

16 Reliability

This topic describes reliability features implemented by the system.

16.1 Reliability Solution Overview

The OLT provides a comprehensive reliability solution, including uplink protection, device protection, and PON downlink protection, enhancing reliability of the entire network.

16.2 xPON Type B Protection

xPON type B protection allows dual-channel redundancy protection for OLT PON ports and backbone fibers on a xPON network. This feature improves ODN network reliability and ensures service continuity.

16.3 xPON Type C Protection

The xPON type C protection switching is implemented through the redundancy configuration of the two PON ports on the ONU, backbone optical fiber, optical splitter, and tributary optical fiber on a xPON network. Each item is in a dual configuration. The protection improves the reliability on the optical distribution network (ODN) and prevents service interruption.

16.4 Redundancy Backup of Control Boards

An OLT configured with two control boards works in the load sharing mode. When working normally, the active and standby control boards concurrently forward service packets.

16.5 Ethernet Port Protection Group

An Ethernet port protection group binds two or more Ethernet ports together. The working port carries services, while the protection port provides backup and does not carry services. If the working port is faulty, the services carried by it are switched to the protection port, automatically or manually as required. Ethernet port protection ensures uninterrupted service transmission and improves reliability of links.

16.6 Ethernet Link Aggregation

Ethernet link aggregation is a process that aggregates two or more Ethernet ports of the same type to a logic port. It increases the link bandwidth without requiring a hardware upgrade and improves link reliability using the link backup mechanism.

16.7 MSTP

The Multiple Spanning Tree Protocol (MSTP) is compatible with STP and RSTP.

16.8 ERPS

Ethernet ring protection switching (ERPS) is a ring network protocol defined in Recommendation ITU-T G.8032. Interoperation is achieved if all devices participating in the ring network support ERPS. On a network composed of ERPS-supporting devices, the service protection solution with quick switching can be implemented using a small number of links.

16.9 VRRP Snooping

VRRP is a fault-tolerant protocol. It allows multiple routers to form a virtual routing device, and provides a mechanism, which ensures that services will be taken over in time by another device once the next hop of a host fails. In this way the continuity and reliability of communication are ensured. VRRP snooping is to snoop (or listen for) VRRP packets.

16.10 Ring Check

The ring check feature is mainly used to detect the user-side, cascade-side, and network-side ring networks, and eliminate the user-side ring network.

16.11 Monitor Link

A monitor link group is composed of one uplink and several downlinks. It is used to monitor the fault of uplinks.

16.1 Reliability Solution Overview

The OLT provides a comprehensive reliability solution, including uplink protection, device protection, and PON downlink protection, enhancing reliability of the entire network.

To ensure reliability of the access network, the OLT supports the following end-to-end (E2E) reliability solution.

Figure 16-1 Reliability scheme in an access network

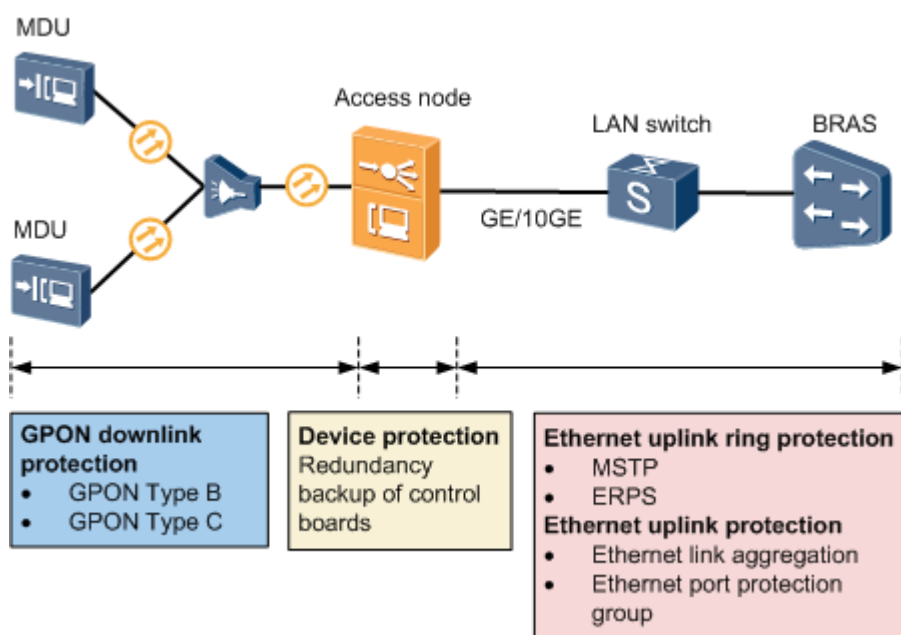


Figure 16-2 Reliability scheme in an access network

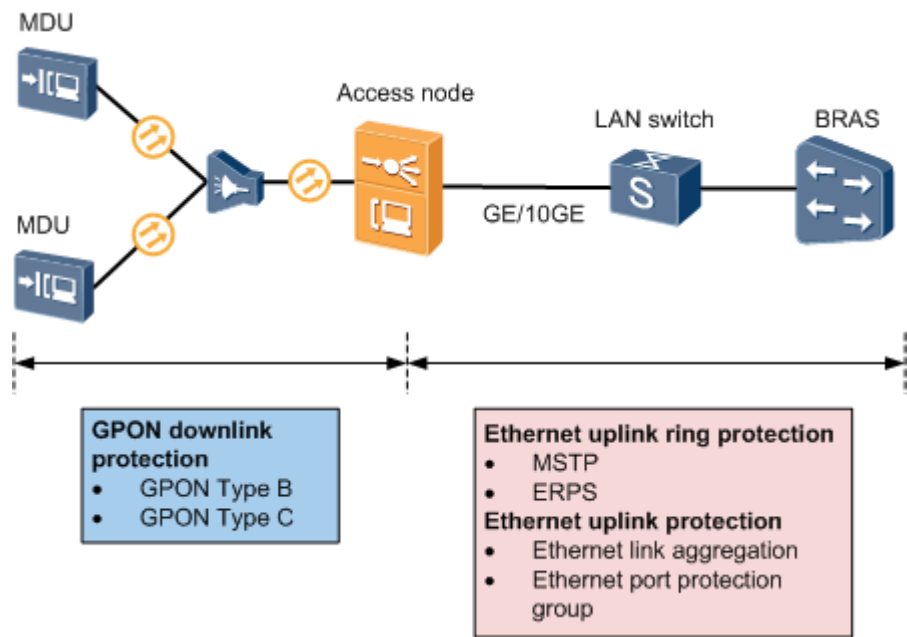


Table 16-1 Reliability scheme

Protected Object	Protection Scheme	Hua wei Pro pri etary Prot ocol or Not	Function and Feature
Device hardware	Redundancy backup of control boards	No	An Ethernet port protection group can be configured only after active/standby redundancy backup of control boards is configured. The load-sharing mode doubles bandwidths and improves data forwarding performance of the device.
Ethernet uplinks or cascade links	Ethernet link aggregation • Manual aggregatio n • LACP aggregatio n	No	Increases uplink bandwidths, achieving load sharing. Members in the aggregation group back up for each other, enhancing uplink reliability. Manual aggregation is required if the OLT is connected to a device that does not support LACP.
	Ethernet port protection group	No	Supports uplink port protection, which can be used with Ethernet link aggregation.

Protected Object	Protection Scheme	Huawei Proprietary Protocol or Not	Function and Feature
Ethernet uplink ring protection	MSTP	No	MSTP prunes a loop network to a loop-free tree network to avoid proliferation and infinite loop of packets in the loop network. MSTP is compatible with STP and RSTP. Furthermore, MSTP remedies drawbacks of STP and RSTP. The convergence time is subject to the network topology.
	ERPS	No	ERPS is a ring network protocol defined in Recommendation ITU-T G.8032. Interoperation is achieved if all devices participating in the ring network support ERPS. In addition, ERPS supports fast convergence, meeting carrier-class reliability requirements.
GPON downlink protection	GPON type B	No	Type B provides redundancy for OLT's GPON ports and feeder fiber. Compared with type C, type B requires a lower cost but the implementation is more difficult. NOTE When the number of ONTs/ONUs connected to a board exceeds 1000, you are advised to configure inter-board Type B protection.
	GPON type C	Yes	Type C provides redundancy for ONU's GPON ports, feeder fibers, splitters, and distribution fibers. Compared with type B, type C provides higher reliability.

16.2 xPON Type B Protection

xPON type B protection allows dual-channel redundancy protection for OLT PON ports and backbone fibers on a xPON network. This feature improves ODN network reliability and ensures service continuity.

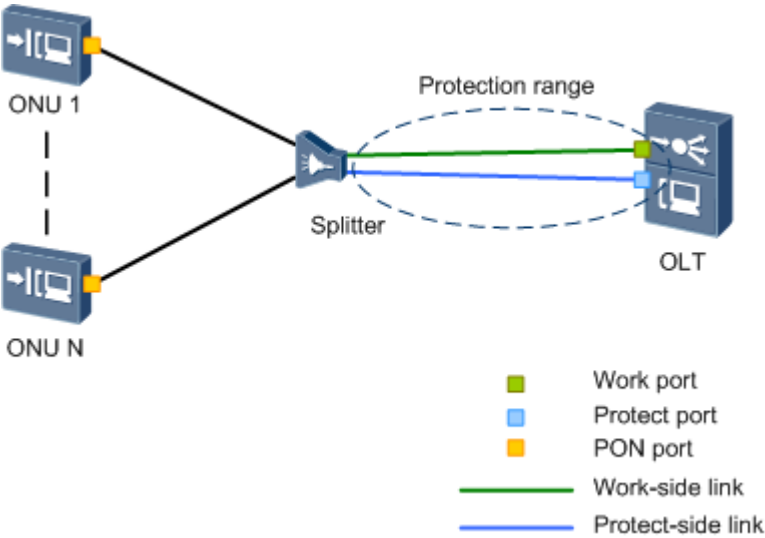
16.2.1 Introduction to xPON Type B Protection

Type B provides protection for the OLT, OLT PON ports, and backbone fiber.

xPON type B applies to single-homing or dual-homing scenarios.

Figure 16-3 shows a single-homed xPON type B protection network. Type B single-homing protection mainly protects the OLT PON port and backbone fibers. When the OLT PON port or the backbone fiber is faulty, services can be automatically switched to another OLT PON port or the backbone fiber.

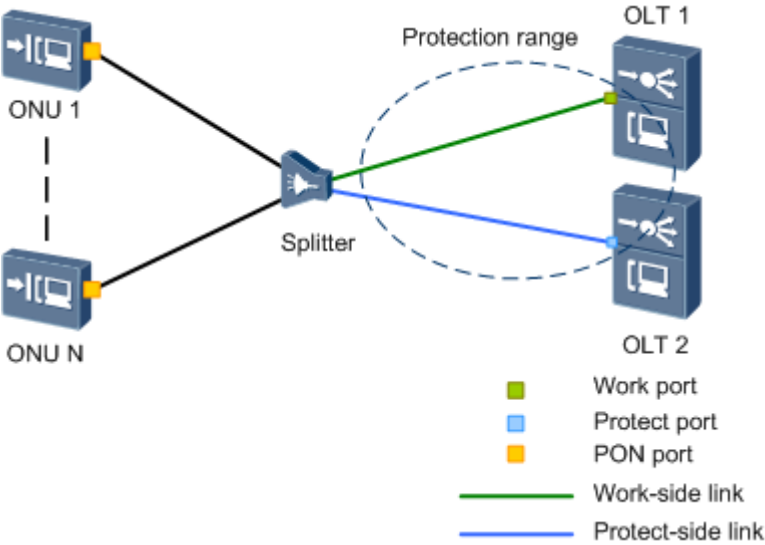
Figure 16-3 Single-homed xPON type B protection network



Networking Scenario	Advantage	Disadvantage
Single homing	Networking, OLT/ONU management, and service provisioning are simple.	An OLT fault will interrupt services. In addition, two optical fibers routed in one pipe may both be broken.

Figure 16-4 shows a dual-homed xPON type B protection network. Type B dual-homing protection mainly protects the OLT, OLT PON port, and backbone fibers. When the OLT, OLT PON port, or backbone fiber is faulty, services can be automatically switched to another OLT, OLT PON port, or backbone fiber.

Figure 16-4 Dual-homed xPON type B protection network



Networking Scenario	Advantage	Disadvantage
Dual homing	Each of the two OLTs connects to a backbone fiber for remote disaster recovery.	The networking is complex, and networking costs are high. In addition, the OLT configuration is complex.

16.2.2 Basic Concepts of xPON Type B Protection

Protection Group

On a single-homed network, two PON ports on an OLT are added to a protection group.

 NOTE

The OLT PON ports can be on the same board or on different boards. The differences are as follows:

- Port redundancy backup on the same board can conserve hardware resources. If the PON service board fails, the services on the entire board are interrupted.
- Port redundancy backup on the different boards requires hardware costs than that on the same board. If the active PON service board fails, the services can be automatically switched over to the PON ports on the standby board without being interrupted.

On a dual-homed network, the PON ports on two OLTs are added to a protection group.

Roles of Protection Group Members

Protection group members have two roles: working and protection.

- One protection group contains a working port and a protection port. The working port and protection port are two different PON ports.
- In normal cases, the working port carries services.
- When the link of the working port becomes faulty, the system automatically switches services from the working port to the protection port to ensure service continuity.

State of Protection Group Members

Protection group members have two states: active and standby. The active port forwards data and the standby port does not forward data.

Switching Types

The switching can be triggered automatically by a fault or performed manually. Manual operations that may cause switching are forcible switching and locking.

- In automatic switching, the OLT and ONU automatically switch to the standby link when the conditions for triggering the switching are met.
- In forcible switching, users run the **force-switch** command on the OLT to perform the switching regardless of whether specific group members are running properly.
- After switching, the working port's state becomes standby. Then, if users run the **lockout** command on the OLT to lock a group member (for a Type B single-homed network, both working and protection ports can be locked; for a Type B dual-homed network, only the protection port can be locked), the switching is performed and the working port's state becomes active.

Switching Condition

Protection group members are switched only when the following conditions are met:

- The protection group is enabled.

NOTE

The status of a protection group can be queried using the **display protect-group** command on the OLT. If **Admin State** is displayed in the output, the protection group is enabled.

- The protection group is not frozen using the **freeze** command on the OLT.
- The protection group is not locked using the **lockout** command on the OLT.
- The protection group member is not forcibly switched using the **force-switch** command on the OLT.

Operation Restriction Relationships in Protection Switching

Table 16-2 Type B single homing protection switching

Current Status				Next Operation									Re ma rks
En abl ed	Fro ze n	Lo ck ed	For cib le sw itc hin g	Enab led	Dis abl ed	Fro ze n	Un fro ze n	Lo ck ed	Un loc ed	For cib le swi tch ing	Ca nce lin g for cib le swi tch ing	Au to ma tic swi tch ing	No ne
No	No	No	No	Supp orted	N/A	N/A	N/A	Supp ort ed	N/A	N/A	N/A	N/A	No ne
No	No	Yes	No	Supp orted	N/A	N/A	N/A	N/A	Supp ort ed	N/A	N/A	N/A	No ne
Yes	No	No	No	N/A	Su pp ort ed	Su pp ort ed	N/A	Su pp ort ed	N/A	Su pp ort ed	N/A	Sup por ted	No ne

Current Status				Next Operation									Re ma rks
En abl ed	Fro ze n	Lo ck ed	For cib le sw itc hin g	Enab led	Dis abl ed	Fro ze n	Un fro ze n	Lo ck ed	Un loc ke d	For cib le swi tch ing	Ca nce lin g for cib le swi tch ing	Au to ma tic swi tch ing	No ne
Yes	No	No	Yes	N/A	Su pp ort ed	Su pp ort ed	N/ A	Su pp ort ed	N/ A	Su pp ort ed	N/ A	N/ A	The forcible switching status will be cleared when the protection switching is disabled or locked.
Yes	No	Yes	No	N/A	Su pp ort ed	Su pp ort ed	N/ A	N/ A	Su pp ort ed	N/ A	N/ A	N/ A	No ne

Current Status				Next Operation									Re ma rks
En abl ed	Fro ze n	Lo ck ed	For cib le sw itc hin g	Enab led	Dis abl ed	Fro ze n	Un fro ze n	Lo ck ed	Un loc ked	For cib le sw itc hin g	Ca nce lin g for cib le sw itc hin g	Au to ma tic sw itc hin g	No ne
Yes	Yes	No	No	N/A	N/A	N/A	Sup port ed	N/A	N/A	N/A	N/A	N/A	No ne
Yes	Yes	No	Yes	N/A	N/A	N/A	Sup port ed	N/A	N/A	N/A	N/A	N/A	No ne
Yes	Yes	Yes	No	N/A	N/A	N/A	Sup port ed	N/A	N/A	N/A	N/A	N/A	No ne

 NOTE

The statuses that are not listed in the preceding table, such as disabled and forcible switching, are unavailable.

Table 16-3 Type B dual homing protection switching

Current Status			Next Operation							Rem arks
Enab led	Lock ed	Forci ble switc hing	Enable d	Disa bled	Lock ed	Unlo cked	Forci ble switc hing	Canc eling forci ble switc hing	Auto mati c switc hing	Non e

Current Status			Next Operation							Remarks
No	No	No	Supported	N/A	Supported	N/A	N/A	N/A	N/A	Protection switching is consistently enabled on the working side, and the supported statuses are available only on the protection side.

Current Status			Next Operation							Remarks
No	Yes	No	Supported	N/A	N/A	Supported	N/A	N/A	N/A	Protection switching is consistently enabled on the working side, and the supported statuses are available only on the protection side.

Current Status			Next Operation							Remarks
Yes	No	No	N/A	Supported	Supported	N/A	Supported	N/A	Supported	Protection switching can be disabled or locked only on the protection side.

Current Status			Next Operation							Remarks
Yes	No	Yes	N/A	Supported	Supported	N/A	Supported	Supported	N/A	Protection switching can be disabled or locked only on the protection side. In either of the statuses, the forcible switching status will be cleared.

Current Status			Next Operation							Remarks
Yes	Yes	No	N/A	Supported	N/A	Supported	N/A	N/A	N/A	Protection switching can be locked only on the protection side.

 NOTE

The statuses that are not listed in the preceding table, such as disabled and forcible switching, are unavailable.

Associated Switching

Associated switching is implemented on a dual-homed network as follows: A protection group is associated on the OLT with the uplink Ethernet port status and BFD/MEP session status. In such a case, when the OLT's upper-layer network or the Layer 2 OLT physical link fails, the active OLT triggers a dual-homing protection switchover so that services will be switched to the standby OLT.

16.2.3 Single-Homing xPON Type B Protection Principles

On a single-homed network, the two PON ports on the OLT are in active/standby state, and they cannot forward packets at the same time. An automatic switchover can be triggered by any of the following conditions:

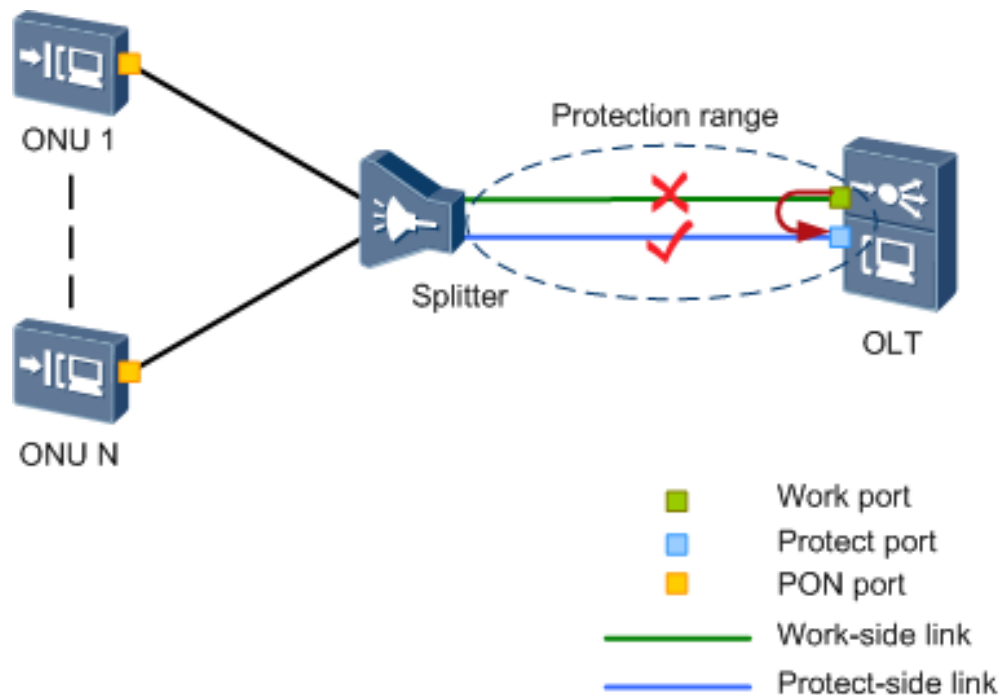
- Active fiber cut
- Active PON port failure
- Line quality deterioration

The following section describes the xPON type B protection switching in different scenarios.

Scenario 1: Active Optical Fiber Is Cut

The active optical fiber is cut when the OLT PON port is working, as shown in [Figure 16-5](#).

Figure 16-5 Active optical fiber is cut

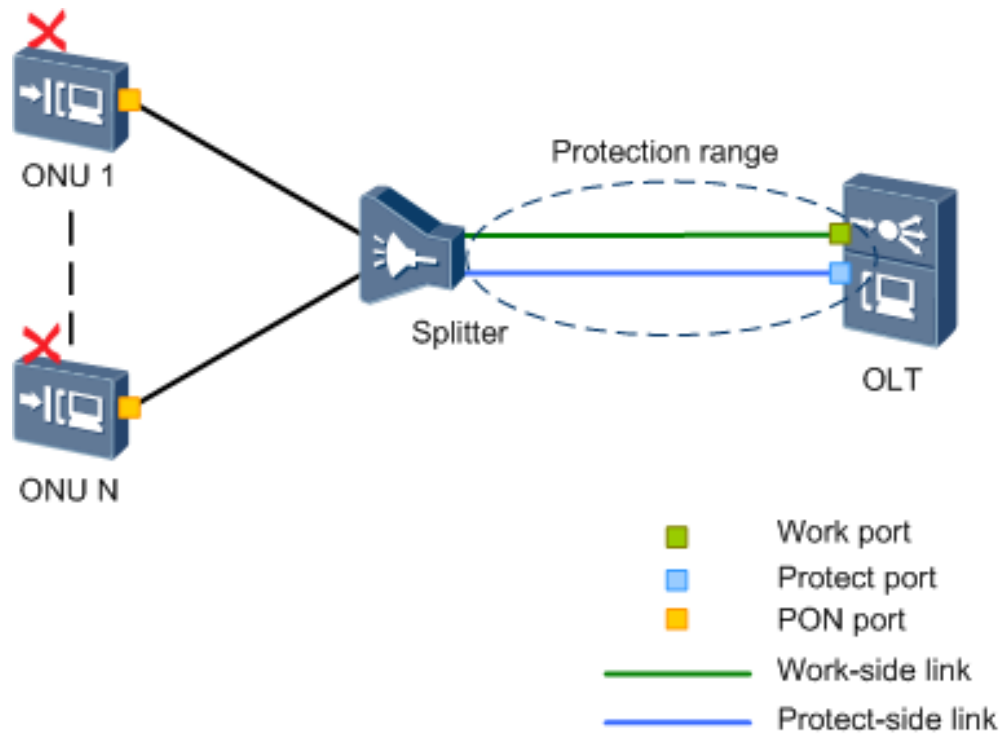


- When detecting a loss of signal (LOS) alarm (generated due to the active optical fiber cut), the working port disables the transmission of the optical module.
- The protection port detects a LOS alarm (generated due to the failure of the ONT to transmit optical signals), enables the transmission function of the optical module, and performs ONU ranging.
- If the optical fiber connected to the protection port is functional, and ONU ranging is successful, the protection port reports an LOS clear alarm.
- The working port switches to the standby state. The protection port switches to the active state. Then, the protection switching ends.

Scenario 2: All ONUs Go Offline

All ONUs connected to the OLT PON port go offline, as shown in [Figure 16-6](#).

Figure 16-6 All ONUs go offline



- When detecting an LOS alarm (generated because all ONUs go offline), the working port disables the transmission of the optical module.
- The protection port detects a LOS alarm (generated due to the failure of the ONT to transmit optical signals), enables the transmission function of the optical module, and performs ONU ranging.
- No ONU connected to a PON port goes online due to a ranging failure. Therefore, the OLT cyclically detects the working and protection ports until an ONU goes online.
- After the ONU goes online, switching is performed between the PON ports if the protection port is detected. If the protection port is not detected, the working port continues working.

16.2.4 Dual-Homing xPON Type B Protection Principles

On a dual-homed network, two OLTs protection work in active/standby mode and they cannot forward packets at the same time. An automatic switchover can be triggered by any of the following conditions:

NOTE

Currently, type B dual-homing protection is mainly used in the passive optical LAN (POL) solution and requires cooperation of the OLT, ONU, and aggregation device. You are advised to set up a cluster or VRRP interconnection on the core switches to work with type B dual-homing protection to enhance the overall reliability of the solution.

- Optical fiber cut from the active OLT
- Active OLT fault
- Active OLT PON port fault

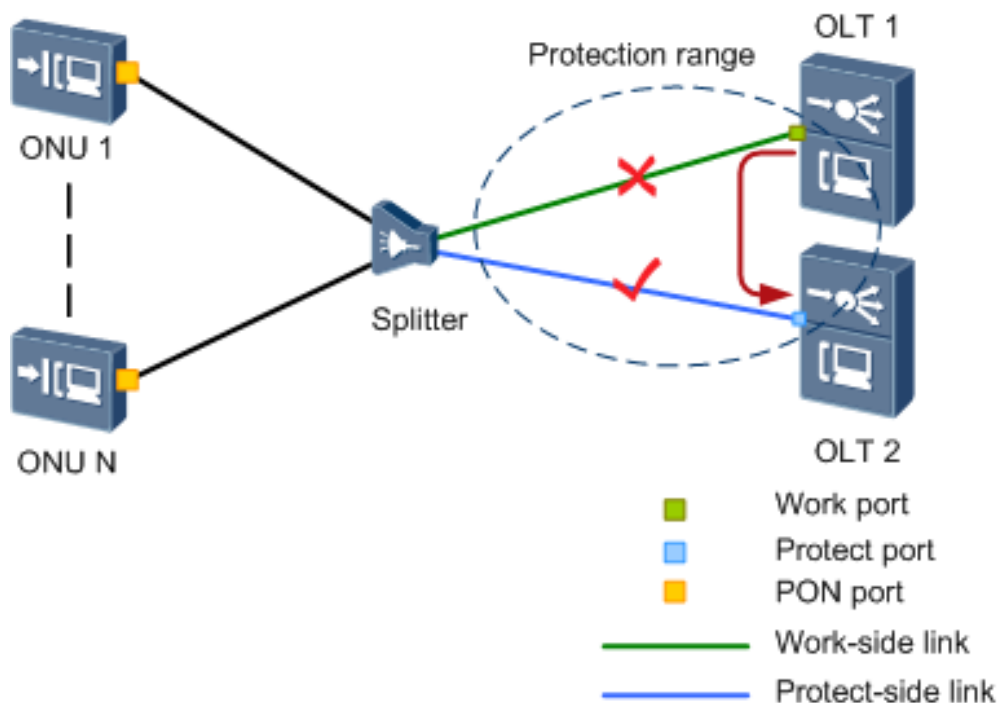
- The OLT's uplink is faulty (this condition triggers automatic switching only in the associated protection switching scenario).
- Active line quality deterioration

The following section describes the xPON type B protection switching in different scenarios.

