

## Reliability Configuration

---

1. Configuring REUP
2. Configuring RLDP
3. Configuring IP Event Dampening

# 1 Configuring REUP

## 1.1 Overview

The Rapid Ethernet Uplink Protection Protocol (REUP) provides a rapid uplink protection function.

In the dual uplink networking, REUP is used to ensure normal communication between links, block redundant links, avoid link loops, and implement fast backup.

The upstream interfaces of REUP are configured in pairs. If both interfaces are normal, an interface works in the backup state. The interface in the backup state does not forward data packets. When the interface in the forward state is faulty, the backup interface switches to the forward state immediately, and provides data transmission. In addition, REUP also sends address update packets to upstream devices so that the upstream devices can update their MAC addresses immediately. This function of REUP ensures that layer-2 data streams can be restored within 50 ms after a link is faulty.

REUP is mutually exclusive with the Spanning Tree Protocol (STP) based on interfaces. In this case, a device runs STP downward and runs REUP upward to implement backup and fault protection for the upstream link. REUP ensures that basic link redundancy is provided when STP is disabled and that millisecond-level fault recovery faster than STP is also provided.

### Protocols and Standards

- REUP is a [proprietary protocol](#) of Orion Alpha A28X Network, and there is no standard and protocol for reference.

## 1.2 Applications

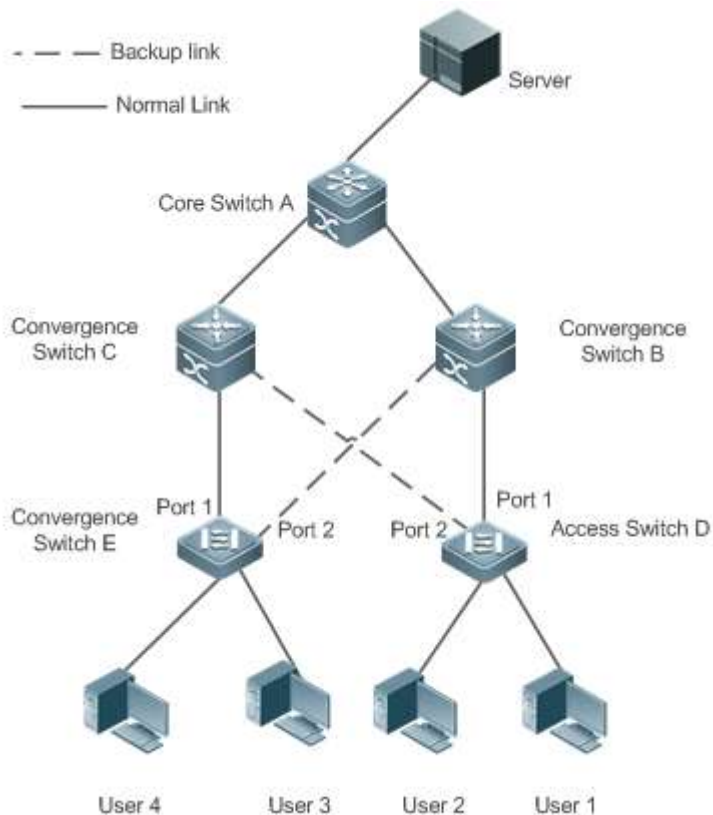
Application	Description
<a href="#">Communication in Dual Uplink Networking</a>	Forward packets in the dual-uplink networking.

### 1.2.1 Communication in Dual Uplink Networking

#### Scenario

For communication in dual uplink networking, the access switch has two uplink paths, as shown in Figure 1-1.

Figure 1-1 Dual uplink networking



## Deployment

- Enable REUP on interface1 and interface2 of the access switch D/E to implement fast switching when a link is faulty.
- Enable MAC address update message receiving of REUP on the interfaces connected to switches A/B/C to rapidly clear the MAC addresses on the interfaces when a link is faulty.

## 1.3 Features

### Basic Concepts

#### ↘ REUP Pair

Specify an interface as the backup interface of another interface to configure an REUP pair. One interface is the active interface and the other interface is the backup interface. When the two interfaces are normal, an interface is configured as the forward interface whereas the other interface is configured as the backup interface. You can determine the interface to be configured as the backup interface. See the related information in the section "Configuring the Preemption Mode and Delay Time of REUP".

#### ↘ MAC Address Update Message

MAC address update messages refer to FLUSH packets sent by Orion Alpha A28X Network to uplink devices through private multicast. When an uplink device of Orion Alpha A28X Network enables the function for receiving MAC address

update messages and receives MAC address update messages, the device updates the MAC addresses of corresponding interfaces.

### ↘ [MAC Address Update Group](#)

Multiple interfaces are added to a group. If one interface in the group receives a MAC address update message, the MAC addresses of other interfaces in the group will be updated. In this case, the group is called MAC address update group.

### ↘ [MAC Address Update Packet](#)

Packets sent to update MAC addresses in order to support uplink devices are called MAC address update packets.

### ↘ [Link Tracking Group](#)

The uplink and downstream interfaces of a device are added to a group. If all upstream interfaces in the group are down, all downstream interfaces in this group are forced down. In this case, this group is called a link tracing group.

## [Overview](#)

Feature	Description
<a href="#">Dual Link Backup of REUP</a>	When a link is faulty, the other link can rapidly switch to the forward state.
<a href="#">Preemption Mode and Delay Time of REUP</a>	When both links are normal, the preemption mode can be used to determine the link that is used for forwarding data and the delay time that is used to determine the waiting time before switching.
<a href="#">MAC Address Update</a>	During link switching, the MAC address of an interface is updated to make packet convergence faster.
<a href="#">VLAN Load Balance</a>	When the two links are normal, the utilization of link bandwidth can be maximized.
<a href="#">Link State Tracking</a>	When the upstream link is faulty, the downstream link is switched.

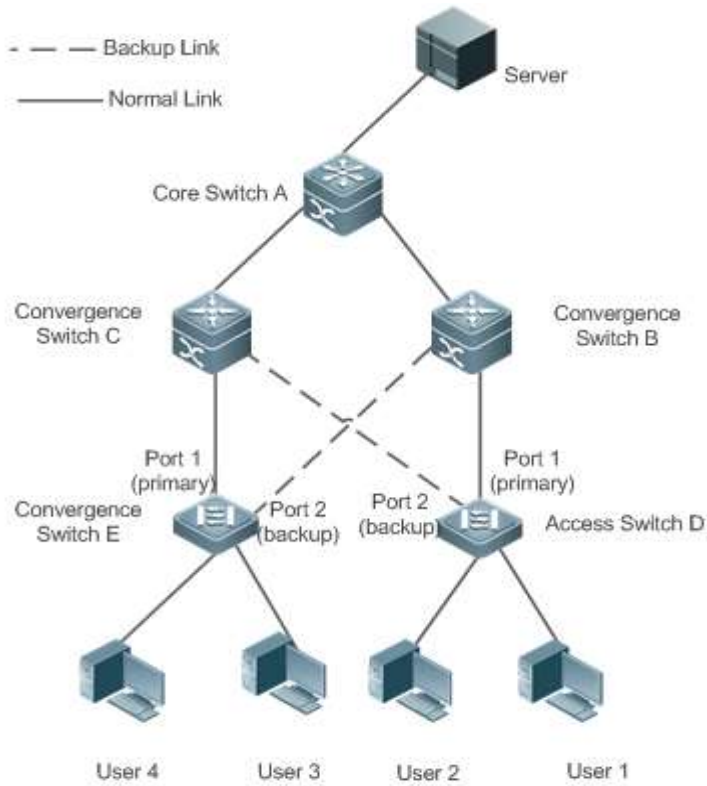
### 1.3.1 Dual Link Backup of REUP

When an active link is faulty, the link in the backup state will rapidly switch to the forward state and start forwarding data, minimizing the service interruption caused by link failure.

#### [Working Principle](#)

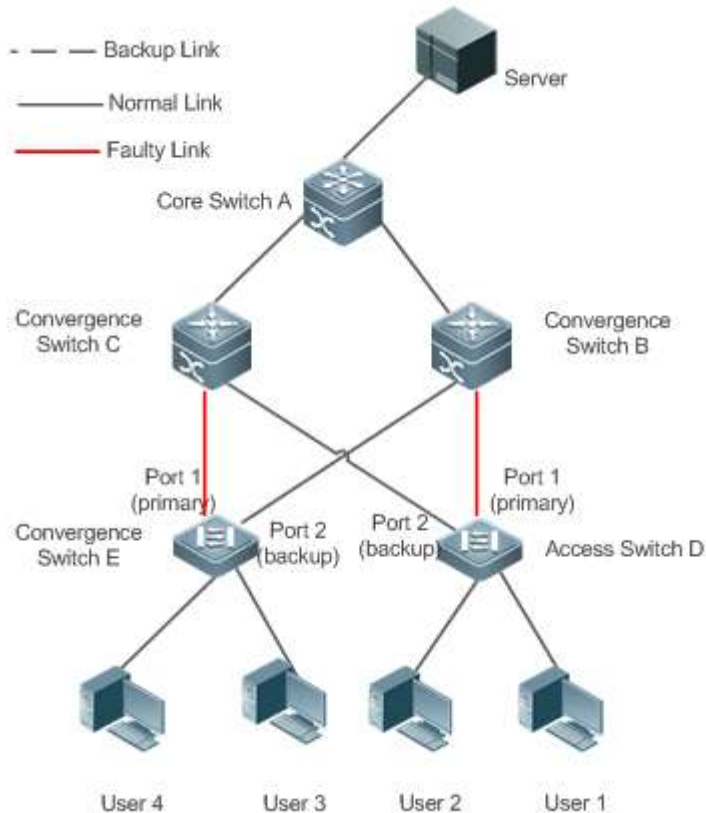
Specify an interface as the backup interface of another interface to configure an REUP pair. When the two interfaces are normal, a link is in the forward state (forwarding data packets) and the other link is in the backup state (not forwarding data). When the active link is faulty, the link in the backup state rapidly switches to the forward state and starts forwarding data. When the faulty link is recovered, the link enters the backup state and does not forward data packets. Of course, you can configure the preemption mode to specify whether a link recovered from failure preempts the link that is in the forward state currently.

