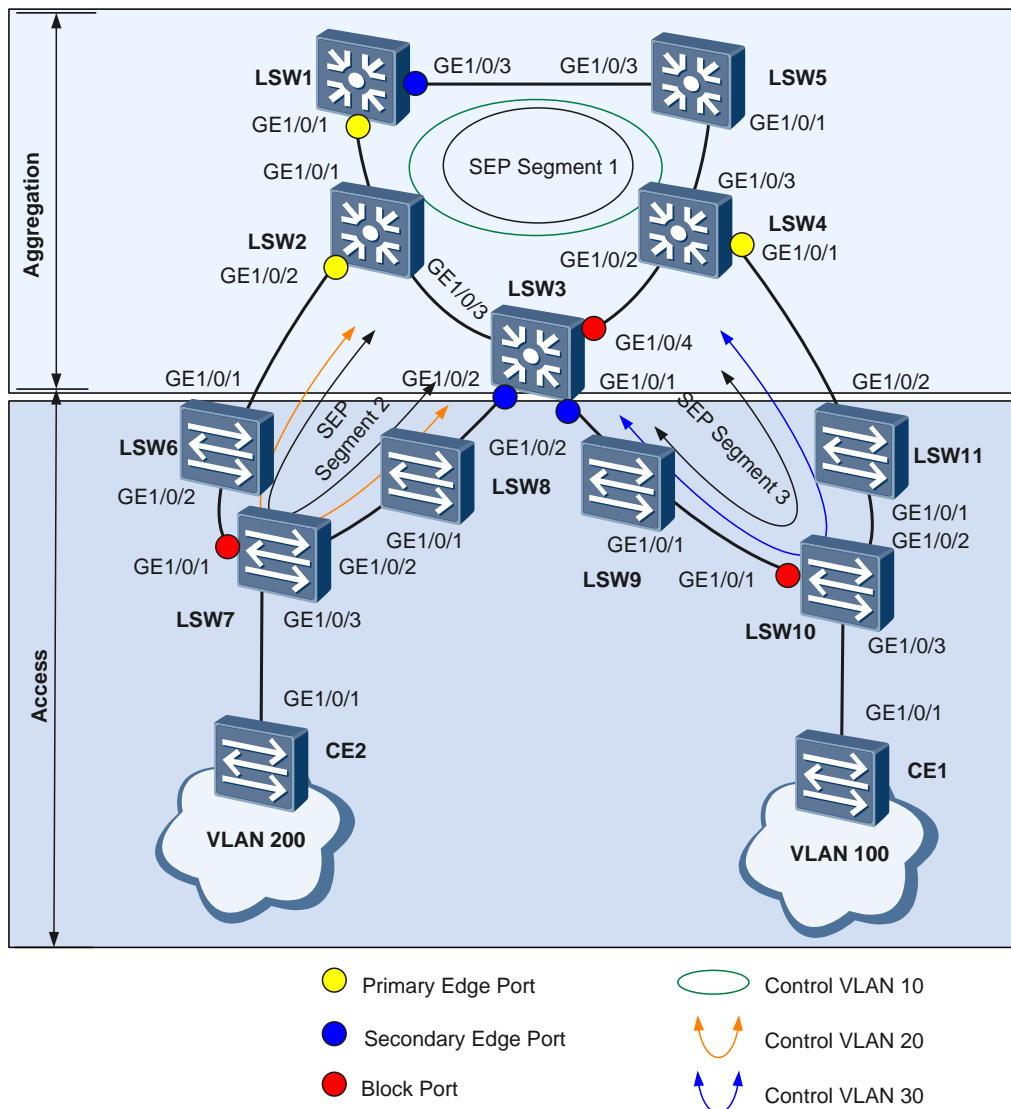
4.2 Example for Configuring SEP on a Multi-Ring Network

4.2.1 Networking Requirements

To implement link backup and enhance network reliability, users access an upper-layer network through redundant links. The use of redundant links, however, may produce loops. The loops cause broadcast storms and make the MAC address table unstable. As a result, communication quality deteriorates, and communication services may even be interrupted. SEP can be deployed on the ring network to eliminate loops and restore communication if a link fails.

In the multi-ring networking, multiple ring networks consisting of Layer 2 switching devices are deployed at the access layer and aggregation layer. SEP runs at the access layer and aggregation layer to implement link redundancy.

Figure 4-2 Multi-ring SEP networking



As shown in Figure 4-2, multiple Layer 2 switching devices form ring networks at the access layer and aggregation layer. SEP runs at the access layer and aggregation layer. When no faulty link exists on the ring network, SEP can eliminate loops on the network. When a link on the ring network fails, SEP can rapidly restore communication between nodes on the ring network.

4.2.2 Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic SEP functions.
 - Configure SEP segments 1 to 3 and configure VLAN 10, VLAN 20, and VLAN 30 as their control VLANs.

Configure SEP segment 1 on LSW1 to LSW5 and configure VLAN 10 as the control VLAN of SEP segment 1.

Configure SEP segment 2 on LSW2, LSW3, and LSW6 to LSW8, and configure VLAN 20 as the control VLAN of SEP segment 2.

Configure SEP segment 3 on LSW3, LSW4, and LSW9 to LSW11, and configure VLAN 30 as the control VLAN of SEP segment 3.

- Add devices on the ring networks to the SEP segments and configure port roles on the edge devices of the SEP segments.

On LSW1 to LSW5, add the ports on the ring network at the access layer to SEP segment 1. Configure the roles of GE1/0/1 and GE1/0/3 on LSW1 in SEP segment 1.

Add GE1/0/2 on LSW2, two ports on LSW6 to LSW8, and GE1/0/2 on LSW3 to SEP segment 2. Configure the roles of GE1/0/2 on LSW2 and GE1/0/2 on LSW3 in SEP segment 2.

Add GE1/0/1 on LSW3, GE1/0/1 and GE1/0/2 on LSW9 to LSW11, and GE1/0/1 on LSW4 to SEP segment 3. Configure the roles of GE1/0/1 on LSW3 and GE1/0/1 on LSW4 in SEP segment 3.

- Specify the ports to be blocked on the devices where the primary edge ports reside in the SEP segments.

In SEP segment 1, specify the port with the highest priority to be blocked.

In SEP segment 2, specify the device name and port name to block the specified port.

In SEP segment 3, specify the blocked port based on the configured hop count.

- Configure the preemption mode on the device where the primary edge port resides.

Configure delayed preemption in SEP segment 1 and manual preemption in SEP segment 2 and SEP segment 3.

- Configure the topology change notification function on the edge devices between SEP segments, namely, LSW2, LSW3, and LSW4.

2. Configure the Layer 2 forwarding function on CE1, CE2, and LSW1 to LSW11.

4.2.3 Procedure

Step 1 Configure basic SEP functions.

1. Configure SEP segments 1 to 3 and configure VLAN 10, VLAN 20, and VLAN 30 as their control VLANs.

Configure LSW1.

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] protected-instance all
[LSW1-sep-segment1] quit
```

Configure LSW2.

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment 1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] protected-instance all
[LSW2-sep-segment1] quit
[LSW2] sep segment 2
[LSW2-sep-segment2] control-vlan 20
[LSW2-sep-segment2] protected-instance all
[LSW2-sep-segment2] quit
```

Configure LSW3.

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
[LSW3-sep-segment1] protected-instance all
[LSW3-sep-segment1] quit
[LSW3] sep segment 2
[LSW3-sep-segment2] control-vlan 20
[LSW3-sep-segment2] protected-instance all
[LSW3-sep-segment2] quit
[LSW3] sep segment 3
[LSW3-sep-segment3] control-vlan 30
[LSW3-sep-segment3] protected-instance all
[LSW3-sep-segment3] quit
```

Configure LSW4.

```
<Quidway> system-view
[Quidway] sysname LSW4
[LSW4] sep segment 1
[LSW4-sep-segment1] control-vlan 10
[LSW4-sep-segment1] protected-instance all
[LSW4-sep-segment1] quit
[LSW4] sep segment 3
[LSW4-sep-segment3] control-vlan 30
[LSW4-sep-segment3] protected-instance all
[LSW4-sep-segment3] quit
```

Configure LSW5.

```
<Quidway> system-view
[Quidway] sysname LSW5
[LSW5] sep segment 1
[LSW5-sep-segment1] control-vlan 10
[LSW5-sep-segment1] protected-instance all
[LSW5-sep-segment1] quit
```

Configure LSW6 to LSW11.

The configurations on LSW6 to LSW11 are similar to the configurations on LSW1 to LSW5 except for the control VLANs of different SEP segments.

For details about the configurations, see the configuration files.



NOTE

- The control VLAN must be a VLAN that has not been created or used, and the configuration file automatically displays the command for creating common VLANs.
- Each SEP segment must be configured with a control VLAN. After a port is added to the SEP segment configured with a control VLAN, the port is automatically added to the control VLAN.

2. Add devices on the ring networks to the SEP segments and configure port roles according to Figure 4-2.



NOTE

If STP is enabled on a port, disable STP on the port before adding the port to a SEP segment.

On LSW1, configure GE1/0/1 as the primary edge port and GE1/0/3 as the secondary edge port.

```
[LSW1] interface gigabitethernet 1/0/1
[LSW1-GigabitEthernet1/0/1] stp disable
[LSW1-GigabitEthernet1/0/1] sep segment 1 edge primary
```

```
[LSW1-GigabitEthernet1/0/1] quit
[LSW1] interface gigabitethernet 1/0/3
[LSW1-GigabitEthernet1/0/3] stp disable
[LSW1-GigabitEthernet1/0/3] sep segment 1 edge secondary
[LSW1-GigabitEthernet1/0/3] quit
```

Configure LSW2.

```
[LSW2] interface gigabitethernet 1/0/1
[LSW2-GigabitEthernet1/0/1] stp disable
[LSW2-GigabitEthernet1/0/1] sep segment 1
[LSW2-GigabitEthernet1/0/1] quit
[LSW2] interface gigabitethernet 1/0/3
[LSW2-GigabitEthernet1/0/3] stp disable
[LSW2-GigabitEthernet1/0/3] sep segment 1
[LSW2-GigabitEthernet1/0/3] quit
[LSW2] interface gigabitethernet 1/0/2
[LSW2-GigabitEthernet1/0/2] stp disable
[LSW2-GigabitEthernet1/0/2] sep segment 2 edge primary
[LSW2-GigabitEthernet1/0/2] quit
```

Configure LSW3.

```
[LSW3] interface gigabitethernet 1/0/3
[LSW3-GigabitEthernet1/0/3] stp disable
[LSW3-GigabitEthernet1/0/3] sep segment 1
[LSW3-GigabitEthernet1/0/3] quit
[LSW3] interface gigabitethernet 1/0/4
[LSW3-GigabitEthernet1/0/4] stp disable
[LSW3-GigabitEthernet1/0/4] sep segment 1
[LSW3-GigabitEthernet1/0/4] quit
[LSW3] interface gigabitethernet 1/0/2
[LSW3-GigabitEthernet1/0/2] stp disable
[LSW3-GigabitEthernet1/0/2] sep segment 2 edge secondary
[LSW3-GigabitEthernet1/0/2] quit
[LSW3] interface gigabitethernet 1/0/1
[LSW3-GigabitEthernet1/0/1] stp disable
[LSW3-GigabitEthernet1/0/1] sep segment 3 edge secondary
[LSW3-GigabitEthernet1/0/1] quit
```

Configure LSW4.

```
[LSW4] interface gigabitethernet 1/0/2
[LSW4-GigabitEthernet1/0/2] stp disable
[LSW4-GigabitEthernet1/0/2] sep segment 1
[LSW4-GigabitEthernet1/0/2] quit
[LSW4] interface gigabitethernet 1/0/3
[LSW4-GigabitEthernet1/0/3] stp disable
[LSW4-GigabitEthernet1/0/3] sep segment 1
[LSW4-GigabitEthernet1/0/3] quit
[LSW4] interface gigabitethernet 1/0/1
[LSW4-GigabitEthernet1/0/1] stp disable
[LSW4-GigabitEthernet1/0/1] sep segment 3 edge primary
[LSW4-GigabitEthernet1/0/1] quit
```

Configure LSW5.

```
[LSW5] interface gigabitethernet 1/0/1
[LSW5-GigabitEthernet1/0/1] stp disable
[LSW5-GigabitEthernet1/0/1] sep segment 1
[LSW5-GigabitEthernet1/0/1] quit
```

```
[LSW5] interface gigabitethernet 1/0/3
[LSW5-GigabitEthernet1/0/3] stp disable
[LSW5-GigabitEthernet1/0/3] sep segment 1
[LSW5-GigabitEthernet1/0/3] quit
```

Configure LSW6 to LSW11.

The configurations on LSW6 to LSW11 are similar to the configurations on LSW1 to LSW5 except that you do not need to configure the roles for ports on LSW6 to LSW11.

For details about the configurations, see the configuration files.

3. Specify a port to be blocked.

On LSW1 where the primary edge port of SEP segment 1 resides, specify the port with the highest priority to be blocked.

```
[LSW1] sep segment 1
[LSW1-sep-segment1] block port optimal
[LSW1-sep-segment1] quit
```

On LSW3, set the priority of GE1/0/4 to 128, which is the highest priority among the ports so that GE1/0/4 will be blocked.