Scenario 1: Active Optical Fiber Is Cut

The active optical fiber is cut when the OLT PON port is working, as shown in [Figure 16-7](#).

Figure 16-7 Active optical fiber is cut

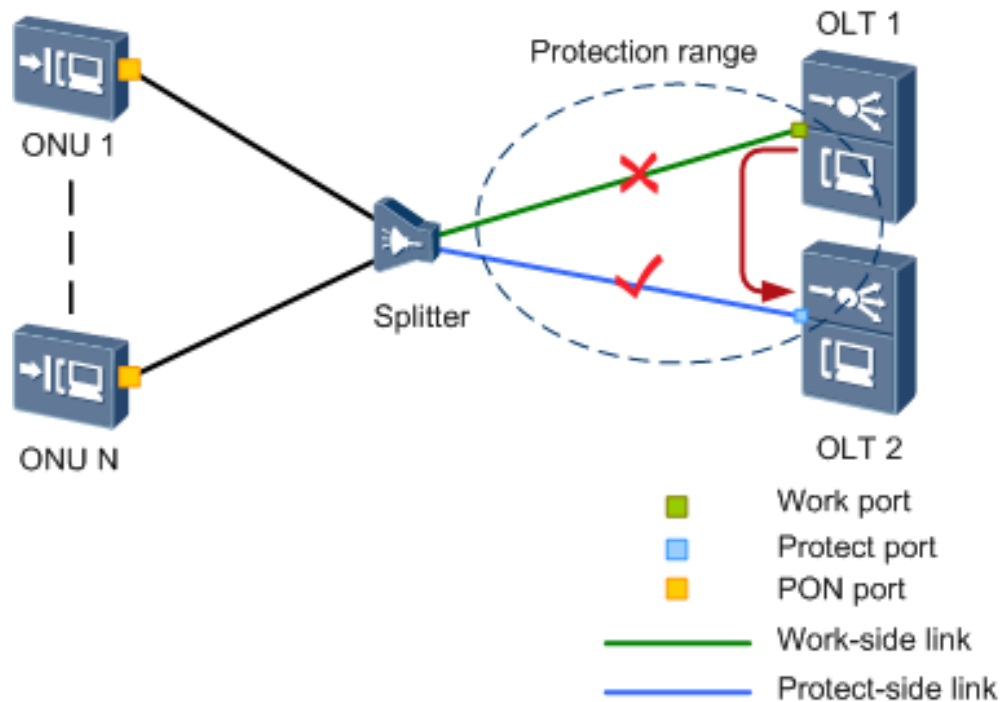


- When detecting a loss of signal (LOS) alarm (generated due to the active optical fiber cut), the working port disables the transmission of the optical module.
- The protection port detects a LOS alarm (generated due to the failure of the ONT to transmit optical signals), enables the transmission function of the optical module, and performs ONU ranging.
- If the optical fiber connected to the protection port is functional, and ONU ranging is successful, the protection port reports an LOS clear alarm.
- The working port switches to the standby state. The protection port switches to the active state. Then, the protection switching ends.

Scenario 2: All ONUs Go Offline

All ONUs connected to the OLT PON port go offline, as shown in [Figure 16-8](#).

Figure 16-8 All ONUs go offline



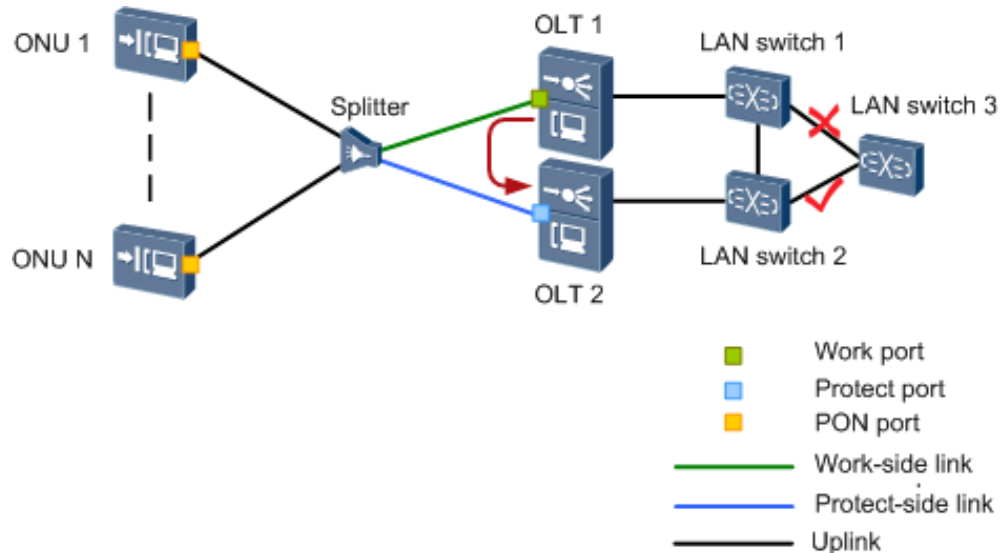
- When detecting an LOS alarm (generated because all ONUs go offline), the working port disables the transmission of the optical module.
- The protection port detects a LOS alarm (generated due to the failure of the ONT to transmit optical signals), enables the transmission function of the optical module, and performs ONU ranging.
- No ONU connected to a PON port goes online due to a ranging failure. Therefore, the OLT cyclically detects the working and protection ports until an ONU goes online.
- After the ONU goes online, switching is performed between the PON ports if the protection port is detected. If the protection port is not detected, the working port continues working.

Scenario 3: Associated Protection Switching Is Caused by a Connection Failure in the OLT's Upstream Transmission Network

If a BFD session has been configured on the OLT, the BFD session can be bound to a protection group for creating an association between them. If CFM has been enabled on an OLT, an MEP session can be bound to a protection group for creating an association between them. Based on the associations, when the upper-layer network connection of the active OLT fails, the active and standby OLTs

perform a switchover and notifies the ONU of the switchover. In this way, services are restored. **Figure 16-9** shows the associated protection switching caused by a connection failure in the OLT's upstream transmission network.

Figure 16-9 OLT's upstream transmission network connection fails

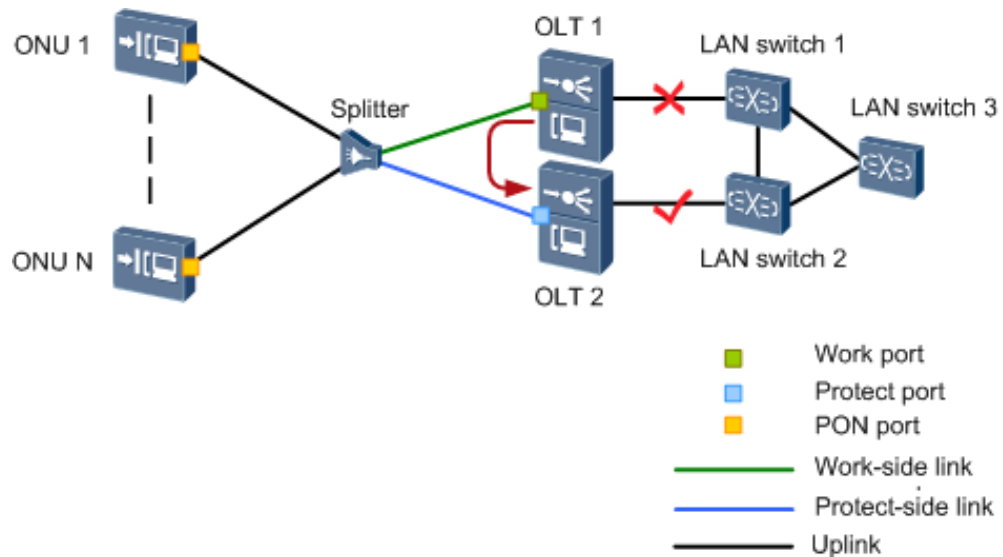


- On the OLT, the dual-homing protection group is associated with the BFD or MEP session. When the upstream route of the working OLT (OLT 1) fails, OLT 1 checks whether the protection OLT (OLT 2) and the upstream route of OLT 2 are functional. If they are functional, and both OLTs do not carry out a forcible switchover or locking operation, OLT 1 data has been synchronized to OLT 2. Then, the two OLTs perform a switchover.
- OLT 2 starts to work. It enables the transmission of the optical module and performs ONU ranging.
- After the switchover, the ONU service data is sent to OLT 2 through the protection port, and service data is transmitted over the protection link. The OLT status changes as follows:
 - OLT 1 becomes standby.
 - OLT 2 becomes active.

Scenario 4: Associated Protection Switching Is Caused by an OLT's Layer 2 Physical Link Fault

An OLT protection group is associated with the uplink Ethernet port status. Based on the association, when the Layer 2 physical link of the active OLT fails, the two OLTs perform a switchover, and notify the ONU of the switchover. In this way, services are restored. **Figure 16-10** shows the associated protection switching caused by an OLT's Layer 2 physical link fault.

Figure 16-10 OLT's Layer 2 physical link fails



- On the OLT, the dual-homing protection group is associated with the uplink Ethernet port status. When the Ethernet port associated with the protection group on the working OLT (OLT 1) becomes **Down**, OLT 1 checks whether the protection OLT (OLT 2) and the physical link of the protection OLT are functional. If they are functional, and both OLTs do not carry out a forcible switchover or locking operation, OLT 1 data has been synchronized to OLT 2. Then, the two OLTs perform a switchover.
- OLT 2 starts to work. It enables the transmission of the optical module and performs ONU ranging.
- After the switchover, the ONU service data is sent to OLT 2 through the protection port, and service data is transmitted over the protection link. The OLT status changes as follows:
 - OLT 1 becomes standby.
 - OLT 2 becomes active.

16.2.5 Configuring xPON Type B Single-Homing Protection

This section describes how to configure xPON type B single-homing protection on an OLT to implement xPON port 1+1 redundancy backup, which ensures that services are not interrupted if a fault occurs on the OLT's PON port or backbone fiber.

Precaution

After xPON type B single-homing protection is configured, the service configurations on an optical network unit (ONU) remain unchanged and data is transmitted or received over the primary xPON port.

NOTE

Configurations of xPON network protection do not affect service configuration. This topic describes how to perform configurations of xPON network protection. For details about how to perform service configuration, see the specific service configuration guide.

Procedure

Step 1 (Optional) Shutdown the laser of the protection member PON port.

 NOTE

This step applies to the following scenarios, Otherwise, skip this step.

- The ONU upstream port works in auto-negotiation mode. That is, the ONU upstream port can work in GPON mode or XG(S)-PON mode according to the port type on the OLT side.
- The optical fiber of the protection member PON port of Type X protection is connected, that is, the physical link is connected. In this case, the physical link is connected but the Type X protection data configuration is not complete. The working and protection member PON ports transmit light at the same time and interact with the ONU. As a result, the upstream port mode of the ONU is repeatedly switched and the ONU is repeatedly reset.

To solve the preceding problem:

1. Run the **shutdown** command to disable the laser on the protection member PON port before the configuration.
2. After the configuration is complete, run the **undo shutdown** command to turn on the laser of the protection member PON port.

Step 2 Run the **protect-group** command to create a protection group for xPON access ports.

 NOTE

1. Set **protect-target** to **gpon-uni-port** when GPON Type B single-homing protection is configured.
2. The working mode of the members in the protection group can only be **timedelay**.

Step 3 Run the **protect-group member** command to add a protection member to the protection group.

Step 4 Run the **protect-group enable** command to enable the protection group.

A created protection group is disabled by default. Enable the protection group to make the protection group take effect.

Step 5 Run the **display protect-group** command to query the information about the protection group and all the members in the protection group.

Step 6 Bind a PPPoE single MAC address pool to a protection group if PPPoE single MAC is enabled.

- To do so, run the **bind mac-pool single-mac** command in the protect-group mode.
- Otherwise, the PPPoE service carried over the xPON port is interrupted when a protection switchover is performed. In this case, users need to dial numbers up again to go online and the service interruption time is based on BRAS configurations. This may fail to meet the switchover performance requirements of no longer than 50 ms for a protection switchover.

Step 7 (Optional) Turn on the laser of the protection member PON port. After the preceding configuration steps are complete, run the **undo shutdown** command to turn on the laser of the protection member PON port.

----End

Result

After the configuration, the primary xPON port on the OLT works in active mode and the secondary xPON port works in standby mode.

An automatic switching can be triggered by any of the following conditions:

- Fractures of optical fibers
- OLT xPON port failure
- Quality deterioration of lines

For a type B inter-board protection group, if the customer needs to change the board that houses the active PON port, trigger type B protection switching to activate the standby PON port, and then migrate the to-be-migrated PON port to the target board.

Example

The following configurations are used as an example to configure GPON type B single-homing protection on the OLT:

NOTE

The data in the example is for reference only. Replace it with the service data in the actual configuration.

- Protection group members: 0/2/0 and 0/2/1 (on the same GPON service board)
- Primary port: 0/2/0
- Secondary port: 0/2/1

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#shutdown 1
huawei(config-if-gpon-0/2)#quit
huawei(config)#protect-group 0 protect-target gpon-uni-port workmode timedelay
huawei(protect-group-0)#protect-group member port 0/2/0 role work
huawei(protect-group-0)#protect-group member port 0/2/1 role protect
huawei(protect-group-0)#protect-group enable
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#undo shutdown 1
huawei(config-if-gpon-0/2)#quit
huawei(config)#save
```

16.2.6 Configuring xPON Type B Dual-Homing Protection

In xPON type B dual-homing protection, 2 backbone fibers connect to 2 OLTs to realize remote disaster recovery.

Prerequisites

An ONU has been added to the active and standby OLTs by running the **ont add** command. All ONU profiles, such as DBA profile and line profiles, are the same on the active and standby OLTs. When adding an ONU to an OLT, ensure that the ONU IDs on the active and standby OLTs are the same.

Precaution

Users must manually configure the same service data on the two OLTs so that the ONU can rapidly switch services from the active OLT to the standby one, minimizing service interruption duration.

NOTE

Configurations of xPON network protection do not affect service configuration. This topic describes how to perform configurations of xPON network protection. For details about how to perform service configuration, see the specific service configuration guide.

Procedure

Step 1 (Optional) Shutdown the laser of the protection member PON port on the Secondary OLT (OLT-B).

NOTE

This step applies to the following scenarios, Otherwise, skip this step.

- The ONU upstream port works in auto-negotiation mode. That is, the ONU upstream port can work in GPON mode or XG(S)-PON mode according to the port type on the OLT side.
- The optical fiber of the protection member PON port of Type X protection is connected, that is, the physical link is connected. In this case, the physical link is connected but the Type X protection data configuration is not complete. The working and protection member PON ports transmit light at the same time and interact with the ONU. As a result, the upstream port mode of the ONU is repeatedly switched and the ONU is repeatedly reset.

To solve the preceding problem:

1. Run the **shutdown** command to disable the laser on the protection member PON port before the configuration.
2. After the configuration is complete, run the **undo shutdown** command to turn on the laser of the protection member PON port.

Step 2 Configure a dual-homing xPON type B protection group on the active OLT (OLT-A).

1. Run the **dual-parenting local-node** command to configure the local IP address, TCP port number, and key.
2. Run the **dual-parenting peer-node** command to configure the peer IP address, TCP port number, and key.
3. Run the **dual-parenting sync** command to enable dual-homing synchronization.
4. Run the **protect-group** command to create a protection group.

Run the **description** command to configure the description of a PG.

5. Run the **protect-group member** command to add a member to the protection group.

NOTE

After a member is added to a dual-homing protection group, the group is automatically enabled.

6. Run the **peer-group-member** command to configure the peer member of the protection group.

Step 3 Configure a dual-homing xPON type B protection group on the standby OLT (OLT-B).

1. Run the **dual-parenting local-node** command to configure the local IP address, TCP port number, and key.
2. Run the **dual-parenting peer-node** command to configure the peer IP address, TCP port number, and key.
3. Run the **dual-parenting sync** command to enable dual-homing synchronization.
4. Run the **protect-group** command to create a protection group.

The description of the protection groups created on the active and standby OLTs must be the same. Run the **description** command to configure the description of a PG.
5. Run the **protect-group member** command to add a member to the protection group.
6. Run the **peer-group-member** command to configure the peer member of the protection group.
7. Run the **protect-group enable** command to enable the protection group.

Step 4 (Optional) Run the **uplink-monitor port** command to associate the protection groups with the uplink Ethernet port status.

 NOTE

If an Ethernet link aggregation group has been configured, make sure that the Ethernet port associated with the dual-homing protection groups is the master port in the aggregation group.

- Run the **uplink-monitor bfd** command to associate the protection groups with a BFD session. For instructions about how to configure a BFD session, see **Configuring a BFD Session**.
- Run the **uplink-monitor mep** command to associate the protection groups with an MEP session. For instructions about how to configure an MEP session, see **Configuring CFM**.

 NOTE

One protection group can be configured only one fault detection type.

Step 5 (Optional) Turn on the laser of the standby PON port. After the preceding configuration steps are complete, run the **undo shutdown** command to turn on the laser of the protection member PON port.

----End

Result

After the configuration, both active and standby OLTs are in working state, and they both check link status for determining a protection switchover.

An automatic switchover can be triggered by any of the following conditions:

- Optical fiber cut from the active OLT
- Active OLT PON port fault
- Active OLT fault
- Active line quality deterioration
- Active OLT uplink failure

Example

The following section uses an example to describe how to configure a dual-homing GPON type B protection group on the active OLT (OLT_A) and standby OLT (OLT_B), respectively:



NOTE

The data in the example is for reference only. Replace it with the service data in the actual configuration.

- GPON service port on the two OLTs: 0/2/0
- Index of the protection groups on the two OLTs: 1
- Associated port with the dual-homing protection groups: 0/3/0
- IP address of the local OLT_A and peer OLT_B: 192.168.68.1; TCP port number: 6076; key: HW_42340000
- IP address of the local OLT_B and peer OLT_A: 192.168.68.8; TCP port number: 6076; key: HW_42340000

Configuration on OLT_B:

```
huawei_B(config)#interface gpon 0/2
huawei_B(config-if-gpon-0/2)#shutdown 0
huawei_B(config-if-gpon-0/2)#quit
```

Configuration on OLT_A:

```
huawei_A(config)#dual-parenting local-node ip-address 192.168.68.1 port 6076 key HW_42340000
huawei_A(config)#dual-parenting peer-node standby ip-address 192.168.68.8 port 6076 key
HW_42340000
huawei_A(config)#dual-parenting sync enable
huawei_A(config)#protect-group 1 protect-target gpon-uni-port workmode dual-parenting
huawei_A(protect-group-1)#protect-group member port 0/2/0 role work
huawei_A(protect-group-1)#peer-group-member peer-node standby peer-port 0/2/0
huawei_A(protect-group-1)#uplink-monitor port 0/3/0
huawei_A(protect-group-1)#quit
```

Configuration on OLT_B:

```
huawei_B(config)#dual-parenting local-node ip-address 192.168.68.8 port 6076 key HW_42340000
huawei_B(config)#dual-parenting peer-node active ip-address 192.168.68.1 port 6076 key
HW_42340000
huawei_B(config)#dual-parenting sync enable
huawei_B(config)#protect-group 1 protect-target gpon-uni-port workmode dual-parenting
huawei_B(protect-group-1)#protect-group member port 0/2/0 role protect
huawei_B(protect-group-1)#peer-group-member peer-node active peer-port 0/2/0
huawei_B(protect-group-1)#protect-group enable
huawei_B(protect-group-1)#uplink-monitor port 0/3/0
huawei_B(protect-group-1)#quit
huawei_B(config)#interface gpon 0/2
huawei_B(config-if-gpon-0/2)#undo shutdown 0
huawei_B(config-if-gpon-0/2)#quit
huawei_B(config)#save
```

16.2.7 xPON Type B Protection Reference Standards and Protocols

Standard No.	Description
ITU-T G.984.1	General Characteristics. This protocol mainly describes the basic features and major protection modes of GPON.

Standard No.	Description
ITU-T G.984.2	Physical Media Dependent (PMD) Layer Specification. This protocol mainly describes the PMD layer parameters, including physical parameters (such as the transmit optical power, receiver sensitivity, and overload optical power) of optical transceivers, and also defines optical budget of different levels, for example, the most common Class B+.
ITU-T G.984.3	Transmission Convergence Layer Specification. This protocol mainly describes the TC layer specifications, including the upstream and downstream frame structures and GPON principle.
ITU-T G.984.4	ONT Management And Control Interface Specification. This protocol mainly describes the GPON management and maintenance protocols, such as OAM, PLOAM, and OMCI.
ITU-T G.984.5	Enhancement Band. This protocol mainly describes the GPON wavelength planning, including reserving bands for next-generation PON.
ITU-T G.984.7	Long Reach. This protocol mainly describes several long reach PON schemes for extending GPON transmission distance.
ITU-T G.988	ONU management and control interface (OMCI) specification.
TR-156	Using GPON Access in the context of TR-101.

16.3 xPON Type C Protection

The xPON type C protection switching is implemented through the redundancy configuration of the two PON ports on the ONU, backbone optical fiber, optical splitter, and tributary optical fiber on a xPON network. Each item is in a dual configuration. The protection improves the reliability on the optical distribution network (ODN) and prevents service interruption.

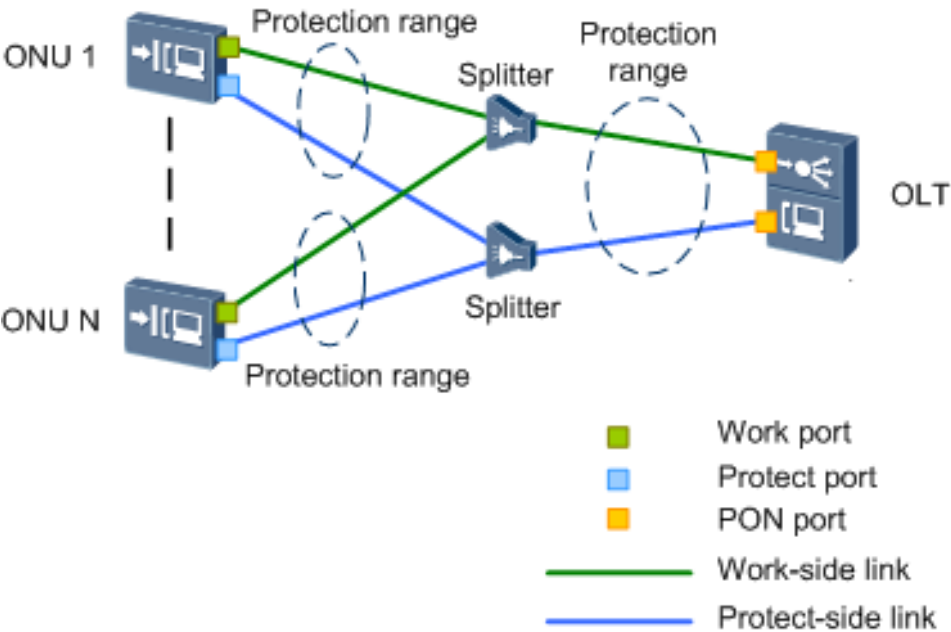
16.3.1 Introduction to xPON Type C Protection

Type C provides redundancy for OLT (dual homing), ONU's PON ports, backbone fibers, optical splitters, and distribution optical fibers. When a fault occurs, services can be automatically switched to the functional link. After the fault is rectified, services are automatically switched back to the original link.

xPON type C protection can be deployed in two networking scenarios: single homing and dual homing.

Figure 16-11 shows the xPON type C protection single homing network.

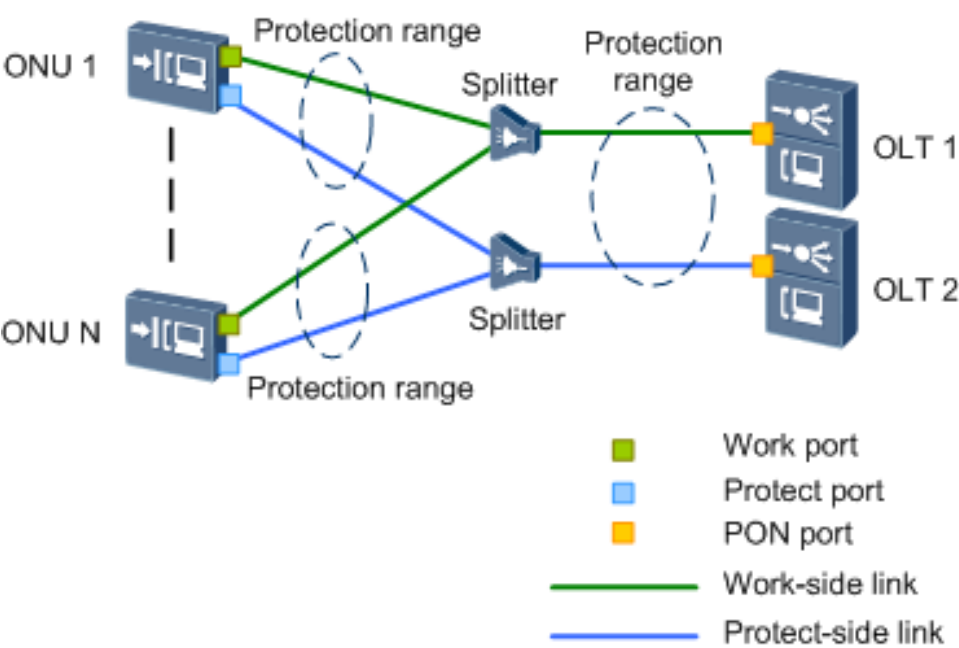
Figure 16-11 xPON type C protection network (single homing)



Networking Mode	Advantage	Disadvantage
Single homing	The networking mode is simple, and OLT and ONU can be managed easily.	When the OLT becomes faulty, services are interrupted. Optical fibers are deployed on the same channel and therefore two optical fibers may be broken at the same time.

Figure 16-12 shows the xPON type C protection dual homing network.

Figure 16-12 xPON type C protection network (dual homing)



Networking Mode	Advantage	Disadvantage
Dual homing	When the active OLT or its uplink fails, services can be switched to the standby OLT.	The networking mode is complicated and costly, and the ONU management is difficult.

16.3.2 Basic Concepts of xPON Type C Protection

Protection Group

On a single-homed network, two PON uplink ports on an ONU connected to different PON ports on an OLT are added to a protection group.

 NOTE

The OLT PON ports can be on the same board or on different boards. The differences are as follows:

- Port redundancy backup on the same board can conserve hardware resources. If the PON service board fails, the services on the entire board are interrupted.
- Port redundancy backup on the different boards requires hardware costs than that on the same board. If the active PON service board fails, the services can be automatically switched over to the PON ports on the standby board without being interrupted.

On a dual-homed network, two PON uplink ports on an ONU connected to two OLTs are added to a protection group. Switching can be performed between two members in a protection group.

Roles of Protection Group Members

Protection group members have two roles: working and protection.

- One protection group contains a working port (the member's role is working) and a protection port (the member's role is protection). The working port and protection port are two different uplink PON ports on the ONU.
- In normal cases, the working port carries services.
- When the link of the working port becomes faulty, the system automatically switches services from the working port to the protection port to ensure service continuity.

State of Protection Group Members

Protection group members have two states: active and standby. The active port forwards data and the standby port does not forward data.

Switching Types

The switching can be triggered automatically by a fault or performed manually. Manual operations that may cause switching are manual switching, forcible switching, and locking.

- In automatic switching, the OLT and ONU automatically switch to the standby link when the conditions for triggering the switching are met.
- In manual switching, users manually switch the protection group by running the **manual-switch** command on the OLT.
- In forcible switching, users run the **force-switch** command on the OLT to perform the switching regardless of whether specific group members are running properly.
- After switching, the working port's state becomes standby. Then, if users run the **lockout** command on the OLT to lock a group member (only the protection port can be locked), the switching is performed and the working port's state becomes active.

NOTE

- In training switching, users run the **exercise-switch** command on the OLT to perform the switching to test the Automatic Protection Switching (APS) function on the ports in a protection group. Services are not switched.
- In automatic switchback, when the working member in the PG recovers to the normal state, the PG automatically switches over after the WTR time expires, and service is still carried on the working member.

Switching Condition

Protection group members are switched only when the following conditions are met:

- The protection group is enabled.

NOTE

The status of a protection group can be queried using the **display protect-group** command on the OLT. If **Admin State** is displayed in the output, the protection group is enabled.

- The protection group is not locked using the **lockout** command on the OLT.
- The protection group member is not forcibly switched using the **force-switch** command on the OLT.

 NOTE

Type C protection requires the cooperation of the OLT and ONU to implement active/standby switching. Third-party ONUs have not been tested with Huawei OLTs. Contact Huawei maintenance engineers to check whether they can work properly.

Operation Restriction Relationships in Protection Switching

Table 16-4 Type C single homing protection switching

Current Status			Next Operation									Remarks
Enabled	Locked	Forcible switching	Enabled	Disabled	Locked	Unlocked	Forcible switching	Cancelling forcible switching	Automatic switching	Manual switching	Training switching	None
No	No	No	Supported	N/A	Supported	N/A	N/A	N/A	N/A	N/A	N/A	None
No	Yes	No	Supported	N/A	N/A	Supported	N/A	N/A	N/A	N/A	N/A	None
Yes	No	No	Not supported	Supported	Supported	N/A	Supported	N/A	Supported	Supported	Supported	None

Current Status			Next Operation									Re mar ks
Yes	No	Yes	Not supp orted	Sup por ted	Sup por ted	N/ A	Sup por ted	Sup por ted	N/ A	N/A	N/A	The forc ible swit chin g stat us will be clea red whe n the prot ecti on swit chin g is disa ble d or lock ed.
Yes	Yes	No	Not supp orted	Sup por ted	N/ A	Sup por ted	N/ A	N/ A	N/ A	N/A	N/A	Non e

 NOTE

The statuses that are not listed in the preceding table, such as disabled and forcible switching, are unavailable.

Table 16-5 Type C dual homing protection switching

Current Status			Next Operation									Re mar ks
Ena ble d	Loc ked	For cibl e swi tchi ng	Enabl ed	Dis abl ed	Loc ked	Unl ock ed	For cibl e swi tchi ng	Can celi ng forc ible swi tchi ng	Aut om atic swi tchi ng	Ma nua l swit chi ng	Trai nin g swit chin g	Non e

Current Status			Next Operation									Re mar ks
No	No	No	Supp orted	N/ A	Sup por ted	N/ A	N/ A	N/ A	N/ A	N/A	N/A	Prot ecti on swit chin g is con sist entl y ena bled on the wor kin g side , and the sup port ed stat use s are avai labl e only on the prot ecti on side .

Current Status			Next Operation									Re mar ks
No	Yes	No	Supp orted	N/ A	N/ A	Sup por ted	N/ A	N/ A	N/ A	N/A	N/A	Prot ecti on swit chin g is con sist entl y ena bled on the wor kin g side , and the sup port ed stat use s are avai labl e only on the prot ecti on side .

Current Status			Next Operation									Re mar ks
Yes	No	No	Not supp orted	Sup por ted	Sup por ted	N/ A	Sup por ted	N/ A	Sup por ted	Sup por ted	Sup por ted	Prot ecti on swit chin g can be disa ble d or lock ed only on the prot ecti on side .

Current Status			Next Operation									Re mar ks
Yes	No	Yes	Not supp orted	Sup por ted	Sup por ted	N/ A	Sup por ted	Sup por ted	N/ A	N/A	N/A	Prot ecti on swit chin g can be disa ble d or lock ed only on the prot ecti on side . In eith er of the stat use s, the forc ible swit chin g stat us will be clea red.

Current Status			Next Operation									Re mar ks
Yes	Yes	No	Not supp orted	Sup por ted	N/ A	Sup por ted	N/ A	N/ A	N/ A	N/A	N/A	Prot ecti on swit chin g can be lock ed only on the prot ecti on side .



NOTE

The statuses that are not listed in the preceding table, such as disabled and forcible switching, are unavailable.

Associated Protection Switching

Associated switching is implemented on a dual-homed network as follows: A protection group is associated on the OLT with the uplink Ethernet port status and BFD/MEP session status. In such a case, when the OLT's upper-layer network or the Layer 2 OLT physical link fails, the OLT determines a protection switchover, ensuring service continuity. Associated protection switching applies on the network enabled with automatic site information transmission.

16.3.3 Single-Homing xPON Type C Protection Principles

On a single homing network, one ONU is connected to two PON ports on an OLT, one working as the active port and the other as standby. The two ports on the OLT cannot forward packets at the same time. An automatic switching can be triggered by any of the following conditions:

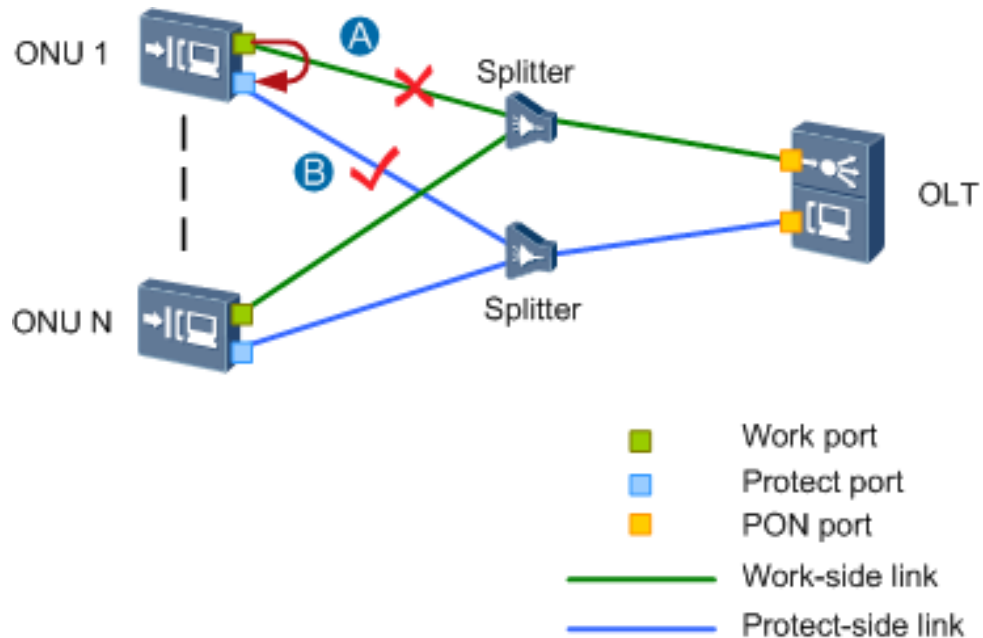
- Loss of signal (LOS) occurs in the input direction.
- The ONU is offline.
- The OLT or ONU hardware is faulty.

The following section describes PON switching processes in three scenarios. The OLT's PON ports are running properly, and the ONU has registered with the OLT. Users have issued the same settings of the PON line to PON port 1 and PON port 2 on the OLT so that services can recover after protection switching.

Scenario 1: Branch Fiber Connected to a Single ONU Becomes Faulty

Figure 16-13 shows the scenario in which the branch fiber connected to a single ONU becomes faulty.

Figure 16-13 Branch fiber connected to a single ONU becomes faulty



1. Both the ONU and OLT check the link status and determine whether to trigger protection switching based on the link status.
 - If the OLT detects a fault on link A in **Figure 16-13**, it automatically switches to the protection link and uses the protection link to send messages to ONU 1 to notify that protection switching has occurred. In addition, the OLT notifies ONU 1 of the switching cause.
 - If ONU 1 detects a fault on link A in **Figure 16-13**, it automatically switches to the protection link and sends messages to the OLT to notify that protection switching has occurred. In addition, the ONU notifies the OLT of the switching cause.
2. After switching, services on ONU 1 are transmitted to the OLT through the protection port, all the feeder fibers connected to the OLT transmitted service packets, and ONU N is not affected. The changes on ONU 1 are as follows:
 - The state of the working port changes to standby.
 - The state of the protection port changes to active, and service packets are transmitted through link B in **Figure 16-13**.
3. After protection switching, ONU 1 can automatically switch back to the working port. The OLT sends an automatic switchback message and the switchback time, called the wait to restore (WTR) time, to the ONU.
 - If the OLT learns that ONU 1's working port and the working line are functioning properly and the working line stays normal during the WTR time, the OLT automatically switches back to the working line when the

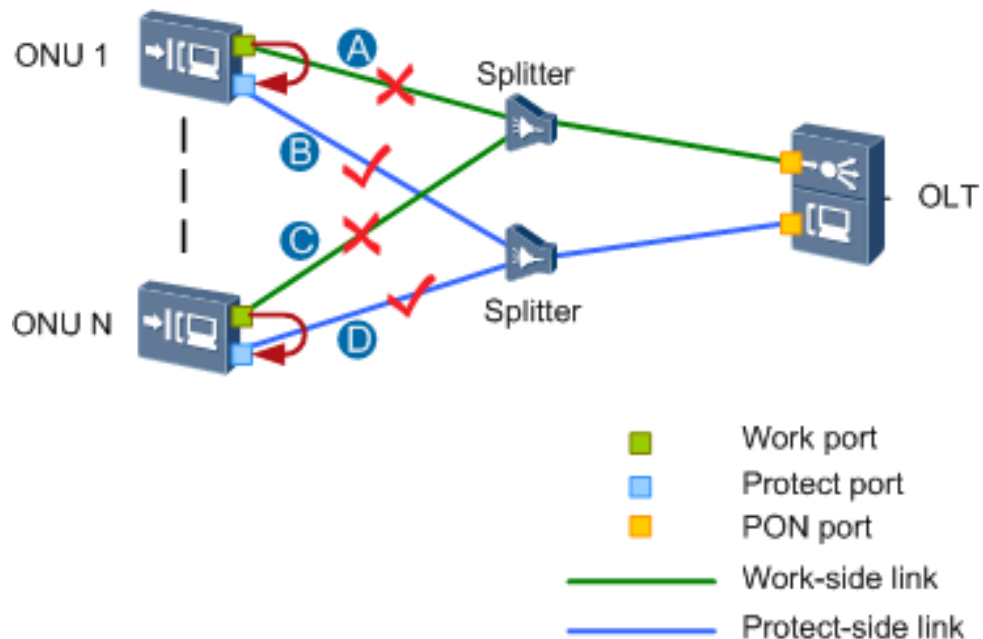
WTR time expires. In addition, the OLT notifies the ONU of the switching and switching cause.

- If ONU 1 learns that its working port and the working line are functioning properly and the working line stays normal during the WTR time, the ONU automatically switches back to the working line when the WTR time expires. In addition, the ONU notifies the OLT of the switching and switching cause.

Scenario 2: All Branch Fibers Connected to the ONU Become Faulty

Figure 16-14 shows the scenario in which all branch fibers connected to the ONU become faulty.

Figure 16-14 All branch fibers connected to the ONU become faulty



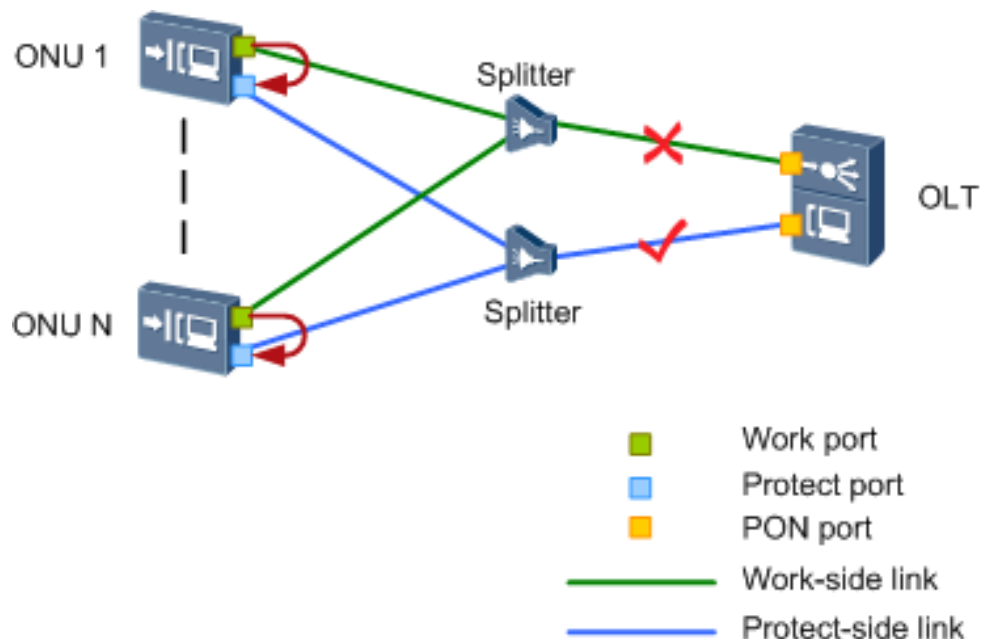
1. Both the ONU and OLT check the link status and determine whether to trigger protection switching based on the link status.
 - If the OLT detects that all branch fibers connected to the working line become faulty, it automatically switches to the protection link and uses the protection link to send messages to all the ONUs to notify that protection switching has occurred. In addition, the OLT notifies all the ONUs of the switching cause.
 - If the ONU detects a fault on all the branch fibers connected to the working link, it automatically switches to the protection link and sends messages to the OLT to notify that protection switching has occurred. In addition, the ONU notifies the OLT of the switching cause.
2. After switching, services on the ONU are transmitted to the OLT through the protection port (that is, service packets are transmitted by the protection link). The changes on the ONU are as follows:

- The state of the working port changes to standby.
 - The state of the protection port changes to active.
3. After protection switching, the ONU can automatically switch back to the working port. The OLT sends an automatic switchback message and the switchback time, called the WTR time, to the ONU.
- If the OLT learns that the working port and working links are functioning properly and link A stays normal during the WTR time, the OLT automatically switches back to the working link when the WTR time expires. In addition, the OLT notifies the ONU of the switching and switching cause.
 - If the ONU learns that the working port and working link are functioning properly and link A stays normal during the WTR time, the ONU automatically switches back to the working link when the WTR time expires. In addition, the ONU notifies the OLT of the switching and switching cause.

Scenario 3: Backbone Fiber Becomes Faulty

Figure 16-15 shows the scenario in which the backbone fiber becomes faulty.

Figure 16-15 Backbone fiber becomes faulty



1. Both the ONU and OLT check the link status and determine whether to trigger protection switching based on the link status.
 - If the OLT detects a fault on the working link, it automatically switches to the protection link and uses the protection link to send messages to all the ONUs to notify that protection switching has occurred. In addition, the OLT notifies all the ONUs of the switching cause.

- If the ONU detects a fault on the working link, it automatically switches to the protection link and sends messages to the OLT to notify that protection switching has occurred. In addition, the ONU notifies the OLT of the switching cause.
- 2. After switching, services on the ONU are transmitted to the OLT through the protection port (that is, service packets are transmitted by the protection link). The changes on the ONU are as follows:
 - The state of the working port changes to standby.
 - The state of the protection port changes to active.
- 3. After protection switching, the ONU can automatically switch back to the working port. The OLT sends an automatic switchback message and the switchback time, called the WTR time, to the ONU.
 - If the OLT learns that the working port and working links are functioning properly and link A stays normal during the WTR time, the OLT automatically switches back to the working link when the WTR time expires. In addition, the OLT notifies the ONU of the switching and switching cause.
 - If the ONU learns that the working port and working link are functioning properly and link A stays normal during the WTR time, the ONU automatically switches back to the working link when the WTR time expires. In addition, the ONU notifies the OLT of the switching and switching cause.

16.3.4 Dual-Homing xPON Type C Protection Principles

On a dual homing network, two PON lines, one working as the active line and one as standby, between an ONU and two OLTs cannot forward packets at the same time. An automatic switchover can be triggered by any of the following conditions:

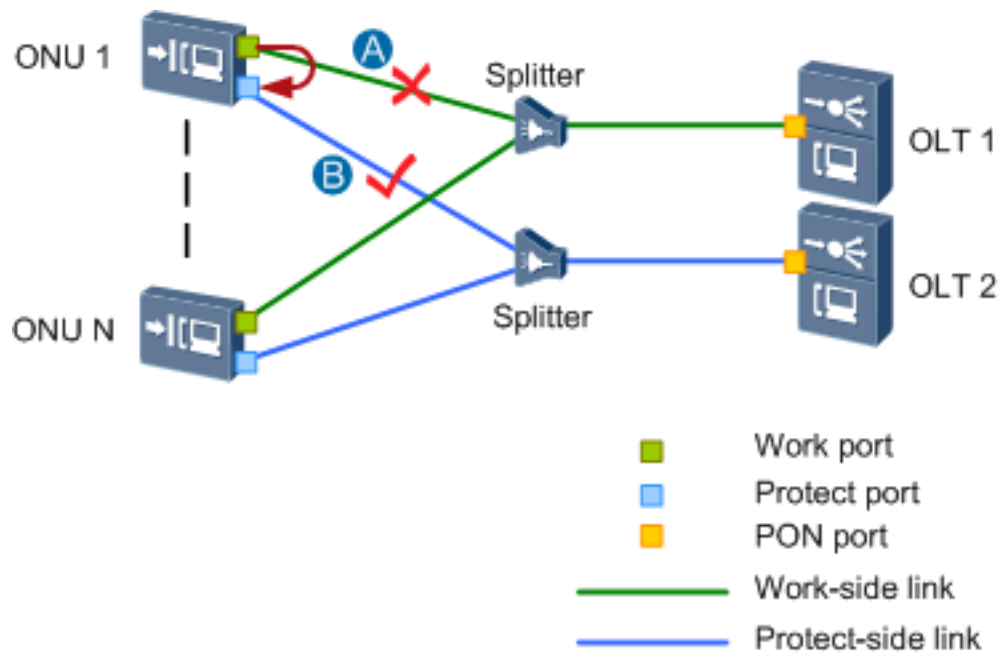
- Loss of signal (LOS) occurs in the input direction.
- The ONU is offline.
- The OLT or ONU hardware is faulty.
- The OLT's uplink is faulty (this condition triggers automatic switching only in the associated protection switching scenario).

The following section describes the PON switching processes in five scenarios. OLT 1 and OLT 2 are running properly, and the ONU has registered with the OLTs. Users issue the PON's configurations to OLT 1 and OLT 2 so that ONU's services can recover after the switching.

Scenario 1: Branch Fiber Connected to a Single ONU Becomes Faulty

Figure 16-16 shows the scenario in which the branch fiber connected to a single ONU becomes faulty.

Figure 16-16 Branch fiber connected to a single ONU becomes faulty

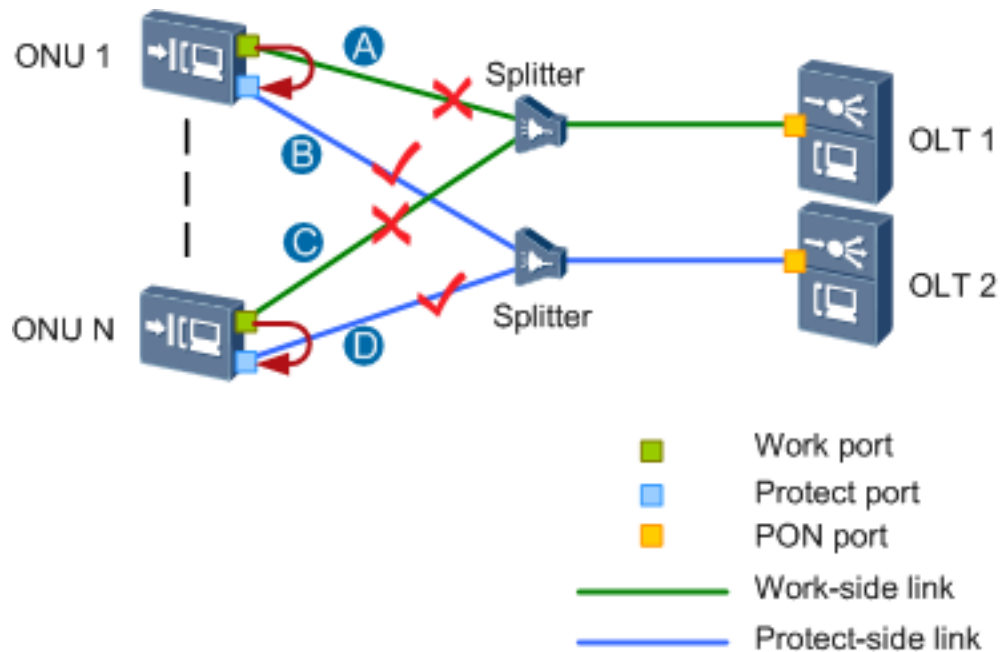


- If ONU 1 detects a fault on link A in [Figure 16-16](#), it automatically switches to the protection link and sends messages to OLT 2 to notify that protection switching has occurred. In addition, the ONU notifies OLT 2 of the switching cause.
- After switching, services on ONU 1 are transmitted to the OLT through the protection port, all the backbone fibers connected to the OLT transmit service packets, and ONU N is not affected. The changes on ONU 1 are as follows:
 - The state of the working port changes to standby.
 - The state of the protection port changes to active and service packets are transmitted through link B in [Figure 16-16](#).
- After protection switching, ONU 1 can automatically switch back to the working port. The OLT sends an automatic switchback message and the switchback time, called the wait to restore (WTR) time, to the ONU. If ONU 1 learns that the working port, working link, and the uplink of OLT 1 are functioning properly and link A stays normal during the WTR time, ONU 1 automatically switches to the working link when the WTR time expires.

Scenario 2: All Branch Fibers Connected to the Active Link Become Faulty

[Figure 16-17](#) shows the scenario in which all branch fibers connected to the active link become faulty.

Figure 16-17 All branch fibers connected to the active link become faulty

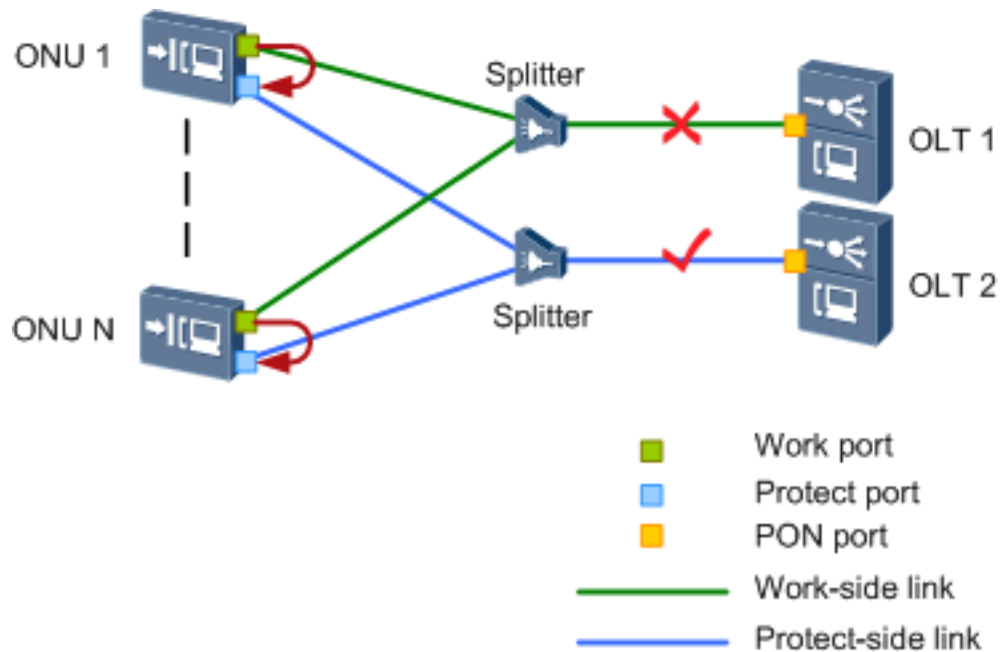


- If the ONU detects a fault on all the branch fibers connected to the working link, it automatically switches to the protection link and sends messages to OLT 2 to notify that protection switching has occurred. In addition, the ONU notifies OLT 2 of the switching cause.
- After switching, services on the ONU are transmitted to OLT 2 through the protection port (that is, service packets are transmitted by the protection link). The changes on the ONU are as follows:
 - The state of the working port changes to standby.
 - The state of the protection port changes to active.
- After protection switching, the ONU can automatically switch back to the working port. The OLT sends an automatic switchback message and the switchback time, called the WTR time, to the ONU. If the ONU learns that the working port, working links, and the uplink of OLT 1 are functioning properly and link A and link C stays normal during the WTR time, the ONU automatically switches to the working links when the WTR time expires.

Scenario 3: Backbone Fiber Becomes Faulty

Figure 16-18 shows the scenario in which the backbone fiber becomes faulty.

Figure 16-18 Backbone fiber becomes faulty

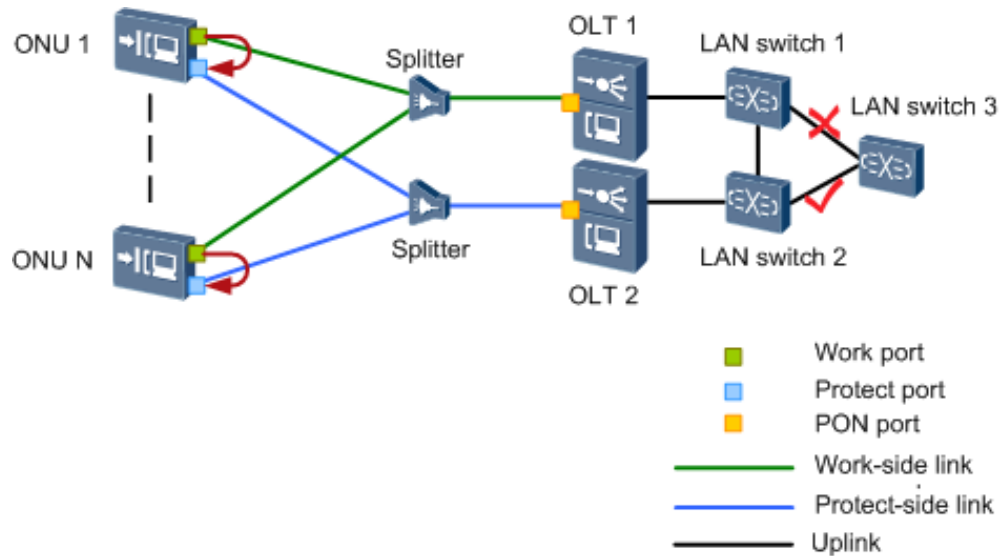


- If the ONU detects a fault on the backbone fiber, it automatically switches to the protection link and sends messages to OLT 2 to notify that protection switching has occurred. In addition, the ONU notifies OLT 2 of the switching cause.
- After switching, services on the ONU are transmitted to OLT 2 through the protection port (that is, service packets are transmitted by the protection link). The changes on the ONU are as follows:
 - The state of the working port changes to standby.
 - The state of the protection port changes to active.
- After protection switching, the ONU can automatically switch back to the working port. The OLT sends an automatic switchback message and the switchback time, called the WTR time, to the ONU. If the ONU learns that the working port, working links, and the uplink of OLT 1 are functioning properly and link A and link C stays normal during the WTR time, the ONU automatically switches to the working links when the WTR time expires.

Scenario 4: Associated Protection Switching Caused by a Fault on the OLT's Uplink

An OLT protection group is associated with the BFD or MEP session. Based on the association, when the upper-layer network connection (or IP layer link) of the OLT fails, the OLT instructs the ONU to trigger protection switching, which ensures service continuity. [Figure 16-19](#) shows the associated protection switching caused by a fault on the OLT's uplink.

Figure 16-19 Associated protection switching caused by a fault on the OLT's uplink

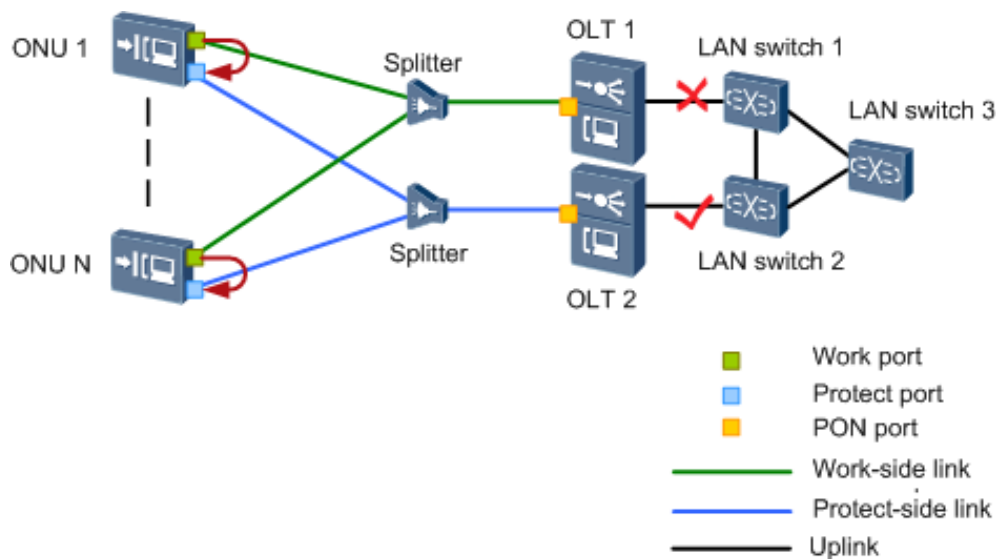


- On the OLT, the dual-homing protection group is associated with the BFD or MEP session. If the upstream route of the OLT fails, the BFD session status becomes **Down** or the MEP detection fails. In such a case, the OLT notifies the ONU of the uplink change.
- After the ONU receives the switching instruction from the OLT, it determines to trigger the switching and switches to the protection link. After the switching, the ONU notifies OLT 1 of the switching using the working link and notifies OLT 2 of the switching using the protection link.
- After switching, services on the ONU are transmitted to OLT 2 through the protection port (that is, service packets are transmitted by the protection link). The changes on the ONU are as follows:
 - The state of the working port changes to standby.
 - The state of the protection port changes to active.
- After protection switching, the ONU can automatically switch back to the working port. The OLT sends an automatic switchback message and the switchback time, called the WTR time, to the ONU. If the ONU learns that the working port, working links, and the uplink of OLT 1 are functioning properly and link A and link C stays normal during the WTR time, the ONU automatically switches to the working links when the WTR time expires.

Scenario 5: Associated Protection Switching Caused by a Fault on the OLT's Layer 2 Physical Link

An OLT protection group is associated with the uplink Ethernet port status. Based on the association, when the Layer 2 physical link of the OLT fails, the OLT instructs the ONU to trigger protection switching, which ensures normal service transmission. [Figure 16-20](#) shows the associated protection switching caused by a fault on the OLT's Layer 2 physical link.

Figure 16-20 Associated protection switching caused by a fault on the OLT's Layer 2 physical link



- On the OLT, the protection group is associated with the uplink Ethernet port status. When the Ethernet port associated with the protection group becomes **Down**, the OLT notifies the ONU of the uplink change.
- After the ONU receives the switching instruction from the OLT, it determines to trigger the switching and switches to the protection link. After the switching, the ONU notifies OLT 1 of the switching using the working link and notifies OLT 2 of the switching using the protection link.
- After switching, services on the ONU are transmitted to OLT 2 through the protection port (that is, service packets are transmitted by the protection link). The changes on the ONU are as follows:
 - The state of the working port changes to standby.
 - The state of the protection port changes to active.
- After protection switching, the ONU can automatically switch back to the working port. The OLT sends an automatic switchback message and the switchback time, called the WTR time, to the ONU. If the ONU learns that the working port, working links, and the uplink of OLT 1 are functioning properly and link A and link C stays normal during the WTR time, the ONU automatically switches to the working links when the WTR time expires.

16.3.5 Configuring xPON Type C Single-Homing Protection

This section describes how to configure xPON type C single-homing protection. Each optical network unit (ONU) provides two xPON uplink ports and connects to two xPON ports on an OLT through different optical splitters. This protects feeder and drop fibers and ensures high network reliability.

Context

After xPON type C single-homing protection is configured, the service configurations on the ONUs remain unchanged and data is transmitted or

received over the active uplink ports on the ONUs and the active xPON port on the OLT.

 NOTE

Configurations of xPON network protection do not affect service configuration. This topic describes how to perform configurations of xPON network protection. For details about how to perform service configuration, see the specific service configuration guide.

Precaution

Procedure

- Step 1** Run the **ont add** command to add a working ONU.
- Step 2** Run the **ont add portid ontid protect-side** command to add a protection ONU.
Ensure that the **protect-side** parameter is selected.
- Step 3** Run the **protect-group protect-target gpon-uni-ont** command to add a xPON Type C protection group. The working mode of the protection group can only be **portstate**.
- Step 4** Run the **protect-group member** command to add the working ONU to the protection group as a working member.
- Step 5** Run the **protect-group member** command to add the protection ONU to the protection group as a protection member.

 NOTE

Ensure that **ont ontid** value is the ONT ID specified in [Step 1](#).

- Step 6** Run the **protect-group enable** command to enable the xPON protection group.
A created protection group is disabled by default.

----End

Result

After the configuration, both the active and standby OLT xPON ports work in active mode. Both the ONU and OLT check the link status and determine whether to perform switchover accordingly.

Automatic protection switchover is triggered if one of the following requirements is met:

- Loss of signal (LOS) occurs in the input direction.
- The OLT or ONU hardware is faulty.

Example

The following configurations are used as an example to configure GPON type C single-homing protection on an OLT and ONUs:

- Ports on the same GPON service board: 0/1/0 and 0/1/1
- Working link: connected to port 0/1/0

- Protection link: connected to port 0/1/1
- ONU ID: 0
- ONU authentication mode: SN; SN: hwhw-10101500; management mode: OMCI
- ID of the line profile bound to the ONU: 10

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 0 sn-auth hwhw-10101500 omci ont-lineprofile-id 10
huawei(config-if-gpon-0/1)#ont add 1 0 protect-side
huawei(config-if-gpon-0/1)#quit
huawei(config)#protect-group protect-target gpon-uni-ont workmode portstate
huawei(protect-group-1)#protect-group member port 0/1/0 ont 0 role work
huawei(protect-group-1)#protect-group member port 0/1/1 ont 0 role protect
huawei(protect-group-1)#protect-group enable
huawei(protect-group-1)#quit
```