Figure 1-2 A topology with two normal links



As shown in Figure 1-2, connect interfaces 1 and 2 of switch D (E) to the uplink switches B and C (C and B) and configure REUP on interfaces 1 and 2. When the links are normal, interface 1 is in the forward state and forwards data packets and interface 2 is in the backup state and does not forward data packets.

Figure 1-3 A topology with interface 1 of switch D (E) faulty



Once interface 1 is faulty, interface 2 immediately starts forwarding data packets and recovers the uplink transmission of the switch. In the non-preemption mode, when the link of interface 1 is recovered, interface 1 is in the backup state and does not forward data packets whereas interface 2 continues forwarding data packets.

## Related Configuration

### ↳ Enabling Dual Link Backup on an interface

By default, dual link backup on an interface is disabled.

You can run the **switchport backup interface** command to configure a layer-2 physical interface (or layer-2 AP interface) as a backup interface and enable the dual link backup function of REUP.

You must enable the dual link backup function of REUP on an interface. The function involves the link switching of REUP only when an interface is faulty.

- ❗ REUP, ERPS, and RERP do not share interfaces.
- ❗ Devices enabled with REUP must disable the storm control function of all layer-2 interfaces.

## 1.3.2 Preemption Mode and Delay Time of REUP

### Working Principle

You can determine which link should be used first by configuring the preemption mode of REUP. If the preemption mode is set to bandwidth first, REUP selects a link with a high bandwidth first. You can also set the preemption mode to forced to select a stable and reliable link first forcibly.

To avoid frequent active/backup link switching caused by abnormal faults, REUP provides a preemption delay function. When the two links are recovered, link switching is performed when the faulty link becomes stable after a delay (35s by default).

## Related Configuration

### Configuring the Preemption Mode and Delay Time of REUP

By default, the preemption mode is disabled and the delay time is 35s.

You can run the **switchport backup interface preemption mode** command to configure the preemption mode.

You can run the **switchport backup interface preemption delay** command to configure the delay time.

A smaller delay means more frequent preemption switching after the faulty link is recovered.

- REUP uses the value of the **Bandwidth** attribute for an AP interface as the actual bandwidth of the AP interface, which is equal to the value of the **Speed** attribute (the number of link up member interfaces x the number of member interfaces).
- When an uplink enables STP, the preemption delay time of REUP is greater than 35s.

### 1.3.3 MAC Address Update

During link switching, the MAC address of an interface is updated to make packet convergence faster.

#### Working Principle

As shown in Figure 1-2, interface 1 and interface 2 of switch D (E) are enabled with dual link backup of REUP. Interface 1 works as the active interface. During normal communication, switch A learns the MAC addresses of users 1 and 2 (users 3 and 4) from the interfaces connecting to switch B (C).

When interface 1 of switch D (E) is faulty, interface 2 rapidly switches to the forward state and starts forwarding data packets. In this case, switch A does not learn the MAC addresses of users 1 and 2 (users 3 and 4) on the interfaces connecting to switch B (C). The data packets sent by the server to users 1 and 2 (users 3 and 4) are forwarded to switch C (B) by switch A, causing that the packets from the server to users 1 and 2 (users 3 and 4) are lost.

To avoid the preceding problems, you can enable the MAC address update function on switch D (E). When interface 2 starts forwarding packets, switch D (E) sends a MAC address update message to interface 2. After receiving the MAC address update message, switch A updates the MAC address on the interface of switch A. In this way, switch A forwards the packets sent by the server to the users to the interfaces of switch B (C) to make packet convergence faster.

In addition, import the setting of a MAC address update group, that is, classify multiple interfaces into the same group. When an interface in this group receives a MAC address update message, the MAC addresses on other interfaces in the group are updated to reduce the side effect of flooding caused by MAC address update.

To be compatible with upstream devices not supporting MAC address update messages, switch D (E) will send MAC address update packets for users 1 and 2 (users 3 and 4) upward when interface 2 switches to the forward state. In this

way, switch A can update the MAC addresses of users 1 and 2 (users 3 and 4) to the corresponding interfaces and recover the downlink data transmission of switch A.

## Related Configuration

### ↳ Enabling Sending of MAC Address Update Messages on an interface

By default, sending of MAC address update messages is disabled on an interface.

You can run the **mac-address-table move update transit** command to enable sending of MAC address updates on all interfaces of a device.

If sending of MAC address update messages is not enabled, MAC address update messages will not be sent when dual link backup switching of REUP is performed.

### ↳ Enabling Receiving of MAC Address Update Messages on an interface

By default, receiving of MAC address update messages is disabled on an interface.

You can run the **mac-address-table move update receive** command to enable receiving of MAC address updates on all interfaces of a device.

If receiving of MAC address update messages is not enabled, a device cannot receive MAC address update messages from downlink devices during dual link backup switching of REUP and will not update the MAC addresses.

### ↳ Configuring a VLAN for Sending MAC Address Update Messages

By default, a VLAN for sending MAC address update messages is the default VLAN to which an interface belongs.

You can run the **mac-address-table move update transit vlan** command to configure the VLAN in which interfaces send MAC address update messages.

If the VLAN in which interfaces send MAC address update messages is configured, the messages are sent in the configured VLAN; otherwise, the messages are sent in the default VLAN to which the interface belongs.

### ↳ Configuring a VLAN for Receiving MAC Address Update Messages

By default, MAC address update messages are received in all VLANs.

You can run the **no mac-address-table move update receive vlan** command to configure a VLAN in which interfaces do not receive MAC address update messages. MAC address update messages are received in remaining VLANs.

If no VLAN in which interfaces receive MAC address update messages is configured, MAC address update messages are received in all the configured VLANs; otherwise, MAC address update messages are received in the remaining VLANs.

### ↳ Configuring a MAC Address Update Group

By default, there is no MAC address update group.

You can run the **mac-address-table update group** command to add an interface to the MAC address update group. The interface is added to the first update group by default.

If no MAC address update group is configured, MAC address update will not be performed when MAC address update packets are received.

### ↳ Configuring the Maximum Number of MAC Address Update Packets Sent Per Second



By default, the maximum number of MAC address update packets sent per second is 150.

You can run the **mac-address-table move updatemax-update-rate** command to configure the maximum number of MAC address update packets sent per second.

The larger the number of packets, the more CPU time used for sending the packets, and the fewer downlink packets are lost.

### 1.3.4 VLAN Load Balance

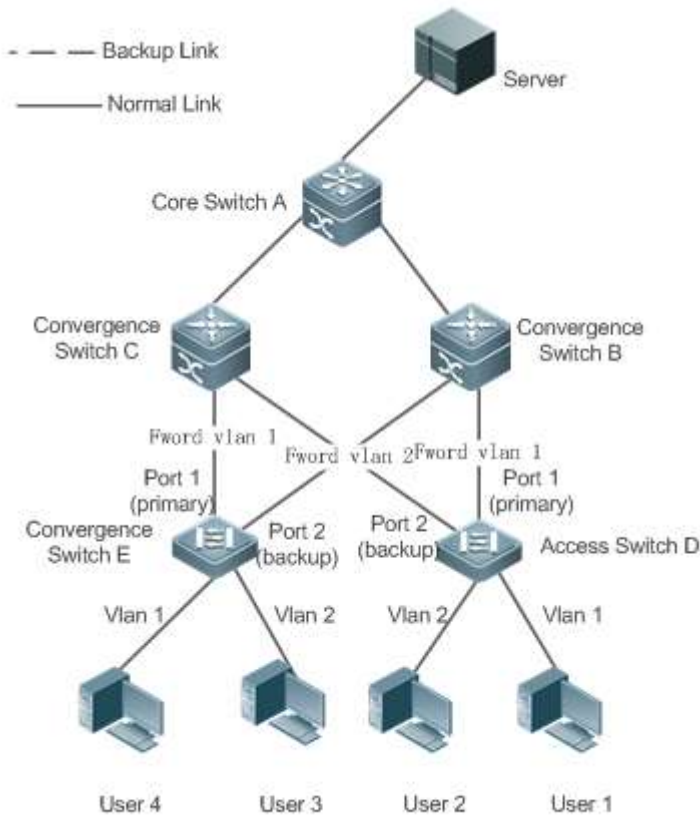
#### Working Principle

The VLAN load balance function allows REUP to forward data packets of mutually exclusive VLANs for two interfaces to make full use of the link bandwidth.

As shown in Figure 1-4, configure dual link backup of REUP and enable VLAN load balance of REUP on interface 1 and interface 2 of switch D, and map VLAN 1 to instance 1 and VLAN 2 to instance 2. Data of VLAN 1 (instance 1) is transmitted through interface 1 and all the other data of VLAN 2 (instance 2) is transmitted through interface 2. Perform the same processing on switch E.

When an interface is faulty, the other interface takes over the transmission of all VLANs. When the faulty interface is recovered and does not become faulty within the preemption delay, the transmission of VLANs is switched back to the recovered interface.

Figure 1-4 A topology with two normal links of load balance



## Related Configuration


### ↳ Enabling VLAN Load Balance on an interface

By default, the VLAN load balance function on an interface is disabled.

You can run the **switchport backup interface prefer instance** command to enable the VLAN load balance function.

If this function is not enabled, the link bandwidth cannot be fully used when packets are forwarded when the two links are normal. You must enable the VLAN load balance function on a port so that the interface can be involved in VLAN load balance.

---

 The instance mapping of REUP VLAN load balance is controlled by the MSTP module in a unified manner. For details about how to configure the instances, see the description in the *Configuring MSTP*.

 The VLAN load balance function can be configured only on trunk, uplink or hybrid interfaces.