```
[LSW3] interface gigabitethernet 1/0/4
[LSW3-GigabitEthernet1/0/4] sep segment 1 priority 128
[LSW3-GigabitEthernet1/0/4] quit
```

Retain the default priority for the other ports in SEP segment 1.

On LSW2 where the primary edge port of SPE segment 2 resides, specify the device name and port name so that the specified port will be blocked.

Before specifying the port to be blocked, you can run the **display sep topology** command to view the current topology information and information about all the ports in the topology. Specify the device name and port name.

```
[LSW2] sep segment 2
[LSW2-sep-segment2] block port sysname LSW7 interface gigabitethernet 1/0/1
[LSW2-sep-segment2] quit
```

On LSW4 where the primary edge port of SEP segment 3 resides, specify the blocked port based on the configured hop count.

```
[LSW4] sep segment 3
[LSW4-sep-segment3] block port hop 5
[LSW4-sep-segment3] quit
```



NOTE

SEP sets the hop count of the primary edge port to 1 and the hop count of the neighbor port of the primary edge port to 2. Hop counts of other ports increase by steps of 1 in the downstream direction of the primary edge port.

4. Configure the preemption mode.

Configure delayed preemption on LSW1.

```
[LSW1] sep segment 1
[LSW1-sep-segment1] preempt delay 30
```

 **NOTE**

- You must set the preemption delay when delayed preemption is used because no default preemption delay time is available.
- After all the faulty ports recover, the edge ports no longer receive fault notification packets. If the primary edge port does not receive any fault notification packet within 3 seconds, the port starts the delay timer. After the delay timer expires, nodes in the SEP segment start blocked port preemption. To implement delayed preemption in this example, simulate a port fault and then rectify the fault. For example, run the **shutdown** command on GE1/0/2 on LSW2 to simulate a port fault, and then run the **undo shutdown** command on GE1/0/1 to rectify the fault.

Configure manual preemption on LSW2.

```
[LSW2] sep segment 2
[LSW2-sep-segment2] preempt manual
```

Configure manual preemption on LSW4.

```
[LSW4] sep segment 3
[LSW4-sep-segment3] preempt manual
```

5. Configure the topology change notification function.

Configure SEP segment 2 to notify SEP segment 1 of topology changes.

Configure LSW2.

```
[LSW2] sep segment 2
[LSW2-sep-segment2] tc-notify segment 1
[LSW2-sep-segment2] quit
```

Configure LSW3.

```
[LSW3] sep segment 2
[LSW3-sep-segment2] tc-notify segment 1
[LSW3-sep-segment2] quit
```

Configure SEP segment 3 to notify SEP segment 1 of topology changes.

Configure LSW3.

```
[LSW3] sep segment 3
[LSW3-sep-segment3] tc-notify segment 1
[LSW3-sep-segment3] quit
```

Configure LSW4.

```
[LSW4] sep segment 3
[LSW4-sep-segment3] tc-notify segment 1
[LSW4-sep-segment3] quit
```

 **NOTE**

The topology change notification function is configured on edge devices between SEP segments so that the upper-layer network can be notified of topology changes on the lower-layer network.

Step 2 Configure the Layer 2 forwarding function on the CEs and LSW1 to LSW11.

For details about the configurations, see the configuration files.

Step 3 Verify the configuration.

Perform the following operations to verify the configuration. LSW1 is used as an example.

Run the **shutdown** command on GE1/0/1 of LSW2 to simulate a port fault, and then run the **display sep interface** command on LSW3 to check whether GE1/0/4 on LSW3 has switched from the Discarding state to the Forwarding state.

```
<LSW3> display sep interface gigabitethernet 1/0/4
SEP segment 1
```

Interface	Port Role	Neighbor Status	Port Status
GE1/0/4	common	up	forwarding

----End

4.2.4 Configuration Files

Configuration file of LSW1

```
#
sysname LSW1
#
vlan batch 10 100 200 300
#
sep segment 1
control-vlan 10
block port optimal
preempt delay 30
protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
port hybrid tagged vlan 10 100 200
stp disable
sep segment 1 edge primary
#
interface GigabitEthernet1/0/2
port hybrid pvid vlan 300
port hybrid tagged vlan 100 200
port hybrid untagged vlan 300
#
interface GigabitEthernet1/0/3
port hybrid tagged vlan 10 100 200 300
stp disable
sep segment 1 edge secondary
#
return
```

Configuration file of LSW2

```
#
sysname LSW2
#
vlan batch 10 20 100 200
#
sep segment 1
control-vlan 10
protected-instance 0 to 48
sep segment 2
control-vlan 20
block port sysname LSW7 interface GigabitEthernet1/0/1
tc-notify segment 1
protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
port hybrid tagged vlan 10 100 200
```

```
    stp disable
    sep segment 1
#
interface GigabitEthernet1/0/2
    port hybrid tagged vlan 20 200
    stp disable
    sep segment 2 edge primary
#
interface GigabitEthernet1/0/3
    port hybrid tagged vlan 10 100 200
    stp disable
    sep segment 1
#
return
```

Configuration file of LSW2

```
#
sysname LSW3
#
vlan batch 10 20 30 100 200
#
sep segment 1
    control-vlan 10
    protected-instance 0 to 48
sep segment 2
    control-vlan 20
    tc-notify segment 1
    protected-instance 0 to 48
sep segment 3
    control-vlan 30
    tc-notify segment 1
    protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
    port hybrid tagged vlan 30 100
    stp disable
    sep segment 3 edge secondary
#
interface GigabitEthernet1/0/2
    port hybrid tagged vlan 20 200
    stp disable
    sep segment 2 edge secondary
#
interface GigabitEthernet1/0/3
    port hybrid tagged vlan 10 100 200
    stp disable
    sep segment 1
#
interface GigabitEthernet1/0/4
    port hybrid tagged vlan 10 100 200
    stp disable
    sep segment 1
    sep segment 1 priority 128
#
return
```

Configuration file of LSW4

```
#
 sysname LSW4
#
 vlan batch 10 30 100 200
#
 sep segment 1
  control-vlan 10
  protected-instance 0 to 48
 sep segment 3
  control-vlan 30
  block port hop 5
  tc-notify segment 1
  protected-instance 0 to 48
#
 interface GigabitEthernet1/0/1
  port hybrid tagged vlan 30 100
  stp disable
  sep segment 3 edge primary
#
 interface GigabitEthernet1/0/2
  port hybrid tagged vlan 10 100 200
  stp disable
  sep segment 1
#
 interface GigabitEthernet1/0/3
  port hybrid tagged vlan 10 100 200
  stp disable
  sep segment 1
#
 return
```

Configuration file of LSW5

```
#
 sysname LSW5
#
 vlan batch 10 100 200 300
#
 sep segment 1
  control-vlan 10
  protected-instance 0 to 48
#
 interface GigabitEthernet1/0/1
  port hybrid tagged vlan 10 100 200
  stp disable
  sep segment 1
#
 interface GigabitEthernet1/0/2
  port hybrid pvid vlan 300
  port hybrid tagged vlan 100 200
  port hybrid untagged vlan 300
#
 interface GigabitEthernet1/0/3
  port hybrid tagged vlan 10 100 200 300
```



```
    stp disable
    sep segment 1
#
return
```

Configuration file of LSW6

```
#
sysname LSW6
#
vlan batch 20 200
#
sep segment 2
control-vlan 20
protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
port hybrid tagged vlan 20 200
stp disable
sep segment 2
#
interface GigabitEthernet1/0/2
port hybrid tagged vlan 20 200
stp disable
sep segment 2
#
return
```

Configuration file of LSW7

```
#
sysname LSW7
#
vlan batch 20 200
#
sep segment 2
control-vlan 20
protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
port hybrid tagged vlan 20 200
stp disable
sep segment 2
#
interface GigabitEthernet1/0/2
port hybrid tagged vlan 20 200
stp disable
sep segment 2
#
interface GigabitEthernet1/0/3
port hybrid tagged vlan 200
#
return
```

Configuration file of LSW8

```
#
```

```
sysname LSW8
#
vlan batch 20 200
#
sep segment 2
control-vlan 20
protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
port hybrid tagged vlan 20 200
stp disable
sep segment 2
#
interface GigabitEthernet1/0/2
port hybrid tagged vlan 20 200
stp disable
sep segment 2
#
return
```

Configuration file of LSW9

```
#
sysname LSW9
#
vlan batch 30 100
#
sep segment 3
control-vlan 30
protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
port hybrid tagged vlan 30 100
stp disable
sep segment 3
#
interface GigabitEthernet1/0/2
port hybrid tagged vlan 30 100
stp disable
sep segment 3
#
return
```

Configuration file of LSW10

```
#
sysname LSW10
#
vlan batch 30 100
#
sep segment 3
control-vlan 30
protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
port hybrid tagged vlan 30 100
stp disable
```

```
    sep segment 3
#
interface GigabitEthernet1/0/2
    port hybrid tagged vlan 30 100
    stp disable
    sep segment 3
#
interface GigabitEthernet1/0/3
    port hybrid tagged vlan 100
#
return
```

Configuration file of LSW11

```
#
sysname LSW11
#
vlan batch 30 100
#
sep segment 3
    control-vlan 30
    protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
    port hybrid tagged vlan 30 100
    stp disable
    sep segment 3
#
interface GigabitEthernet1/0/2
    port hybrid tagged vlan 30 100
    stp disable
    sep segment 3
#
return
```

Configuration file of CE1

```
#
sysname CE1
#
vlan batch 100
#
interface GigabitEthernet1/0/1
    port hybrid tagged vlan 100
#
return
```

Configuration file of CE2

```
#
sysname CE2
#
vlan batch 200
#
interface GigabitEthernet1/0/1
    port hybrid tagged vlan 200
#
```

return

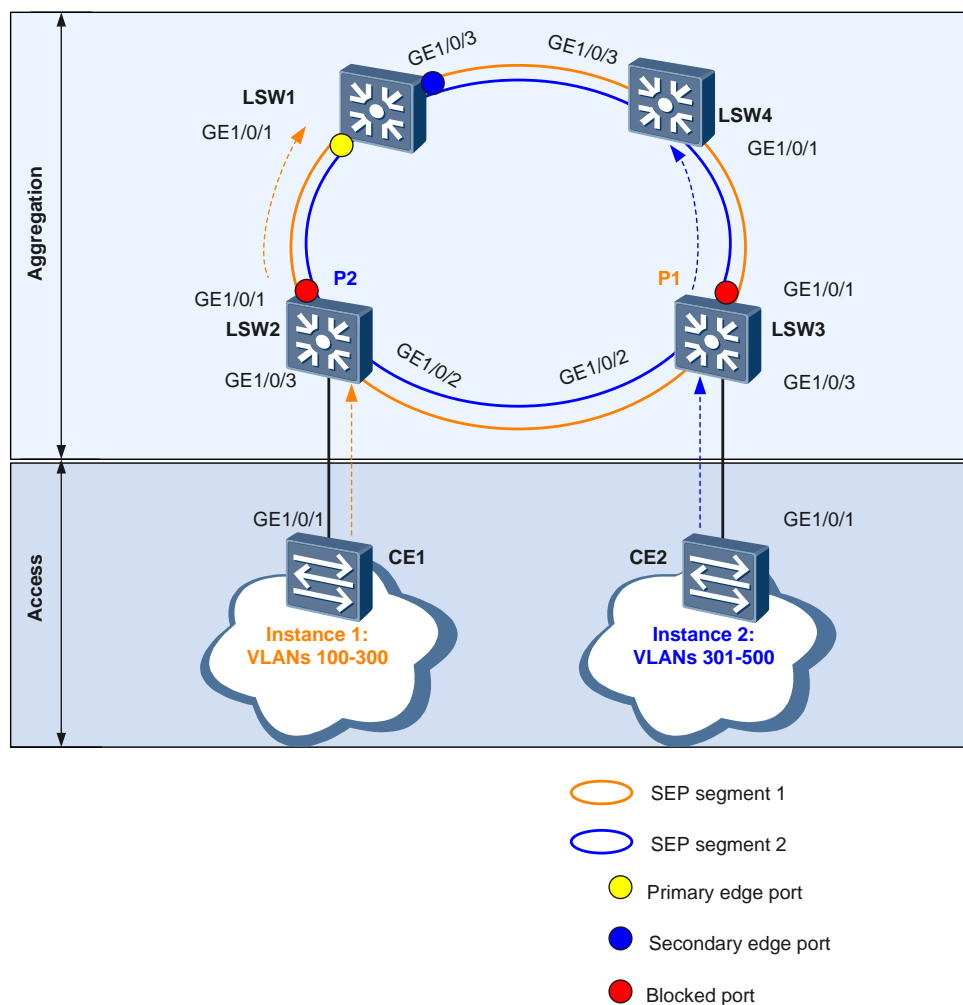
4.3 Example for Configuring SEP Multi-Instance

4.3.1 Networking Requirements

As shown in Figure 4-3, on a common SEP network, a physical ring network can be configured with only one SEP segment in which only one port can be blocked. If a port in a complete SEP segment is blocked, all user data is transmitted along only one path. The path where the blocked port resides remains idle, wasting bandwidth.

To improve bandwidth efficiency and implement load balancing, Huawei develops SEP multi-instance.

Figure 4-3 SEP multi-instance on a closed ring network



Layer 2 switching devices LSW1 to LSW4 form a ring network, which is connected to the core network. SEP runs at the aggregation layer. SEP multi-instance is configured on LSW1

to LSW4 to allow for two SEP segments to improve bandwidth efficiency, implement load balancing, and provide link backup.

4.3.2 Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic SEP functions.
 - Create two SEP segments and a control VLAN on LSW1 to LSW4. Different SEP segments can use the same control VLAN.
 - Configure SEP protected instances, and set mappings between the instances and user VLANs to ensure that topology changes affect only corresponding VLANs.
 - Add all the devices on the ring network to the SEP segments, and configure GE1/0/1 as the primary edge port and GE1/0/3 as the secondary edge port on LSW1.
 - Configure the port blocking mode on the device where the primary edge port resides.
 - Configure the preemption mode to ensure that the specified port is blocked when a fault is rectified.
2. Configure the Layer 2 forwarding function on CE1, CE2, and LSW1 to LSW4.

4.3.3 Procedure

Step 1 Create SEP segments and a control VLAN.

1. Configure SEP segment 1 on LSW1 to LSW4 and configure VLAN 10 as the control VLAN of SEP segment 1.

Configure LSW1.

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] quit
```

Configure LSW2.