16.3.6 Configuring xPON Type C Dual-Homing Protection

Type C dual-homing protection protects any node between an optical network unit (ONU) and the two dual-homed OLTs.

Context

Precaution

Compared with xPON type C single-homing protection, xPON type C dual-homing protection features enhanced protection capabilities but more complicated networking and higher deployment costs.

NOTE

Configurations of xPON network protection do not affect service configuration. This topic describes how to perform configurations of xPON network protection. For details about how to perform service configuration, see the specific service configuration guide.

Procedure

Step 1 Configure xPON type C dual-homing protection on the active OLT.

1. Run the **ont add** command to add a working ONU.
2. Run the **protect-group** command to create a protection group.

Run the **description** command to configure the description of a PG.

3. Run the **protect-group member** command to add a working member to the protection group.

NOTE

After this step is performed, the protection group is automatically enabled.

Step 2 Configure xPON type C dual-homing protection on the standby OLT.

1. Run the **ont add** command to add a protection ONU.

NOTE

Ensure that all profiles on the ONUs connected to the active and standby OLTs are the same. The profiles include the dynamic bandwidth allocation (DBA) profile and line profile.

2. Run the **protect-group** command to create a protection group.
Run the **description** command to configure the description of a PG.
 3. Run the **protect-group member** command to add a protection member to the protection group.
 4. Run the **protect-group enable** command to enable the protection group.
- End

Result

After the configuration, both the active and standby OLTs are in the working state. The ONU and active/standby OLTs check the link status to determine whether to perform switchover accordingly.

An automatic switchover can be triggered by any of the following conditions:

- Loss of signal (LOS) occurs in the input direction.
- The OLT or ONU hardware is faulty.

Example

The following configurations are used as an example to configure GPON type C dual-homing protection on two OLTs:

- Active OLT: OLT_A; standby OLT: OLT_B
- GPON service ports: 0/1/0 on the two OLTs
- ID of the protection groups: 1
- ONU ID: 0
- ONU authentication mode: SN; SN: hwhw-10101500; management mode: OMCI
- ID of the line profile bound to the ONU: 10

OLT_A configurations:
huawei_A(config)#**interface gpon 0/1**
huawei_A(config-if-gpon-0/1)#**ont add 1 0 sn-auth hwhw-10101500 omci ont-lineprofile-id 10**
huawei_A(config-if-gpon-0/1)#**quit**
huawei_A(config)#**protect-group 1 protect-target gpon-uni-ont workmode dual-parenting**
huawei_A(protect-group-1)#**protect-group member port 0/1/0 ont 0 role work**
OLT_B configurations:
huawei_B(config)#**interface gpon 0/1**
huawei_B(config-if-gpon-0/1)#**ont add 1 0 sn-auth hwhw-10101500 omci ont-lineprofile-id 10**
huawei_B(config-if-gpon-0/1)#**quit**
huawei_B(config)#**protect-group 1 protect-target gpon-uni-ont workmode dual-parenting**
huawei_B(protect-group-1)#**protect-group member port 0/1/0 ont 0 role protect**
huawei_B(protect-group-1)#**protect-group enable**

16.3.7 xPON Type C Protection Reference Standards and Protocols

Standard No.	Description
ITU-T G.984.1	General Characteristics. This protocol mainly describes the basic features and major protection modes of GPON.

Standard No.	Description
ITU-T G.984.2	Physical Media Dependent (PMD) Layer Specification. This protocol mainly describes the PMD layer parameters, including physical parameters (such as the transmit optical power, receiver sensitivity, and overload optical power) of optical transceivers, and also defines optical budget of different levels, for example, the most common Class B+.
ITU-T G.984.3	Transmission Convergence Layer Specification. This protocol mainly describes the TC layer specifications, including the upstream and downstream frame structures and GPON principle.
ITU-T G.984.4	ONT Management And Control Interface Specification. This protocol mainly describes the GPON management and maintenance protocols, such as OAM, PLOAM, and OMCI.
ITU-T G.984.5	Enhancement Band. This protocol mainly describes the GPON wavelength planning, including reserving bands for next-generation PON.
ITU-T G.984.7	Long Reach. This protocol mainly describes several long reach PON schemes for extending GPON transmission distance.
ITU-T G.988	ONU management and control interface (OMCI) specification.
TR-156	Using GPON Access in the context of TR-101.

16.4 Redundancy Backup of Control Boards

An OLT configured with two control boards works in the load sharing mode. When working normally, the active and standby control boards concurrently forward service packets.

16.4.1 Introduction to Control Board Redundancy Backup

Definition

In this feature, two control boards, one working as the active and the other working as the standby, are configured to back up each other. When the two control boards work normally in load sharing mode, active and standby control boards concurrently forward service packets, and redundancy backup improves reliability of services as well as doubling bandwidth and enhancing data forwarding performance.

The redundancy backup of control boards benefits customers with the following capabilities:

- Quick switching between active and standby control boards
- Uninterrupted data forwarding during active/standby switchover
- Concurrent upgrade of the active and standby control boards

NOTE

The MA5800 configured with two control boards does not support the active/standby mode for the forwarding plane.

NOTE

In the case of dual control boards, the dual-uplink networking must be configured.

Introduction

The MA5800 configured with two control boards uses active/standby mode for the control plane and load sharing mode for the forwarding plane.

- On the control plane, the two control boards work in the active/standby mode. The CPU on the active control board manages the system and processes control protocol packets while the CPU on the standby control board is in the standby state.
- On the forwarding plane, the active and standby control boards share loads. Both boards forward data.

The MA5800 supports decoupling of the control plane and forwarding plane for the control board. When the **system switch-over** command is executed to trigger an active/standby switchover of the control plane, the forwarding plane of the standby control board continuously works and service bandwidths are not affected. This feature reduces impacts on services of the forwarding plane brought by a control plane reset in fault and upgrade scenarios for the control board, improving system In-Service Software Upgrade (ISSU) capabilities and reliability.

The MA5800 supports hot reset of the active or standby control board. During a hot reset, the forwarding plane continuously works and service bandwidths are not affected.

- Run the **reboot active hot** command to perform a hot reset on the active control board. After the CPU of the active control board resets, the system automatically switches to the standby control board. Then, the original active control board becomes the standby control board, ongoing online services are not offline, and bandwidths of existing services are not lowered.

- Run the **reboot standby hot** command to perform a hot reset on the standby control board. After the CPU of the standby control board resets, ongoing online services are not offline, and bandwidths of existing services are not lowered.

16.4.2 Principle of Active/Standby Mode

Switchover Modes

- **Automatic active/standby switchover**

When the active control board fails, the system automatically performs an active/standby switchover. Specifically, the system resets the active control board, and the standby control board functions as the new active control board. During the whole process, the system continues processing data and services are not interrupted.

- **Manual active/standby switchover**

When you need to replace the active control board or upgrade the system software, manually perform an active/standby switchover using one of the following methods:

- Run the **system switch-over** command.
- Run the **reboot active [hot]** command to reset the active control board.
- Press the RESET button on the active control board to reset the board.
- Remove the active control board.

NOTICE

- During system running, if an active/standby switchover is performed by removing the active control board or pressing the RESET button, the hardware may be faulty or software data is not synchronized, leading to service failures. In this case, it is not recommended to remove the active control board or press the RESET button to perform an active/standby switchover. Specially, do not remove or install the active control board frequently in a short period of time.
 - If the active control board has a daughter board and the standby control board does not have one, the BFD configuration will be lost after an active/standby switchover. Therefore, you are not advised to perform an active/standby switchover.
-

Communication Between the Active and Standby Control Boards

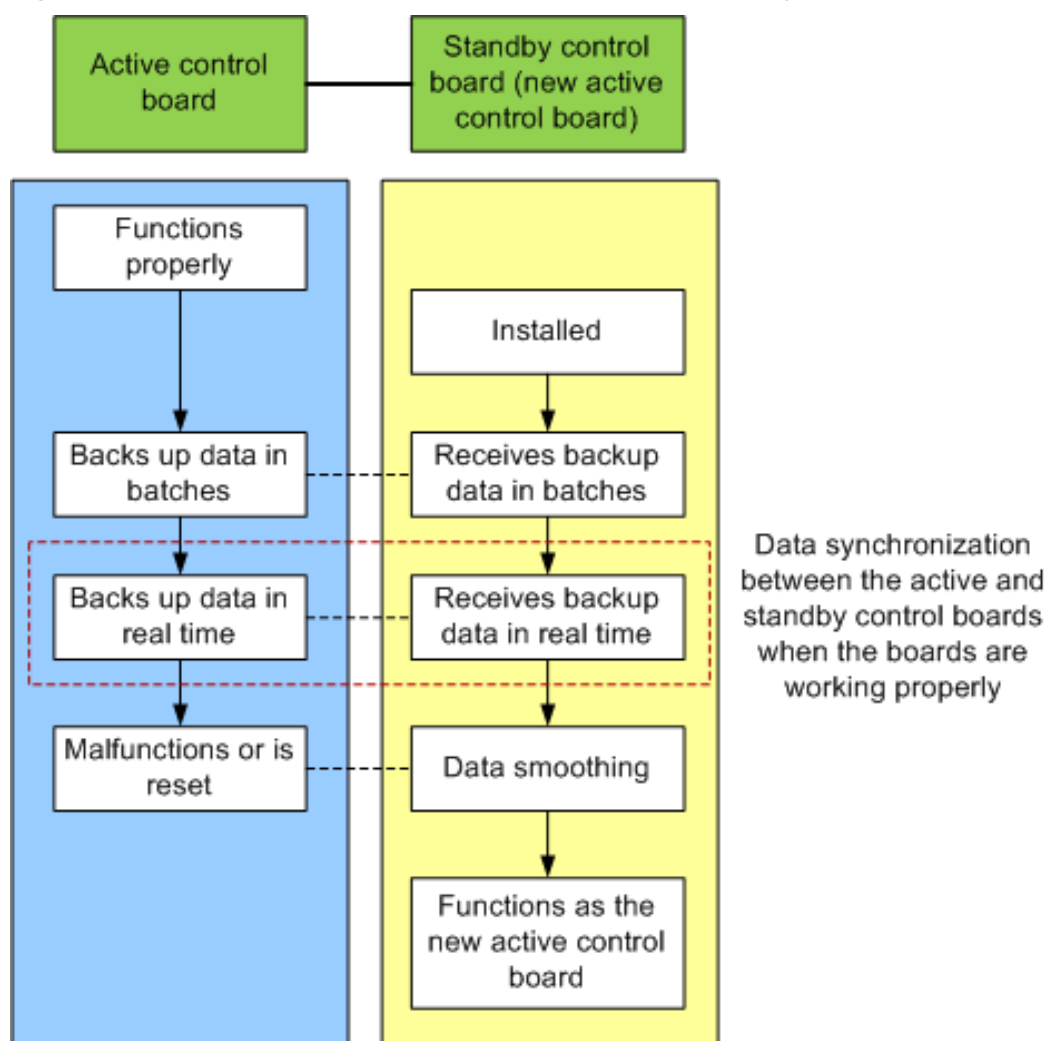
When two control boards are configured, the active control board is working and the standby control board is in the standby state. The standby control board exchanges information only with the active control board. The maintenance Ethernet port (designated with the ETH silkscreen) on the standby control board does not receive configuration commands. The serial port (designated with the CON silkscreen) on the standby control board receives configuration commands and forwards the commands to the active control board. Then the active control board issues the configurations to service boards. You can log in to the device only at the local end through the local serial port. The user name and password are

used for authentication. The serial port is enabled by default and is usually used during device deployment. If the serial port is enabled for a long time, security risks may exist. You are advised to run the **sysman console disable** command to disable the serial port if it is not needed.

The active and standby control boards achieve data consistency between them using high availability (HA) mechanisms such as batch backup and real-time backup. When learning that the active control board fails or receiving an active/standby switchover command, the standby control board takes over as the active control board and reports switchover events.

Figure 16-21 shows the state transition between the active and standby control boards in active/standby mode.

Figure 16-21 State transition between the active and standby control boards



- **Batch backup**

After the standby control board is installed, the active control board automatically backs up data of all modules to the standby control board in batches.

- **Real-time backup**

After batch backup is complete, the system enters the real-time backup state. In this state, the active control board backs up data to the standby control board in real time. When both control boards function properly, the system stays in the real-time backup state.

Real-time backup maintains data consistency (also called data synchronization) between the active and standby control boards. The following data needs to be synchronized:

- Configuration data: core data, also the static data, running in the system, including all configurations manually issued by users and data that is generated based on user configurations in system initialization and ensures normal system running.
- Basic operating data: data that may change rarely during system running, including the device status (such as board status and port status), operation logs, and alarms. The basic operating data changes when the system status changes, for example, a board is faulty or a port connection status changes.
- Dynamic service data: data that changes in real time during system running, including data generated by a call service (such as a PPPoE dialup) and data changing quickly (such as an ARP entry change). The dynamic service data takes a majority of data to be synchronized, and it is the most difficult to be completely synchronized. Data smoothing is mainly performed for such data.

You can run the **display data sync state** command to query the data synchronization status (complete synchronization or incomplete synchronization).

- When all data on the standby control board is completely synchronized with that on the active control board, it is called complete synchronization.

An active/standby switchover performed when data is completely synchronized is called a **normal switchover**. A normal switchover does not interrupt services. A normal switchover can be performed only after data (including configuration data, basic operating data, and dynamic service data) is completely synchronized and the cyclic redundancy check (CRC) results on the active and standby control boards are the same.

- When data on the standby control board is not completely synchronized with that on the active control board, it is called incomplete synchronization.

An active/standby switchover performed when the data is not completely synchronized is called a **forced switchover**. [Table 16-6](#) lists three conditions of incomplete synchronization and whether forced switchover is supported in each condition.

Table 16-6 Active/standby switchover in the case of incomplete synchronization

Data Incompletely Synchronized	Supports Forced Switchover by Commands	Supports Forced Switchover by Board Reset (Manually or Using Commands) or Board Removal	Switchover Results
Configuration data	No	Yes	The system resets and services are interrupted. Forced switchover is not recommended.
Basic data	No	Yes	The system does not reset but the service board may reset and some services are interrupted. Forced switchover is not recommended.
Some dynamic service data	Yes	Yes	Data that is not synchronized to the standby control board is lost after the switchover, but services are not affected, and data about connections, alarms, and logs is not lost.

• **Data smoothing**

In the real-time backup state, if an active/standby switchover occurs, the standby control board will be promoted to the active role. Before the standby control board becomes active, modules on the standby control board collect and synchronize data from service boards. The data collection and synchronization process is called data smoothing. During data smoothing, modules on the standby control board actively communicate with service boards to confirm and synchronize hardware status, link layer status, and configuration data. In this manner, data and status information are consistent through the entire system so that the system can run normally after the switchover.

The data smoothing duration is very short. After data smoothing is complete, the standby control board works as the new active control board.

Communication Between Service Boards and Control Boards

Service boards are connected to the active and standby control boards through buses. Data of service boards and data of the standby control board come from the active control board.

When working normally, service boards and the active control board exchange control protocol packets. When an active/standby switchover occurs, service boards check out the switchover through hardware signals and then exchange control protocol packets with the original standby control board (now functions as the active control board).

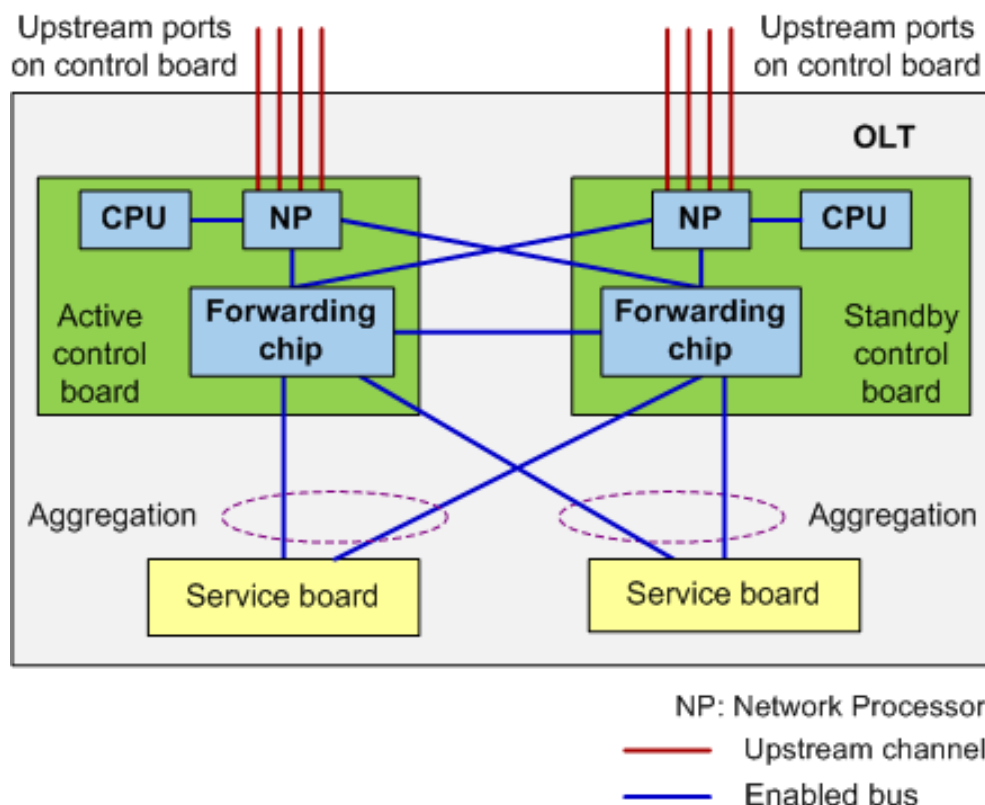
16.4.3 Principle of Load-sharing Mode

The MA5800 supports separation between the control plane and forwarding plane. When both active and standby control boards work normally, their CPUs manage their forwarding planes respectively. When the CPU of the active board is faulty, an active/standby switchover occurs, and the forwarding plane is not affected. When the CPU of the standby control board is faulty, the standby control board automatically restarts, and the forwarding plane is not affected either. The two control boards work in load sharing mode on forwarding planes, that is, both of them forward data and upstream ports are in working state at the same time. Also, traffic is sent from service boards to active and standby control boards in load sharing mode.

NOTE

When the main control board fails to start, both the control plane and forwarding plane fail.

Figure 16-22 Principle of load-sharing mode



16.5 Ethernet Port Protection Group

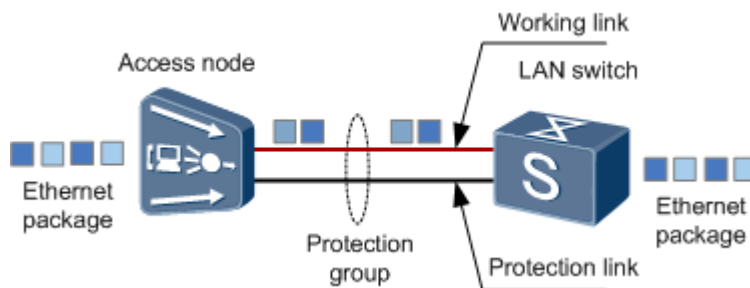
An Ethernet port protection group binds two or more Ethernet ports together. The working port carries services, while the protection port provides backup and does not carry services. If the working port is faulty, the services carried by it are switched to the protection port, automatically or manually as required. Ethernet port protection ensures uninterrupted service transmission and improves reliability of links.

16.5.1 Introduction to Protection Group of Ethernet Ports

Access network users, especially corporations and large residential communities, are posing stringent requirements on network reliability. If the upstream links of access devices are not protected, services carried over these upstream links will be interrupted if the links break or the upper-layer devices are malfunctioning. For the access devices that provide services to tens of thousands of users, carriers usually demand protection for the upstream ports. Specifically, services can be switched between links automatically or manually, depending on your requirements, for example, when the upstream link is broken. Such a protection group ensures that an upstream link is always available, improving reliability.

Figure 16-23 shows an example of an Ethernet port protection group between two interconnected devices. In this protection group, two Ethernet ports are bound. One Ethernet port protection group has two members. One member carries services over the working link, and the other member provides backup over the protection link.