---

### 1.3.5 Link State Tracking

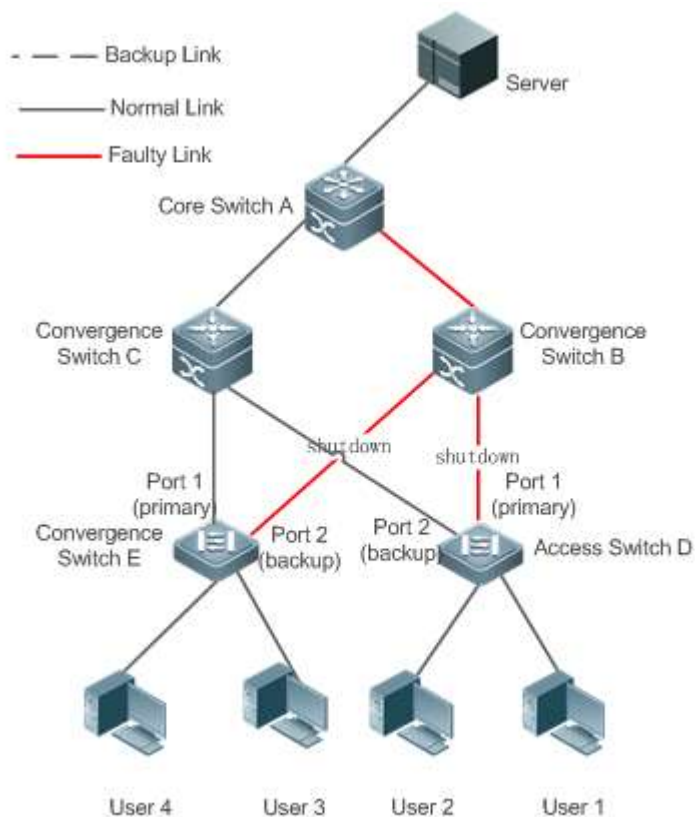
Link tracking means that when the upstream link is faulty, services are switched to the downstream link so that the backup interface can continue forwarding packets.

#### Working Principle

Link state tracking provides the function of notifying downlink devices for link switching when the upstream link is faulty. You can configure the uplink and downstream interfaces of a link state tracking group and bind the link status of multiple downstream interfaces to the interfaces of multiple upstream links to implement link status synchronization. When all upstream links in a tracking group are faulty, the interfaces of the downstream links are shut down forcibly to ensure that the transmission of the downstream links is switched from the active link to the backup link.

As shown in Figure 1-5, when the upstream link of switch B is faulty, link state tracking rapidly shuts down the downstream interface of switch B so that the uplink transmission of switch D is switched to switch C.

Figure 1-5 A topology where the upstream link of the active link is faulty



## Related Configuration

### ▾ Enabling Link Tracking

Link tracking is disabled by default.

You can run the **link state track** *[number]* command to enable a link tracking group. The value of **number** ranges from 1 to 2. The first link tracking group is enabled by default (the default value of **number** is 1).

If link tracking is not enabled, the status of a corresponding upstream interface cannot be detected and packet forwarding switching cannot be implemented in time.

### ▾ Enabling the Downlink Delay Up Function for a Link Tracking Group

By default, the downlink delay for link tracking is 0s.

You can run the **link state track** *number up-delay timer* command to enable a link tracking group. The value of **number** ranges from 1 to 2. The first link tracking group is enabled by default (the default value of **number** is 1). The value of **timer** ranges from 0 to 300s, which is 0s by default.

By enabling the downlink delay up function, you can avoid frequent downlink switching caused by uplink flapping in a link tracking group. That is, when the upstream link becomes up, the downstream link becomes up after a delay.






### ▾ Adding an interface to a Link Tracking Group

By default, an interface is not added to a link tracking group.

You can run the **link state group** *[number]* {**upstream** | **downstream**} command to set upstream interfaces and downstream interfaces of the link tracking group. The value of **number** ranges from 1 to 2. An interface is added to the first link tracking group by default (the default value of number is 1).

If an interface is not added to a tracking group, the status of a corresponding upstream interface cannot be detected and packet forwarding switching cannot be implemented in time.

## 1.4 Configuration

Configuration	Description and Command	
<a href="#">Configuring Basic Functions of REUP</a>	 (Mandatory) It is used to enable dual link backup of REUP.	
	<b>switchport backup interface</b>	Enables dual link backup of REUP.
<a href="#">Configuring the Preemption Mode and Delay Function of REUP</a>	 (Optional) It is used to determine the preemption mode and delay time. The default values are used if they are not configured.	
	<b>switchport backup interface preemption mode</b>	Sets the preemption mode.
	<b>switchport backup interface preemption delay</b>	Sets the delay time for preemption.
<a href="#">Configuring MAC Address Update</a>	 (Optional) It is used to enable rapid update of MAC addresses.	
	<b>mac-address-table update group</b>	Sets the MAC address update group ID of a switch.
	<b>mac-address-table move update transit</b>	Enables sending of MAC address update messages.
	<b>mac-address-table move update transit vlan</b>	Enables sending of the VLAN ID of MAC address update messages.
	<b>mac-address-table move update</b>	Configures the maximum number of MAC address update packets sent per second. The value ranges from 0 to 32000. The default value is 150.
	<b>mac-address-table move update receive</b>	Enables receiving of MAC address update messages.
	<b>mac-address-table move update receive vlan</b>	Configures the VLAN range for processing MAC address update messages.
<a href="#">Configuring VLAN Load Balance</a>	 (Optional) It is used to enable VLAN load balance.	
	<b>switchport backup interface prefer instance</b>	Configures the link VLAN load balance of REUP.
<a href="#">Configuring Link Tracking</a>	 (Optional) It is used to enable link tracking.	

Configuration	Description and Command	
	<b>link state track up-delay</b>	Enables the downlink delay up for a link state tracking group.
	<b>link state track</b>	Enables a link state tracking group.
	<b>link state group</b>	Add an interface as an upstream interface or a downstream interface of a specified link state tracking group.

## 1.4.1 Configuring Basic Functions of REUP

### Configuration Effect

- When a link is faulty, the other normal link is switched to the forward state immediately for forwarding packets.

### Notes

- An interface belongs to only one REUP pair. Each active link has only one backup link. A backup link can be used as the backup link of only one active link. The active and backup links must use different interfaces.
- REUP supports layer-2 physical interfaces and AP interfaces, but does not support AP member interfaces.
- The active and backup interfaces may be of different types and have different rates. For example, an AP interface can be used as the active interface whereas a physical interface is configured as the backup interface.
- Interfaces configured with REUP are not involved in STP calculation.
- Each device can be configured with a maximum of 16 REUP pairs.
- Interfaces successfully configured with REUP cannot change interfaces to layer-3 interfaces or be added to an AP.

### Configuration Steps

#### 📌 Enabling Dual Link Backup of REUP

- Mandatory.
- If there is no special requirement, dual link backup of REUP should be enabled on an interface of the receiving switch.

### Verification

Run the **show interfaces switchport backup [detail]** command to check whether dual link backup of REUP is configured.

### Related Commands

#### 📌 Enabling Dual Link Backup of REUP

<b>Command</b>	<b>switchport backup interface</b> <i>interface-id</i>
<b>Parameter Description</b>	<i>interface-id</i> : Indicates the backup interface ID.
<b>Command Mode</b>	Interface configuration mode
<b>Usage Guide</b>	If the interface where the mode resides is the active interface, the interface corresponding to the <b>interface-</b>

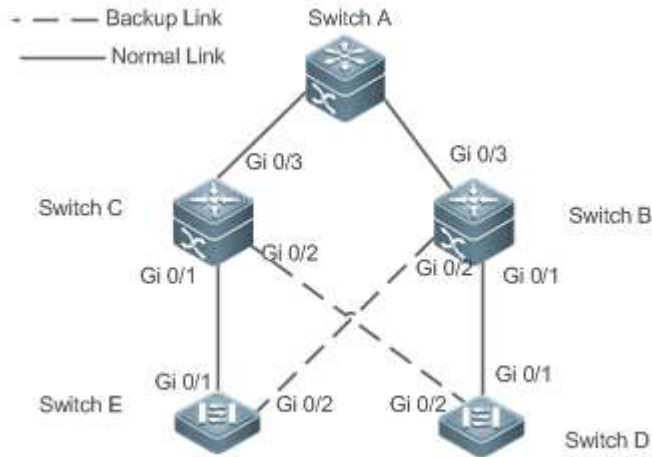
**id** parameter is the backup interface. When the active link is faulty, rapidly recover the transmission of the backup link.

## Configuration Example

### Enabling Dual Link Backup of REUP

#### Scenario Figure 1-6 Dual uplink networking

As shown in Figure 1-6, there are two upstream links from switch D to switch A, which are switch D > switch B > switch A and switch D > switch C > switch A. There are two upstream links from switch E to switch A, which are switch E > switch B > switch A and switch E > switch C > switch A.



#### Configuration Steps

- Configure dual link backup (the interface Gi0/1 is the active interface and Gi0/2 is the backup interface) of REUP on the access switch D (E).

#### D

```
SwitchD> enable
SwitchD# configure terminal
SwitchD(config)# interface GigabitEthernet 0/1
SwitchD(config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface GigabitEthernet 0/2
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

#### E

```
SwitchE> enable
SwitchE# configure terminal
SwitchE(config)# interface GigabitEthernet 0/1
SwitchE(config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchE(config-if-GigabitEthernet 0/1)#switchport backup interface GigabitEthernet 0/2
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

<b>Verification</b>	<ul style="list-style-type: none"> <li>● Check the dual link backup information configured for switch D (E).</li> </ul>
<b>D</b>	<pre>SwitchD#show interfaces switchport backup detail  Switch Backup Interface Pairs:  Active Interface      Backup Interface      State ----- Gi0/1                 Gi0/2                 Active Up/Backup Standby  Interface Pair : Gi0/1, Gi0/2  Preemption Mode : off  Preemption Delay : 35 seconds  Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)</pre>
<b>E</b>	<pre>SwitchE#show interfaces switchport backup detail  Switch Backup Interface Pairs:  Active Interface      Backup Interface      State ----- Gi0/1                 Gi0/2                 Active Up/Backup Standby  Interface Pair : Gi0/1, Gi0/2  Preemption Mode : off  Preemption Delay : 35 seconds  Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)</pre>

### Common Errors

- Other REUP pairs are configured on a configured interface.
- A configured interface is not a layer-2 physical interface or AP interface.

## 1.4.2 Configuring the Preemption Mode and Delay Function of REUP

### Configuration Effect

- Restrict the preemption mode and preemption delay time for REUP link switching.

### Notes

- Dual link backup of REUP must be configured.

## Configuration Steps

- Optional.
- If the active link needs to always forward packets or the link bandwidth needs to be used to determine the link for forwarding packets, the corresponding preemption mode and delay time must be configured.