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] quit
```

Configure LSW3.

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
[LSW3-sep-segment1] quit
```

Configure LSW4.

```
<Quidway> system-view
[Quidway] sysname LSW4
[LSW4] sep segment 1
[LSW4-sep-segment1] control-vlan 10
```

```
[LSW4-sep-segment1] quit
```

2. Configure SEP segment 2 on LSW1 to LSW4 and configure VLAN 10 as the control VLAN of SEP segment 2.

Configure LSW1.

```
[LSW1] sep segment 2  
[LSW1-sep-segment2] control-vlan 10  
[LSW1-sep-segment2] quit
```

Configure LSW2.

```
[LSW2] sep segment2  
[LSW2-sep-segment2] control-vlan 10  
[LSW2-sep-segment2] quit
```

Configure LSW3.

```
[LSW3] sep segment 2  
[LSW3-sep-segment2] control-vlan 10  
[LSW3-sep-segment2] quit
```

Configure LSW4.

```
[LSW4] sep segment 2  
[LSW4-sep-segment2] control-vlan 10  
[LSW4-sep-segment2] quit
```



NOTE

- The control VLAN must be a VLAN that has not been created or used, and the configuration file automatically displays the command for creating common VLANs.
- Each SEP segment must be configured with a control VLAN. After a port is added to the SEP segment configured with a control VLAN, the port is automatically added to the control VLAN.

Step 2 Configure SEP protected instances, and set mappings between the instances and user VLANs.

Configure LSW1.

```
[LSW1] vlan batch 100 to 500  
[LSW1] sep segment 1  
[LSW1-sep-segment1] protected-instance 1  
[LSW1-sep-segment1] quit  
[LSW1] sep segment 2  
[LSW1-sep-segment2] protected-instance 2  
[LSW1-sep-segment2] quit  
[LSW1] stp region-configuration  
[LSW1-mst-region] instance 1 vlan 100 to 300  
[LSW1-mst-region] instance 2 vlan 301 to 500  
[LSW1-mst-region] active region-configuration  
[LSW1-mst-region] quit
```

The configurations on LSW2 to LSW4 are similar to the configuration on LSW1. For details about the configurations, see the configuration files.

Step 3 Add all the devices on the ring network to the SEP segments and configure port roles.



NOTE

If STP is enabled on a port, disable STP on the port before adding the port to a SEP segment.

On LSW1, configure GE1/0/1 as the primary edge port and GE1/0/3 as the secondary edge port.

```
[LSW1] interface gigabitethernet 1/0/1
[LSW1-GigabitEthernet1/0/1] stp disable
[LSW1-GigabitEthernet1/0/1] sep segment 1 edge primary
[LSW1-GigabitEthernet1/0/1] sep segment 2 edge primary
[LSW1-GigabitEthernet1/0/1] quit
[LSW1] interface gigabitethernet 1/0/3
[LSW1-GigabitEthernet1/0/3] stp disable
[LSW1-GigabitEthernet1/0/3] sep segment 1 edge secondary
[LSW1-GigabitEthernet1/0/3] sep segment 2 edge secondary
[LSW1-GigabitEthernet1/0/3] quit
```

Configure LSW2.

```
[LSW2] interface gigabitethernet 1/0/1
[LSW2-GigabitEthernet1/0/1] stp disable
[LSW2-GigabitEthernet1/0/1] sep segment 1
[LSW2-GigabitEthernet1/0/1] sep segment 2
[LSW2-GigabitEthernet1/0/1] quit
[LSW2] interface gigabitethernet 1/0/2
[LSW2-GigabitEthernet1/0/2] stp disable
[LSW2-GigabitEthernet1/0/2] sep segment 1
[LSW2-GigabitEthernet1/0/2] sep segment 2
[LSW2-GigabitEthernet1/0/2] quit
```

Configure LSW3.

```
[LSW3] interface gigabitethernet 1/0/1
[LSW3-GigabitEthernet1/0/1] stp disable
[LSW3-GigabitEthernet1/0/1] sep segment 1
[LSW3-GigabitEthernet1/0/1] sep segment 2
[LSW3-GigabitEthernet1/0/1] quit
[LSW3] interface gigabitethernet 1/0/2
[LSW3-GigabitEthernet1/0/2] stp disable
[LSW3-GigabitEthernet1/0/2] sep segment 1
[LSW3-GigabitEthernet1/0/2] sep segment 2
[LSW3-GigabitEthernet1/0/2] quit
```

Configure LSW4.

```
[LSW4] interface gigabitethernet 1/0/1
[LSW4-GigabitEthernet1/0/1] stp disable
[LSW4-GigabitEthernet1/0/1] sep segment 1
[LSW4-GigabitEthernet1/0/1] sep segment 2
[LSW4-GigabitEthernet1/0/1] quit
[LSW4] interface gigabitethernet 1/0/3
[LSW4-GigabitEthernet1/0/3] stp disable
[LSW4-GigabitEthernet1/0/3] sep segment 1
[LSW4-GigabitEthernet1/0/3] sep segment 2
[LSW4-GigabitEthernet1/0/3] quit
```

Step 4 Specify a port to be blocked.

On LSW1 where the primary edge port resides, configure delayed preemption and block a port based on the device name and port name.

```
[LSW1] sep segment 1
[LSW1-sep-segment1] block port sysname LSW3 interface gigabitethernet 1/0/1
[LSW1-sep-segment1] preempt delay 15
```

```
[LSW1-sep-segment1] quit
[LSW1] sep segment 2
[LSW1-sep-segment2] block port sysname LSW2 interface gigabitethernet 1/0/1
[LSW1-sep-segment2] preempt delay 15
[LSW1-sep-segment2] quit
```



NOTE

In this configuration example, you need to simulate a port fault and then rectify it to implement delayed preemption. To ensure that delayed preemption takes effect on the two SEP segments, simulate a port fault in the two SEP segments. For example:

- In SEP segment 1, run the **shutdown** command on GE1/0/1 of LSW2 to simulate a port fault, and then run the **undo shutdown** command to simulate port fault recovery.
- In SEP segment 2, run the **shutdown** command on GE1/0/1 of LSW3 to simulate a port fault, and then run the **undo shutdown** command to simulate port fault recovery.

Step 5 Configure the Layer 2 forwarding function on CE1, CE2, and LSW1 to LSW4.

For details about the configurations, see the configuration files.

Step 6 Verify the configuration.

Simulate a fault, and then check whether the status of the blocked port changes from the Discarding state to the Forwarding state.

Run the **shutdown** command on GE1/0/1 of LSW2 to simulate a port fault.

Run the **display sep interface** command on LSW3 to check whether the status of GE1/0/1 in SEP segment 1 has changed from the Discarding state to the Forwarding state.

```
[LSW3] display sep interface gigabitethernet 1/0/1
SEP segment 1
-----
Interface          Port Role   Neighbor Status   Port Status
-----
GE1/0/1            common     up                 forwarding
SEP segment 2
-----
Interface          Port Role   Neighbor Status   Port Status
-----
GE1/0/1            common     up                 forwarding
```

The preceding command output shows that the status of GE1/0/1 changes from the Discarding state to the Forwarding state and the forwarding path change in SEP segment 1 does not affect the forwarding path in SEP segment 2.

----End

4.3.4 Configuration Files

Configuration file of LSW1

```
#
 sysname LSW1
#
 vlan batch 10 100 to 500
#
 stp region-configuration
 instance 1 vlan 100 to 300
 instance 2 vlan 301 to 500
```



```
    active region-configuration
#
sep segment 1
    control-vlan 10
    block port sysname LSW3 interface GigabitEthernet1/0/1
    preempt delay 15
    protected-instance 1
sep segment 2
    control-vlan 10
    block port sysname LSW2 interface GigabitEthernet1/0/1
    preempt delay 15
    protected-instance 2
#
interface GigabitEthernet1/0/1
    port hybrid tagged vlan 10 100 to 500
    stp disable
    sep segment 1 edge primary
    sep segment 2 edge primary
#
interface GigabitEthernet1/0/3
    port hybrid tagged vlan 10 100 to 500
    stp disable
    sep segment 1 edge secondary
    sep segment 2 edge secondary
#
return
```

Configuration file of LSW2

```
#
sysname LSW2
#
vlan batch 10 100 to 500
#
stp region-configuration
    instance 1 vlan 100 to 300
    instance 2 vlan 301 to 500
    active region-configuration
#
sep segment 1
    control-vlan 10
    protected-instance 1
sep segment 2
    control-vlan 10
    protected-instance 2
#
interface GigabitEthernet1/0/1
    port hybrid tagged vlan 10 100 to 500
    stp disable
    sep segment 1
    sep segment 2
#
interface GigabitEthernet1/0/2
    port hybrid tagged vlan 10 100 to 500
    stp disable
    sep segment 1
```

```
    sep segment 2
#
interface GigabitEthernet1/0/3
    port hybrid tagged vlan 100 to 300
#
return
```

Configuration file of LSW2

```
#
sysname LSW3
#
vlan batch 10 100 to 500
#
stp region-configuration
    instance 1 vlan 100 to 300
    instance 2 vlan 301 to 500
    active region-configuration
#
sep segment 1
    control-vlan 10
    protected-instance 1
sep segment 2
    control-vlan 10
    protected-instance 2
#
interface GigabitEthernet1/0/1
    port hybrid tagged vlan 10 100 to 500
    stp disable
    sep segment 1
    sep segment 2
#
interface GigabitEthernet1/0/2
    port hybrid tagged vlan 10 100 to 500
    stp disable
    sep segment 1
    sep segment 2
#
interface GigabitEthernet1/0/3
    port hybrid tagged vlan 301 to 500
#
return
```

Configuration file of LSW4

```
#
sysname LSW4
#
vlan batch 10 60 100 to 500
#
stp region-configuration
    instance 1 vlan 100 to 300
    instance 2 vlan 301 to 500
    active region-configuration
#
sep segment 1
    control-vlan 10
```

```
protected-instance 1
sep segment 2
control-vlan 10
protected-instance 2
#
interface GigabitEthernet1/0/1
port hybrid tagged vlan 10 100 to 500
stp disable
sep segment 1
sep segment 2
#
interface GigabitEthernet1/0/3
port hybrid tagged vlan 10 100 to 500
stp disable
sep segment 1
sep segment 2
#
return
```

Configuration file of CE1

```
#
sysname CE1
#
vlan batch 100 to 300
#
interface GigabitEthernet1/0/1
port hybrid tagged vlan 100 to 300
#
return
```