Figure 16-23 Example of Ethernet port protection



According to the number of upstream Ethernet ports, members in a protection group can be ports or LAGs. Access devices support Timedelay Ethernet port protection group. A Timedelay Ethernet port protection group also switches services based on port status, but the protection port is disabled when the working port is functioning properly. If the working port is faulty, the protection port remains enabled for a predefined period of time. Services are switched to the protection port if this port is functioning properly during this period. If the protection port is malfunctioning during this period, the Timedelay protection group retries the working port while it keeps the protection port disabled. The protection group will repeat the preceding process until one port restores the normal state, and then switch services to it.

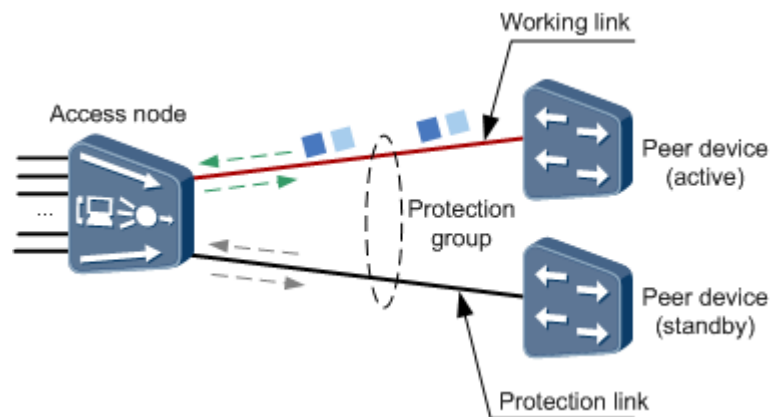
16.5.2 Principle of Timedelay Protection

Establishment of a Timedelay Protection Group

A Timedelay protection group is established after it is configured, and the interconnected devices implement protection without the need of negotiation.

In the protection group, the working port is enabled to transceive data and a service is transmitted over the link carried by the port; the protection port is disabled and no service is transmitted over the link carried by it. In the Timedelay protection scenario, the access device can be either single-homed or dual-homed to the upper-layer devices. [Figure 16-24](#) shows how data is transceived in the dual-homing scenario.

Figure 16-24 Data transceiving within a Timedelay protection group



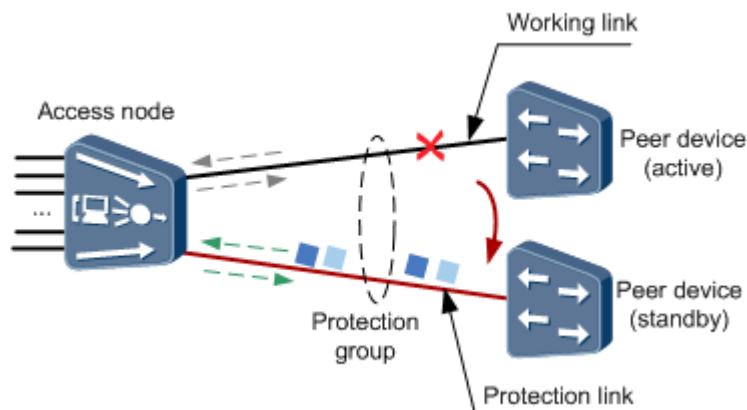
Protection Switching

A Timedelay protection group undergoes protection switching on any of the following conditions:

- The working port is faulty.
- Users manually start a forced protection switching.

If the working link is faulty, services are switched to the protection link to ensure uninterrupted forwarding, as shown in [Figure 16-25](#).

Figure 16-25 Data transceiving within a Timedelay protection group (after protection switching)



Timedelay protection switching is implemented as follows:

1. The access device detects a working port failure and immediately enables its protection port.
2. In the Timedelay protection group, the access device plays an "active" role and immediately switches services after detecting a working port failure. Services are then switched to the protection link.

NOTICE

The working and protection ports on peer devices must be enabled.

Protection Reversion

If the protection switching is triggered by a forced switching command or a working port failure, services will not be switched back to the original link even if the original working port restores the normal state. Instead, the services are still carried over the protection link.

The **reversion enable** command is used to enable the reversion function of a protection group.

- The priority for a working member in a protection group to carry the service is higher than the priority for a protection member in the protection group to carry the service. When a fault that occurs on the working member causes the protection switch, if the time for the fault of the working member to recover exceeds the WTR time, the switch reversion is performed. The protection switch refers the switch under which the working member switches to the protection member, and the switch reversion refers to the switch under which the protection member switches to the working member.
- If the switch of a protection group is initiated by a manual switch or a forced switch, the switch of the protection group cannot be reversed.
- If the cancel manual switch and cancel forced switch operations are performed and the working member is normal, the switch reversion operation is performed after the WTR time expires.

16.5.3 Configuring a Timedelay Protection Group

A Timedelay protection group applies to the following scenario: The active and standby control boards or upstream service boards on an access device each provide an upstream Ethernet port, and users want port to carry services and the other port to back up. If the working port is faulty, the system switches services to the protection port to implement uninterrupted forwarding.

Prerequisites

- The boards and ports on the access device support Ethernet port protection groups.
- In the protection group, a static MAC address is configured only on the working port. You can run the **display mac-address** command to query the static MAC address.
- In a protection group, the two interconnected ports have the same data configurations and allow MAC address transfer.

Procedure

Step 1 (Optional) Configure the optical port shutdown function.

Run the **offline-tx-off-time** command to specify the time for keeping an optical port shut down in the case of a Linkdown. The optical port shutdown function helps improve protection switching performance.

Step 2 Create a Timedelay protection group.

Run the **protect-group** command to create a protection group (select **eth-nni-port** as the protection level and **Timedelay** as the protection type).

Step 3 Add a working port and a protection port to the protection group.

Run the **protect-group member** command to add one port on the control board or on the upstream board as the working port, and the other port on the board as the protection port in the protection group.

Step 4 Enable the protection group.

Run the **protect-group enable** command to enable the protection group.

Step 5 Query configurations about the protection group.

Run the **display protect-group** command to query configurations about the protection group. The configurations include the protection level, member ports, protection type, and reversion mode.

----End

Example

This example assumes a scenario in which the MA5800 connects to the upstream network through ports 0/9/0 and 0/9/1 which form a Timedelay protection group.

```
huawei(config)#protect-group 0 protect-target eth-nni-port workmode timedelay
huawei(protect-group-0)#protect-group member port 0/9/0 role work
huawei(protect-group-0)#protect-group member port 0/9/1 role protect
```

```
huawei(protect-group-0)#protect-group enable
huawei(protect-group-0)#display protect-group 0
```

Group ID	: 0
Protect Target	: Port of Ethernet nni
Work Mode	: timedelay
Description	:
Admin State	: enable
Operation	: none
Reversion	: disable
Reversion Time(s)	: 720

Member	Role	Operation	State	PeerMember
0/9/0	work	none	active	none
0/9/1	protect	none	standby	none

16.6 Ethernet Link Aggregation

Ethernet link aggregation is a process that aggregates two or more Ethernet ports of the same type to a logic port. It increases the link bandwidth without requiring a hardware upgrade and improves link reliability using the link backup mechanism.

16.6.1 Introduction to Ethernet Link Aggregation

As broadband services are widely used, carriers require higher bandwidth and reliability for Ethernet links.

Hardware upgrades can increase Ethernet link bandwidth but at high costs. In addition, hardware upgrades are less flexible than software upgrades. Ethernet link aggregation addresses these issues and supports the following functions:

- The maximum bandwidth of a link aggregation group (LAG) is equal to the total bandwidths of all links in a LAG. Hardware upgrades are not required and costs are curtailed.
- Traffic in a LAG is distributed to member links using the load sharing algorithm, implementing load sharing and improving link usage.
- Member links in a LAG dynamically back up each other. When one link is interrupted, a backup link immediately takes over.
- Link aggregation functions between interconnected devices only and is independent of the network topology.

A logical link aggregating several physical links is called a LAG.

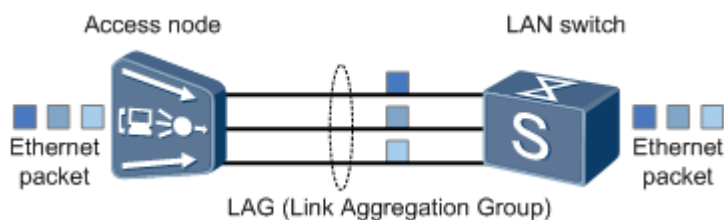


NOTE

Link aggregation is also called port aggregation because each link corresponds to two specific ports on an Ethernet network.

As shown in [Figure 16-26](#), two devices are interconnected through several pairs of Ethernet ports. These ports are bound into a logical link, called a LAG.

Figure 16-26 Link aggregation



16.6.2 Principle of LACP

Definition

LACP was developed based on IEEE 802.1AX. LACP dynamically aggregates and deaggregates Ethernet links using the following functions:

- Enables the data switching device to use a standard negotiation mode for link aggregation.

After LACP is enabled, the access device aggregates multiple links according to its configuration and enables the aggregation link to transmit and receive data.

Member ports in a LAG send LACP packets to notify the peer device of the information, including the system priority, system MAC address, port priority, port ID, and administrative key.

After receiving the information, the peer device compares the information with the one saved on other ports to select ports that can be aggregated. The interconnected devices reach an agreement on the ports that can transmit and receive data and determine which links carry traffic.

The LACP packets are sent in any of the following modes:

- Event-triggered transmission

A change in the state of the local device or in the local configuration triggers the generation and transmission of a new LACP packet.

- Periodic transmission

When an aggregation link is stable, the system state is periodically exchanged to maintain the aggregation link.

- Maintains the aggregation link by periodically exchanging the system state when the link is stable.

After aggregation links are generated, LACP maintains link status. When the aggregation condition changes, LACP automatically adjusts the links in the aggregation group. The aggregation condition changes if one or more of the following occurs:

- Physical port status changes.
- Board status changes.
- Results negotiated with the peer end are changed.

LACP Priority

LACP priority includes system priority and port priority. Priority setting allows negotiation of aggregation information between LAGs at two ends and real-time maintenance on link status.

Priority Type	Function	Description
System priority	Specifies the priority of a LAG on the device.	Determines which party in the interconnected devices is dominant in protocol negotiation. A device with a higher priority is dominant in LACP protocol negotiation, and the information provided by it prevails for such operations as selection of an active port. NOTE If interconnected devices have the same system priority, compare the system MAC addresses. The device with a smaller MAC address is dominant in LACP protocol negotiation.
Port priority	Specifies the priority of a port in a LAG.	Specifies the active ports in a LAG that will carry services with preference. Active ports in a LAG can be adjusted based on port priorities. NOTE In a LAG, if two ports have the same priority, the port with smaller subrack ID, slot ID, and port ID (<i>frameid/slotid/portid</i>) is preferentially selected as the active one.

NOTE

System priority and port priority work together to determine which ports in a LAG are used to carry services with preference. System priority prevails over port priority.

Timeout Time for Exchanging LACP Packets

The access device periodically sends and receives LACP packets to prevent information loss. If the device does not receive any LACP packets within three LACP packet exchanging periods, the device determines that the port is faulty.

To ensure detection sensitivity, LACP defines long timeout and short timeout.

The device uses short time for exchanging LACP packets by default except that the peer device requires long timeout.

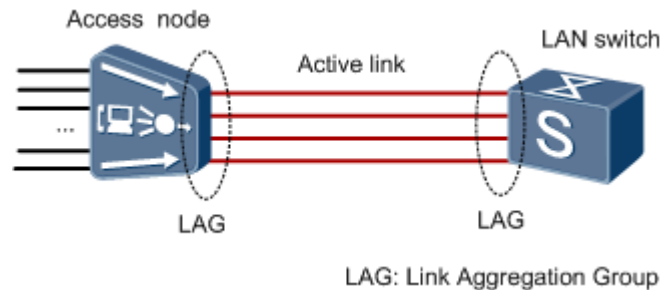
16.6.3 Introduction to Load Bearing

The device supports load sharing and load non-sharing for a LAG. Both load sharing and load non-sharing increase link bandwidth and improve link reliability, but they achieve this in different ways.

Load Sharing Link Aggregation

Each member link in a load sharing LAG carries traffic. Member links in the LAG share the load, as shown in [Figure 16-27](#).

Figure 16-27 Load Sharing link aggregation



To ensure packets carried on member links are correctly received on the peer device and ensure load balancing over member links in a LAG, the device allocates packets using hash algorithms based on:

- Source MAC addresses
- Source MAC addresses + destination MAC addresses
- Source IP addresses + destination IP addresses
- MPLS labels
- Packet quintuple (protocol, source IP address, destination IP address, source port, and destination port)

NOTE

Applications vary depending on device capabilities. Traffic distribution is calculated based on the hash algorithm. Therefore, bandwidth cannot be evenly allocated among links and different ports may differ significantly in traffic.

If member links in a LAG change or some member links become faulty, the device automatically reallocates traffic.

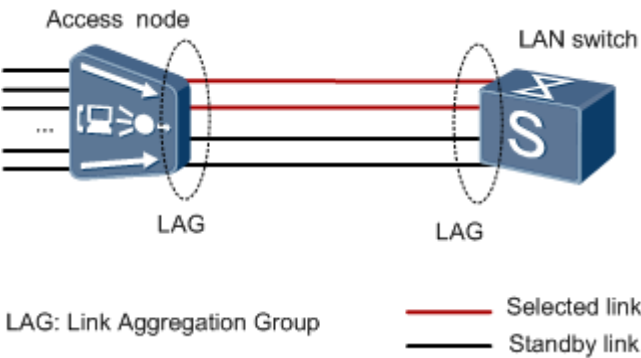
Load Non-Sharing Link Aggregation (Active/Standby Mode)

In a load non-sharing LAG, only some member links carry traffic and other links are in the standby state. Member links work in a hot standby mechanism, as shown in [Figure 16-28](#).

NOTE

Load non-sharing link aggregation is implemented by configuring the maximum number of links in a LAG, and it applies to a scenario where the device is single-homed to the upstream device.

Figure 16-28 Load non-sharing link aggregation (active/standby mode)



When the selected link fails, the device selects a link from the standby links to take over.

16.6.4 Introduction to LAG Type

The device supports manual aggregation and LACP aggregation for a LAG. [Table 16-7](#) defines them and describes their characteristics. If both interconnected devices support LACP, LACP aggregation is recommended.

Table 16-7 LAG type and characteristics

LAG Type	Definition	Application Scenario	Impact on Services
Manual aggregation	LACP is not enabled on the device. The device determines whether to aggregate a port according to its physical status (up or down), working mode, and rate.	The device is interconnected with the device that does not support LACP.	Interconnected devices do not fully negotiate with each other to aggregate links. In this case, when links work in forced GE mode and the receive or transmit direction of a member link fails (for example, when the optical fiber connected to a receive or transmit Ethernet port is cut), or when the link is incorrectly connected, the service transmit end cannot detect the fault. As a result, data may be lost.

LAG Type	Definition	Application Scenario	Impact on Services
LACP aggregation	LACP is enabled on the device. By running LACP, interconnected devices have the same aggregation information, including physical port status, working mode, rate, and LACP priority. An LACP LAG has more accurate and effective control over link aggregation than a manual LAG.	The device is interconnected with the device that supports LACP.	None

Table 16-8 lists the relationship between LAG type and load sharing mode.

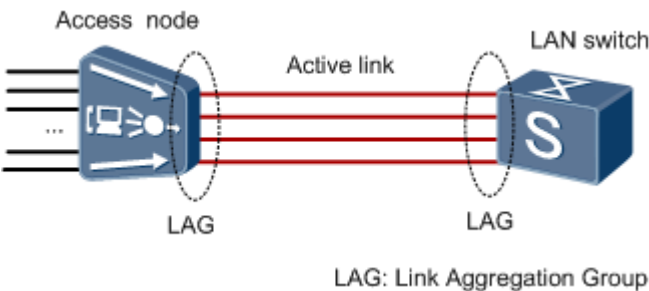
Table 16-8 Relationship between LAG type and load sharing mode

LAG Type	Load Sharing	Load Non-Sharing (Active/Standby Mode)
Manual aggregation	Supported	Not supported
LACP aggregation	Supported	Supported

Manual Aggregation

Figure 16-29 shows manual aggregation. In this type, load is shared on all member links, and there is no standby link.

Figure 16-29 Load Sharing link aggregation



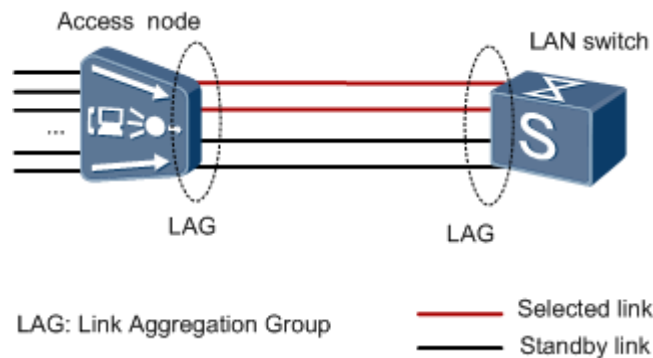
LACP Aggregation

LACP aggregation has the advantages of manual aggregation and LACP. In LACP aggregation, LACP is enabled only on the specified port, facilitating network topology control.

The network topology of LACP aggregation in load sharing is the same as that of manual aggregation, as shown in [Figure 16-29](#).

[Figure 16-30](#) shows LACP aggregation in load non-sharing.

Figure 16-30 Load non-sharing link aggregation (active/standby mode)



Member links in an LACP LAG are either selected links or standby links.

- A selected port is a working port that carries traffic.
- A standby port does not carry traffic.

The selected or standby state of a port changes with the change in system running or external environment.

- The port status change results in port status changes at the LACP layer. For example, if a port is faulty in a LAG, its state is switched to standby at the LACP layer.
- The LACPDU exchange may result in port status changes at the LACP layer. For example, a device may change the status of its ports after it receives an LACPDU from its peer device.

NOTE

For details about the frame structure of LACPDUs, see IEEE 802.1AX-2008.

16.6.5 Introduction to Port Type

Member ports in a LAG are classified into primary ports and secondary ports.

Table 16-9 Port type and characteristics

Port Type	Definition	Port Characteristics	
Primary port	Logical port representing a LAG in service configuration, used in service configuration and query.	Similarity: the primary and secondary ports are defined logically.	Difference • The primary port represents the LAG to participate in service configuration whereas secondary ports cannot participate in service configuration. • A LAG has only one primary port but can have several secondary ports. • The primary port can quit its affiliated LAG only after the LAG is deleted. A secondary port can be added to or deleted from a LAG. • After a LAG is deleted, its services are still carried by the primary port.
Secondary port	All member ports except for the primary port.		

 NOTE

- An Ethernet port can be added to only one LAG.
- If the primary port is faulty, secondary ports work. However, service-related operations can only be performed on the primary port.
- The device supports a LAG containing only one port. When the LAG requires expansion, you only need to add ports to the LAG but do not need to modify services.
- When a service is configured on ports in an inter-board LAG group, the service can be successfully configured only if all ports in this group support this service. If a port in the group does not support this service, the system displays message "The port does not support this operation" or "The board does not support this operation".

16.6.6 Principle of LAG Setup Process

 NOTE

A manual LAG does not use LACP. Therefore, principles of a manual LAG are not described here. For details, see IEEE 802.1AX.

The process of setting up an LACP LAG is as follows:

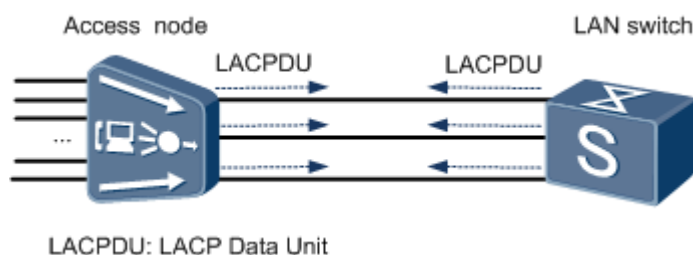
1. Interconnected devices send LACPDUs to each other.
2. Interconnected devices determine the actor (indicating the party that is dominant in negotiation) based on LACP system priorities and system IDs.

- Interconnected devices determine active ports (ports carrying traffic) based on the port LACP priorities and port IDs of the Actor.

Exchanging LACPDU Between Interconnected Devices

An LACP LAG is set up on interconnected devices, and member ports are added to the LAG. The member ports are enabled with LACP, enabling interconnected devices to exchange LACPDU to each other, as shown in [Figure 16-31](#).

Figure 16-31 Exchanging LACPDU between interconnected devices of an LACP LAG

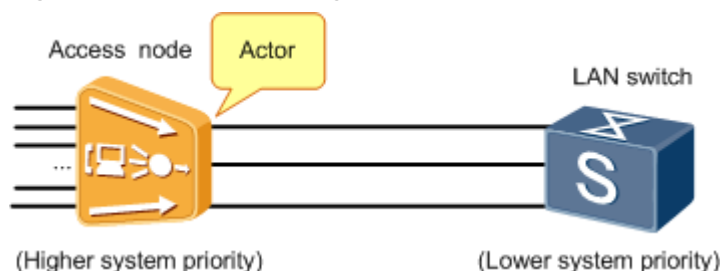


Determining the Actor

Interconnected devices receive LACPDU from each other. Use the LAN switch shown in [Figure 16-32](#) as an example to describe the process. After receiving LACPDU from the access node, the LAN switch checks and records information about the access node and compares system priorities. If the system priority of the access node is higher than that of the LAN switch, the access node acts as the actor.

If the system priority of the access node is the same as that of the LAN switch, the party with a smaller MAC address in the system ID functions as the actor.

Figure 16-32 Determining the actor

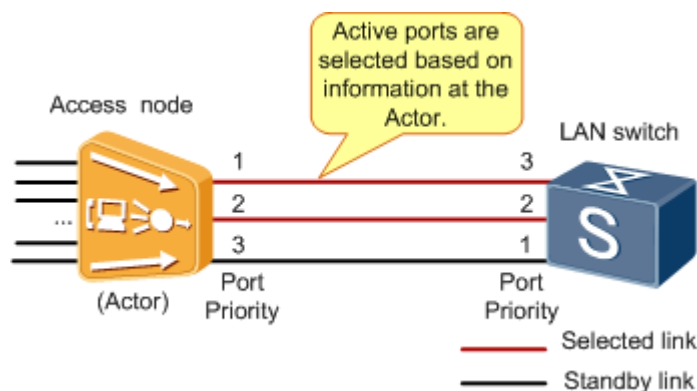


Selecting Active Ports

Interconnected devices select active ports based on the priorities of ports on the actor after the actor is selected.

After the same active port is selected, selected links in the LAG are determined, and traffic is distributed in load sharing across the links, as shown in [Figure 16-33](#).

Figure 16-33 Selecting active ports



16.6.7 Principle of LAG Link Switchover and Reversion

Switching Condition

In an LACP LAG, a link switchover is triggered if a device at one end detects one of the following events:

- A selected link goes Down.
- LACP detects a link failure.
- An active port becomes unavailable.

Switchover Process

When any of the preceding trigger conditions is met, the link switchover is performed in one of the following processes:

For load non-sharing LAGs:

1. The faulty link is disabled.
2. The standby link with the highest priority is selected to replace the faulty selected link.
3. The standby link with the highest priority becomes the selected link and then forwards data.

For load sharing LAGs:

1. The faulty link is disabled.
2. Traffic is reallocated to member links using the load sharing algorithm.

Switchover Reversion Process

If an LACP LAG works in load sharing mode and the active port before switchover recovers, the original faulty link is enabled, and traffic is reallocated using the load sharing algorithm.

If an LACP LAG works in load non-sharing mode, you can set the link revertive mode to revertive or non-revertive.

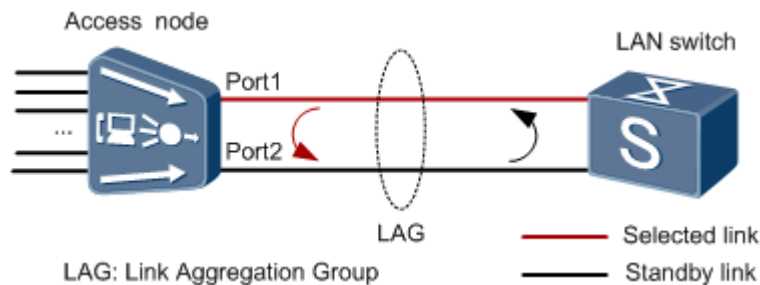
- When an LACP load non-sharing LAG is set to revertive, services are switched back to the link of a higher priority after this link recovers, as shown in [Figure 16-34](#).
- When an LACP load non-sharing LAG is set to non-revertive, services are not switched back to the selected link after this link recovers, but are still transmitted on the current link.

As shown in [Figure 16-34](#), ports 1 and 2 are member ports in an LACP LAG, port 1 is the active port (working in the selected link), and port 2 is the inactive port (working in the standby link).

After port 1 fails, port 2 takes over as the active port.

After port 1 recovers, port 1 works as an active port, and port 2 still works as an inactive port.

Figure 16-34 Reversing a switchover (LACP LAG)



16.6.8 Configuring Ethernet Link Aggregation

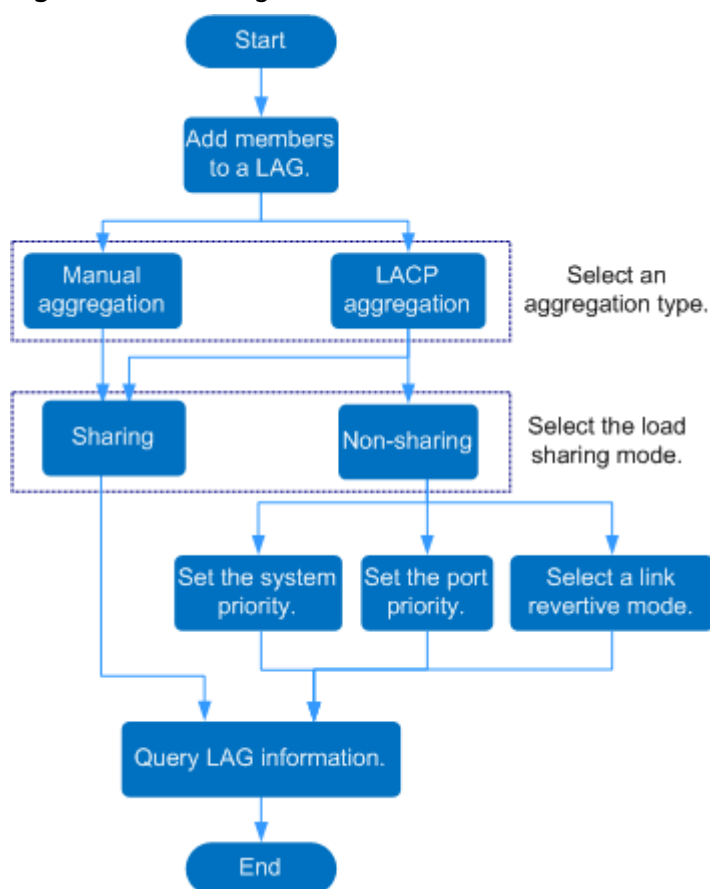
Configure Ethernet link aggregation to increase link bandwidth and improve link reliability, without performing a hardware upgrade.

Prerequisites

- Interconnected devices, hardware, and port attributes must support LAGs.
- The member ports of LAG do not have static MAC addresses. You can run the **display mac-address** command to query whether an aggregated port has static MAC address.

Context

[Figure 16-35](#) shows the flowchart for configuring a LAG.

Figure 16-35 Configuration flowchart

Procedure

Step 1 Create a LAG and select the aggregation type.

Run the **link-aggregation** command to add multiple upstream Ethernet ports to the same LAG to implement protection and load sharing between ports. The port with the smallest port ID is the master port.