## Verification

Run the **show interfaces switchport backup [detail]** command to check whether the preemption mode and delay time are consistent with the configurations.

## Related Commands

### ▾ Configuring the Preemption Mode of REUP

<b>Command</b>	<b>switchport backup interface</b> <i>interface-id</i> <b>preemption mode</b> {forced bandwidth off}
<b>Parameter Description</b>	<i>interface-id</i> : Indicates the backup interface ID. <b>mode</b> : Sets the preemption mode: <b>forced</b> : Indicates the forced mode. <b>bandwidth</b> : Indicates the bandwidth mode. <b>off</b> : Indicates that the preemption mode is off.
<b>Command Mode</b>	Interface configuration mode
<b>Usage Guide</b>	The preemption modes include forced, bandwidth and off. In the bandwidth mode, an interface with a high bandwidth is selected first to transmit data; in the forced mode, the active interface is selected first to transmit data; in the off mode, no preemption is performed. The default mode is off.

### ▾ Configuring the Delay Time of REUP

<b>Command</b>	<b>switchport backup interface</b> <i>interface-id</i> <b>preemption delay</b> <i>delay-time</i>
<b>Parameter Description</b>	<i>interface-id</i> : Indicates the backup interface ID. <i>delay-time</i> : Indicates the delay time.
<b>Command Mode</b>	Interface configuration mode
<b>Usage Guide</b>	Preemption delay indicates the delay time after a faulty link is recovered to the time when link switching is performed again.

## Configuration Example

### ▾ Configuring the Preemption Mode and Delay Time of REUP

<b>Scenario</b>	As shown in Figure 1-6, there are two upstream links from switch D to switch A, which are switch D > switch B > switch A and switch D > switch C > switch A. There are two upstream links from switch E to switch A, which are switch E > switch B > switch A and switch E > switch C > switch A.
<b>Configuration Steps</b>	<ul style="list-style-type: none"><li>• Configure the preemption mode to bandwidth on the access switch D (E) and the delay time to 40s.</li></ul>



```

D
SwitchD> enable

SwitchD# configure terminal

SwitchD(config)# interface GigabitEthernet 0/1

SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi 0/2 preempt mode
bandwidth

SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi 0/2 preempt delay 40

SwitchD(config-if-GigabitEthernet 0/1)# exit

```

```

E
SwitchE> enable

SwitchE# configure terminal

SwitchD(config)# interface GigabitEthernet 0/1

SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi 0/2 preempt mode
bandwidth

SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi 0/2 preempt delay 40

SwitchD(config-if-GigabitEthernet 0/1)# exit

```

**Verification** ● Check the dual link backup information configured for switch D (E).

```

D
SwitchD#show interfaces switchport backup detail

Switch Backup Interface Pairs:

Active Interface      Backup Interface      State
-----
Gi0/1                 Gi0/2                 Active Up/Backup Standby

Interface Pair : Gi0/1, Gi0/2

Preemption Mode : bandwidth

Preemption Delay : 40 seconds

Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)

```

```

E
SwitchE#show interfaces switchport backup detail

Switch Backup Interface Pairs:

Active Interface      Backup Interface      State
-----
Gi0/1                 Gi0/2                 Active Up/Backup Standby

```

	Interface Pair : Gi0/1, Gi0/2 Preemption Mode : bandwidth Preemption Delay : 40 seconds Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)
--	---

## Common Errors

- A configured interface is not a layer-2 physical interface or AP interface.

### 1.4.3 Configuring MAC Address Update

#### Configuration Effect

- Rapidly delete and update MAC addresses of an interface during link switching to make packet convergence faster.

#### Notes

- Dual link backup of REUP must be configured.
- Each device can be configured with a maximum of 8 address update groups. Each address update group can have a maximum of 8 member interfaces and an interface can belong to multiple address update groups.

#### Configuration Steps

- Mandatory.
- If there is no special requirement, the MAC address update function should be configured.

#### Verification

Run the **show mac-address-table update group [detail]** command to view the update group configuration.

#### Related Commands

##### ↘ Configuring the MAC Address Update Group ID of a Switch

<b>Command</b>	<b>mac-address-table update group</b> [ <i>group-num</i> ]
<b>Parameter Description</b>	<i>group-num</i> : Indicates the MAC address update group ID.
<b>Command Mode</b>	Interface configuration mode
<b>Usage Guide</b>	In order to reduce large flooding caused by MAC address update which may affect normal data transmission of the switch, we add a setting of a MAC address update group. Only after all interfaces on a switching path are added to the same MAC address update group, transmission of downlink data can be rapidly recovered.

##### ↘ Enabling Sending of MAC Address Update Messages

<b>Command</b>	<b>mac-address-table move update transit</b>
<b>Parameter Description</b>	-
<b>Command Mode</b>	Command Mode
<b>Usage Guide</b>	To reduce link switching and loss of downlink data streams, you need to enable sending of MAC address update messages on a switch that performs switching.

#### ↘ Enabling Sending of the VLAN ID of MAC Address Update Messages

<b>Command</b>	<b>mac-address-table move update transit vlan <i>vid</i></b>
<b>Parameter Description</b>	<i>vid</i> : Indicates the VLAN ID for sending MAC address update messages.
<b>Command Mode</b>	Interface configuration mode
<b>Usage Guide</b>	After sending of MAC address update messages is enabled, MAC address update messages can be sent to uplink devices during link switching.

Configure the maximum number of MAC address update packets sent per second.

#### ↘ Configuring the Maximum Number of MAC Address Update Packets Sent Per Second

<b>Command</b>	<b>mac-address-table move update max-update-rate <i>pkts-per-second</i></b>
<b>Parameter Description</b>	<i>pkts-per-second</i> : Indicates the maximum number of MAC address update packets sent per second. The value ranges from 0 to 32000. The default value is 150.
<b>Command Mode</b>	Configuration mode
<b>Usage Guide</b>	During link switching, REUP sends MAC address update packets of a specified quantity to uplink devices per second to recover the downlink data transmission of the uplink device.

#### ↘ Enabling Receiving of MAC Address Update Messages

<b>Command</b>	<b>mac-address-table move update receive</b>
<b>Parameter Description</b>	-
<b>Command Mode</b>	Configuration mode
<b>Usage Guide</b>	During switching of dual link backup, downlink data streams may be lost since the MAC address table of the uplink switch is not updated in real time. In order to reduce loss of layer-2 data streams, you need to update the MAC address table of the uplink switch. In this case, you need to enable receiving of MAC address update messages on the uplink switch.

#### ↘ Configuring the VLAN Range for Processing MAC Address Update Messages

<b>Command</b>	<b>mac-address-table move update receive vlan <i>vlan-range</i></b>
<b>Parameter Description</b>	<i>vlan-range</i> : Indicates the VLAN range for processing MAC address update messages.

<b>Command Mode</b>	Configuration mode
<b>Usage Guide</b>	This command is used to disable the function for processing MAC address update messages on certain VLANs. For a VLAN disabled with the function for processing MAC address update messages, MAC address update packets can be used to recover the downlink transmission of uplink devices; however, the convergence performance for link faults will be decreased.

## Configuration Example

### Configuring MAC Address Update

<b>Scenario</b>	As shown in Figure 1-6, there are two upstream links from switch D to switch A, which are switch D > switch B > switch A and switch D > switch C > switch A. There are two upstream links from switch E to switch A, which are switch E > switch B > switch A and switch E > switch C > switch A.
<b>Configuration Steps</b>	<ul style="list-style-type: none"> <li>● Enable sending of MAC address update messages on the access switch D (E).</li> <li>● Enable receiving of MAC address update packets on switch B (C).</li> <li>● Add all interfaces on the REUP switching path to the same MAC address update group.</li> <li>● In the environment, Gi0/1 and Gi0/3 of switch B are the interfaces on the switching path of switch D's uplink, and Gi0/3 and Gi0/2 are the interfaces on the switching path of switch E's uplink. You can add interfaces Gi0/1, Gi0/2 and Gi0/3 to the same address update group. Similarly, you can obtain the configuration of switch C.</li> <li>● Enable receiving of MAC address update packets on switch A.</li> <li>● Add all interfaces on the REUP switching path of switch A to the same MAC address update group.</li> </ul>
<b>D</b>	<pre>SwitchD&gt; enable SwitchD# configure terminal SwitchD(config)# mac-address-table move update transit SwitchD(config)# exit</pre>
<b>E</b>	<pre>SwitchE&gt; enable SwitchE# configure terminal SwitchE((config)# mac-address-table move update transit SwitchE(config)# exit</pre>
<b>B</b>	<pre>SwitchB# configure terminal SwitchB(config)# mac-address-table move update receive SwitchB(config)# interface range gigabitEthernet 0/1 -3 SwitchB(config-if-range)#switchport mode trunk SwitchB(config-if-range)# mac-address-table update group 1</pre>

	SwitchB(config-if-range)# end
<b>C</b>	<pre>SwitchB# configure terminal SwitchB(config)# mac-address-table move update receive SwitchB(config)# interface range gigabitEthernet 0/1 -3 SwitchB(config-if-range)#switchport mode trunk SwitchB(config-if-range)# mac-address-table update group 1 SwitchB(config-if-range)# end</pre>
<b>A</b>	<pre>SwitchA# configure terminal SwitchA(config)# mac-address-table move update receive SwitchA(config)# interface range gigabitEthernet 0/1 -2 SwitchA(config-if-range)# switchport mode trunk SwitchA(config-if-range)# mac-address-table update group 1 SwitchA(config-if-range)# end</pre>
<b>Verification</b>	Check the information about the address update groups on switches D, E, C, B and A.
<b>D</b>	<pre>SwitchD# show run   incl mac-ad mac-address-table move update transit</pre>
<b>E</b>	<pre>SwitchE# show run   incl mac-ad mac-address-table move update transit</pre>
<b>B</b>	<pre>SwitchB# show mac-address-table update group detail show mac-address-table update group detailMac-address-table Update Group:1 Received mac-address-table update message count:0 Group member          Receive Count    Last Receive Switch-ID    Receive Time ----- Gi0/1                  0                0000.0000.0000 Gi0/2                  0                0000.0000.0000 Gi0/3                  0                0000.0000.0000</pre>
<b>C</b>	<pre>SwitchC# show mac-address-table update group detail Mac-address-table Update Group:1</pre>

	<pre>Received mac-address-table update message count:0 Group member          Receive Count    Last Receive Switch-ID    Receive Time ----- Gi0/1                 0               0000.0000.0000 Gi0/2                 0               0000.0000.0000 Gi0/3                 0               0000.0000.0000</pre>
<b>A</b>	<pre>SwitchA# show mac-address-table update group detail Mac-address-table Update Group:1 Received mac-address-table update message count:0 Group member          Receive Count    Last Receive Switch-ID    Receive Time ----- Gi0/1                 0               0000.0000.0000 Gi0/2                 0               0000.0000.0000</pre>

### Common Errors

- A configured interface is not a layer-2 physical interface or AP interface.