Configuration file of CE2

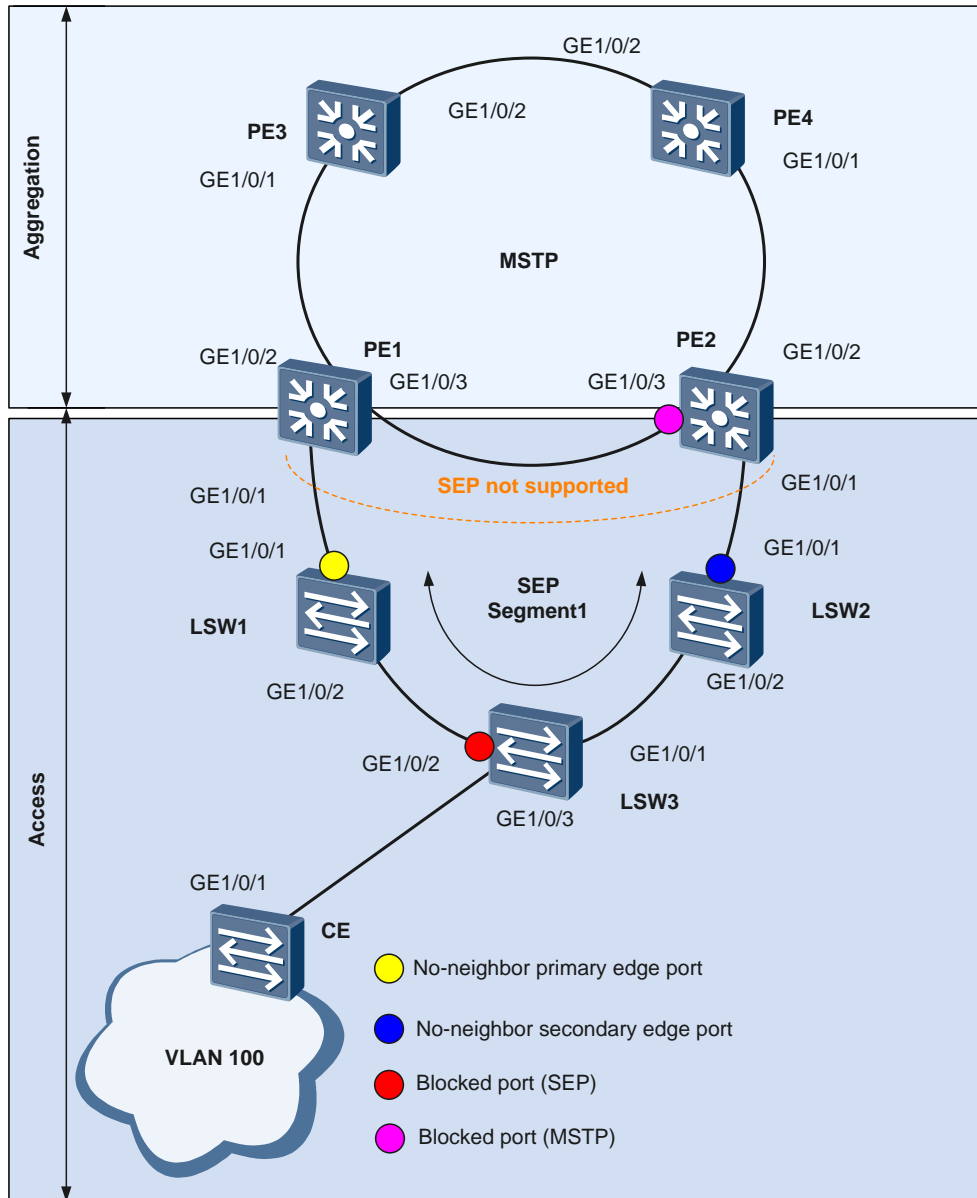
```
#
sysname CE2
#
vlan batch 301 to 500
#
interface GigabitEthernet1/0/1
port hybrid tagged vlan 301 to 500
#
return
```

4.4 Example for Configuring a Hybrid SEP+MSTP Network

4.4.1 Networking Requirements

To implement link backup and enhance network reliability, users access an upper-layer network through redundant links. The use of redundant links, however, may produce loops. The loops cause broadcast storms and make the MAC address table unstable. As a result, communication quality deteriorates, and communication services may even be interrupted. SEP can be deployed on the ring network to eliminate loops and restore communication if a link fails.

Figure 4-4 Hybrid SEP+MSTP networking



As shown in Figure 4-4, multiple Layer 2 switching devices form a ring network at the access layer, and multiple Layer 3 devices form a ring network at the aggregation layer. Multiple Spanning Tree Protocol (MSTP) has been deployed at the aggregation layer to eliminate redundant links. The two devices where the access layer and the aggregation layer are intersected do not support SEP. You can configure SEP at the access layer to implement protection switching and configure the topology change notification function on an edge device in a SEP segment. This function enables an upper-layer network to promptly detect topology changes on a lower-layer network.

- When no faulty link exists on the ring network, SEP can eliminate loops on the network.
- When a link on the ring network fails, SEP can rapidly restore communication between nodes on the ring network.

- The topology change notification function must be configured on an edge device in a SEP segment. This function enables an upper-layer network to promptly detect topology changes on a lower-layer network.
- After receiving a message indicating a topology change on a lower-layer network, an edge device on the upper-layer network sends TC packets to instruct other devices to delete their original MAC address entries and learn new MAC addresses after the topology of the lower-layer network changes. This ensures uninterrupted traffic forwarding.

4.4.2 Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic SEP functions.
 - Configure SEP segment 1 on LSW1 to LSW3 and configure VLAN 10 as the control VLAN of SEP segment 1.
 - Add LSW1 to LSW3 to SEP segment 1 and configure port roles on the edge devices (LSW1 and LSW2) of SEP segment 1.



NOTE

PE1 and PE2 do not support SEP; therefore, the ports on LSW1 and LSW2 connected to the PEs must be no-neighbor edge ports.

- On the device where the no-neighbor primary edge port resides, specify the port in the middle of the SEP segment as the port to be blocked.
 - Configure manual preemption.
 - Configure the topology change notification function so that the upper-layer network running MSTP can be notified of topology changes in the SEP segment.
2. Configure basic MSTP functions.
 - Add PE1 to PE4, LSW1, and LSW2 to MST region RG1.
 - Create a VLAN on PE1 to PE4, LSW1, and LSW2, and add ports on the STP ring to the VLAN.
 - Configure PE3 as the root bridge and PE4 as the backup root bridge.
 3. Configure the Layer 2 forwarding function on the CE and LSW1 to LSW3.

4.4.3 Procedure

Step 1 Configure basic SEP functions.

1. Configure SEP segment 1 on LSW1 to LSW3 and configure VLAN 10 as the control VLAN of SEP segment 1.

Configure LSW1.

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] protected-instance all
[LSW1-sep-segment1] quit
```

Configure LSW2.

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment 1
[LSW2-sep-segment1] control-vlan 10
```

```
[LSW2-sep-segment1] protected-instance all  
[LSW2-sep-segment1] quit
```

Configure LSW3.

```
<Quidway> system-view  
[Quidway] sysname LSW3  
[LSW3] sep segment 1  
[LSW3-sep-segment1] control-vlan 10  
[LSW3-sep-segment1] protected-instance all  
[LSW3-sep-segment1] quit
```



NOTE

- The control VLAN must be a VLAN that has not been created or used, and the configuration file automatically displays the command for creating common VLANs.
- Each SEP segment must be configured with a control VLAN. After a port is added to the SEP segment configured with a control VLAN, the port is automatically added to the control VLAN.

2. Add LSW1 to LSW3 to SEP segment 1 and configure port roles.

Configure LSW1.

```
[LSW1] interface gigabitethernet 1/0/1  
[LSW1-GigabitEthernet1/0/1] sep segment 1 edge no-neighbor primary  
[LSW1-GigabitEthernet1/0/1] quit  
[LSW1] interface gigabitethernet 1/0/2  
[LSW1-GigabitEthernet1/0/2] stp disable  
[LSW1-GigabitEthernet1/0/2] sep segment 1  
[LSW1-GigabitEthernet1/0/2] quit
```

Configure LSW2.

```
[LSW2] interface gigabitethernet 1/0/1  
[LSW2-GigabitEthernet1/0/1] sep segment 1 edge no-neighbor secondary  
[LSW2-GigabitEthernet1/0/1] quit  
[LSW2] interface gigabitethernet 1/0/2  
[LSW2-GigabitEthernet1/0/2] stp disable  
[LSW2-GigabitEthernet1/0/2] sep segment 1  
[LSW2-GigabitEthernet1/0/2] quit
```

Configure LSW3.

```
[LSW3] interface gigabitethernet 1/0/1  
[LSW3-GigabitEthernet1/0/1] stp disable  
[LSW3-GigabitEthernet1/0/1] sep segment 1  
[LSW3-GigabitEthernet1/0/1] quit  
[LSW3] interface gigabitethernet 1/0/2  
[LSW3-GigabitEthernet1/0/2] stp disable  
[LSW3-GigabitEthernet1/0/2] sep segment 1  
[LSW3-GigabitEthernet1/0/2] quit
```

3. Specify a port to be blocked.

On LSW1 where the no-neighbor primary edge port in SEP segment 1 resides, specify the port in the middle of the SEP segment as the port to be blocked.

```
[LSW1] sep segment 1  
[LSW1-sep-segment1] block port middle
```

4. Configure the preemption mode.

Configure manual preemption on LSW1.

```
[LSW1-sep-segment1] preempt manual
```

5. Configure the topology change notification function.

```
# Configure SEP segment 1 to notify the MSTP network of topology changes.
# Configure LSW1.
[LSW1-sep-segment1] tc-notify stp
[LSW1-sep-segment1] quit
# Configure LSW2.
[LSW2] sep segment 1
[LSW2-sep-segment1] tc-notify stp
[LSW2-sep-segment1] quit
```

Step 2 Configure basic MSTP functions.

1. Configure an MST region.

```
# Configure PE1.
<Quidway> system-view
[Quidway] sysname PE1
[PE1] stp region-configuration
[PE1-mst-region] region-name RG1
[PE1-mst-region] active region-configuration
[PE1-mst-region] quit
# Configure PE2.
<Quidway> system-view
[Quidway] sysname PE2
[PE2] stp region-configuration
[PE2-mst-region] region-name RG1
[PE2-mst-region] active region-configuration
[PE2-mst-region] quit
# Configure PE3.
<Quidway> system-view
[Quidway] sysname PE3
[PE3] stp region-configuration
[PE3-mst-region] region-name RG1
[PE3-mst-region] active region-configuration
[PE3-mst-region] quit
# Configure PE4.
<Quidway> system-view
[Quidway] sysname PE4
[PE4] stp region-configuration
[PE4-mst-region] region-name RG1
[PE4-mst-region] active region-configuration
[PE4-mst-region] quit
# Configure LSW1.
[LSW1] stp region-configuration
[LSW1-mst-region] region-name RG1
[LSW1-mst-region] active region-configuration
[LSW1-mst-region] quit
# Configure LSW2.
[LSW2] stp region-configuration
[LSW2-mst-region] region-name RG1
[LSW2-mst-region] active region-configuration
[LSW2-mst-region] quit
```

2. Create a VLAN and add ports on the ring network to the VLAN.

On PE1, create VLAN 100 and add GE1/0/1, GE1/0/2, and GE1/0/3 to VLAN 100.

```
[PE1] vlan 100
[PE1-vlan100] quit
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port hybrid tagged vlan 100
[PE1-GigabitEthernet1/0/1] quit
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port hybrid tagged vlan 100
[PE1-GigabitEthernet1/0/2] quit
[PE1] interface gigabitethernet 1/0/3
[PE1-GigabitEthernet1/0/3] port hybrid tagged vlan 100
[PE1-GigabitEthernet1/0/3] quit
```

On PE2, PE3, and PE4, create VLAN 100 and add GE1/0/1, GE1/0/2, and GE1/0/3 to VLAN 100.

The configurations on PE2, PE3, and PE4 are similar to the configuration on PE1. For details about the configurations, see the configuration files.

Create VLAN 100 on LSW1 and LSW2 and add GE1/0/1 to VLAN 100. The configurations on LSW1 and LSW2 are similar to the configuration on PE1. For details about the configurations, see the configuration files.

3. Enable MSTP.

Configure PE1.

```
[PE1] stp enable
```

Configure PE2.

```
[PE2] stp enable
```

Configure PE3.

```
[PE3] stp enable
```

Configure PE4.

```
[PE4] stp enable
```

Configure LSW1.

```
[LSW1] stp enable
```

Configure LSW2.

```
[LSW2] stp enable
```

4. Configure PE3 as the root bridge and PE4 as the backup root bridge.

Set the priority of PE3 to 0 in MSTI 0 to ensure that PE3 functions as the root bridge.

```
[PE3] stp root primary
```

Set the priority of PE4 to 4096 in MSTI 0 to ensure that PE4 functions as the backup root bridge.

```
[PE4] stp root secondary
```

Step 3 Configure the Layer 2 forwarding function on the CE and LSW1 to LSW3.

For details about the configurations, see the configuration files.

Step 4 Verify the configuration.

After the preceding configurations are complete and the network topology becomes stable, perform the following operations to verify the configuration. LSW1 is used as an example.