NOTE

If the device is interconnected with the device that supports LACP, static aggregation is recommended. If the device is interconnected with the device that does not support LACP, only manual aggregation can be used.

Step 2 (Optional) Add a LAG member port.

Perform this step when the LAG bandwidth or link reliability needs to be improved further. Run the **link-aggregation add-member** command to add an Ethernet port to an existing LAG to increase the LAG bandwidth and improve the link reliability.

 NOTE

If the port to be added to or deleted from a LAG is connected to the peer device, run the **shutdown(Ethernet)** command to deactivate the Ethernet port or remove the optical fiber to prevent loops.

Step 3 (Optional) Select the load carrying type. **NOTE**

If the load sharing type is not configured, a LAG works in load sharing mode by default.

This step is required only when a static LAG is configured.

Configuring the maximum selected links in a LAG implements traffic allocation in load non-sharing mode. For example, M+N links are configured in a LAG. Then, run the link-aggregation max-link-number command to specify N selected links. The remaining M links are standby ones. If a selected link is disconnected, a standby link automatically changes to the selected one.

Step 4 (Optional) Set the system priority and port priority.

This step is required only when a static LAG is configured.

- LACP system priority: If the access device is dual homed to two convergence devices, the access device determines the selected and standby LAGs. Run the **lacp priority system** command to set the LACP system priority of the access device to be higher than that of the peer device.
- LACP port priority: LACP port priority must be used together with the maximum number of links. If a port is required preferentially for carrying services, set its priority higher. Run the **lacp priority port** command to change the link priority so that the standby link and the selected link can be switched over.

Step 5 (Optional) Selected the link revertive mode.

When a static LAG in load non-sharing mode is configured, run the **lacp preempt** command to set whether traffic is switched back to the original link if the link failure is rectified.

Step 6 (Optional) Query LAG information.

Run the **display link-aggregation** command to query the LAG information, including primary port, number of links, aggregation type (manual or static), and maximum number of links.

----End

Example

Assume the following configurations: The MA5800 transmits services upstream using the upstream ports, upstream ports 0/9/0 and 0/9/1 are configured in an upstream port LAG, packets are distributed to the LAG member ports according to the source MAC address, and the working mode is LACP static aggregation. To perform these configurations, run the following commands:

```
huawei(config)#link-aggregation 0/9 0-1 ingress workmode lacp-static
huawei(config)#display link-aggregation all
```

Master port	Link aggregation mode	Port NUM	Work mode	Max link number
0/9/0	ingress	2	lacp-static	-
Total: 1 link aggregation(s)				

16.6.9 Ethernet Link Aggregation Reference Standards and Protocols Compliance

Ethernet link aggregation complies with IEEE 802.1AX-2008, IEEE standard for local and metropolitan area networks (link aggregation).

16.7 MSTP

The Multiple Spanning Tree Protocol (MSTP) is compatible with STP and RSTP.

16.7.1 Introduction to MSTP

Definition

The Spanning Tree Protocol (STP) applies to a loop network to realize path redundancy through certain algorithms. STP also prunes a loop network into a loop-free tree network. This helps to avoid proliferation and infinite loop of packets in the loop network.

The Rapid Spanning Tree Protocol (RSTP) is an improvement on STP. The rapidness of RSTP relies on the greatly shortened delay for the designated port and the root port to turn into the forwarding state in a certain condition. For details, see "Principle of RSTP" in "[16.7.2 Principle of MSTP](#)." This helps to shorten the time for stabilizing the network topology.

The Multiple Spanning Tree Protocol (MSTP) is compatible with STP and RSTP.

Purpose

Although STP can prune a loop network into a loop-free network, it fails to transit fast. Even a port in a point-to-point link or an edge port has to wait double Forward Delay time before it can turn into the forwarding state.

RSTP features fast convergence; however, like STP, RSTP still has the following defects:

- All the bridges in a local area network (LAN) share a same spanning tree, and fail to block redundant links by VLAN.
- The packets of all the VLANs are forwarded along the same spanning tree. Therefore, load sharing of data traffic cannot be implemented between VLANs.

MSTP can be a remedy to the defects of STP and RSTP. It not only realizes fast convergence, but also enables traffic of different VLANs to be forwarded along their respective paths. This helps to provide a better load sharing mechanism for redundant links.

MSTP sets VLAN mapping tables (relationship tables between VLANs and spanning trees) to associate VLANs and spanning trees. MSTP divides a switching

network into multiple regions. Each region contains multiple spanning trees, and each spanning tree is independent from others.

MSTP prunes a loop network to a loop-free tree network to avoid proliferation and infinite loop of packets in the loop network. It also provides multiple redundant paths for data forwarding to realize load sharing of VLAN data during forwarding.

16.7.2 Principle of MSTP

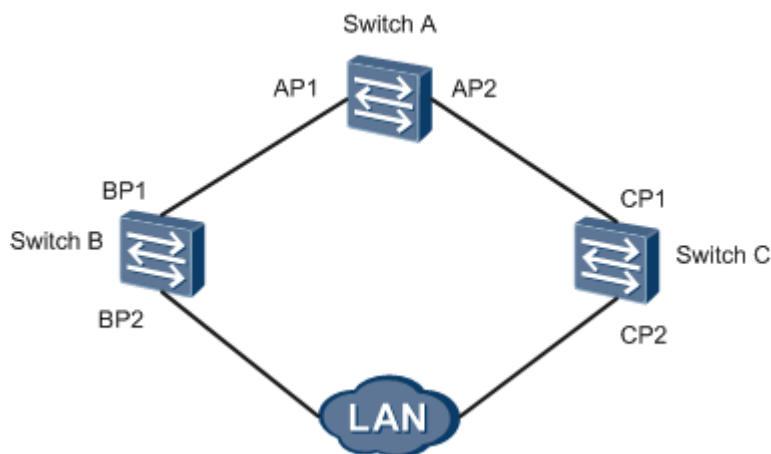
Principle of STP

STP determines the topology of a network by transmitting a certain special message (configuration message as defined in IEEE 802.1D) between bridges. A configuration message contains sufficient information to enable the bridge to complete the calculation of the spanning tree.

The following defines the designated port and the designated bridge:

- For a bridge (such as bridge A), the designated bridge is a bridge that is directly connected to bridge A and forwards data packets to bridge A. The designated port is the port in the designated bridge through which the data packets are forwarded to bridge A.
- For a LAN, the designated bridge is a bridge that forwards data packets to the LAN. The designated port is the port in the designated bridge through which the data packets are forwarded to the LAN.

Figure 16-36 Schematic drawing of designated bridge and designated port



As shown in [Figure 16-36](#):

- AP1, AP2, BP1, BP2, CP1, and CP2 are ports in Switch A, Switch B, and Switch C respectively.
- Switch A forwards data to Switch B through port AP1, and then the designated bridge of Switch B is Switch A, and the designated port is port AP1 in Switch A.

- Switch B and Switch C are connected to the LAN. If Switch B forwards data packets to the LAN, the designated bridge of the LAN is Switch B, and the designated port is port BP2 in Switch B.

In STP, the configuration message is forwarded as follows:

1. In network initialization, all the bridges work as the root bridge of the spanning tree.
2. The designated port of a bridge takes the hello time as the interval for sending its configuration messages. If the port that receives the configuration message is a root port, the bridge increases the message age contained in the configuration message by degrees and enables the timer to time the configuration message.
3. If a path fails, the root port on this path receives new configuration messages no longer, and the old configuration messages are discarded due to timeout. This results in recalculation of the spanning tree. A new path then is created to replace the faulty path and recover the network connectivity.

The new configuration message upon the recalculation, however, will not immediately spread throughout the entire network. In this case, the old root port and designated port that fail to discover the topology change will forward their data along the old paths. If the selected root port and designated port forward data immediately, a temporary loop may be created.

Therefore, STP adopts a state transition mechanism. That is, the root port and the designated port have to experience a transition state before they can re-forward data. The transition state turns into the forwarding state upon Forward Delay. This delay guarantees that the new configuration message has spread throughout the entire network.

Defects of STP

- In case of topology change or link failure, a port has to wait double Forward Delay time before it can turn from the blocking state to the forwarding state. Therefore, in case of topology change, double Forward Delay time (at least scores of seconds) is required to restore the network connectivity.
- The entire bridged LAN uses a single spanning tree instance. Therefore, when the network is large, a longer convergence time may be required or the topology changes frequently.

Principle of RSTP

RSTP is an improvement on STP. The rapidness of RSTP relies on the greatly shortened delay for the designated port and the root port to turn into the forwarding state in a certain condition. This helps to shorten the time for stabilizing the network topology.

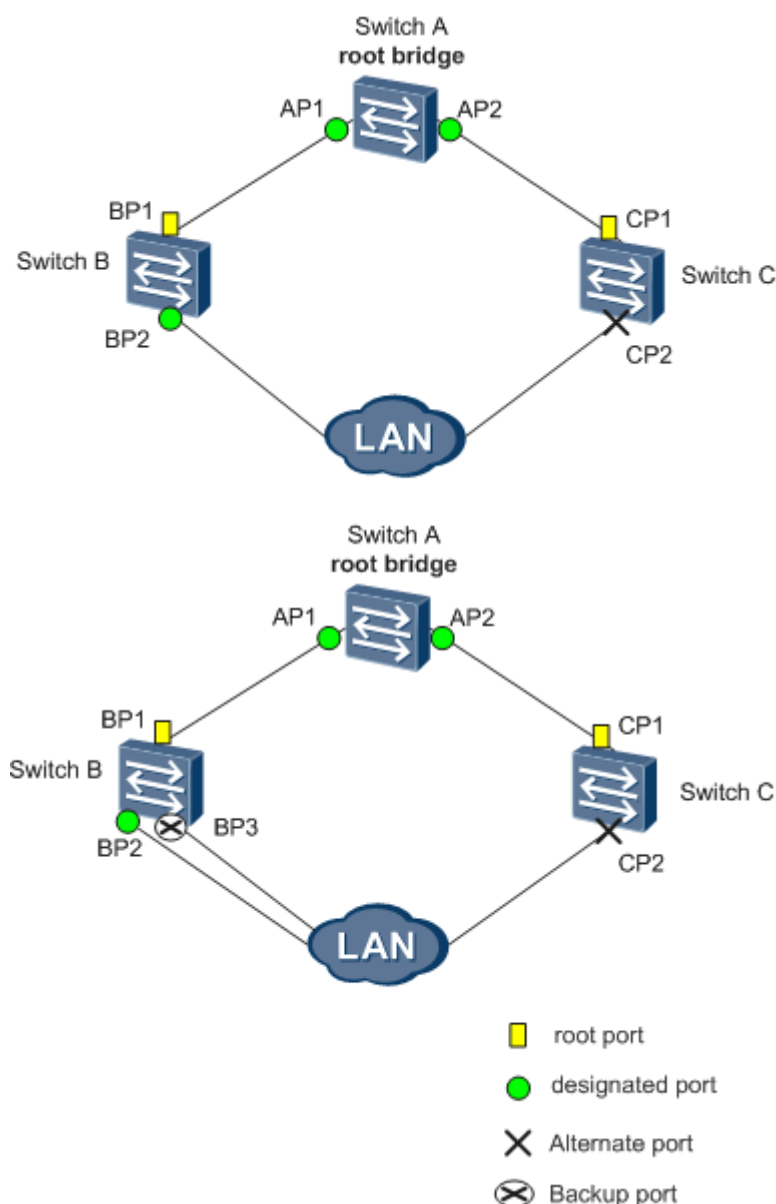
In comparison with STP, RSTP improves in the following aspects:

- First improvement:
 - The alternate port and backup port are set for rapid switching of the root port and designated port.
 - When the root port fails, the alternate port quickly switches to the new root port and turns into the forwarding state without delay.

- When the designated port fails, the backup port quickly switches to the new designated port and turns into the forwarding state without delay.
- Second improvement:
 - In a point-to-point link connected with two switching ports, a designated port turns into the forwarding state without delay after one handshake with the downstream bridge.
 - In a shared link connected with at least three bridges, the downstream bridge does not respond to the handshake request sent from the upstream designated port, and the designated port has to wait double Forward Delay time before it turns into the forwarding state.
- Third improvement:
 - A port that is directly connected to a terminal and is not connected to any other bridge is defined as an edge port. The edge port can directly turn into the forwarding state without delay.
 - Because a bridge does not know whether a port is directly connected to a terminal, the edge port must be configured manually.

RSTP defines four port roles: root port, designated port, alternate port, and backup port. As shown in [Figure 16-37](#).

Figure 16-37 Diagram of port roles



The functions of the root port and designated port are the same as those defined in STP. The alternate port and backup port are described as follows:

- From the perspective of configuration BPDU transmission:
 - An alternate port is blocked after learning the configuration BPDUs sent by other bridges.
 - A backup port is blocked after learning the configuration BPDUs sent by itself.
- From the perspective of user traffic
 - An alternate port backs up the root port and provides an alternate path from the designated bridge to the root bridge.
 - A backup port backs up the designated port and provides an alternate path from the root node to the leaf node.

After all RSTP-capable ports are assigned roles, topology convergence is completed.

The bridges that adopt RSTP are compatible with the bridges which adopt STP. The bridges that adopt RSTP can identify both STP and RSTP packets and apply them to calculation of the spanning tree.

Defects of RSTP

Although RSTP features fast convergence, like STP, RSTP still has the following defects: All the bridges in a LAN share a same spanning tree, and thus the packets of all the VLANs cannot be forwarded equally. Furthermore, the packets of some VLANs cannot be forwarded.

Principle of MSTP

MSTP can compensate for the defects of STP and RSTP. It not only realizes fast convergence, but also enables traffic of different VLANs to be forwarded along their respective paths. This helps to provide a better load sharing mechanism for redundant links.

MSTP sets VLAN mapping tables (relationship tables between VLANs and spanning trees) to associate VLANs and spanning trees. MSTP divides a switching network into multiple regions. Each region contains multiple spanning trees, and each spanning tree is independent from others. Multiple spanning trees can run on each bridge to forward the packets of different VLANs.

MSTP divides the entire Layer 2 network into multiple spanning tree (MST) regions. These regions and the other bridges and LANs are connected into a single common spanning tree (CST). Multiple spanning trees are created in a region through calculation. Each spanning tree is defined as a multiple spanning tree instance (MSTI). MSTI 0 is defined as an internal spanning tree (IST). MSTP connects all bridges and LANs with a single common and internal spanning tree (CIST) which consists of the CST and the IST. Like RSTP, MSTP calculates the spanning tree according to the configuration message. The configuration message, however, contains the message of MSTP on the bridge.

- Calculation of CIST
 - Select a bridge with the highest priority within the entire network as the CIST root by comparing the configuration messages.
 - In each MST region, MSTP creates an IST through calculation. Meanwhile, MSTP regards each MST region as a single bridge, and then creates a CST between regions.
 - The CST and IST form the CIST that connects all the bridges in a bridge network.
- Calculation of MSTI

In an MST region, MSTP creates different MSTIs for different VLANs according to the mapping between the VLANs and the spanning tree instances. Each spanning tree is calculated independently. The process is similar to that in which the RSTP calculates the spanning tree.

Based on RSTP, MSTP has two additional port types. MSTP ports can be root ports, designated ports, alternate ports, backup ports, edge ports, master ports, and regional edge port.

The functions of root ports, designated ports, alternate ports, backup ports, and edge ports have been defined in RSTP. [Table 16-10](#) lists all port roles in MSTP.

 NOTE

Except edge ports, all ports participate in MSTP calculation.

A port can play different roles in different spanning tree instances.

Table 16-10 Port roles

Port Role	Description
Root port	A root port is the non-root bridge port closest to the root bridge. Root bridges do not have root ports. Root ports are responsible for sending data to root bridges. As shown in Figure 16-38, Switch A is the root; BP1 is the root port on Switch B; CP1 is the root port on Switch C.
Designated port	The designated port on a switching device forwards BPDUs to the downstream switching device. As shown in Figure 16-38, AP1 and AP2 are designated ports on Switch A; BP2 is a designated port on Switch B.
Alternate port	- From the perspective of sending BPDUs, an alternate port is blocked after a BPDU sent by another bridge is received. - From the perspective of user traffic, an alternate port provides an alternate path to the root bridge. This path is different than using the root port. As shown in Figure 16-38, CP2 is an alternate port.
Backup port	- From the perspective of sending BPDUs, a backup port is blocked after a BPDU sent by itself is received. - From the perspective of user traffic, a backup port provides a backup/redundant path to a segment where a designated port already connects. As shown in Figure 16-38, BP3 is a backup port.
Master port	A master port is on the shortest path connecting MST regions to the CIST root. BPDUs of an MST region are sent to the CIST root through the master port. Master ports are special regional edge ports, functioning as root ports on ISTs or CISTs and master ports in instances. As shown in Figure 16-39, Switch A, Switch B, Switch C, and Switch D form an MST region. AP1 on Switch A, being the nearest port in the region to the CIST root, is the master port.

Port Role	Description
Regional edge port	A regional edge port is located at the edge of an MST region and connects to another MST region or an SST. During MSTP calculation, the roles of a regional edge port in the MSTI and the CIST instance are the same. If the regional edge port is the master port in the CIST instance, it is the master port in all the MSTIs in the region. As shown in Figure 16-39, AP1, DP1, and DP2 in an MST region are directly connected to other regions, and therefore they are all regional edge ports of the MST region. AP1 is a master port in the CIST. Therefore, AP1 is the master port in every MSTI in the MST region.
Edge port	An edge port is located at the edge of an MST region and does not connect to any switching device. Generally, edge ports are directly connected to terminals.

Figure 16-38 Root port, designated port, alternate port, and backup port

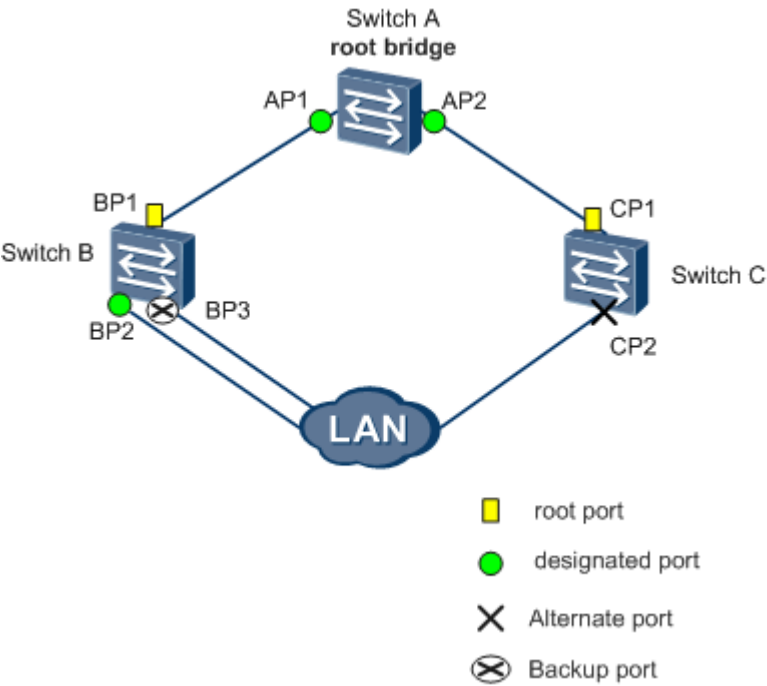
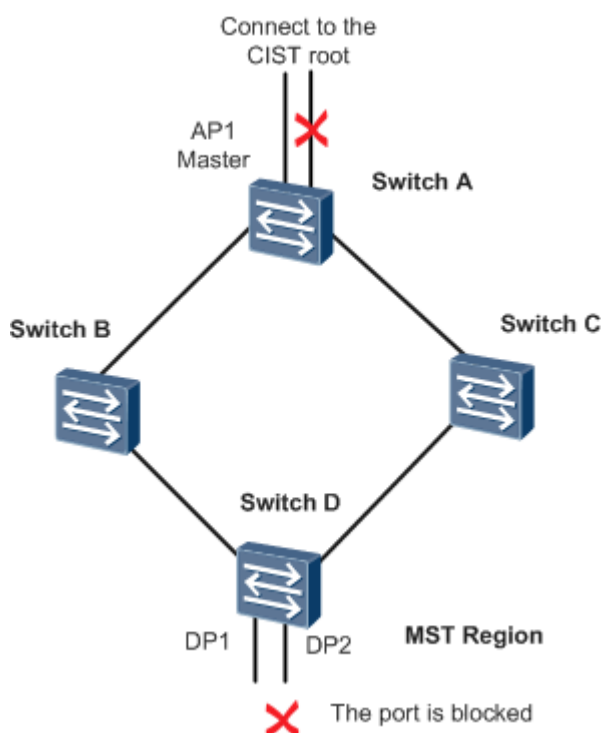


Figure 16-39 Master port and regional edge port

Implementation of MSTP on the MA5800

MSTP is compatible with STP and RSTP. The bridges that adopt MSTP can identify both STP and RSTP packets and apply them to calculate spanning tree.

Besides the basic functions of MSTP, the MA5800 provides some special functions, such as:

- BPDU protection

For an access device, the access port is generally connected to a terminal (such as a PC) or file server. In this case, the access port is set to an edge port for the purpose of fast transition. When receiving a configuration message (BPDU), the edge port switches to a non-edge port automatically, the spanning tree is re-calculated and the topology changes accordingly.

In normal conditions, an edge port cannot receive STP configuration messages. If the bridge is maliciously attacked by forged configuration messages, the network will be attacked. The BPDU protection function can prevent such network attacks.

After the BPDU protection function is enabled on the MA5800, if an edge port receives a configuration message, the system shuts down the edge port, and notifies the network management system of the related information. Only network administrators can enable the port that is shut down.

It is recommended that you enable the BPDU protection function on the MA5800 which is configured with an edge port.

- Root protection

Because of wrong configurations by the maintenance personnel or malicious network attacks, a legal root bridge in the network may receive a configuration message with a higher priority. In this case, this root bridge may become a non-root bridge and the topology changes accordingly. Such illegal change results in transfer of traffic in high-speed links to low-speed links, thus causing network congestion.

The root protection function is a solution to this problem.

When the root protection function is enabled for a port, the port is always a designated port. If the port receives a configuration message with a higher priority, and is to become a non-designated port, the port will turn into the listening state and will not forward packets (that is, the link connected to the port is disconnected). If the port does not receive a configuration message of a much higher priority within a certain long period of time, the port will turn into the normal state.

- Loop protection

A bridge maintains the states of the root port and other blocked ports by continuously receiving BPDUs from the upstream bridge.

In case of link congestion or failure, these ports fail to receive BPDUs from the upstream bridge. For this reason, the bridge will re-select its root bridge. The previous root bridge switches to the designated port, and the blocked ports turn to the forwarding state. As a result, loops are created in the switching network.

The loop protection function is a solution to this problem.

After receiving the BPDUs (excluding the TCN packets) again, a port under loop protection normally processes the packets, selects the role, and resets the forwarding state of the port. The port is not always in the blocked state.

When the loop protection function is enabled, if the root port switches to a non-root port, it will turn into the discarding state, and the blocked ports will remain in the discarding state. Therefore, no packets are forwarded, and no loop is created in the network.

 NOTE

The three protection functions conflict with each other.

16.7.3 Configuring the MSTP

The MA5800 supports the application of the Multiple Spanning Tree Protocol (MSTP), Spanning Tree Protocol (STP), and Rapid Spanning Tree Protocol (RSTP). The MA5800 supports the MSTP ring network, which can meet various networking requirements.

Context

- MSTP applies to a redundant network. It makes up for the drawback of STP and RSTP. MSTP makes the network converge fast and the traffic of different VLANs distributed along their respective paths, which provides a better load-sharing mechanism.
- MSTP trims a loop network into a loop-free tree network. It prevents the proliferation and infinite cycling of the packets in the loop network. In addition, MSTP supports load sharing by VLAN during data transmission.

- The status of the transparent transmission for bridge protocol data unit (BPDU) packets configured by running the **bpdu tunnel** command determines the destination MAC address of MSTP packets.
 - If the transparent transmission of BPDU packets is disabled in all VLANs, the destination MAC address of MSTP packet is 00:E0:FC:00:00:00.
 - If the transparent transmission of BPDU packets is enabled in any VLAN, the destination MAC address of MSTP packet is 00:E0:FC:00:00:08.

Procedure

Step 1 Enabling the MSTP function.

- By default, the MSTP function is disabled.
 - After the MSTP function is enabled, the device determines whether it works in STP compatible mode or MSTP mode based on the configured protocol.
 - After the MSTP function is enabled, MSTP maintains dynamically the spanning tree of the VLAN based on the received BPDU packets. After the MSTP function is disabled, the MA5800 becomes a transparent bridge and does not maintain the spanning tree.
1. Run the **stp enable** command to enable the MSTP function of the bridge.
 2. Run the **stp port enable** command to enable the MSTP function of the port.
 3. Run the **display stp** command or the **display stp port** command to query the MSTP state of the bridge or the port.

Step 2 Configuring the MST region name.

1. Run the **stp region-configuration** command to enter MST region mode.
 2. Run the **region-name** command to configure the name of the MST region.
- By default, the MST region name is the bridge MAC address of the device.

Step 3 Configuring the MSTP instance.

The MSTP protocol configures the VLAN mapping table (mapping between the VLAN and the spanning tree), which maps the VLAN to the spanning tree.

1. Run the **stp region-configuration** command to switch over to MST region mode.
2. Run the **instance vlan** command to map the specified VLAN to the specified MSTP instance.
 - By default, all VLANs are mapped to CIST, that is, instance 0.
 - One VLAN can be mapped to only one instance. If you re-map a VLAN to another instance, the original mapping is disabled.
 - A maximum of 10 VLAN sections can be configured for an MSTP instance.

NOTE

A VLAN section refers to the consecutive VLAN IDs from the start VLAN ID to the end VLAN ID.

3. Run the **check region-configuration** command to query the parameters of the current MST region.

Step 4 Activating the configuration of the MST region.

1. Run the **stp region-configuration** command to switch over to MST region mode.
2. Run the **active region-configuration** command to activate the configuration of the MST region.
3. Run the **display stp region-configuration** command to query the effective configuration of the MST region.

Step 5 Setting the priority of the device in the specified spanning tree instance.

1. Run the **stp priority** command to set the priority of the device in the specified spanning tree instance.
2. Run the **display stp** command to query the MSTP configuration of the device.

Step 6 Other optional configurations.

- Setting the MST region parameters.
 - Run the **stp md5-key** command to set the MD5-Key for the MD5 encryption algorithm configured on the MST region. MD5 is an insecure encryption algorithm. Therefore, using an algorithm with a higher security level is recommended.
 - In the MSTP region mode, run the **vlan-mapping module** command to map all VLANs to the MSTP instances by modular arithmetic.
 - In the MSTP region mode, run the **revision-level** command to set the MSTP revision level of the device.
 - Run the **reset stp region-configuration** command to restore the default settings to all parameters of the MST region.
- Specifying the device as a root bridge or a backup root bridge.
 - Run the **stp root** command to specify the device as a root bridge or a backup root bridge.
- Setting the time parameters of the specified network bridge.
 - Run the **stp timer forward-delay** command to set the Forward Delay of the specified network bridge.
 - Run the **stp timer hello** command to set the Hello Time of the specified network bridge.
 - Run the **stp timer max-age** command to set the Max Age of the specified network bridge.
 - Run the **stp time-factor** command to set the timeout time factor of the specified network bridge.
- Setting the parameters of the specified port.
 - Run the **stp port transmit-limit** command to set the number of packets transmitted by the port within the Hello Time.
 - Run the **stp port edged-port enable** command to set the port as an edge port.
 - Run the **stp port cost** command to set the path cost of a specified port.
 - Run the **stp port port-priority** command to set the priority of the specified port.
 - Run the **stp port point-to-point** command to set whether the link that is connected to the port is a point-to-point link.