## 1.4.4 Configuring VLAN Load Balance

### Configuration Effect

- Maximize the utilization of link bandwidth.

### Notes

- Dual link backup of REUP must be configured.
- The Access interface cannot be shared by VLAN load balance and STP.
- For interfaces successfully configured with VLAN load balance, you cannot modify the attributes of the interfaces but can modify the VLAN attributes of the interfaces.

### Configuration Steps

- If maximizing bandwidth utilization is not required, this configuration is optional.
- If there is a requirement for VLAN load balance, corresponding configuration must be performed.

### Verification

Run the **show interfaces switchport backup [detail]** command to check whether VLAN load balance is configured.

### Related Commands

- [Configuring VLAN Load Balance](#)

<b>Command</b>	<b>switchport backup interface</b> <i>interface-id</i> <b>prefer instance</b> <i>instance-range</i>
<b>Parameter</b>	<i>interface-id</i> : Indicates the backup interface ID.
<b>Description</b>	<i>instance-range</i> : Indicates the load instance range of the backup interface.
<b>Command Mode</b>	Interface configuration mode
<b>Usage Guide</b>	You can modify the mapping between instances and VLANs by using the instance mapping function of MSTP.

## Configuration Example

### Configuring VLAN Load Balance

<b>Scenario</b>	As shown in Figure 1-6, there are two upstream links from switch D to switch A, which are switch D > switch B > switch A and switch D > switch C > switch A. There are two upstream links from switch E to switch A, which are switch E > switch B > switch A and switch E > switch C > switch A.
<b>Configuration Steps</b>	<ul style="list-style-type: none"> <li>Configure instance mappings on switch D (E) to map VLAN 1 to instance 1, VLAN 2 to instance 2, VLAN 3 to instance 3, and VLAN 4 to instance 4. For details, see the <i>MSTP Configuration Guide</i>.</li> <li>Configure the VLAN load balance function on switch D (E).</li> </ul>
<b>D</b>	<pre>SwitchD&gt; enable SwitchD# configure terminal SwitchD(config)# interface GigabitEthernet 0/1 SwitchD(config-if-GigabitEthernet 0/1)# switchport mode trunk SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi0/2 prefer instance 2 SwitchD(config-if-GigabitEthernet 0/1)# exit</pre>
<b>E</b>	<pre>SwitchE&gt; enable SwitchE# configure terminal SwitchE(config)# interface GigabitEthernet 0/1 SwitchE(config-if-GigabitEthernet 0/1)# switchport mode trunk SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi0/2 prefer instance 4 SwitchD(config-if-GigabitEthernet 0/1)# exit</pre>
<b>Verification</b>	<ul style="list-style-type: none"> <li>Check the dual link backup information configured for switch D (E).</li> </ul>
<b>D</b>	<pre>SwitchD#show interfaces switchport backup detail  Switch Backup Interface Pairs:  Active Interface          Backup Interface          State ----- </pre>

	<pre> Gi0/1                Gi0/2                Active Up/Backup Up  Instances Preferred on Active Interface: Instance 0-1,3-64     Mapping VLAN 1,3-4094  Instances Preferred on Backup Interface: Instance 2     Mapping VLAN 2  Interface Pair : Gi0/1, Gi0/2 Preemption Mode : balance Preemption Delay : 35 seconds Bandwidth : Gi0/1(800 kbits), Gi0/2(100000 kbits) </pre>
<p><b>E</b></p>	<pre> SwitchE#show interfaces switchport backup detail  Switch Backup Interface Pairs:  Active Interface      Backup Interface      State ----- Gi0/1                Gi0/2                Active Up/Backup Up  Instances Preferred on Active Interface: Instance 0-3,5-64     Mapping VLAN 1-3,5-4094  Instances Preferred on Backup Interface: Instance 4     Mapping VLAN 4  Interface Pair : Gi0/1, Gi0/2 Preemption Mode : balance Preemption Delay : 35 seconds Bandwidth : Gi0/1(800 kbits), Gi0/2(100000 kbits) </pre>

### Common Errors

- The mappings between VLAN IDs and instances are not configured.



## 1.4.5 Configuring Link Tracking

### Configuration Effect

- After detecting that the upstream link is disconnected, forcibly disconnect the downstream link so that link switching can be performed.

### Notes

- Dual link backup of REUP must be configured.
- For the link state tracking function, each interface belongs to only one link state tracking group and each device can be configured with up to 2 link state tracking groups. Each link state tracking group can have 8 upstream interfaces and 256 downstream interfaces.

### Configuration Steps

- Mandatory.
- If there is no special requirement, the uplink tracking function should be configured.

### Verification

Run the **show link state group** command to view the configured link tracking information.

### Related Commands

#### ▾ Enabling a Link State Tracking Group

<b>Command</b>	<b>link state track [ num]</b>
<b>Parameter Description</b>	<i>num</i> : Indicates the ID of a link state tracking group.
<b>Command Mode</b>	Configuration mode
<b>Usage Guide</b>	You can create a link tracking group and then add an interface to the specified tracking group.

#### ▾ Enabling the Downlink Delay Up for a Link State Tracking Group

<b>Command</b>	<b>link state track num up-delay timer</b>
<b>Parameter Description</b>	<i>num</i> : Indicates the ID of a link state tracking group. <i>Timer</i> : Indicates the downlink delay up time, which is 0s by default.
<b>Command Mode</b>	Configuration mode
<b>Usage Guide</b>	You must enable the delay function so that the downstream link can be up after the delay.

#### ▾ Adding an interface to a Link Tracking Group

<b>Command</b>	<b>ink stategroup num {upstream   downstream}</b>
<b>Parameter Description</b>	<i>num</i> : Indicates the ID of a link state tracking group. <b>upstream</b> : Adds the interface as an upstream interface of the tracking group. <b>downstream</b> : Adds the interface as a downstream interface of the tracking group.

<b>Command Mode</b>	Interface configuration mode
<b>Usage Guide</b>	You can create a link tracking group and then add an interface to the specified tracking group.

## Configuration Example

### Configuring a Link Tracking Group

<b>Scenario</b>	As shown in <b>Figure 1-6</b> , there are two upstream links from switch D to switch A, which are switch D > switch B > switch A and switch D > switch C > switch A. There are two upstream links from switch E to switch A, which are switch E > switch B > switch A and switch E > switch C > switch A.
<b>Configuration Steps</b>	<ul style="list-style-type: none"> <li>● Create link tracking group 1 on switch B (C).</li> <li>● On switch B (C), add the interfaces Gi0/1 and Gi0/2 as downstream interfaces of the link tracking group and add the interface Gi0/3 as an upstream interface of the link tracking group.</li> </ul>
<b>B</b>	<pre>SwitchB&gt; enable SwitchB# configure terminal SwitchB(config)# link state track 1 SwitchB(config)# interface GigabitEthernet 0/1 SwitchB(config-if-GigabitEthernet 0/1)#link state group 1 downstreamSwitchB(config-if-GigabitEthernet 0/1)#exit SwitchB(config)# interface GigabitEthernet 0/2 SwitchB(config-if-GigabitEthernet 0/2)# link state group 1 downstream SwitchB(config-if-GigabitEthernet 0/2)#exit SwitchB(config)# interface GigabitEthernet 0/3 SwitchB(config-if-GigabitEthernet 0/3)#link state group 1 upstream SwitchB(config-if-GigabitEthernet 0/3)#exit</pre>
<b>C</b>	<pre>SwitchC&gt; enable SwitchC# configure terminal SwitchC(config)# link state track 1 SwitchC(config)# interface GigabitEthernet 0/1 SwitchC(config-if-GigabitEthernet 0/1)#link state group 1 downstreamSwitchC(config-if-GigabitEthernet 0/1)#exit SwitchC(config)# interface GigabitEthernet 0/2 SwitchC(config-if-GigabitEthernet 0/2)# link state group 1 downstream SwitchC(config-if-GigabitEthernet 0/2)#exit SwitchC(config)# interface GigabitEthernet 0/3</pre>

	<pre>SwitchC(config-if-GigabitEthernet 0/3)#link state group 1 upstream SwitchC(config-if-GigabitEthernet 0/3)#exit</pre>
<b>Verification</b>	Check the link tracking group information configured for switch B (C).
<b>B</b>	<pre>SwitchB#show link state group Link State Group:1  Status: enabled, Down Upstream Interfaces :Gi0/3(Down) Downstream Interfaces : Gi0/2(Down)</pre>

## Common Errors


- Interfaces are added to a link tracking group when the link tracking group is not enabled.

## 1.5 Monitoring

### Displaying

Description	Command
Displays the dual link backup information of REUP.	<b>show interfaces</b> [ <i>interface-id</i> ] <b>switchport backup</b> [ <b>detail</b> ]
Displays the configurations of an MAC address update group.	<b>show mac-address-table update group</b> [ <b>detail</b> ]
Displays the REUP statistics about sent MAC address update messages.	<b>show mac-address-table move update</b>
Displays the information about a link state tracking group.	<b>show link state group</b>

### Debugging

-  System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Enables all REUP debugging.	<b>debug reup all</b>
Debugs the normal running process of REUP.	<b>debug reup process</b>
Debugs MAC address update messages of REUP.	<b>debug reup packet</b>
Debugs MAC address update packets of REUP.	<b>debug reup macupdt</b>

Description	Command
Debugs hot backup.	<b>debug reup ha</b>
Debugs errors occurring in REUP running.	<b>debug reup error</b>
Debugs received events.	<b>debug reup evnet</b>
Debugs statistics when <b>show</b> operations are performed.	<b>debug reup status</b>

## 2 Configuring RLDP

### 2.1 Overview

The Rapid Link Detection Protocol (RLDP) achieves rapid detection of unidirectional link failures, directional forwarding failures and downlink loop failures of an Ethernet. When a failure is found, relevant ports will be closed automatically according to failure treatment configuration or the user will be notified to manually close the ports to avoid wrong flow forwarding or an Ethernet layer-2 loop.