Run the **shutdown** command on GE1/0/1 of LSW2 to simulate a port fault, and then run the **display sep interface** command on LSW3 to check whether GE1/0/2 on LSW3 has switched from the Discarding state to the Forwarding state.

```
<LSW3> display sep interface gigabitethernet 1/0/2
SEP segment 1
-----
Interface          Port Role   Neighbor Status   Port Status
-----
GE1/0/2            common     up                 forwarding
----End
```

4.4.4 Configuration Files

Configuration file of LSW1

```
#
sysname LSW1
#
vlan batch 10 100
#
stp enable
#
stp region-configuration
 region-name RG1
 active region-configuration
#
sep segment 1
 control-vlan 10
 block port middle
 tc-notify stp
 protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
 port hybrid tagged vlan 10 100
 sep segment 1 edge no-neighbor primary
#
interface GigabitEthernet1/0/2
 port hybrid tagged vlan 10 100
 stp disable
 sep segment 1
#
return
```

Configuration file of LSW2

```
#
sysname LSW2
#
vlan batch 10 100
#
stp enable
#
stp region-configuration
 region-name RG1
```

```
    active region-configuration
#
sep segment 1
    control-vlan 10
    tc-notify stp
    protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
    port hybrid tagged vlan 10 100
    sep segment 1 edge no-neighbor secondary
#
interface GigabitEthernet1/0/2
    port hybrid tagged vlan 10 100
    stp disable
    sep segment 1
#
return
```

Configuration file of LSW2

```
#
sysname LSW3
#
vlan batch 10 100
#
sep segment 1
    control-vlan 10
    protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
    port hybrid tagged vlan 10 100
    stp disable
    sep segment 1
#
interface GigabitEthernet1/0/2
    port hybrid tagged vlan 10 100
    stp disable
    sep segment 1
#
interface GigabitEthernet1/0/3
    port hybrid tagged vlan 10 100
#
return
```

Configuration file of PE1

```
#
sysname PE1
#
vlan batch 100
#
stp enable
#
stp region-configuration
    region-name RG1
    active region-configuration
#
```

```
interface GigabitEthernet1/0/1
  port hybrid tagged vlan 100
#
interface GigabitEthernet1/0/2
  port hybrid tagged vlan 100
#
interface GigabitEthernet1/0/3
  port hybrid tagged vlan 100
#
return
```

Configuration file of PE2

```
#
sysname PE2
#
vlan batch 100
#
stp enable
#
stp region-configuration
  region-name RG1
  active region-configuration
#
interface GigabitEthernet1/0/1
  port hybrid tagged vlan 100
#
interface GigabitEthernet1/0/2
  port hybrid tagged vlan 100
#
interface GigabitEthernet1/0/3
  port hybrid tagged vlan 100
#
return
```

Configuration file of PE3

```
#
sysname PE3
#
vlan batch 100 200
#
stp instance 0 root primary
stp enable
#
stp region-configuration
  region-name RG1
  active region-configuration
#
interface GigabitEthernet1/0/1
  port hybrid tagged vlan 100
#
interface GigabitEthernet1/0/2
  port hybrid tagged vlan 100 200
#
interface GigabitEthernet1/0/3
  port hybrid pvid vlan 200
```

```
port hybrid tagged vlan 100
port hybrid untagged vlan 200
#
return
```

Configuration file of PE4

```
#
sysname PE4
#
vlan batch 100 200
#
stp instance 0 root secondary
stp enable
#
stp region-configuration
region-name RG1
active region-configuration
#
interface GigabitEthernet1/0/1
port hybrid tagged vlan 100
#
interface GigabitEthernet1/0/2
port hybrid tagged vlan 100 200
#
interface GigabitEthernet1/0/3
port hybrid pvid vlan 200
port hybrid tagged vlan 100
port hybrid untagged vlan 200
#
return
```

Configuration file of the CE

```
#
sysname CE
#
vlan batch 100
#
interface GigabitEthernet1/0/1
port hybrid tagged vlan 100
#
return
```

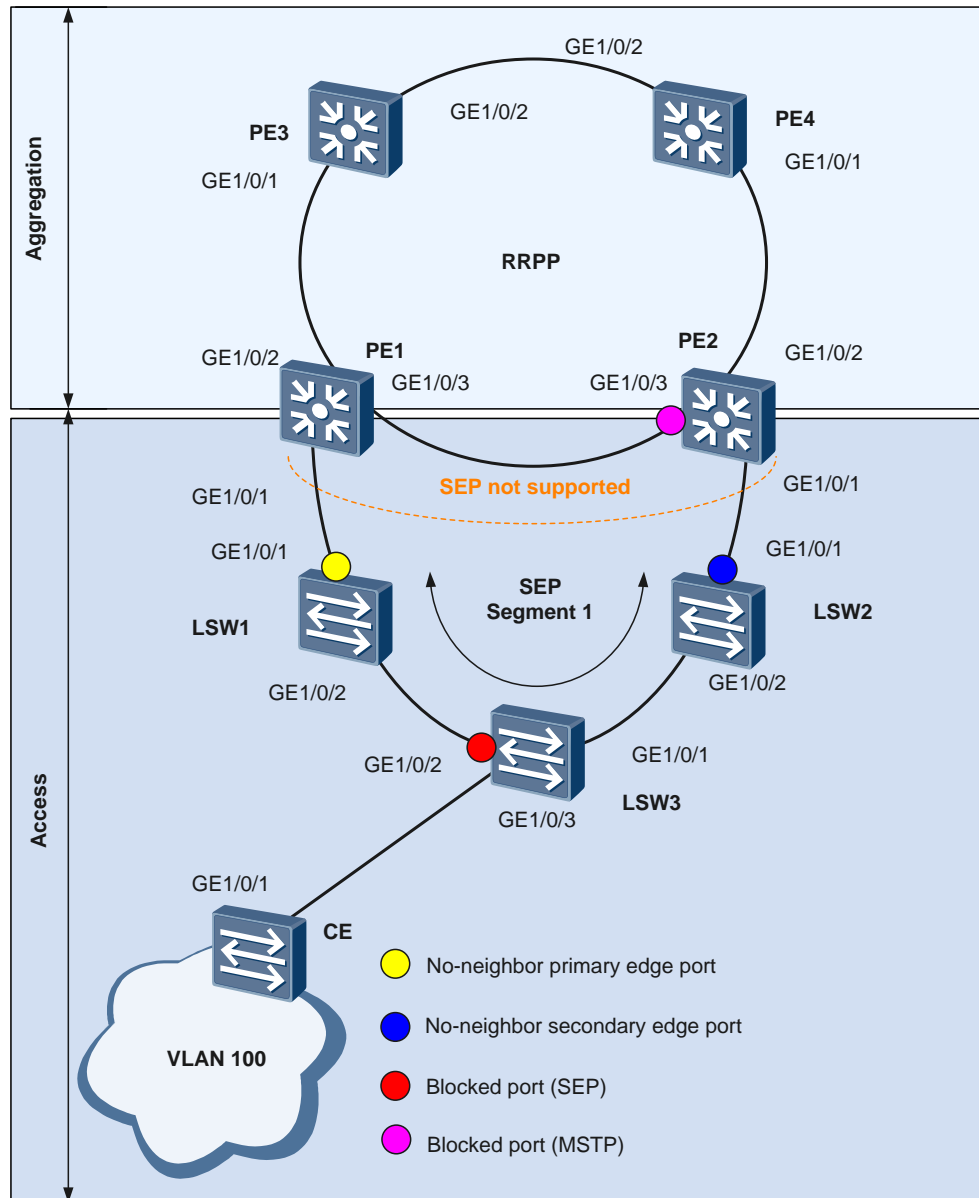
4.5 Example for Configuring a Hybrid SEP+RRPP Network

4.5.1 Networking Requirements

To implement link backup and enhance network reliability, users access an upper-layer network through redundant links. The use of redundant links, however, may produce loops. The loops cause broadcast storms and make the MAC address table unstable. As a result, communication quality deteriorates, and communication services may even be interrupted.

SEP can be deployed on the ring network to eliminate loops and restore communication if a link fails.

Figure 4-5 Hybrid SEP+RRPP networking



As shown in Figure 4-5, multiple Layer 2 switching devices at the access layer and aggregation layer form a ring network to access the core layer. RRPP has been configured at the aggregation layer to eliminate loops. In this case, SEP needs to run at the access layer.

- When no faulty link exists on the ring network, SEP can eliminate loops on the network.
- When a link on the ring network fails, SEP can rapidly restore communication between nodes on the ring network.

- The topology change notification function must be configured on an edge device in a SEP segment. This function enables an upper-layer network to promptly detect topology changes on a lower-layer network.
- After receiving a message indicating a topology change on a lower-layer network, an edge device on the upper-layer network sends TC packets to instruct other devices to delete their original MAC address entries and learn new MAC addresses after the topology of the lower-layer network changes. This ensures uninterrupted traffic forwarding.

4.5.2 Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic SEP functions.
 - Configure SEP segment 1 on PE1, PE2, and LSW1 to LSW3 and configure VLAN 10 as the control VLAN of SEP segment 1.
 - Add PE1, PE2, and LSW1 to LSW3 to SEP segment 1, and configure port roles on the edge devices (PE1 and PE2) of SEP segment 1.
 - Configure the port blocking mode on the device where the primary edge port resides.
 - Configure the preemption mode to ensure that the specified port is blocked when a fault is rectified.
 - Configure the topology change notification function so that the upper-layer network running RRPP can be notified of topology changes in the SEP segment.
2. Configure basic RRPP functions.
 - Add PE1 to PE4 to RRPP domain 1. Create control VLAN 5 on PE1 to PE4, and configure a protected VLAN.
 - Configure PE1 as the master node and PE2 to PE4 as transit nodes on the major ring, and configure the primary and secondary ports on the major ring.
 - Create a VLAN on PE1 to PE4 and add ports on the RRPP ring to the VLAN.
3. Configure the Layer 2 forwarding function on the CE, LSW1 to LSW3, and PE1 to PE4.

4.5.3 Procedure

Step 1 Configure basic SEP functions.

1. Configure SEP segment 1 and configure VLAN 10 as the control VLAN of SEP segment 1.

Configure PE1.

```
<Quidway> system-view
[Quidway] sysname PE1
[PE1] sep segment 1
[PE1-sep-segment1] control-vlan 10
[PE1-sep-segment1] protected-instance all
[PE1-sep-segment1] quit
```

Configure PE2.

```
<Quidway> system-view
[Quidway] sysname PE2
[PE2] sep segment 1
[PE2-sep-segment1] control-vlan 10
[PE2-sep-segment1] protected-instance all
[PE2-sep-segment1] quit
```

Configure LSW1.

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] protected-instance all
[LSW1-sep-segment1] quit
```

Configure LSW2.

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment 1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] protected-instance all
[LSW2-sep-segment1] quit
```

Configure LSW3.

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
[LSW3-sep-segment1] protected-instance all
[LSW3-sep-segment1] quit
```

2. Add PE1, PE2, and LSW1 to LSW3 to SEP segment 1 and configure port roles.



NOTE

If STP is enabled on a port, disable STP on the port before adding the port to a SEP segment.

Configure PE1.

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] stp disable
[PE1-GigabitEthernet1/0/1] sep segment 1 edge primary
[PE1-GigabitEthernet1/0/1] quit
```

Configure LSW1.

```
[LSW1] interface gigabitethernet 1/0/1
[LSW1-GigabitEthernet1/0/1] stp disable
[LSW1-GigabitEthernet1/0/1] sep segment 1
[LSW1-GigabitEthernet1/0/1] quit
[LSW1] interface gigabitethernet 1/0/2
[LSW1-GigabitEthernet1/0/2] stp disable
[LSW1-GigabitEthernet1/0/2] sep segment 1
[LSW1-GigabitEthernet1/0/2] quit
```

Configure LSW2.

```
[LSW2] interface gigabitethernet 1/0/1
[LSW2-GigabitEthernet1/0/1] stp disable
[LSW2-GigabitEthernet1/0/1] sep segment 1
[LSW2-GigabitEthernet1/0/1] quit
[LSW2] interface gigabitethernet 1/0/2
[LSW2-GigabitEthernet1/0/2] stp disable
[LSW2-GigabitEthernet1/0/2] sep segment 1
[LSW2-GigabitEthernet1/0/2] quit
```

Configure LSW3.

```
[LSW3] interface gigabitethernet 1/0/1
[LSW3-GigabitEthernet1/0/1] stp disable
```

```
[LSW3-GigabitEthernet1/0/1] sep segment 1
[LSW3-GigabitEthernet1/0/1] quit
[LSW3] interface gigabitethernet 1/0/2
[LSW3-GigabitEthernet1/0/2] stp disable
[LSW3-GigabitEthernet1/0/2] sep segment 1
[LSW3-GigabitEthernet1/0/2] quit
```

Configure PE2.

```
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] stp disable
[PE2-GigabitEthernet1/0/1] sep segment 1 edge secondary
[PE2-GigabitEthernet1/0/1] quit
```

After the preceding configurations are complete, run the **display sep topology** command on PE1 to check the topology of SEP segment 1. The command output shows that the blocked port is one of the last two ports that complete neighbor negotiations.

```
[PE1] display sep topology
SEP segment 1
-----
System Name          Port Name          Port Role          Port Status
-----
PE1                   GE1/0/1            primary            forwarding
LSW1                   GE1/0/1            common             forwarding
LSW1                   GE1/0/2            common             forwarding
LSW3                   GE1/0/2            common             forwarding
LSW3                   GE1/0/1            common             forwarding
LSW2                   GE1/0/2            common             forwarding
LSW2                   GE1/0/1            common             forwarding
PE2                   GE1/0/1            secondary          discarding
```

3. Specify a port to be blocked.

On PE1 where the primary edge port in SEP segment 1 resides, specify the port in the middle of the SEP segment as the port to be blocked.

```
[PE1] sep segment 1
[PE1-sep-segment1] block port middle
```

4. Configure the preemption mode.

Configure manual preemption on PE1.

```
[PE1-sep-segment1] preempt manual
```

5. Configure the topology change notification function.

Configure SEP segment 1 to notify the RRPP network of topology changes.

Configure PE1.

```
[PE1-sep-segment1] tc-notify rrpp
[PE1-sep-segment1] quit
```

Configure PE2.

```
[PE2] sep segment 1
[PE2-sep-segment1] tc-notify rrpp
[PE2-sep-segment1] quit
```

6. Perform the following operations to verify the configuration. PE1 is used as an example. Run the **display sep topology** command on PE1 to view the topology of SEP segment 1. The command output shows that GE1/0/2 on LSW3 is in Discarding state, and the other ports are in Forwarding state.

```
[PE1] display sep topology
```



```
SEP segment 1
-----
```

System Name	Port Name	Port Role	Port Status
PE1	GE1/0/1	primary	forwarding
LSW1	GE1/0/1	common	forwarding
LSW1	GE1/0/2	common	forwarding
LSW3	GE1/0/2	common	discarding
LSW3	GE1/0/1	common	forwarding
LSW2	GE1/0/2	common	forwarding
LSW2	GE1/0/1	common	forwarding
PE2	GE1/0/1	secondary	forwarding

Run the **display sep interface verbose** command on PE1 to view detailed information about the ports in the SEP segment.

```
[PE1] display sep interface verbose
SEP segment 1
Control-vlan          :10
Preempt Delay Timer   :0
TC-Notify Propagate to :rrpp
-----
Interface              :GE1/0/1
Port Role               :Config = primary / Active = primary
Port Priority          :64
Port Status            :forwarding
Neighbor Status        :up
Neighbor Port          :LSW1 - GE1/0/1 (00e0-0829-7c00.0000)
NBR TLV                rx :2124          tx :2126
LSP INFO TLV          rx :2939          tx :135
LSP ACK TLV           rx :113           tx :768
PREEMPT REQ TLV       rx :0            tx :3
PREEMPT ACK TLV       rx :3            tx :0
TC Notify              rx :5            tx :3
EPA                    rx :363          tx :397
```

Step 2 Configure basic RRPP functions.