- Configuring the device protection function.
 - Run the **stp bpd protection enable** command to enable the BPDU protection function of the device.
 - Run the **stp port loop-protection enable** command to enable the loop protection function of the port.
 - Run the **stp port root-protection enable** command to enable the root protection function of the port.
- Setting the maximum number of hops of the MST region.
 - Run the **stp max-hops** command to set the maximum number of hops of the MST region.
- Setting the diameter of the switching fabric.
 - Run the **stp bridge-diameter** command to set the diameter of the switching fabric.
- Setting the calculation standard for the path cost.
 - Run the **stp pathcost-standard** command to set the calculation standard for the path cost.
- Clear the MSTP protocol statistics.
 - Run the **reset stp statistics** command to clear the MSTP protocol statistics.

----End

Example

Configure the MSTP parameters as follows:

- Enable the MSTP function.
- Enable the MSTP function on port 0/9/0.
- Set the MSTP running mode to MSTP compatible mode.
- Configure MST region parameters:
 - Configure the MD5-Key for the MD5 encryption algorithm to 0x11ed224466.
 - Configure the MST region name to test-mstp-bridge.
 - Map VLAN2-VLAN10 and VLAN12-VLAN16 to MSTP instance 3.
 - Map all the VLANs to the specified MSTP instances using module 16.
 - Configure the MSTP revision level of the device to 100.
- Configure the maximum hops for the MST region to 10.
- Activate the configuration of the MST region manually.
- Configure the priority of the device in spanning tree instance 2 to 4096.
- Configure the current device as the root bridge of MSTP instance 2.
- Configure the diameter of the switching network to 6.
- Configure the calculation standard for the path cost to IEEE 802.1t.
- Configure the time parameters of a specified bridge:
 - Configure the forward delay to 2000 centiseconds.
 - Configure the hello time to 1000 centiseconds.

- Configure the max age to 3000 centiseconds.
 - Configure the timeout time factor to 6.
- Configure the parameters of a specified port:
 - Configure the maximum number of packets transmitted in a hello time period to 16.
 - Configure port 0/9/0 to be an edge port.
 - Configure the path cost of the port in a specified spanning tree instance to 1024.
 - Configure the priority of the port to 64.
 - The link connected to port 0/9/0 is a point-to-point link.
- Enable the BPDU protection function on the device.

```
huawei(config)#stp enable
Change global stp state may active region configuration,it may take several
minutes,are you sure to change global stp state? [Y/N][N]y
huawei(config)#stp port 0/9/0 enable
huawei(config)#stp mode mstp
huawei(config)#stp md5-key 11ed224466
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#region-name test-mstp-bridge
huawei(stp-region-configuration)#instance 3 vlan 2 to 10 12 to 16
huawei(stp-region-configuration)#vlan-mapping module 16
huawei(stp-region-configuration)#revision-level 100
huawei(stp-region-configuration)#active region-configuration
huawei(stp-region-configuration)#quit
huawei(config)#stp instance 2 priority 4096
huawei(config)#stp instance 2 root primary
huawei(config)#stp max-hops 10
huawei(config)#stp bridge-diameter 6
huawei(config)#stp pathcost-standard dot1t
huawei(config)#stp timer forward-delay 2000
huawei(config)#stp timer hello 1000
huawei(config)#stp timer max-age 3000
huawei(config)#stp time-factor 6
huawei(config)#stp port 0/9/0 transmit-limit 16
huawei(config)#stp port 0/9/0 edged-port enable
huawei(config)#stp port 0/9/0 instance 0 cost 1024
huawei(config)#stp port 0/9/0 instance 0 port-priority 64
huawei(config)#stp port 0/9/0 point-to-point force-true
huawei(config)#stp bpdu-protection enable
```

16.7.4 MSTP Reference Standards and Protocols

The following lists the reference documents of MSTP:

- IEEE Std 802.1d, 1998 Edition, Spanning Tree Protocol
- IEEE Std 802.1w-2001, Rapid Spanning Tree Protocol
- IEEE Std 802.1s-2002, Multiple Spanning Tree Protocol

16.8 ERPS

Ethernet ring protection switching (ERPS) is a ring network protocol defined in Recommendation ITU-T G.8032. Interoperation is achieved if all devices participating in the ring network support ERPS. On a network composed of ERPS-supporting devices, the service protection solution with quick switching can be implemented using a small number of links.

16.8.1 Introduction to ERPS

To resolve loop issues, Huawei has supported equipment supporting the Spanning Tree Protocol (STP) and Rapid Ring Protection Protocol (RRPP). The following challenges need to be addressed:

- As higher requirements are posed on the switching time for Layer 2 Ethernet, STP supports link recovery on a basis of seconds, falling short of the carrier-class convergence performance requirements.
- RRPP is a proprietary protocol. Interoperation is not supported if a ring network is composed of devices of multiple vendors.

Ethernet ring protection switching (ERPS) is a ring network protocol defined in Recommendation ITU-T G.8032. Interoperation is achieved if all devices participating in the ring network support ERPS. In addition, ERPS supports fast convergence, meeting carrier-class reliability requirements.

- V1 supports only single-ring protection, single Ethernet ring protection (ERP) instance, and revertive switching.
- Based on V1, V2 supports multiple-ring protection, multiple ERP instances, and non-revertive switching. V2 also optimizes the flushing mechanism for the filtering database (FDB), and supports commands for a forced switchover, manual switchover, or a clearing operation.

The MA5800 implements functions of the V1 protocol using the V2 state machine, supports V1 and V2 message reception and V1 message transmission, and supports all functions of V1 and the multiple instances defined by V2.

Recommendation ITU-T G.8032 only protects MAC address+VLAN services; the MA5800 extends the protocol by protecting multicast and Layer 3 services.

The following explains the concepts involved in the description above.

Concept	Description
Single ring	An ERPS ring physically composed of a set of devices that are connected to form a closed loop.
Multiple rings	A complex network composed of multiple interconnected single rings. The single rings may be interconnected through an interconnection point or through dual interconnection nodes.
Single instance	A mechanism that allows only one logical ERPS ring to run on a physical ring network. All services are protected by this ring.

Concept	Description
Multiple instances	A mechanism that implements protection switching for ERPS rings based on Multiple Spanning Tree Protocol (MSTP) instances. Multiple logical ERPS rings can run on one physical ring network. The topologies of the rings are independent of each other. These rings implement ring automatic protection switching (R-APS) protocol message exchange, fault processing, and service switchover. Therefore, each of the rings must protect a specific type of service. When the network runs in normal conditions, each ERPS ring can select its own blocking point to load balance service traffic over the rings. The selection can be implemented through configuration.
Revertive switching	A mechanism that blocks the ring protection link (RPL) and reverts to the original faulty link to carry service traffic when the fault causing the switch is cleared and the wait-to-restore (WTR) timer expires.
Non-revertive switching	A mechanism that still blocks the original faulty link after the fault causing the switch is cleared.
Forced switching	A port configured with forced switching is immediately blocked, regardless of whether other links on the ring have encountered a fault.
Manual switching	A port configured with manual switching is blocked only when the ring does not contain a faulty link or a port configured with forced switching.
clear command	A command that clears the forced switching and manual switching locally configured.

16.8.2 Basic Concepts of ERPS

This topic describes basic concepts related to the Ethernet ring protection switching (ERPS) feature to help you understand the working principles of the ERPS ring.

ERPS Ring

An ERPS ring is composed of a group of interconnected Layer 2 switches that are configured with the same control VLAN. An ERPS ring is the basic element for implementing the ITU-T G.8032 protocol. A Layer 2 switch participating in the ERPS ring is called a node. On the node, the ports that participate in the ERPS ring are called ring ports.

Port Roles

The ITU-T G.8032 protocol defines two port roles: ring protection link (RPL) owner port and common port. The link where an RPL owner port resides is called a ring

protection link. The device where an RPL owner port resides is called an RPL owner node.

- **RPL owner port**

An ERPS ring has only one RPL owner port, which can be configured by users. Loop avoidance is achieved on an ERPS ring by blocking the RPL owner port. A blocked RPL owner port cannot forward data but can send ring automatic protection switching (R-APS) messages.

As defined in the IEEE 802.1ag protocol, the down maintenance end point (MEP) on the RPL owner port can receive and send Ethernet OAM messages.

When an RPL owner node receives a fault message and learns that a node or link on the ERPS ring is faulty, the RPL owner node automatically enables the RPL owner port. Then, the RPL owner port resumes traffic reception and transmission, ensuring uninterrupted traffic.

 NOTE

For load balancing purposes, it is recommended to select a device with the following characteristics as an RPL owner node: the device is located close to the user side; an equivalent (or approximately so) number of nodes are located on the link between each of the two ring ports of the device and the convergence node.

- **Common port**

On an ERPS ring, all ports except the RPL owner port are common ports. Common ports are responsible for monitoring the status of their directly connected links, and notifying any link status changes to the ports on other nodes.

Port States

On an ERPS ring, a port has two states:

- **Forwarding**

In forwarding state, a port can forward data, and receive and send R-APS messages.

- **Discarding**

In discarding state, a port cannot forward data, but can receive and send R-APS, EFM, CFM, LLDP, and 802.1x messages.

R-APS Messages

Defined in the ITU-T G.8032 protocol, R-APS messages are protocol messages that run on ERPS rings to notify nodes of fault occurrence or fault clearing. R-APS messages include the following types:

- **R-APS signal fail (SF)**

indicates a link failure. When detecting a link failure, a node sends an R-APS (SF) message to notify other nodes on the ring. When receiving an R-APS (SF), the RPL owner node unblocks the RPL owner port so that the RPL owner port forwards data. Other nodes determine whether to flush the FDB according to the DNF flag in the R-APS (SF) message.

- **R-APS no request (NR)**

indicates a link recovery. When detecting a link recovery, a node sends an R-APS (NR) message to notify other nodes on the ring. When receiving an R-

APS (NR), the RPL owner node starts the WTR timer. Other nodes determine whether to flush the FDB according to the DNF flag in the R-APS (NR) message.

- **R-APS no request, RPL blocked (NR, RB)**

An R-APS (NR, RB) message is a type of R-APS (NR). It is sent by an RPL owner to signal that the network is normal and the RPL has been blocked. When receiving an R-APS (NR, RB), other nodes on the ring will unblock the common ports, and determine whether to flush the FDB according to the DNF flag in the message.

The following explains the acronyms involved in the description above.

Acronym	Full Name	Meaning
NR	No request	The network is in normal conditions.
RB	RPL blocked	An RPL is blocked.
DNF	Do not flush	A flag in the R-APS message fields and indicates whether to flush the FDB.
FDB	Filtering database	A forwarding database on a node.
SF	Signal fail	The network encounters a fault.

Timers

The ITU-T G.8032 protocol defines the following timers for an ERPS ring.

- **Guard timer**

After a node on a Layer 2 network running ERPS recovers from a link fault or node fault, the node sends an R-APS (NR) message to other nodes on the ring and starts the guard timer. The node does not receive R-APS messages before the timer expires, which prevents the node from unblocking a recovered port after receiving expired R-APS (SF) messages. The unblocking will cause a loop on the network. If the node receives R-APS (SF) messages after the timer expires, the node changes its port state to forwarding.

- **Holdoff timer**

Layer 2 networks running ERPS require different protection switching sequences. For example, when a node becomes faulty in a multiple-layer service application, carriers prefer a duration to rectify the fault and the duration is not perceived by subscribers. To meet the carrier requirement, protection switching is not performed immediately after a fault occurs. The fault is reported only if it is not rectified after the holdoff timer expires.

- **WTR timer**

On a Layer 2 network running ERPS, an RPL owner port enters the forwarding state when a node or link on the ERPS ring fails. When the node or link recovers, some ports on the node or link may still stay in the Down state (that is, not Up yet). If the RPL owner port is immediately blocked upon the fault recovery, and finds that there are still ports in the Down state, the RPL owner port will enter the forwarding state again. To avoid such toggling protection

states in the case of intermittent faults, the RPL owner port starts a wait-to-restore (WTR) timer when receiving the R-APS (NR) message from the other ports.

- If the RPL owner port receives the R-APS (SF) message from the other ports before the WTR timer times out, the RPL owner port stops the WTR timer and stays in the forwarding state.
- If the RPL owner port does not receive the R-APS (SF) message when the WTR timer times out, the RPL owner port is blocked and sends the R-APS (NR, RB) message to other ports. When receiving the R-APS (NR, RB) message, the other ports switch to the forwarding state.

16.8.3 Principle of ERPS

This topic uses ERPS network diagrams to describe the fault detection and recovery processes of an ERPS ring.

Network Diagram

Figure 16-40 shows the network diagram of an ERPS single ring. The nodes on the ERPS ring exchange R-APS messages to notify each other of the port status changes and coordinate to implement protection switching for services. The port status changes on a ring node depend on detection of local port status, Ethernet OAM detection results, and the port status changes on other nodes of the ring.

Figure 16-40 Network diagram of an ERPS single ring

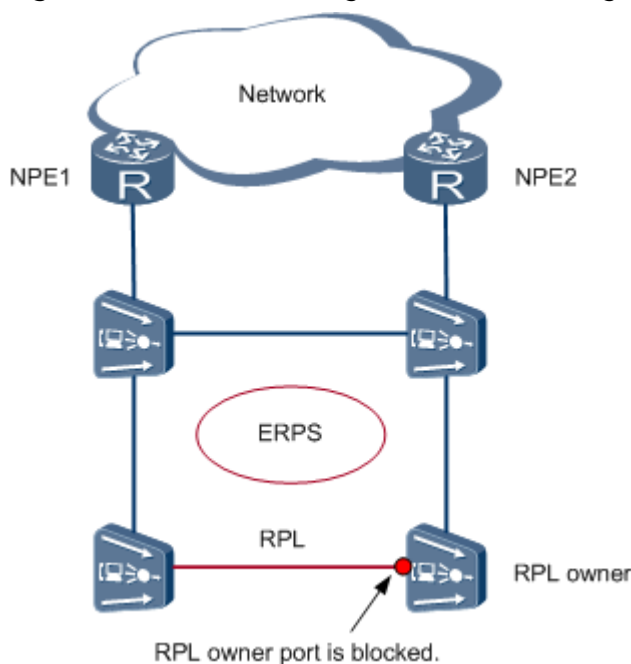
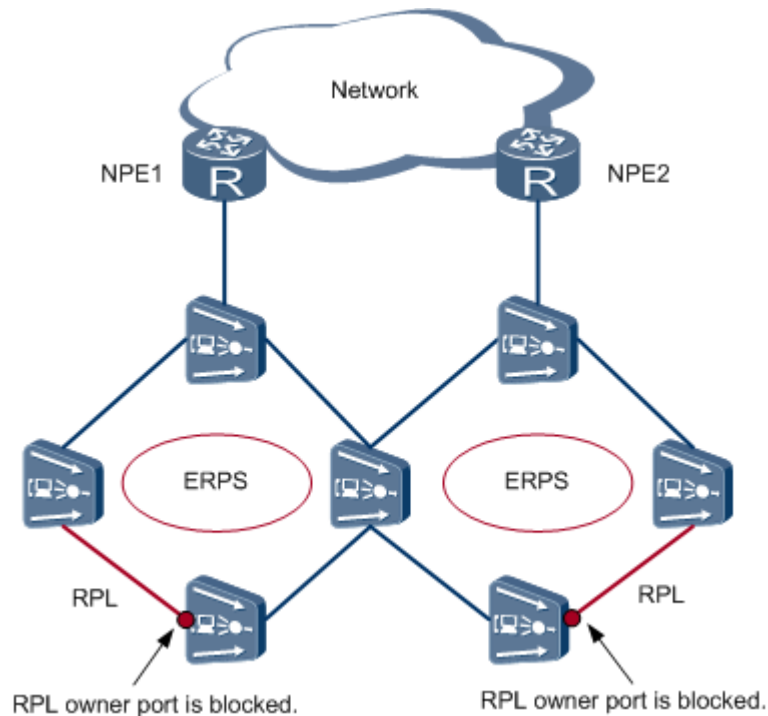


Figure 16-41 shows the network diagram of ERPS interconnected rings. The two physical ring networks are interconnected through one node. Four ports on the interconnection node are configured with ERPS. Two of the four ports locate on one ring, and the other two on the other ring. Except the interconnection node, other nodes on the two interconnected rings function in the same mechanism as the nodes on a single ring. The R-APS protocol messages of the two rings are independent of each other, so the two rings need different control VLANs.

The interconnection node can be configured with multiple ERPS rings, and the rings can have different numbers of nodes.

Figure 16-41 ERPS rings interconnected through one node



Configuration Items of ERPS Ring

Each ring node must be configured with the following items:

- Control VLAN
The control VLAN transmits ERPS messages and does not forward data messages, which improves ERPS security.
- Protection instance
Protection instances are implemented by configuring mappings between MSTP instances and VLANs. On a Layer 2 network with ERPS enabled, the VLAN that transmits ERPS messages and data messages must be mapped to a protection instance so the ERPS ring forwards or blocks the messages based on the blocking principles. Without proper forwarding or blocking, the messages may cause a broadcast storm on the ring network and render the network unavailable.
- Port role
Configuration related to port roles is to add ports to an ERPS ring, and specify the RPL owner port on the RPL owner node.

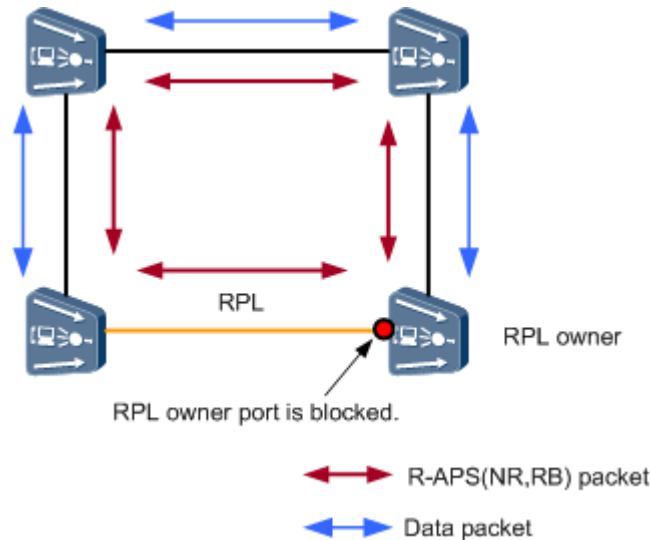
Fault Detection and Recovery

The following uses a single ERPS ring as an example to describe the fault detection and recovery processes of an ERPS ring.

In normal conditions, all links on the network are in the UP state, and the RPL owner port is blocked, therefore forming link redundancy backup and avoiding

loops. Service traffic is forwarded through all links except the RPL. In this situation, the R-APS messages travelling on the network are all R-APS (NR, RB) messages that are sent by the RPL owner node, as shown in [Figure 16-42](#).

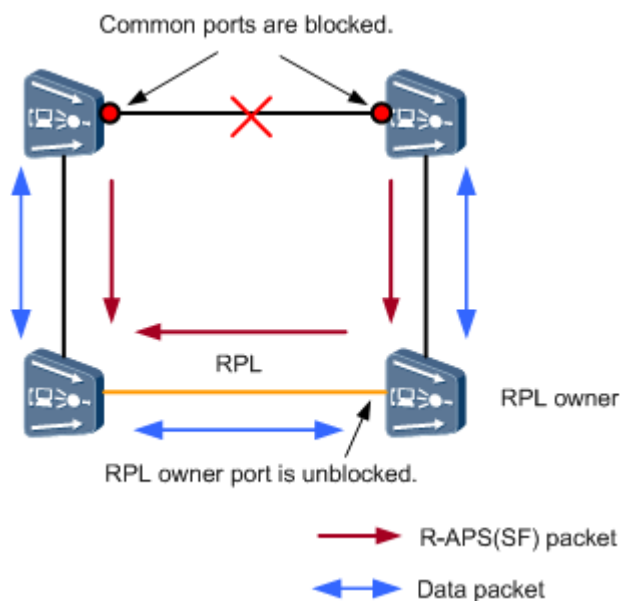
Figure 16-42 An ERPS ring network in the normal state



When a fault occurs on a link, the nodes connected to the faulty link detect the fault and start the holdoff timer. If the fault persists after the holdoff timer times out, the nodes block the ports on the faulty link, and send R-APS (SF) messages to other nodes on the ring. After receiving the R-APS (SF) message, the RPL owner node unblocks the RPL owner port, and switches to the RPL to transmit service traffic. In this way, ring network protection is implemented. When receiving the R-APS (SF) message for the first time, the node will flush its FDB, and the ring network enters the protection state, as shown in [Figure 16-43](#). The node will not trigger any operation when receiving subsequent R-APS (SF) messages.

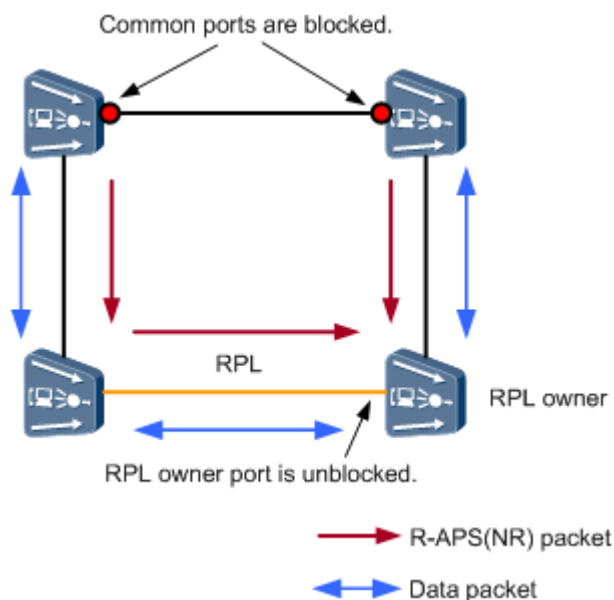
To implement fast switching, each node detecting the link fault will rapidly send 3 R-APS (SF) messages, at a 3.33 ms interval, which equals the interval of fast detection by using CCM messages. After sending the 3 R-APS (SF) messages, the node will send one R-APS (SF) message every 5s. Such a mechanism ensures fast network switching without burdening the devices.

Figure 16-43 An ERPS ring network in the protection state



When the fault recovers on the link, the nodes connected to the originally faulty link detect the fault recovery, start the guard timer, and stay in the blocked state. At the same time, the nodes send R-APS (NR) messages to the RPL owner node, notifying the RPL owner node that the RPL owner port can be blocked, as shown in [Figure 16-44](#).

Figure 16-44 ERPS ring network status after fault recovers and before WTR timer times out



After receiving the R-APS (NR) message, the RPL owner node blocks the RPL owner port only after the WTR timer expires. Meanwhile, the RPL owner node sends the R-APS (NR, RB) message. The other nodes on the ring flush their FDB when receiving the R-APS (NR, RB) message. After the guard timer times out, the node that detects the fault recovery stops periodically sending R-APS (NR)

messages and unblocks the local ports. When the network resumes the normal state, the RPL owner node continues to send R-APS (NR, RB) messages.

16.8.4 Configuring ERPS

The device supports ERPS as defined in ITU-T G.8032. Interoperation is achieved if all devices participating in the ring network support ERPS. The ERPS feature enables fast convergence and meets carrier-class reliability requirements.

Prerequisites

The service VLANs to be protected have been configured.

Context

- In the single ERPS ring scenario, the ring must be configured on all nodes participating in the ring. In the multiple-ERPS-ring scenario, each ring has its own configurations.
- Note that the system does not have a restriction mechanism for some configuration items. When planning and configuring such items, make sure that they are planned and configured correctly, in line with system requirements. The following table provides the configuration restrictions on ERPS.

Table 16-11 ERPS configuration restrictions

Item	Limitation	Does the Device Check the Limitation?
Control VLAN	• A control VLAN must be a standard VLAN and cannot be used by a Rapid Ring Protection Protocol (RRPP) ring or a smart link. • A control VLAN cannot be a reserved VLAN. • An ERPS ring cannot be modified or deleted if a port is added to the ring. To modify or delete a control VLAN, delete the port from the ERPS ring first. • Different ERPS rings must be configured with control VLANs of different IDs on the same node.	Yes

Item	Limitation	Does the Device Check the Limitation?
	• The control VLAN must be different from the service VLAN. • A control VLAN cannot be configured as a native VLAN. • The attribute of a control VLAN must be common. • All the devices in an ERPS ring must be configured with the same control VLAN.	No. The user must correctly configure this item.
Ring port	• Each node supports up to 2 ports to join the same ERPS ring. • MSTP, RRPP, smart link, Ethernet port protection, and ERPS are mutually exclusive. • Upstream ports and cascade ports can function as ring ports, but user-side ports cannot.	Yes

Item	Limitation	Does the Device Check the Limitation?
	- When a control VLAN is created for an ERPS ring or a port is added to an ERPS ring, the port is not added to the control VLAN forcibly. Ensure that all the ports added to the ERPS ring are in the control VLAN. If a port is not in the control VLAN, the ERPS packets sent to the port are discarded. - A ring port must not be configured with static MAC addresses or static ARP entries. - On all nodes except the convergence node, it is not allowed to isolate two ring ports using the port isolation function. - On all nodes, ensure that packets of the control VLAN can be transmitted and received between two ring ports of the same node. - The ring ports on the interconnection node of an access-layer ERPS ring and a convergence network can be configured as cascade ports or upstream ports, but the ring ports on other nodes on the rings can be configured as upstream ports only. - In a network where an access-layer ERPS ring is connected to the upstream network through multiple nodes, the ring ports on all nodes of the ERPS ring must be upstream ports. - The interconnection node of an access-layer ERPS ring and a convergence network does not support associated routes or Neighbor Discovery (ND) entries. If the interconnection node is enabled to automatically generate associated routes and ND entries, when the topology of the ERPS ring changes, the DHCPv6 users under all nodes on the ring must dial up again. Otherwise, services may fail.	No. The user must correctly configure this item.

Item	Limitation	Does the Device Check the Limitation?
Protection instance	- One ERPS ring can be configured with one or multiple protection instances. Each protection instance maps one or multiple VLAN services. - One ERPS ring can be configured with one or multiple protection instances. Each protection instance maps one or multiple VLAN services.	No. The user must correctly configure this item.

Procedure

Step 1 Run the **vlan** command to create a control VLAN.

Step 2 Run the **port vlan** command to add ERPS ring ports to the control VLAN.

Step 3 Map the control VLAN and service VLANs to the protection instances.

- Run the **stp region-configuration** command to enter the MSTP region mode.
- Run the **instance vlan** command to map the service VLANs and the control VLAN to the specified MSTP instance.
- Run the **active region-configuration** command to activate the configuration of the MSTP region.
- Run the **quit** command to quit the MSTP region mode.

Step 4 Run the **erps ring** to create an ERPS ring and enter the ring mode.

The nodes on the same ring must be configured with the same ring ID.

Step 5 Run the **control-vlan** command to configure the control VLAN for the ERPS ring.

vlan-id must be the same as the *vlan-id* specified in the **vlan** command.

Step 6 Run the **protected-instance** command to configure the protection instance for the ERPS ring.

instance-id must be the same as the *instance-id* specified in the **instance vlan** command.

Step 7 Run the **port** command to add the ports to the ERPS ring.

port-id must be the same as the *port-id* specified in the **port vlan** command. Specify the **rpl owner** parameter when configuring the RPL owner port.

Step 8 (Optional) Configure ERPS parameters.