### 2.2 Applications

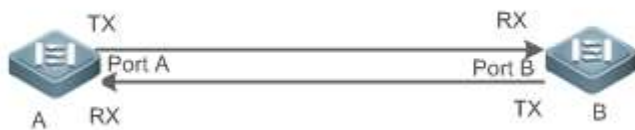
Application	Description
<a href="#">Unidirectional Link Detection</a>	Detect a unidirectional link failure.
<a href="#">Bidirectional Forwarding Detection</a>	Detect a bidirectional link failure.
<a href="#">Downlink Loop Detection</a>	Detect a link loop.

#### 2.2.1 Unidirectional Link Detection

##### Scenario

As shown in the following figure, A is connected to B via optical fiber. The two lines are the Tx and Rx lines of optical fiber. Unidirectional link detection is enabled on A and B. If any of the Tx of Port A, Rx of Port B, Tx of Port B and Rx of Port A fails, a unidirectional failure will be detected and treated under the RLDP. If the failure is eliminated, the administrator may manually restore the RLDP on A and B and resume detection.

Figure 2-1



<b>Remarks</b>	A and B are layer-2 or layer-3 switches. The Tx of Port A of A is connected to the Rx of Port B of B. The Rx of Port A of A is connected to the Tx of Port B of B.
----------------	--

##### Deployment

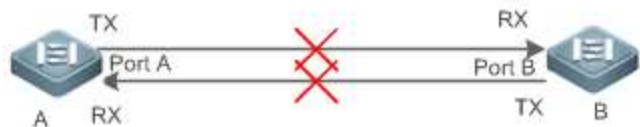
- Global RLDP is enabled.
- Configure unidirectional link detection under Port A and Port B and define a method for failure treatment.

## 2.2.2 Bidirectional Forwarding Detection

### Scenario

As shown in the following figure, A is connected to B via optical fiber, and the two lines are Tx and Rx lines of optical fiber. Unidirectional link detection is enabled on A and B. If the Tx of Port A, Rx of Port B, Rx of Port A and Tx of Port B all fail, a bidirectional failure will be detected and treated under the RLDP. If the failure is eliminated, the administrator may manually restore the RLDP on A and B and resume detection.

Figure 2-2



<b>Remarks</b>	A and B are layer-2 or layer-3 switches. The Tx of Port A of A is connected to the Rx of Port B of B. The Rx of Port A of A is connected to the Tx of Port B of B.
----------------	--

### Deployment

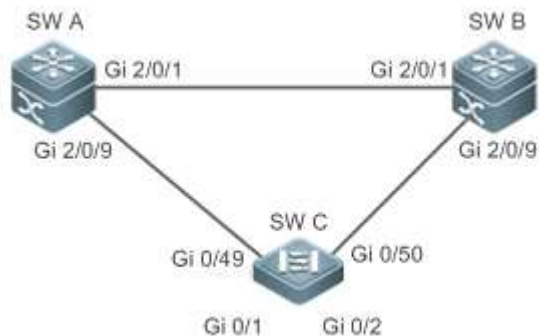
- Global RLDP is enabled.
- Configure BFD under Port A and Port B and define a method for failure treatment.

## 2.2.3 Downlink Loop Detection

### Scenario

As shown in the following figure, A, B and C are connect into a loop. Downlink loop detection is enabled on A, and a loop is detected and treated.

Figure 2-3



<b>Remarks</b>	A, B and C are layer-2 or layer-3 switches. A, B and C are interconnected via exchange ports.
----------------	--

### Deployment

- Global RLDP is enabled on A.
- Configure downlink loop detection on the Gi 2/0/1 and Gi 2/0/9 ports of A, and define a method for failure treatment.

## 2.3 Features

Most Ethernet link detection mechanisms detect link connectivity through automatic physical-layer negotiation. However, in some cases devices are connected on the physical layer and operate normally but layer-2 link communication is disabled or abnormal. The RLDP recognizes a neighbor device and detects a link failure through exchanging Prob packets, Echo packets or Loop packets with the device.

### Basic Concepts

---

#### ↘ Unidirectional Link Failure

A unidirectional link failure occurs in case of a cross-connected optical fiber, a disconnected optical fiber, an open-circuit optical fiber, one open-circuit line in a twisted-pair cable, or unidirectional open circuit of an intermediate device between two devices. In such cases, one end of a link is connected and the other disconnected so that flow is forwarded wrongly or a loop guard protocol (for example, the STP) fails.

#### ↘ Bidirectional Link Failure

A bidirectional link failure occurs in case of two optical fibers, two open-circuit lines in a twisted-pair cable, or bidirectional open circuit of an intermediate device between two devices. In such cases, the both ends of a link are disconnected so that flow is forwarded wrongly.

#### ↘ Loop Failure

A downlink device is wrongly connected to form a loop, resulting in a broadcast storm.

#### ↘ RLDP Packet

The RLDP defines three types of packets: Prob packets, Echo packets and Loop packets.

- Prob packets are layer-2 multicast packets for neighbor negotiation, and unidirectional or bidirectional link detection. The default encapsulation format is SNAP, which changes automatically to EthernetII if a neighbor sends EthernetII packets.
- Echo packets are layer-2 unicast packets as response to Prob packets and used for unidirectional or bidirectional link detection. The default encapsulation format is SNAP, which changes automatically to EthernetII if a neighbor sends EthernetII packets.
- Loop packets are layer-2 multicast packets for downlink loop detection. They can only be received. The default encapsulation format is SNAP.

#### ↘ RLDP Detection Interval and Maximum Detection Times

A detection interval and the maximum detection times can be configured for the RLDP. A detection interval determines the period of sending Prob packets and Loop packets. When a device receives a Prob packet, it replies with an Echo packet

immediately. A detection interval and the maximum detection times determine the maximum detection time (equal to a detection interval  $\times$  the maximum detection times + 1) for unidirectional or bidirectional link detection. If neither Prob nor Echo packet from a neighbor can be received within the maximum detection time, the treatment of unidirectional or bidirectional failure will be triggered.

### ↘ **RLDP Neighbor Negotiation**

When configured with unidirectional or bidirectional link detection, a port can learn a peer-end device as its neighbor. One port may learn one neighbor, which is variable. If negotiation is enabled, unidirectional or bidirectional link detection starts after a port finds a neighbor through negotiation, which succeeds when a port receives a Prob packet from the neighbor. However, if the RLDP is enabled under a failure, the port cannot learn a neighbor so that detection cannot start. In this case, recover the link state before enabling the RLDP.

### ↘ **Treatment for Failed Port under RLDP**

- Warning: Only print Syslog to indicate a failed port and a failure type.
- Shutdown SVI: Print Syslog, and then inquire an SVI according to the Access VLAN or Native VLAN of a port and shut down the SVI if the port is a physical exchange port or layer-2 AP member port.
- Port violation: Print Syslog, and configure a failed port as in violation state, and the port will enter Linkdown state physically.
- Block: Print Syslog, and configure the forward state of a port as Block, and the port will not forward packets.

### ↘ **Recovery of Failed Port under RLDP**

- Manual reset: Manually reset all failed ports to initialized state and restart link detection.
- Manual or automatic errdisable recovery: Recover all failed ports to initialized state manually or regularly (30s by default and configurable) and restart link detection.
- Automatic recovery: Under unidirectional or bidirectional link detection, if the treatment for failed ports is not specified as port violation, recover ports to initialized state based on Prob packets and restart link detection.

### ↘ **Port State under RLDP**

- normal: Indicates the state of a port after link detection is enabled.
- error: Indicates the state of a port after a unidirectional or bidirectional link failure or a loop failure is detected.

### ↘ **Overview**

Feature	Description
<a href="#">Deploying RLDP Detection</a>	Enable unidirectional or bidirectional link detection or downlink loop detection for failures and implement treatment.

## 2.3.1 Deploying RLDP Detection

The RLDP provides unidirectional link detection, bidirectional forwarding detection and downlink loop detection.



## Working Principle

### Unidirectional Link Detection

When this function is enabled, a port sends Prob packets and receives Echo packets from a neighbor regularly as well as receiving Prob packets from a neighbor and replying with Echo packets. Within the maximum detection time, if the port receives Prob packets but no Echo packets, or none of them, treatment for a unidirectional failure will be triggered and detection will stop.

### Bidirectional Forwarding Detection

When this function is enabled, a port sends Prob packets and receives Echo packets from a neighbor regularly as well as receiving Prob packets from a neighbor and replying with Echo packets. Within the maximum detection time, if the port receives neither Prob packets nor Echo packets from a neighbor, treatment for a bidirectional failure will be triggered and detection will stop.

### Downlink Loop Detection

When this function is enabled, a port sends Loop packets regularly. In the following cases, a loop failure will be triggered after the same port or a different port receives the packets: in one case, the egress and ingress ports are the same routed port or layer-3 AP member port; in another case, the egress and ingress ports are exchange ports or layer-2 AP member ports in a same default VLAN and in Forward state. Treatment for the failure will be implemented and detection will stop.

## Related Configuration



- Configuring RLDP Detection



By default, RLDP detection is disabled.

You may run the global command **rldp enable** or the interface command **rldp port** to enable RLDP detection and specify a detection type and treatment.

You may run the **rldp neighbor-negotiation** command to neighbor negotiation, the **rldp detect-interval** to specify a detection interval, the **rldp detect-max** to specify detection times, or the **rldp reset** to recover a failed port.

## 2.4 Configuration

Configuration	Description and Command
<a href="#">Configuring Basic RLDP Functions</a>	 (Mandatory) It is used to enable RLDP detection under global configuration mode.
	<b>rldp enable</b> Enables global RLDP detection on all ports.
	 (Mandatory) It is used to specify under interface configuration mode a detection type and failure treatment for an interface.
<b>rldp port</b> Enables RLDP detection on a port and specifies a detection type and failure treatment.	