1. Add PE1 to PE4 to RRPP domain 1. Create control VLAN 5 on PE1 to PE4, and configure a protected VLAN.

Configure PE1.

```
[PE1] stp region-configuration
[PE1-mst-region] instance 1 vlan 5 6 100
[PE1-mst-region] active region-configuration
[PE1-mst-region] quit
[PE1] rrpp domain 1
[PE1-rrpp-domain-region1] control-vlan 5
[PE1-rrpp-domain-region1] protected-vlan reference-instance 1
```

Configure PE2.

```
[PE2] stp region-configuration
[PE2-mst-region] instance 1 vlan 5 6 100
[PE2-mst-region] active region-configuration
[PE2-mst-region] quit
[PE2] rrpp domain 1
[PE2-rrpp-domain-region1] control-vlan 5
[PE2-rrpp-domain-region1] protected-vlan reference-instance 1
```

Configure PE3.

```
[PE3] stp region-configuration
[PE3-mst-region] instance 1 vlan 5 6 100
[PE3-mst-region] active region-configuration
[PE3-mst-region] quit
[PE3] rrpp domain 1
[PE3-rrpp-domain-region1] control-vlan 5
[PE3-rrpp-domain-region1] protected-vlan reference-instance 1
```

Configure PE4.

```
[PE4] stp region-configuration
[PE4-mst-region] instance 1 vlan 5 6 100
[PE4-mst-region] active region-configuration
[PE4-mst-region] quit
[PE4] rrpp domain 1
[PE4-rrpp-domain-region1] control-vlan 5
[PE4-rrpp-domain-region1] protected-vlan reference-instance 1
```

2. Create a VLAN and add ports on the ring network to the VLAN.

On PE1, create VLAN 100 and add GE1/0/1, GE1/0/2, and GE1/0/3 to VLAN 100.

```
[PE1] vlan 100
[PE1-vlan100] quit
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] stp disable
[PE1-GigabitEthernet1/0/1] port link-type trunk
[PE1-GigabitEthernet1/0/1] port trunk allow-pass vlan 100
[PE1-GigabitEthernet1/0/1] quit
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] stp disable
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk allow-pass vlan 100
[PE1-GigabitEthernet1/0/2] quit
[PE1] interface gigabitethernet 1/0/3
[PE1-GigabitEthernet1/0/3] stp disable
[PE1-GigabitEthernet1/0/3] port link-type trunk
[PE1-GigabitEthernet1/0/3] port trunk allow-pass vlan 100
[PE1-GigabitEthernet1/0/3] quit
```

On PE2, create VLAN 100 and add GE1/0/1, GE1/0/2, and GE1/0/3 to VLAN 100.

```
[PE2] vlan 100
[PE2-vlan100] quit
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] stp disable
[PE2-GigabitEthernet1/0/1] port link-type trunk
[PE2-GigabitEthernet1/0/1] port trunk allow-pass vlan 100
[PE2-GigabitEthernet1/0/1] quit
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] stp disable
[PE2-GigabitEthernet1/0/2] port link-type trunk
[PE2-GigabitEthernet1/0/2] port trunk allow-pass vlan 100
[PE2-GigabitEthernet1/0/2] quit
[PE2] interface gigabitethernet 1/0/3
[PE2-GigabitEthernet1/0/3] stp disable
[PE2-GigabitEthernet1/0/3] port link-type trunk
[PE2-GigabitEthernet1/0/3] port trunk allow-pass vlan 100
[PE2-GigabitEthernet1/0/3] quit
```

On PE3, create VLAN 100 and add GE1/0/1 and GE1/0/2 to VLAN 100.

```
[PE3] vlan 100
[PE3-vlan100] quit
[PE3] interface gigabitethernet 1/0/1
[PE3-GigabitEthernet1/0/1] stp disable
[PE3-GigabitEthernet1/0/1] port link-type trunk
[PE3-GigabitEthernet1/0/1] port trunk allow-pass vlan 100
[PE3-GigabitEthernet1/0/1] quit
[PE3] interface gigabitethernet 1/0/2
[PE3-GigabitEthernet1/0/2] stp disable
[PE3-GigabitEthernet1/0/2] port link-type trunk
[PE3-GigabitEthernet1/0/2] port trunk allow-pass vlan 100
[PE3-GigabitEthernet1/0/2] quit
```

On PE4, create VLAN 100 and add GE1/0/1 and GE1/0/2 to VLAN 100.

```
[PE4] vlan 100
[PE4-vlan100] quit
[PE4] interface gigabitethernet 1/0/1
[PE4-GigabitEthernet1/0/1] stp disable
[PE4-GigabitEthernet1/0/1] port link-type trunk
[PE4-GigabitEthernet1/0/1] port trunk allow-pass vlan 100
[PE4-GigabitEthernet1/0/1] quit
[PE4] interface gigabitethernet 1/0/2
[PE4-GigabitEthernet1/0/2] stp disable
[PE4-GigabitEthernet1/0/2] port link-type trunk
[PE4-GigabitEthernet1/0/2] port trunk allow-pass vlan 100
[PE4-GigabitEthernet1/0/2] quit
```

3. Configure PE1 as the master node and PE2 to PE4 as transit nodes on the major ring, and configure the primary and secondary ports on the major ring.

Configure PE1.

```
[PE1] rrpp domain 1
[PE1-rrpp-domain-region1] ring 1 node-mode master primary-port
gigabitethernet1/0/2 secondary-port gigabitethernet1/0/3 level 0
[PE1-rrpp-domain-region1] ring 1 enable
```

Configure PE2.

```
[PE2] rrpp domain 1
[PE2-rrpp-domain-region1] ring 1 node-mode transit primary-port
gigabitethernet1/0/2 secondary-port gigabitethernet1/0/3 level 0
[PE2-rrpp-domain-region1] ring 1 enable
```

Configure PE3.

```
[PE3] rrpp domain 1
[PE3-rrpp-domain-region1] ring 1 node-mode transit primary-port
gigabitethernet1/0/1 secondary-port gigabitethernet1/0/2 level 0
[PE3-rrpp-domain-region1] ring 1 enable
```

Configure PE4.

```
[PE4] rrpp domain 1
[PE4-rrpp-domain-region1] ring 1 node-mode transit primary-port
gigabitethernet1/0/1 secondary-port gigabitethernet1/0/2 level 0
[PE4-rrpp-domain-region1] ring 1 enable
```

4. Enable RRPP.

Configure PE1.

```
[PE1] rrpp enable
# Configure PE2.
[PE2] rrpp enable
# Configure PE3.
[PE3] rrpp enable
# Configure PE4.
[PE4] rrpp enable
```

5. After the preceding configurations are complete, run the **display rrpp brief** or **display rrpp verbose domain** command on PE1 to check the RRPP configuration.

```
[PE1] display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Enable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 0 sec (0 sec default)
Number of RRPP Domains: 1

Domain Index   : 1
Control VLAN   : major 5   sub 6
Protected VLAN : Reference Instance 1
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   GigabitEthernet1/0/2  GigabitEthernet1/0/3  Yes
```

The command output shows that RRPP is enabled on PE1. In RRPP domain 1, VLAN 5 is the major control VLAN, VLAN 6 is the sub-control VLAN, Instance 1 is the protected VLAN, and PE1 is the master node in major ring 1, and the primary and secondary ports are GE1/0/2 and GE1/0/3 on PE1 respectively.

```
[PE1] display rrpp verbose domain 1
Domain Index   : 1
Control VLAN   : major 5   sub 6
Protected VLAN : Reference Instance 1
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Complete
Is Enabled     : Enable
Primary port   : GigabitEthernet1/0/2      Port status: UP
Secondary port : GigabitEthernet1/0/3      Port status: BLOCKED
Is Active: Yes
```

The command output shows that in RRPP domain 1, the major control VLAN is VLAN 5, the sub-control VLAN is VLAN 6, and the protected VLAN is Instance 1. In RRPP domain 1, PE1 is the major node in Complete state, and the primary and secondary ports are GE1/0/2 and GE1/0/3 on PE1 respectively.

Step 3 Configure the Layer 2 forwarding function on the CE, LSW1 to LSW3, and PE1 to PE4.

For details about the configurations, see the configuration files.

Step 4 Verify the configuration.

After the preceding configurations are complete and the network topology becomes stable, perform the following operations to verify the configuration. LSW1 is used as an example.

Run the **shutdown** command on GE1/0/1 of LSW2 to simulate a port fault, and then run the **display sep interface** command on LSW3 to check whether GE1/0/2 on LSW3 has switched from the Discarding state to the Forwarding state.

```
[LSW3] display sep interface gigabitethernet 1/0/2
SEP segment 1
-----
Interface          Port Role   Neighbor Status   Port Status
-----
GE1/0/2            common     up                 forwarding
----End
```

4.5.4 Configuration Files

Configuration file of LSW1

```
#
 sysname LSW1
#
 vlan batch 10 100
#
 sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
 interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100
 stp disable
 sep segment 1
#
 interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 10 100
 stp disable
 sep segment 1
#
 return
```

Configuration file of LSW2

```
#
 sysname LSW2
#
 vlan batch 10 100
#
 sep segment 1
 control-vlan 10
 protected-instance 0 to 48
#
 interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 100
```

```
    stp disable
    sep segment 1
#
interface GigabitEthernet1/0/2
    port link-type trunk
    port trunk allow-pass vlan 10 100
    stp disable
    sep segment 1
#
return
```

Configuration file of LSW2

```
#
sysname LSW3
#
vlan batch 10 100
#
sep segment 1
    control-vlan 10
    protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk allow-pass vlan 10 100
    stp disable
    sep segment 1
#
interface GigabitEthernet1/0/2
    port link-type trunk
    port trunk allow-pass vlan 10 100
    stp disable
    sep segment 1
#
interface GigabitEthernet1/0/3
    port link-type trunk
    port trunk allow-pass vlan 100
#
return
```

Configuration file of PE1

```
#
sysname PE1
#
vlan batch 5 to 6 10 100
#
rrpp enable
#
stp region-configuration
    instance 1 vlan 5 to 6 100
    active region-configuration
#
rrpp domain 1
    control-vlan 5
    protected-vlan reference-instance 1
```

```
ring 1 node-mode master primary-port GigabitEthernet 1/0/2 secondary-port
GigabitEthernet 1/0/3 level 0
ring 1 enable
#
sep segment 1
control-vlan 10
block port middle
tc-notify rrpp
protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk allow-pass vlan 10 100
stp disable
sep segment 1 edge primary
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk allow-pass vlan 5 to 6 100
stp disable
#
interface GigabitEthernet1/0/3
port link-type trunk
port trunk allow-pass vlan 5 to 6 100
stp disable
#
return
```

Configuration file of PE2

```
#
sysname PE2
#
vlan batch 5 to 6 10 100
#
rrpp enable
#
stp region-configuration
instance 1 vlan 5 to 6 100
active region-configuration
#
rrpp domain 1
control-vlan 5
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet 1/0/2 secondary-port
GigabitEthernet 1/0/3 level 0
ring 1 enable
#
sep segment 1
control-vlan 10
tc-notify rrpp
protected-instance 0 to 48
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk allow-pass vlan 10 100
```

```
    stp disable
    sep segment 1 edge secondary
#
interface GigabitEthernet1/0/2
    port link-type trunk
    port trunk allow-pass vlan 5 to 6 100
    stp disable
#
interface GigabitEthernet1/0/3
    port link-type trunk
    port trunk allow-pass vlan 5 to 6 100
    stp disable
#
return
```

Configuration file of PE3

```
#
sysname PE3
#
vlan batch 5 to 6 100 200
#
rrpp enable
#
stp region-configuration
    instance 1 vlan 5 to 6 100
    active region-configuration
#
rrpp domain 1
    control-vlan 5
    protected-vlan reference-instance 1
    ring 1 node-mode transit primary-port GigabitEthernet 1/0/1 secondary-port
GigabitEthernet 1/0/2 level 0
    ring 1 enable
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk allow-pass vlan 100
    stp disable
#
interface GigabitEthernet1/0/2
    port link-type trunk
    port trunk allow-pass vlan 5 to 6 100 200
    stp disable
#
interface GigabitEthernet1/0/3
    port default vlan 200
    port trunk allow-pass vlan 5 to 6 100
#
return
```