 (Optional) It is used to configure a detection interval, detection times and neighbor negotiation under global configuration mode.	
<b>rldp detect-interval</b>	Modifies global RLDP parameters on all ports, such as the detection interval, maximum detection times and neighbor negotiation.
<b>rldp detect-max</b>	
<b>rldp neighbor-negotiation</b>	
 (Optional) It is used under privileged mode.	
<b>rldp reset</b>	Recovers all ports.

## 2.4.1 Configuring Basic RLDP Functions

### Configuration Effect

- Enable RLDP unidirectional link detection, bidirectional forwarding detection, or downlink loop detection to discover failures.

### Notes

- Loop detection is effective to all member ports of an AP when configured on one of the ports. Unidirectional link detection and bidirectional forwarding detection are effective only on an AP member port.
- The loop detection on a physical port added to an AP shall be configured the same as that of the other member ports. There are three cases. First, if loop detection is not configured on a newly-added port but on the existing member ports, the new port adopts the configuration and detection results of the existing ports. Second, if loop detection is configured on a newly-added port but not on the existing member ports, the new port clears loop detection and joins the AP. Third, if a newly-added port and the existing member ports have different loop detection configuration, the new port adopts the configuration and detection results of the existing ports.
- When configuring the RLDP on an AP port, you may configure failure treatment only as "shutdown-port", to which other configurations will be modified.
- When "shutdown-port" is configured on a port, RLDP detection cannot be restored in case of a failure. After troubleshooting, you may run the **rldp reset** or **errdisable recovery** command to restore the port and resume detection. For configuration of the **errdisable recovery** command, please refer to the *SWITCH-INTF-SCG.doc*.

### Configuration Steps

#### ↘ Enabling RLDP

- Mandatory.
- Enable RLDP detection on all ports under global configuration mode.

#### ↘ Enabling Neighbor Negotiation

- Optional.
- Enable the function under global configuration mode, and port detection will be started under successful neighbor negotiation.

#### ↘ **Configuring Detection Interval**

- Optional.
- Specify a detection interval under global configuration mode.

#### ↘ **Configuring Maximum Detection Times**

- Optional.
- Specify the maximum detection times under global configuration mode.

#### ↘ **Configuring Detection under Port**

- Mandatory.
- Configure unidirectional RLDP detection, bidirectional RLDP detection or downlink loop detection under interface configuration mode, and specify failure treatment.

#### ↘ **Restoring All Failed Ports**

- Optional.
- Enable this function under privileged mode to restore all failed ports and resume detection.

### Verification

- Display the information of global RLDP, port and neighbor.

### Related Commands

#### ↘ **Enabling Global RLDP Detection**

<b>Command</b>	<b>rldp enable</b>
<b>Parameter</b>	N/A
<b>Description</b>	
<b>Command Mode</b>	Global configuration mode
<b>Usage Guide</b>	Enable global RLDP detection.

#### ↘ **Enabling RLDP Detection on Interface**

<b>Command</b>	<b>rldp port { unidirection-detect   bidirection-detect   loop-detect } { warning   shutdown-svi   shutdown-port   block }</b>
<b>Parameter</b>	<b>unidirection-detect:</b> Indicates unidirectional link detection.
<b>Description</b>	<b>bidirection-detect:</b> Indicates bidirectional forwarding detection.

	<p><b>loop-detect:</b> Indicates downlink loop detection.</p> <p><b>warning:</b> Indicate the failure treatment is warning.</p> <p><b>shutdown-svi:</b> Indicate the failure treatment is closing the SVI that the interface is on.</p> <p><b>shutdown-port:</b> Indicates the failure treatment is port violation.</p> <p><b>block:</b> Indicates the failure treatment is disabling learning and forwarding of a port.</p>
<b>Command Mode</b>	Interface configuration mode
<b>Usage Guide</b>	The interfaces include layer-2 switch ports, layer-3 routed ports, layer-2 AP member ports, and layer-3 AP member ports.

### ↘ Modifying Global RLDP Detection Parameters

<b>Command</b>	<b>rldp {detect-interval <i>interval</i>   detect-max <i>num</i>   neighbor-negotiation }</b>
<b>Parameter Description</b>	<p><b>detect-interval <i>interval</i>:</b> Indicates a detection interval.</p> <p><b>detect-max <i>num</i>:</b> Indicates detection times.</p> <p><b>neighbor-negotiation:</b> Indicates neighbor negotiation.</p>
<b>Command Mode</b>	Global configuration mode
<b>Usage Guide</b>	Modify all RLDP parameters on all ports when necessary.

### ↘ Recovering Failed Port

<b>Command</b>	<b>rldp reset</b>
<b>Parameter Description</b>	N/A
<b>Command Mode</b>	Privileged mode
<b>Usage Guide</b>	Recover all failed ports to initialized state and resume detection.

### ↘ Displaying RLDP State Information

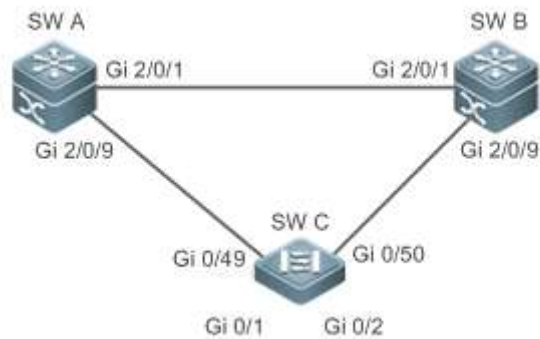
<b>Command</b>	<b>show rldp [ interface <i>interface-name</i> ]</b>
<b>Parameter Description</b>	<i>interface-name</i> : Indicates the interface to display information of.
<b>Command Mode</b>	Privileged mode, global configuration mode, or interface configuration mode
<b>Usage Guide</b>	Display RLDP state information.

## Configuration Example

### ↘ Enabling RLDP Detection in Ring Topology

<b>Scenario Figure 2-4</b>	As shown in the following figure, the aggregation and access sections are in a ring topology. The STP is enabled on all devices to prevent loop and provide redundancy protection. To avoid a unidirectional or bidirectional link failure resulting in STP failure, RLDP unidirectional and bidirectional link detection is enabled between aggregation devices as well as between an aggregation device and the access device.
----------------------------	--

To avoid loop due to wrong downlink connection of the aggregation devices, enable RLDP downlink loop detection on the downlink ports of the aggregation devices and of the access device. To avoid loop due to wrong downlink connection of the access device, enable RLDP downlink loop detection on the downlink ports of the access device.



**Configuration Steps**

- SW A and SW B are aggregation devices, and SW C is an access device. Users connected to SW C. SW A, SW B and SW C are structured in a ring topology, and the STP is enabled on each of them. For STP configuration, refer to relevant configuration guide.
- Enable the RLDP on SW A, enable unidirectional and bidirectional link detection on the two ports, and enable loop detection on the downlink port.
- Enable the RLDP on SW B, enable unidirectional and bidirectional link detection on the two ports, and enable loop detection on the downlink port.
- Enable the RLDP on SW C, enable unidirectional and bidirectional link detection on the two uplink ports, and enable loop detection on the two downlink ports.

**A**

```

A#configure terminal
A(config)#rldp enable
A(config)#interface GigabitEthernet 2/0/1
A(config-if-GigabitEthernet 2/0/1)#rldp port unidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#rldp port bidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)# exit
A(config)#interface GigabitEthernet 2/0/9
A(config-if-GigabitEthernet 2/0/1)#rldp port unidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#rldp port bidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#rldp port loop-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#exit
  
```

**B**

Apply the configuration on SW A.

**C**

```

C#configure terminal
C(config)#rldp enable
  
```

```

C(config)#interface GigabitEthernet 0/49
C(config-if-GigabitEthernet 0/49)#rldp port unidirection-detect shutdown-port
C(config-if-GigabitEthernet 0/49)#rldp port bidirection-detect shutdown-port
C(config-if-GigabitEthernet 0/49)# exit
C(config)#interface GigabitEthernet 0/50
C(config-if-GigabitEthernet 0/50)#rldp port unidirection-detect shutdown-port
C(config-if-GigabitEthernet 0/50)#rldp port bidirection-detect shutdown-port
C(config-if-GigabitEthernet 0/50)#exit
C(config)#interface GigabitEthernet 0/1
C(config-if-GigabitEthernet 0/1)# rldp port loop-detect shutdown-port
C(config-if-GigabitEthernet 0/1)#exit
C(config)#interface GigabitEthernet 0/2
C(config-if-GigabitEthernet 0/2)# rldp port loop-detect shutdown-port
C(config-if-GigabitEthernet 0/2)#exit

```

**Verification**

- Check the RLDP information on SW A, SW B and SW C. Take SW A for example.

**A**

```

A#show rldp
rldp state          : enable
rldp hello interval: 3
rldp max hello      : 2
rldp local bridge   : 00d0.f822.33aa
-----
Interface GigabitEthernet 2/0/1
port state          : normal
neighbor bridge    : 00d0.f800.51b1
neighbor port      : GigabitEthernet 2/0/1
unidirection detect information:
    action: shutdown-port
    state  : normal
bidirection detect information:
    action: shutdown-port
    state  : normal

Interface GigabitEthernet 2/0/9

```

```

port state      : normal

neighbor bridge : 00d0.f800.41b0

neighbor port   : GigabitEthernet 0/49

unidirection detect information:

    action: shutdown-port

    state : normal

bidirection detect information:

    action: shutdown-port

    state : normal

loop detect information:

    action: shutdown-port

    state : normal

```

## Common Errors

- RLDP functions and private multicast address authentication or TPP are enabled at the same time.
- Neighbor negotiation is not enabled when configuring unidirectional or bidirectional link detection. The RLDP should be enabled on a neighbor device, or otherwise a unidirectional or bidirectional failure will be detected.
- If RLDP detection is configured to be implemented after neighbor negotiation while configuring unidirectional or bidirectional link detection, detection cannot be implemented as no neighbor can be learned due to a link failure. In this situation, you are suggested to recover the link state first.
- You are suggested not to specify the failure treatment as Shutdown SVI under a routed port.
- You are suggested not to specify the failure treatment as Block for a port, on which a loop protection protocol is enabled, for example, the STP.

## Common Errors

- When the **exec-cmd** command is executed for interface configuration, the input of the corresponding AP wired port is incorrect.
- When the RLDP loop detection configurations are modified, the **no exec-cmd** command is not executed to delete the original configurations or the **exec-cmd** command is not re-executed to cancel the configurations.

## 2.5 Monitoring

### Displaying

Description	Command
Displays RLDP state.	<b>show rldp [ interface <i>interface-name</i> ]</b>

## 3 Configuring IP Event Dampening


### 3.1 Overview

When the Layer-3 port on a Layer-3 device frequently goes Up and Down due to manual enabling/disabling or other external causes, the routing table on the device will flap repeatedly. If a routing protocol is configured, the protocol may propagate the flap to the entire network, causing repeated updates and recalculation of neighboring routes, which wastes network bandwidths and destabilizes the network. Repeated route updates and recalculation on devices consume many CPU resources, which affects the normal running of customer networks.

IP Event Dampening detects abnormal Up/Down flapping and automatically suppresses frequent port state changes, which prevents the propagation of single-point link failures by a routing protocol. When the port is restored, it will be automatically unsuppressed, thus reducing network flaps and CPU resource consumption while improving network stability.

#### Protocols and Standards

- RFC2439: BGP Route Flap Dampening

 At its core, the suppression algorithm used by IP Event Dampening is the same as that used by BGP Route Flap Dampening.

### 3.2 Applications

Application	Description
<a href="#">Routed Port Flap Dampening</a>	Monitors the state change of the Layer-3 port on a router, and suppresses frequent port flapping.

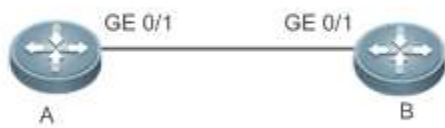
#### 3.2.1 Routed Port Flap Dampening

##### Scenario

In a network that runs a routing protocol, when a port on a router connected to another router frequently goes Up and Down, neighboring routes will be repeatedly updated and recalculated. The routing protocol may propagate the flap to the entire network, causing a network flap. IP Event Dampening can be enabled on the connected routers to monitor port state changes and suppress frequent port flapping, thus reducing network flaps and CPU resource consumption while improving network stability.



Figure 6-7



<b>Remarks</b>	A and B are routers.
----------------	----------------------

## Deployment

Configure IP Event Dampening on portGE0/1 on Router A and portGE0/1 on Router B respectively.

 The subinterfaces and the virtual templates of interfaces on routers do not support the dampening feature.

## 3.3 Features

### Basic Concepts

#### ↳ Penalty

A port that goes Up or Down gets a penalty for each state change, but the penalty decays exponentially when the port is stable. In this way, port behaviors can be sensed and controlled intelligently.

#### ↳ Suppress Threshold

When the cumulative penalty of a port exceeds a suppress threshold, the port is considered to flap and will be suppressed.

#### ↳ Half-Life Period

The half-life period is the period required for the penalty to decrease to half of the original value when the port is stable. It defines the speed at which the penalty decays exponentially. The shorter the half-life period, the faster the penalty decays, and the faster the port is detected to be stable, but the flap detection sensitivity is reduced.

#### ↳ Reuse Threshold

When the port no longer flaps and its penalty decays to a certain degree (below the suppress threshold), the port is considered to be stable and is unsuppressed.

#### ↳ Maximum Suppress Time

When a port keeps flapping and reaches a very large penalty, the port will not be usable for a long time. To avoid this problem, the maximum suppress time is defined to always maintain the port suppression duration below a certain value no matter how long the port has flapped.

### Overview

Feature	Description
<a href="#">Port Flap Suppression</a>	Configure the criteria and parameters of flap suppression on ports to enable switches or routers to identify and suppress frequently flapping ports, which ensures route stability and avoids route flap propagation.

### 3.3.1 Port Flap Suppression

#### Working Principle

A port configured with IP Event Dampening is assigned a penalty. The port gets a penalty of 1,000 each time when it goes Down, but the penalty decreases with time. If the port goes Down again, the penalty increases accordingly. When the cumulative penalty exceeds the suppress threshold, the port will be suppressed. For the affected upper-layer protocol, the suppressed port is always Down no matter what the actual port state is. When the penalty decreases to the reuse threshold, the port will be unsuppressed, and the upper-layer protocol can sense the actual port state.

If a Layer-3 port is not configured with IP Event Dampening, or is not suppressed by it, the routing protocol or other protocol concerned about the port status still work normally. When the port is suppressed, the upper-layer protocol considers the port to be Down. Any state change of the port before the port is unsuppressed does not affect the routing table and the route calculation and advertisement performed by the upper-layer routing protocol.

#### Related Configuration

##### ▾ [Configuring IP Event Dampening](#)

- By default, IP Event Dampening is disabled on Layer-3 ports.
- Run the **dampening** [ *half-life-period* [ *reuse-threshold* *suppress-threshold* *max-suppress* [ **restart** [ *restart-penalty* ] ] ] command to enable or disable IP Event Dampening on Layer-3 ports.

## 3.4 Configuration

Configuration	Description and Command
<a href="#">Enabling IP Event Dampening</a>	 (Mandatory) It is used to suppress Layer-3 port flapping.
	<b>dampening</b> Configures IP Event Dampening.

### 3.4.1 Enabling IP Event Dampening

#### Configuration Effect

When a port configured with IP Event Dampening keeps flapping until the predefined threshold is exceeded, the port is set to Down.

#### Notes

- When a Layer-3 port on a switch is converted to a Layer-2 port (for example, from a routed port to a switch port), the IP Event Dampening configuration on the port will be deleted.

- Only the main interface on a router can be configured with IP Event Dampening. The configuration takes effect for all subinterfaces of the main interface, but you cannot run the **dampening** command directly on subinterfaces and virtual templates.

## Configuration Steps

### ▾ Configuring IP Event Dampening

- Mandatory.
- Perform the configuration in Layer-3 interface configuration mode.
- You can specify the half-life period, reuse threshold, suppress threshold, maximum suppress time, and initial penalty. If you do not set these parameters, their default values will be used.

## Verification

Use any one of the following commands to check whether the configuration takes effect:

- **show running-config**
- **show interfaces [ interface-id ] dampening**, which is used to check the IP Event Dampening configuration on a specified port

## Related Commands

### ▾ Enabling IP Event Dampening on a Port


<b>Command</b>	<b>dampening</b> [ <i>half-life-period</i> [ <i>reuse-threshold</i> <i>suppress-threshold</i> <i>max-suppress</i> [ <b>restart</b> [ <i>restart-penalty</i> ] ] ] ]
<b>Parameter Description</b>	<p><i>half-life-period</i>: Indicates the half-life period. Value range: &lt;1–30&gt;; default value: 5s.</p> <p><i>reuse-threshold</i>: Indicates the reuse threshold. Value range: &lt;1–20,000&gt;; default value: 1,000.</p> <p><i>suppress-threshold</i>: Indicates the suppress threshold. Value range: &lt;1–20,000&gt;; default value: 2,000.</p> <p><i>max-suppress</i>: Indicates the maximum suppress time. Value range: &lt;1–255&gt;; default value: four times the half-life period.</p> <p><b>restart</b> <i>restart-penalty</i>: Indicates the initial penalty. Value range: &lt;1–20,000&gt;; default value: 2,000.</p>
<b>Command Mode</b>	Interface configuration mode
<b>Usage Guide</b>	<p>IP Event Dampening can affect direct routes, host routes, static routes, dynamic routes, and VRRP. When a port is suppressed based on the configured criteria, the affected modules determine that the port is Down and therefore delete corresponding routes. No data packet will be transmitted through the port.</p> <p>When the <b>dampening</b> command is rerun on a port configured with IP Event Dampening, the dampening information on the port will be cleared, but the flap count is retained, unless you use the <b>clear counters</b> command to clear the counters on the port.</p> <p>If the <b>max-suppress</b> parameter is set to a very small value, making the maximum penalty smaller than the suppress threshold, the port will never be suppressed. When such a configuration error occurs, the following message indicating a configuration failure will be printed:</p> <pre>% Maximum penalty (10) is less than suppress penalty (2000). Increase maximum suppress time</pre>

If the available system memory is insufficient to run the **dampening** command, the following message indicating a configuration failure will be printed:

```
% No memory, configure dampening fail!
```

## Configuration Example

### Configuring IP Event Dampening on Layer-3 Ports

<b>Scenario</b> <b>Figure 6-8</b>	
<b>Configuration Steps</b>	Enable IP Event Dampening on port GigabitEthernet 0/1 on Router A and on port GigabitEthernet 0/1 on Router B respectively, and set <b>half-time-period</b> to 30s, <b>reuse-threshold</b> to 1,500, <b>suppress-threshold</b> to 10,000, and <b>max-suppress</b> to 120s.
<b>A</b>	<pre>Orion Alpha A28X(config)#interface GigabitEthernet 0/1 Orion Alpha A28X(config-if-GigabitEthernet 0/1)#dampening 30 1500 10000 100</pre>
<b>B</b>	<pre>Orion Alpha A28X(config)#interface GigabitEthernet 0/1 Orion Alpha A28X(config-if-GigabitEthernet 0/1)#dampening 30 1500 10000 100</pre>
<b>Verification</b>	Run the <b>show interfaces dampening</b> command to check the IP Event Dampening configuration on the corresponding ports.
	<pre>Orion Alpha A28X#show interfaces dampening GigabitEthernet 0/1    Flaps Penalty Supp   ReuseTm HalfL   ReuseV  SuppV  MaxSTm  MaxP   Restart   0      0      FALSE  0      30      1500   1000   100    15119  0</pre>


## Common Errors

- The port on a Layer-3 switch is not converted to a routed port by using the **no swithport** command before IP Event Dampening is configured.

## 3.5 Monitoring

### Clearing

Description	Command
Clears the interface counters.	<b>clear counters</b>

 For details about the **clear counter** command, see the related chapter for the "Interface" command.


## Displaying

---

Description	Command
Displays the counters on suppressed ports.	<b>show dampening interface</b>
Displays the IP Event Dampening configuration on ports.	<b>show interfaces dampening</b>

## Debugging

---

 System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Enables debugging of IP Event Dampening.	<b>debug dampening interface</b>