Configuration file of PE4

```
#
sysname PE4
#
vlan batch 5 to 6 100 200
```



```
#
  rrpp enable
#
  stp region-configuration
    instance 1 vlan 5 to 6 100
  active region-configuration
#
rrpp domain 1
  control-vlan 5
  protected-vlan reference-instance 1
  ring 1 node-mode transit primary-port GigabitEthernet 1/0/1 secondary-port
GigabitEthernet 1/0/2 level 0
  ring 1 enable
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk allow-pass vlan 100
  stp disable
#
interface GigabitEthernet1/0/2
  port link-type trunk
  port trunk allow-pass vlan 5 to 6 100 200
  stp disable
#
interface GigabitEthernet1/0/3
  port default vlan 200
  port trunk allow-pass vlan 5 to 6 100
#
return
```

Configuration file of CE1

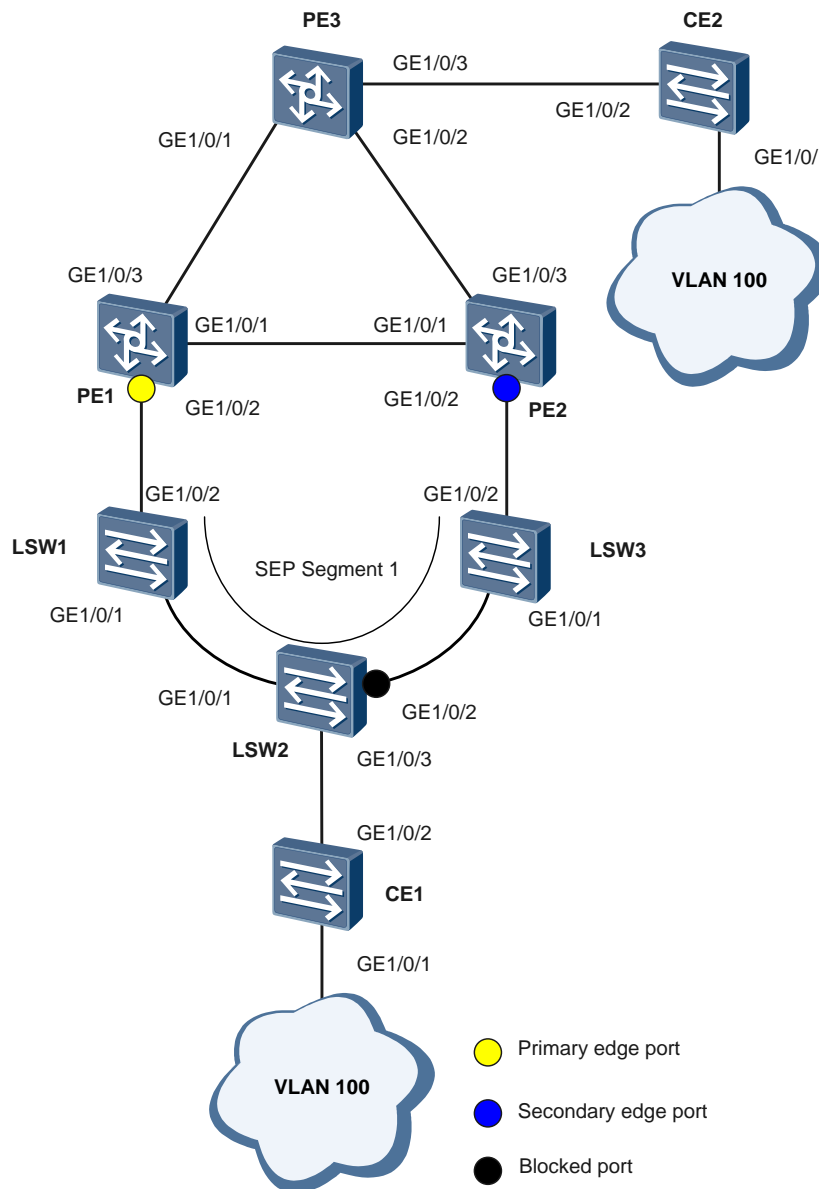
```
#
  sysname CE1
#
  vlan batch 100
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk allow-pass vlan 100
#
return
```

4.6 Example for Configuring Association Between SEP and VPLS

4.6.1 Networking Requirements

As shown in Figure 4-6, CE1 is connected to a virtual private LAN segment (VPLS) network through an open ring network. SEP is enabled on the open ring network to eliminate redundant links. When a link on the ring network fails, SEP can rapidly restore communication between nodes on the ring network. The traffic between CEs, however, is still interrupted.

Figure 4-6 Association between SEP and VPLS



To solve the problem, association between SEP and VPLS must be enabled on PE1 and PE2. With association between SEP and VPLS, PE1 and PE2 can detect topology changes on the SEP network immediately after a fault occurs on the SEP network. This ensures reliable traffic transmission.

Table 4-1 Mapping between ports on devices and VLANIF interfaces

Device	Interface	VLANIF Interface	IP Address
PE1	GE1/0/1	VLANIF 20	10.1.1.1/30
	GE1/0/2	VLANIF 100	-
	GE1/0/3	VLANIF 30	20.1.1.1/30

Device	Interface	VLANIF Interface	IP Address
	Loopback1	-	1.1.1.9/32
PE2	GE1/0/1	VLANIF 20	10.1.1.2/30
	GE1/0/2	VLANIF 100	-
	GE1/0/3	VLANIF 40	30.1.1.1/30
	Loopback1	-	2.2.2.9/32
PE3	GE1/0/1	VLANIF 30	20.1.1.2/30
	GE1/0/2	VLANIF 40	30.1.1.2/30
	GE1/0/3	VLANIF 100	-
	Loopback1	-	3.3.3.9/32

4.6.2 Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic SEP functions.
 - Create a SEP segment and a control VLAN.
 - Add all the devices on the ring network to the SEP segment and configure port roles.



NOTE

When being added to multiple SEP segments, a port must be configured with the same role; otherwise, SEP multi-instance fails to be configured.

- Configure the port blocking mode on the device where the primary edge port resides.
 - Configure the preemption mode to ensure that the specified port is blocked when a fault is rectified.
2. Configure VPLS on PE1 to PE3.
 3. Configure association between SEP and VPLS so that VPLS can detect a fault on the SEP network and trigger forwarding path update.
 4. Configure the Layer 2 forwarding function on CE1, CE2, LSW1 to LSW3, and PE1 to PE3.

4.6.3 Procedure

Step 1 Configure basic SEP functions.

1. Create a SEP segment and a control VLAN.

Configure PE1.

```
<Quidway> system-view
[Quidway] sysname PE1
[PE1] sep segment 1
[PE1-sep-segment1] control-vlan 10
[PE1-sep-segment1] protected-instance all
[PE1-sep-segment1] quit
```

Configure LSW1.

```
<Quidway> system-view
[Quidway] sysname LSW1
[LSW1] sep segment 1
[LSW1-sep-segment1] control-vlan 10
[LSW1-sep-segment1] protected-instance all
[LSW1-sep-segment1] quit
```

Configure LSW2.

```
<Quidway> system-view
[Quidway] sysname LSW2
[LSW2] sep segment1
[LSW2-sep-segment1] control-vlan 10
[LSW2-sep-segment1] protected-instance all
[LSW2-sep-segment1] quit
```

Configure LSW3.

```
<Quidway> system-view
[Quidway] sysname LSW3
[LSW3] sep segment 1
[LSW3-sep-segment1] control-vlan 10
[LSW3-sep-segment1] protected-instance all
[LSW3-sep-segment1] quit
```

Configure PE2.

```
<Quidway> system-view
[Quidway] sysname PE2
[PE2] sep segment 1
[PE2-sep-segment1] control-vlan 10
[PE2-sep-segment1] protected-instance all
[PE2-sep-segment1] quit
```



NOTE

- The control VLAN must be a VLAN that has not been created or used, and the configuration file automatically displays the command for creating common VLANs.
- Each SEP segment must be configured with a control VLAN. After a port is added to the SEP segment configured with a control VLAN, the port is automatically added to the control VLAN. If the port type is Trunk, the configuration file automatically displays the **port trunk allow-pass vlan** command in the view of the port added to the SEP segment. If the port type is Hybrid, the configuration file automatically displays the **port hybrid tagged vlan** command in the view of the port added to the SEP segment.

2. Add all the devices on the ring network to SEP segment 1 and configure port roles according to Figure 4-6.

Configure GE1/0/2 on PE1 as the primary edge port, GE1/0/2 on PE2 as the secondary edge port, and other ports as common ports.

Configure PE1.

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] stp disable
[PE1-GigabitEthernet1/0/2] sep segment 1 edge primary
[PE1-GigabitEthernet1/0/2] quit
```

Configure PE2.

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] stp disable
[PE2-GigabitEthernet1/0/2] sep segment 1 edge secondary
[PE2-GigabitEthernet1/0/2] quit
```

Configure LSW1.

```
[LSW1] interface gigabitethernet 1/0/1
[LSW1-GigabitEthernet1/0/1] stp disable
[LSW1-GigabitEthernet1/0/1] sep segment 1
[LSW1-GigabitEthernet1/0/1] quit
[LSW1] interface gigabitethernet 1/0/2
[LSW1-GigabitEthernet1/0/2] stp disable
[LSW1-GigabitEthernet1/0/2] sep segment 1
[LSW1-GigabitEthernet1/0/2] quit
```

Configure LSW2.

```
[LSW2] interface gigabitethernet 1/0/1
[LSW2-GigabitEthernet1/0/1] stp disable
[LSW2-GigabitEthernet1/0/1] sep segment 1
[LSW2-GigabitEthernet1/0/1] quit
[LSW2] interface gigabitethernet 1/0/2
[LSW2-GigabitEthernet1/0/2] stp disable
[LSW2-GigabitEthernet1/0/2] sep segment 1
[LSW2-GigabitEthernet1/0/2] quit
```

Configure LSW3.

```
[LSW3] interface gigabitethernet 1/0/1
[LSW3-GigabitEthernet1/0/1] stp disable
[LSW3-GigabitEthernet1/0/1] sep segment 1
[LSW3-GigabitEthernet1/0/1] quit
[LSW3] interface gigabitethernet 1/0/2
[LSW3-GigabitEthernet1/0/2] stp disable
[LSW3-GigabitEthernet1/0/2] sep segment 1
[LSW3-GigabitEthernet1/0/2] quit
```

After the preceding configurations are complete, run the **display sep topology** command on PE1 to check the topology of SEP segment 1. The command output shows that the blocked port is one of the last two ports that complete neighbor negotiations.

```
[PE1] display sep topology
SEP segment 1
```

System Name	Port Name	Port Role	Port Status
PE1	GE1/0/2	primary	forwarding
LSW1	GE1/0/2	common	forwarding
LSW1	GE1/0/1	common	forwarding
LSW2	GE1/0/1	common	forwarding
LSW2	GE1/0/2	common	forwarding
LSW3	GE1/0/1	common	forwarding
LSW3	GE1/0/2	common	forwarding
PE2	GE1/0/2	secondary	discarding

3. Specify a port to be blocked.

Configure the port blocking mode.

On PE1 where the primary edge port of SEP segment 1 resides, specify the port with the highest priority to be blocked.

```
[PE1] sep segment 1
[PE1]-sep-segment1] block port optimal
```

Set the priority of GE1/0/2 on LSW2 to 128. Retain the default priority for the other ports in SEP segment 1.

```
[LSW2] interface gigabitethernet 1/0/2
```

```
[LSW2-GigabitEthernet1/0/2] sep segment 1 priority 128
[LSW2-GigabitEthernet1/0/2] quit
```

Configure the preemption mode.

Configure delayed preemption on PE1 where the primary edge port resides.

```
[PE1-sep-segment1] preempt delay 600
[PE1-sep-segment1] quit
```



NOTE

- You must set the preemption delay when delayed preemption is used because no default preemption delay time is available.
- After all the faulty ports recover, the edge ports no longer receive fault notification packets. If the primary edge port does not receive any fault notification packet within 3 seconds, the port starts the delay timer. After the delay timer expires, nodes in the SEP segment start blocked port preemption.

4. After the preceding configurations are complete, check the topology of the SEP segment. PE1 is used as an example.

Run the **display sep topology** command on PE1 to view the topology of SEP segment 1.

```
[PE1] display sep topology
SEP segment 1
```

System Name	Port Name	Port Role	Port Status
PE1	GE1/0/2	primary	forwarding
LSW1	GE1/0/2	common	forwarding
LSW1	GE1/0/1	common	forwarding
LSW2	GE1/0/1	common	forwarding
LSW2	GE1/0/2	common	discarding
LSW3	GE1/0/1	common	forwarding
LSW3	GE1/0/2	common	forwarding
PE2	GE1/0/2	secondary	forwarding

The command output shows that GE1/0/2 on LSW2 is in Discarding state, and the other ports are in Forwarding state.

Step 2 Configure VPLS.

1. Configure an IP address for each port, and configure an Interior Gateway Protocol (IGP) on the VPLS backbone network to connect PEs. In this example, Intermediate System to Intermediate System (IS-IS) is used as an IGP.

Configure VPLS connections between the PEs. Configure the VPLS connections using the LDP signaling and set the virtual switching instance (VSI) name to **ldp1**. For details about the configurations, see the configuration files.

After the preceding configurations are complete, the PEs can ping each other successfully.

```
[PE3] ping 10.1.1.1
PING 10.1.1.1: 56 data bytes, press CTRL_C to break
  Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=255 time=80 ms
  Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=255 time=100 ms
  Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=255 time=80 ms
  Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=255 time=130 ms
  Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=255 time=80 ms

--- 10.1.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
```

```
round-trip min/avg/max = 80/94/130 ms
[PE1] ping 2.2.2.9
PING 2.2.2.9: 56 data bytes, press CTRL_C to break
Reply from 2.2.2.9: bytes=56 Sequence=1 ttl=255 time=140 ms
Reply from 2.2.2.9: bytes=56 Sequence=2 ttl=255 time=100 ms
Reply from 2.2.2.9: bytes=56 Sequence=3 ttl=255 time=110 ms
Reply from 2.2.2.9: bytes=56 Sequence=4 ttl=255 time=90 ms
Reply from 2.2.2.9: bytes=56 Sequence=5 ttl=255 time=60 ms

--- 2.2.2.9 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 60/100/140 ms
```

2. Bind VLANIF interfaces to VSIs on PEs.

Configure PE1.

```
[PE1] vlan 100
[PE1-vlan100] quit
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port hybrid tagged vlan 100
[PE1-GigabitEthernet1/0/2] quit
[PE1] interface Vlanif 100
[PE1-Vlanif100] l2 binding vsi ldp1
[PE1-Vlanif100] quit
```

Configure PE2.

```
[PE2] vlan 100
[PE2-vlan100] quit
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port hybrid tagged vlan 100
[PE2-GigabitEthernet1/0/2] quit
[PE2] interface Vlanif 100
[PE2-Vlanif100] l2 binding vsi ldp1
[PE2-Vlanif100] quit
```

Configure PE3.

```
[PE3] vlan 100
[PE3-vlan100] quit
[PE3] interface Vlanif 100
[PE3-Vlanif100] l2 binding vsi ldp1
[PE3-Vlanif100] quit
```

After the preceding configurations are complete, run the **display vsi name ldp1 verbose** command on PE1. The command output shows that VSI **ldp1** has established pseudo wires (PWs) to PE2 and PE3, and the status of the VSI is Up.

```
[PE1] display vsi name ldp1 verbose
***VSI Name          : ldp1
Administrator VSI    : no
Isolate Spoken       : disable
VSI Index            : 0
PW Signaling         : ldp
Member Discovery Style : static
PW MAC Learn Style   : unqualify
Encapsulation Type   : vlan
MTU                  : 1500
```

```
Diffserv Mode      : uniform
Mpls Exp           : --
DomainId           : 255
Domain Name        :
Ignore AcState     : disable
P2P VSI           : disable
Create Time        : 0 days, 0 hours, 13 minutes, 7 seconds
VSI State          : up

VSI ID             : 1
*Peer Router ID   : 2.2.2.9
primary or secondary : primary
ignore-standby-state : no
VC Label           : 1026
Peer Type          : dynamic
Session            : up
Tunnel ID          : 0x5
Broadcast Tunnel ID : 0x5
Broad BackupTunnel ID : 0x0
CKey               : 2
NKey               : 1
StpEnable          : 0
PwIndex            : 0
*Peer Router ID   : 3.3.3.9
primary or secondary : primary
ignore-standby-state : no
VC Label           : 1027
Peer Type          : dynamic
Session            : up
Tunnel ID          : 0x6
Broadcast Tunnel ID : 0x6
Broad BackupTunnel ID : 0x0
CKey               : 4
NKey               : 3
StpEnable          : 0
PwIndex            : 0

Interface Name     : Vlanif100
State              : up
Access Port        : false
Last Up Time       : 2010/07/05 19:59:31
Total Up Time      : 0 days, 0 hours, 10 minutes, 45 seconds

**PW Information:

*Peer Ip Address   : 2.2.2.9
PW State           : up
Local VC Label     : 1026
Remote VC Label    : 1026
PW Type            : label
Tunnel ID          : 0x5
Broadcast Tunnel ID : 0x5
Broad BackupTunnel ID : 0x0
Ckey               : 0x2
Nkey               : 0x1
```



```

Main PW Token      : 0x5
Slave PW Token     : 0x0
Tnl Type           : LSP
OutInterface       : Vlanif20
Backup OutInterface :
Stp Enable         : 0
PW Last Up Time    : 2010/07/05 20:00:21
PW Total Up Time   : 0 days, 0 hours, 9 minutes, 55 seconds
*Peer Ip Address   : 3.3.3.9
PW State           : up
Local VC Label     : 1027
Remote VC Label    : 1026
PW Type            : label
Tunnel ID          : 0x6
Broadcast Tunnel ID : 0x6
Broad BackupTunnel ID : 0x0
Ckey               : 0x4
Nkey               : 0x3
Main PW Token      : 0x6
Slave PW Token     : 0x0
Tnl Type           : LSP
OutInterface       : Vlanif30
Backup OutInterface :
Stp Enable         : 0
PW Last Up Time    : 2010/07/05 20:09:01
PW Total Up Time   : 0 days, 0 hours, 1 minutes, 15 seconds

```

Step 3 Configure association between SEP and VPLS.

Configure PE1.

```

[PE1] sep segment 1
[PE1]-sep-segment1] tc-notify vpls
[PE1]-sep-segment1] quit

```

Configure PE2.

```

[PE2] sep segment 1
[PE2]-sep-segment1] tc-notify vpls
[PE2]-sep-segment1] quit

```

Step 4 Configure the Layer 2 forwarding function on CE1, CE2, and LSW1 to LSW3.

For details about the configurations, see the configuration files.

Step 5 Verify the configuration.

Simulate a fault, and then check whether the status of the blocked port changes from the Discarding state to the Forwarding state.

Run the **shutdown** command on GE1/0/1 of LSW2 to simulate a port fault.

Run the **display sep interface** command on LSW2 to check whether the status of GE1/0/2 in SEP segment 1 has changed from the Discarding state to the Forwarding state.

```

[LSW2] display sep interface GigabitEthernet 1/0/2
SEP segment 1
-----
Interface      Port Role   Neighbor Status   Port Status

```

GE1/0/2 common up forwarding

CEs can still ping each other successfully.

----End

4.6.4 Configuration Files

Configuration file of PE1

```
#
 sysname PE1
#
 vlan batch 10 20 30 100
#
 sep segment 1
 control-vlan 10
 block port optimal
 preempt delay 600
 tc-notify vpls
 protected-instance 0 to 4094
#
 mpls lsr-id 1.1.1.9
 mpls
#
 mpls l2vpn
#
 vsi ldp1 static
 pwsignal ldp
 vsi-id 1
 peer 2.2.2.9
 peer 3.3.3.9
#
 mpls ldp
#
 isis 1
 is-level level-2
 network-entity 49.0010.0100.1009.00
#
 interface Vlanif20
 ip address 10.1.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls ldp
#
 interface Vlanif30
 ip address 20.1.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls ldp
#
 interface Vlanif100
 l2 binding vsi ldp1
#
 interface GigabitEthernet1/0/1
```

```
port hybrid tagged vlan 20
#
interface GigabitEthernet1/0/2
port hybrid tagged vlan 10 100
stp disable
sep segment 1 edge primary
#
interface GigabitEthernet1/0/3
port hybrid tagged vlan 30
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
isis enable 1
#
return
```

Configuration file of PE2

```
#
sysname PE2
#
vlan batch 10 20 40 100
#
sep segment 1
control-vlan 10
tc-notify vpls
protected-instance 0 to 4094
#
mpls lsr-id 2.2.2.9
mpls
#
mpls l2vpn
#
vsi ldpl static
pwsignal ldp
vsi-id 1
peer 1.1.1.9
peer 3.3.3.9
#
mpls ldp
#
isis 1
is-level level-2
network-entity 49.0020.0200.2009.00
#
interface Vlanif20
ip address 10.1.1.2 255.255.255.252
isis enable 1
mpls
mpls ldp
#
interface Vlanif40
ip address 30.1.1.1 255.255.255.252
isis enable 1
mpls
mpls ldp
```

```
#
interface Vlanif100
  l2 binding vsi ldp1
#
interface GigabitEthernet1/0/1
  port hybrid tagged vlan 20
#
interface GigabitEthernet1/0/2
  port hybrid tagged vlan 10 100
  stp disable
  sep segment 1 edge primary
#
interface GigabitEthernet1/0/3
  port hybrid tagged vlan 40
#
interface LoopBack1
  ip address 2.2.2.9 255.255.255.255
  isis enable 1
#
return
```

Configuration file of PE3

```
#
sysname PE3
#
vlan batch 30 40 100
#
mpls lsr-id 3.3.3.9
mpls
#
mpls l2vpn
#
vsi ldp1 static
  pwsignal ldp
  vsi-id 1
  peer 1.1.1.9
  peer 2.2.2.9
#
mpls ldp
#
isis 1
  is-level level-2
  network-entity 49.0030.0300.3009.00
#
interface Vlanif30
  ip address 20.1.1.2 255.255.255.252
  isis enable 1
  mpls
  mpls ldp
#
interface Vlanif40
  ip address 30.1.1.2 255.255.255.252
  isis enable 1
  mpls
  mpls ldp
```

```
#
interface Vlanif100
  l2 binding vsi ldp1
#
interface GigabitEthernet1/0/1
  port hybrid tagged vlan 30
#
interface GigabitEthernet1/0/2
  port hybrid tagged vlan 40
#
interface GigabitEthernet1/0/3
  port hybrid tagged vlan 100
#
interface LoopBack1
  ip address 3.3.3.9 255.255.255.255
  isis enable 1
#
return
```

Configuration file of LSW1

```
#
sysname LSW1
#
vlan batch 10
#
sep segment 1
  control-vlan 10
  protected-instance 0 to 4094
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk allow-pass vlan 10 100
  stp disable
  sep segment 1
#
interface GigabitEthernet1/0/2
  port link-type trunk
  port trunk allow-pass vlan 10 100
  stp disable
  sep segment 1
#
return
```

Configuration file of LSW2

```
#
sysname LSW2
#
vlan batch 10
#
sep segment 1
  control-vlan 10
  protected-instance 0 to 4094
#
interface GigabitEthernet1/0/1
  port link-type trunk
```

```
port trunk allow-pass vlan 10 100
stp disable
sep segment 1
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk allow-pass vlan 10 100
stp disable
sep segment 1
sep segment 1 priority 128
#
interface GigabitEthernet1/0/3
port link-type trunk
port trunk allow-pass vlan 100
#
return
```

Configuration file of LSW2

```
#
sysname LSW3
#
vlan batch 10
#
sep segment 1
control-vlan 10
protected-instance 0 to 4094
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk allow-pass vlan 10 100
stp disable
sep segment 1
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk allow-pass vlan 10 100
stp disable
sep segment 1
#
return
```

Configuration file of CE1

```
#
sysname CE1
#
vlan batch 100
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk allow-pass vlan 100
#
```

```
return
```

Configuration file of CE2

```
#
sysname CE2
#
vlan batch 100
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk allow-pass vlan 100
#
Return
```

5 Troubleshooting

5.1 Traffic Forwarding Fails After SEP Is Configured

Common Causes

Ports in the SEP segment are not configured to allow traffic from data VLANs to pass, leading to a failure in forwarding user data traffic.

Troubleshooting Procedure

- Step 1** Run the **interface** *interface-type interface-number* command to enter the view of a port in the SEP segment.

```
[Quidway] interface GigabitEthernet 1/0/1  
[Quidway-GigabitEthernet1/0/1]
```

- Step 2** Run the **display this** command in the interface view to check information about the VLAN allowed on the port.

```
[Quidway-GigabitEthernet1/0/1] display this  
port link-type trunk  
port trunk allow-pass vlan 10  
stp disable  
sep segment 1 edge primary  
#  
return
```

The command output shows that GE1/0/1 allows traffic only from VLAN 10 to pass and traffic from data VLANs cannot pass through GE1/0/1.

- Step 3** Run the **port trunk allow-pass vlan** { { *vlan-id1* [*to vlan-id2*] }&<1-10> | **all** } command to add the port to VLAN 100.

```
[Quidway-GigabitEthernet1/0/1] port trunk allow-pass vlan 100
```


6 FAQ

6.1 What Advantages Does SEP Have Compared with Other Ring Network Protocols?

SEP supports fast convergence in milliseconds and applies to Layer 2 networks requiring short convergence time. In addition, SEP has the following advantages:

- Applies to diverse scenarios, and supports various network topologies and flexible configurations.
- Allows selective port blocking, which effectively implements traffic load balancing.
- Prevents traffic from being switched back after link recovery, which improves network stability.
- Displays the SEP network topology from any node, which facilitates management and improves network maintainability.

A Acronyms and Abbreviations

SEP	Smart Ethernet Protection
RRPP	Rapid Ring Protection Protocol
STP	Spanning Tree Protocol
ERPS	Ethernet ring protection switching
VLAN	Virtual local area network
QoS	Quality of service
CFM	Connectivity fault management
VPLS	Virtual private LAN service
MAC	Media access control
TLV	Type-length-value

B References

The following table lists references for this document.

Document	Description	Remarks
SEP Feature Description	Allows you to better understand SEP implementation on Huawei devices.	To obtain these documents, access http://support.huawei.com/enterprise/ .
SEP Configuration Guide	Allows you to better understand the SEP configuration process and precautions on Huawei devices.	
SEP Command Reference	Describes how to use SEP commands.	
Switch Configuration Examples	Describes common SEP networking modes and configuration procedure.	
Switch FAQs	Provides answers to frequently asked questions (FAQs) on SEP.	