NOTE

You are advised to configure the same ERPS parameters on all nodes of the ring.

- Configure the timers.
 - Run the **guard-timer** command to configure the guard timer started by a node when the node detects a fault recovery.

- Run the **holdoff-timer** command to configure the holdoff timer started by a node when the node detects a fault.
- Run the **wtr-timer** command to configure the WTR timer started by a node when the node receives an R-APS (NR) message.
- Run the **description** command to configure the description of the ERPS ring.
- Run the **priority** command to set the 802.1p priority of ERPS messages on the ERPS ring.
- Run the **raps-mel** command to set the value for the MEL field in the ring automatic protection switching (RAPS) messages on the ERPS ring.

Step 9 Run the **display erps** command to query the ERPS configuration.

----End

Example

The following is an example of configuring the RPL owner node by using the following ERPS parameters:

- ERPS ring ID: 1
- Control VLAN ID: 20
- Protection instance ID: 3; mapping service VLAN IDs: IDs 2-10, 12-16
- Ring ports: 0/9/0 and 0/9/1, of which 0/9/0 is the RPL owner port
- ERPS ring description: ERPS Ring 1. The other parameters use their default values.

```
huawei(config)#vlan 20 standard
huawei(config)#port vlan 20 0/9 0,1
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#instance 3 vlan 2 to 10 12 to 16 20
huawei(stp-region-configuration)#active region-configuration
huawei(stp-region-configuration)#quit
huawei(config)#erps ring 1
huawei(config-erps-ring1)#control-vlan 20
huawei(config-erps-ring1)#protected-instance 3
huawei(config-erps-ring1)#port 0/9/0 rpl owner
huawei(config-erps-ring1)#port 0/9/1
huawei(config-erps-ring1)#description ERPS Ring 1
huawei(config-erps-ring1)#quit
huawei(config)#display erps
```

Ring ID	Control VLAN	WTR Timer (min)	Guard Timer (csec)	Port 1	Port 2
1	20	5	200	(D,R)0/9/0	(D)0/9/1

D : Discarding, F : Forwarding, R : RPL Owner
Total number of rings configured : 1

16.8.5 ERPS Reference Standards and Protocols

The reference standards and protocols of the ERPS feature are as follows:

- ITU-T G.8032 V1
- ITU-T G.8032 V2

16.9 VRRP Snooping

VRRP is a fault-tolerant protocol. It allows multiple routers to form a virtual routing device, and provides a mechanism, which ensures that services will be taken over in time by another device once the next hop of a host fails. In this way the continuity and reliability of communication are ensured. VRRP snooping is to snoop (or listen for) VRRP packets.

16.9.1 Introduction to VRRP Snooping

Definition

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant protocol. It allows multiple routers to form a virtual routing device, and provides a mechanism, which ensures that services will be taken over in time by another device once the next hop of a host fails. In this way the continuity and reliability of communication are ensured.

VRRP snooping is to snoop (or listen for) VRRP packets. According to VRRP packets the listening device can confirm the port to which the upstream master router is connected. Then, the listening device will transmit the unicast service stream to the master router and at the same time transparently transmit the VRRP packets of any of other routers to another router in the same VRRP group.

Purpose

To enhance system reliability, the MA5800 is directly dual-homed to two or more BRASs in the upstream direction, and the BRASs run the VRRP protocol. When the MA5800 works in the SVLAN+CVLAN forwarding mode and MAC address learning is disabled, the upstream ports of the MA5800 need to be isolated from each other in order to prevent unknown unicast broadcast storm. However, when the upstream ports are isolated, the upstream BRASs cannot interoperate VRRP packets. VRRP snooping is adopted for forwarding VRRP packets because VRRP snooping enables the BRASs to interoperate VRRP packets so that the BRASs can run VRRP normally.

To prevent asynchronous VRRP status, Huawei develops the VRRP Group Management Protocol (VGMP), which is extended based on VRRP. VGMP manages the VRRP status of each backup group in a unified manner. VGMP provides a mechanism for managing the status synchronization, preemption, and channels of multiple VRRP backup groups. When the MA5800 works in the SVLAN+CVLAN mode, the VGMP protocol may fail to run if the upstream ports are isolated. To enable the BRASs to interoperate VGMP packets, the MA5800 can transparently transmit VGMP packets.

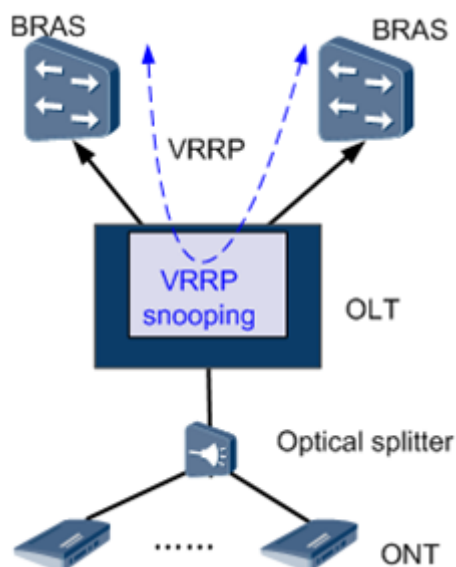
16.9.2 Principle of VRRP Snooping

Basic Principle of VRRP Snooping

In a network, the failure of a single router may cause failure of the entire network. To address this problem, multiple VRRP-running routers on the upper layer of the

MA5800 can form a set of virtual routers. Thus, another router will automatically take over the forwarding service if the master router fails. Viewed from the MA5800 there is still only one router, but this router may be interconnected to two upstream ports of the MA5800. When the path switches from one port to the other, the upstream router will send free ARP packets to update the forwarding path.

Figure 16-45 Network topology of VRRP snooping



As shown in [Figure 16-45](#), to solve the problem of MAC address insufficiency, the MA5800 adopts the SVLAN+CVLAN forwarding mode. In this forwarding mode, MAC address learning needs to be disabled, and the upstream ports of the MA5800 need to be isolated to avoid broadcast storm of unknown unicast packets.

After the upstream ports of the MA5800 are isolated, the multiple upstream routers directly connected to the MA5800 cannot forward VRRP packets to each other through the upstream port of the MA5800. The result will be that the routers fail to run the VRRP protocol. To address this problem, the MA5800 needs to use software forwarding in order to implement VRRP protocol packet exchange between the isolated ports.

When MAC address learning is disabled, packets going upstream may be forwarded to the two upstream ports at the same time, which is a waste of bandwidth. In this case, a static MAC address needs to be configured so that unicast packets are forwarded to the master router only. The MA5800 listens to VRRP packets and free ARP packets to learn the upstream port to which the master router is currently connected. By using the static MAC address, the MA5800 forwards Layer 2 service data to this upstream port.

When the router sends free ARP packets to the MA5800 for switching the forwarding path, the free ARP packets may be lost due to network reasons. If ARP packets are lost, the MA5800 listens to VRRP packets to update the ARP entry. This prevents a condition where Layer 3 forwarding services are interrupted for a long time because the forwarding path is not updated in time.

VRRP Snooping in the VLAN+MAC Forwarding Mode

In the VLAN+MAC forwarding mode, the two routers to which the MA5800 is dual-homed can run the VRRP protocol without additional processing on the MA5800 as long as the following condition is met: The two upstream ports connected to the two routers can interoperate, which allows for normal forwarding of VRRP packets between the two routers. When the network condition is good, or when the MA5800 needs not consider the loss of free ARP packets (a router may provide for retransmission of free ARP packets), VRRP snooping needs not be enabled on the MA5800 when the MA5800 runs in the VLAN+MAC forwarding mode.

16.9.3 Configuring VRRP Transparent Transmission in the S+C Forwarding Mode

In the S+C forwarding mode, after VRRP snooping is enabled, VRRP packets can be forwarded between two isolated upstream ports.

Context

To enhance the system reliability, the MA5800 is directly connected to two or more routers in the upstream direction for dual homing.

- In the S+C forwarding mode, the MAC address learning function needs to be disabled. In addition, to prevent broadcast storms, two upstream ports of the MA5800 need to be isolated. Therefore, the VRRP packets between upper-layer routers cannot be forwarded through the upstream ports of the MA5800. To solve this problem, enable the VRRP transparent transmission function.
- In the VLAN+MAC forwarding mode, the VRRP transparent transmission function may not be enabled.

Procedure

Step 1 Configuring an isolation group.

Run the **isolate group** command to configure an isolation group. To avoid forwarding downstream service packets to another upstream port, you can add the upstream ports to an isolation group.

Step 2 Configure a snooping port.

Run the **vrrp-snoop port** command to configure the upstream port connecting the MA5800 and the router as a snooping port.

Step 3 Configure the virtual IP address and VLAN to be snooped.

Run the **vrrp-snoop ip** command to configure the IP address and VLAN of the virtual router to be snooped.

Step 4 Enable VRRP snooping.

Run the **vrrp-snoop enable** command to enable VRRP snooping.

----End

Example

Assume the following configurations: The MA5800 is connected to two routers through upstream ports 0/9/0 and 0/9/1. The VRRP packets between the routers need to be transparently transmitted through the upstream ports of the MA5800. The VLAN forwarding mode is S+C, the VLAN ID is 100, and the IP address of the virtual router is 10.71.10.1. To perform these configurations, do as follows:

```
huawei(config)#isolate group port 0/9/0 0/9/1
huawei(config)#vrrp-snoop port 0/9/0
huawei(config)#vrrp-snoop port 0/9/1
huawei(config)#vrrp-snoop ip 10.71.10.1 vlan 100
huawei(config)#vrrp-snoop enable
```

16.9.4 VRRP Snooping Reference Standards and Protocols

The reference standards and protocols of this feature are as follows:

- RFC3768, Virtual Router Redundancy Protocol (VRRP)
- RFC2787, Definitions of Managed Objects for the Virtual Router Redundancy Protocol

16.10 Ring Check

The ring check feature is mainly used to detect the user-side, cascade-side, and network-side ring networks, and eliminate the user-side ring network.

16.10.1 Introduction to Ring Check

Definition

The Ring Check feature enables the device to send the Ring Check packets periodically and monitors the Ring Check packets received on the user-side, cascade-side, and network-side to detect whether a loop occurs on the network of the carrier. If a loop occurs, the MA5800 deactivates the subscriber port on the loop and reports the corresponding alarm to the NMS. This ensures that the device runs in the normal state and that legal users are not affected.

Purpose

Ring check is used to quickly locate the user-side, cascade-side, and network-side ring network, and eliminate the ring network according to requirements.

- To prevent the self-loop on a single user port from occurring
- To prevent the loop between user ports from occurring
- To prevent the loop between a user port and a network port, or between a subscriber port and a cascade port from occurring

Benefit

For carriers

The Ring check feature enables the system to detect the carrier's network and report an alarm to the NMS when a loop occurs. The alarm enables the carrier to

know the network fault in the shortest period of time so that the fault can be quickly rectified to resume the normal running of the network.

For users

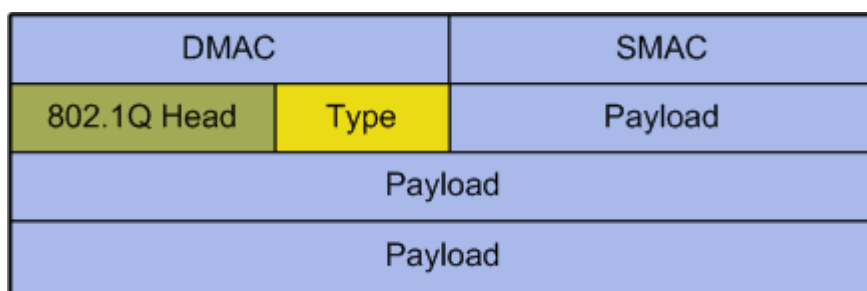
The Ring check feature enables the device to deactivate the user port on a loop to ensure that authorized users receive a good network service rather than be affected.

16.10.2 Principle of Ring Check

Format of the Ring Check Packet

The ring check feature enables the device to transmit the ring check packets to the user port, cascade side, and network side port periodically, and to monitor the ring check packets received on the user side, cascade side, and the network side to check whether a loop occurs on the network of the carrier. **Figure 16-46** shows the format of the ring check packet.

Figure 16-46 Format of the ring check packet



- DMAC indicates the broadcast MAC address with value ff-ff-ff-ff-ff-ff and SMAC indicates the bridge MAC address.
- 802.1Q Head is optional according to flow attributes on the user side.
- Type indicates the proprietary Ethernet type, which can be configured.
- Payload of the packet content is proprietary and it needs not be configured.

Principle

After the ring check function is enabled on the user side, cascade side, and network side, the device periodically transmits private ring check packets to the user port, the cascade port, and the network port, and captures the user-side, cascade-side, and network-side ring check packets on the network and user sides simultaneously.

- For the ring check packets (that are sent from the user side, cascade-side, or network side of the local device) captured on the cascade side or network side, the system reports an alarm to the NMS.
- For the user-side, cascade-side, and network-side ring check packets captured on the user side, the system reports an alarm to the NMS and deactivates the port receiving the packets, eliminating the ring network.

NOTE

After the fault is solved, the port will be activated after some time. If you want to enable the port quickly, the port needs to be deactivated and activated again.

- Detects a maximum of 12 up traffic streams per second. If the system has 8000 up traffic streams, 666.67s (8000/12) is required for detecting a loop if a loop exists.

Figure 16-47 shows the use-side ring network scenarios in FTTH/DSLAM applications.

- In the case of (1), (2), and (3), after receiving the ring check packets captured on the user side, the system reports an alarm to the NMS and deactivates the port receiving the packets, eliminating the ring network.
- In the case of (4), after detecting the ring network between the network side or cascade side and user side, the system reports an alarm to the NMS and deactivate the port on the user side, eliminating the ring network.

Figure 16-47 Use-side ring network scenarios in FTTH/DSLAM applications

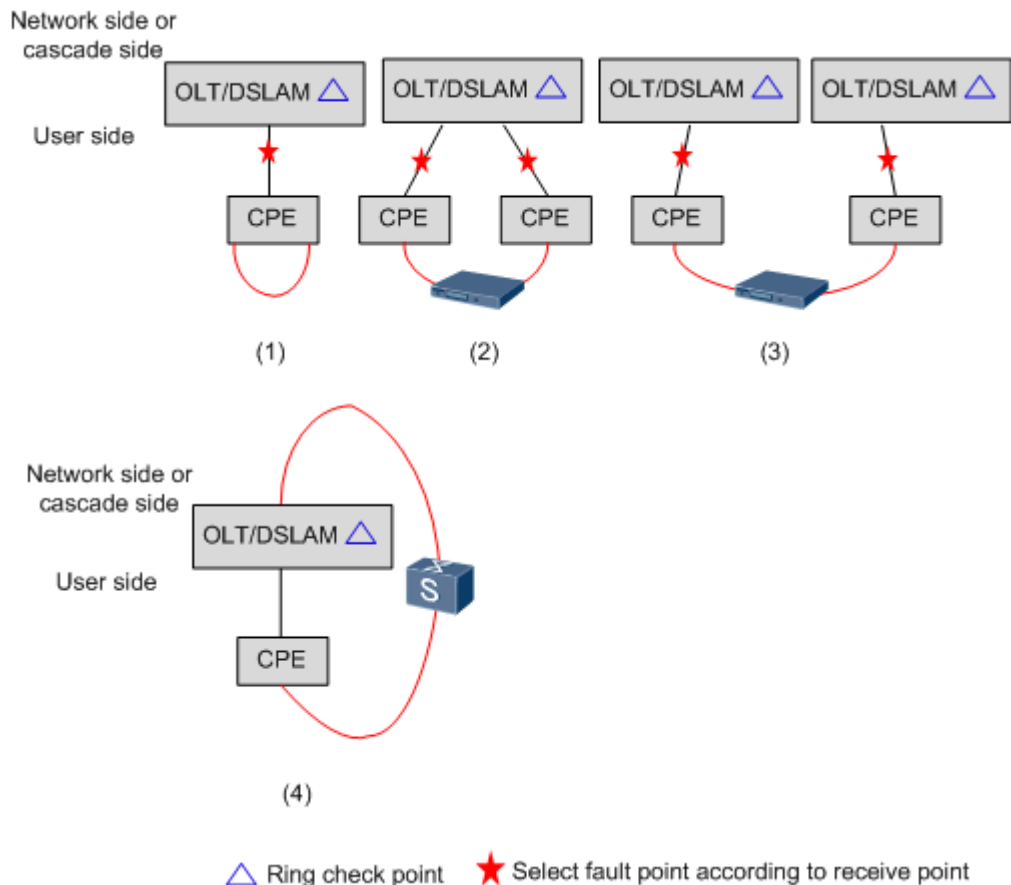
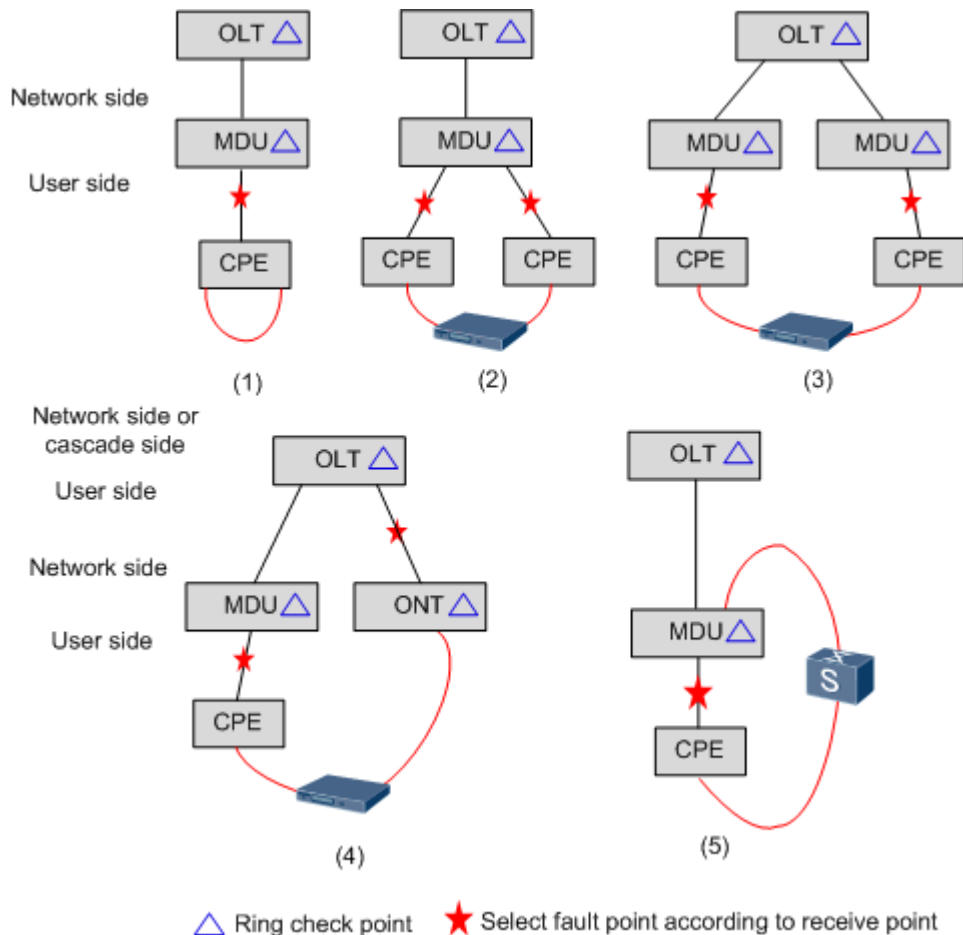


Figure 16-48 shows the use-side ring network scenarios in FTTB/FTTC applications.

- The Ethernet Types of ring check packets of the OLT and the MDU are recommended to be the same.

- If Ethernet Types of ring check packets of the OLT and the MDU are the same, the ring check packets are captured on the OLT and the MDU and are judged.
- If Ethernet Types of ring check packets of the OLT and the MDU are different, the OLT and the MDU capture its own ring check packets. In the case of (4), the system cannot detect a ring network because the MxU and OLT do not identify ring check packets sent by the peer.
- In the case of (1), (2), (3), and (4), after receiving the ring check packets captured on the user side, the system reports an alarm to the NMS and the system deactivates the port receiving the packets, eliminating the ring network.
- In the case of (5), the MDU captures ring check packets sent from its user side on the network side, reports an alarm to the NMS, and sends network-side ring check packets to the user side. After receiving ring check packets sent from the network side, the user side deactivates the port receiving the packets, eliminating the ring network.

Figure 16-48 Use-side ring network scenarios in FTTB/FTTC applications



16.10.3 Configuring the Ring Network Detection

This topic describes how to configure the ring network detection on the user side, cascade-side, and network side to prevent the services from being affected by the ring network.

Context

- By default, the ring network detection is disabled.
- After the ring network detection is enabled, the system automatically detects the ring network.

NOTICE

To ensure the security of the device, it is recommended that the ring network detection is enabled.

Procedure

Step 1 (Option) Run the **ring check private-ethtype** command to configure the private Ethernet protocol type of ring network detection packets. If the default Ethernet protocol type (0x8300) of ring network detection packets is the same as the existing protocol type on the network, change the protocol type of the ring detection packets to be different from the protocol type on the network.

Step 2 (Option) Run the **ring check resume-interval** command to set the auto-activation interval for the port in ring check.

After the auto-activation interval is set, when detecting a ring network, the system automatically activates the port that sends the ring check packet.

Step 3 (Option) Run the **ring check trap-notify** command to set the user-side ring check trap notification mode to alarm.

NOTE

By default, the user-side ring check trap is notified as an event.

Step 4 Enable the ring network detection.

- Run the **ring check enable** command to enable the user-side ring network detection.
- Run the **ring check uplink detection enable** command to enable the network-side ring network detection.
- Run the **ring check cascade detection enable** command to enable the cascade-side ring network detection.

Step 5 Run the **display ring check config** command to query the status of the ring network detection.

Step 6 Run the **display ring check record** command to query the records of the ports, ONTs, or CNUs which were deactivated after ring check is enabled.

----End

Example

To enable the ring network detection, do as follows:

- Set the private Ethernet type of the ring check packet to 0x2233.
- Set the auto-activation interval to 200 minutes.
- Set the user-side ring check trap notification mode to alarm.

```
huawei(config)#ring check private-ethtype 0x2233
huawei(config)#ring check resume-interval 200
huawei(config)#ring check trap-notify alarm
huawei(config)#ring check enable
huawei(config)#ring check uplink detection enable
Warning: If the interconnected port is in user role and user-side ring check
is enabled, this operation may lead to shutdown of the interconnected port. Are
you sure you want to continue?(y/n)[n]:y
huawei(config)#ring check cascade detection enabling check cascade detection enable
Warning: If the interconnected port is in user role and user-side ring check
is enabled, this operation may lead to shutdown of the interconnected port. Are
you sure you want to continue?(y/n)[n]:y
huawei(config)#display ring check config
Ring check switch status      : enable
Ring check private ethtype    : 0x2233
Ring check resume-interval(min) : 200
Ring check trap-notify        : alarm
Ring check uplink detection    : enable
Ring check cascade detection   : enable
```

16.11 Monitor Link

A monitor link group is composed of one uplink and several downlinks. It is used to monitor the fault of uplinks.

16.11.1 Introduction to Monitor Link

Definition

A monitor link group is composed of one uplink and several downlinks. It is used to monitor the fault of uplinks. After a monitor link group is created, the downstream device can detect the fault of upstream link and switch to a normal uplink.

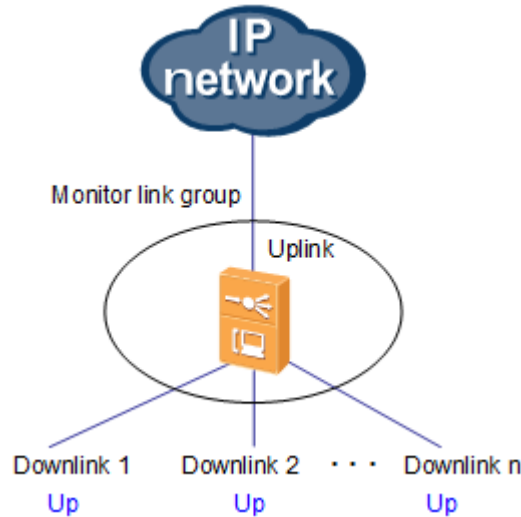
Purpose

The monitor link group is used in the scenario when a device on an aggregation point needs notify uplink faults to cascaded devices. A downstream device working in dual uplink mode can switch to the backup uplink according to the fault status notified by the monitor link group.

16.11.2 Principles of Monitor Link

Basic Concepts

Figure 16-49 Composition of a monitor link group



The following describes some basic concepts related to the monitor link feature.

- **Monitor link group**
A monitor link group is composed of one uplink and several downlinks.

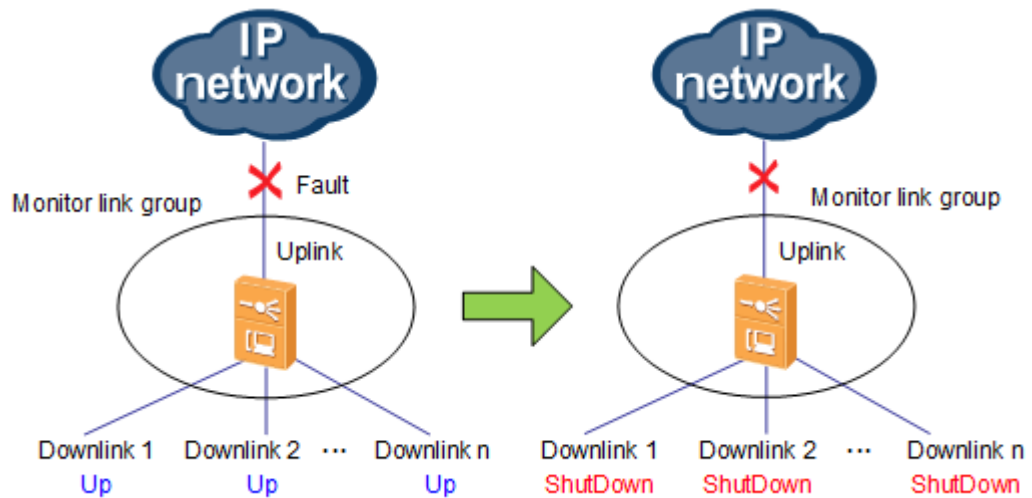
NOTE

The link in a monitor link group may not be a single link, but may be a certain type of link group. The uplink can be an aggregation group or protect group. The downlink can only be a single link. The status of the downlink changes according to the status of the uplink.

- **Uplink**
When the uplink in a monitor link group fails, it indicates that the monitor link group fails. In this case, the downlinks in the monitor link group will be blocked by force.
- **Downlink**
When a downlink in a monitor link group fails, it does not affect the uplink or the other downlinks.

Working Principle

Figure 16-50 Working principle of the monitor link feature



After a monitor link group is configured, its uplink will be monitored in real time. Once the uplink fails, all the UP downlinks in the monitor link group will be blocked by force. When the uplink recovers from the fault, the downlinks are resumed.

When the uplink is an aggregation group or protect group, the uplink is considered failed only when the entire aggregation group or protect group fails.

16.11.3 Configuring the Monitor Link Group

Procedure

- Step 1** Run the **monitor-link group** command to create a monitor link group, and enter the monitor link group mode.
- Step 2** Run the **member port** command to add members to a monitor link group, including the uplink and downlinks.
- Step 3** (Optional) Run the **recover-time** command to configure the recovery time of a monitor-link group. The recovery time of a monitor-link group refers to the jitter-preventing time after which the faulty up link of the monitor-link group becomes normal.
- Step 4** Run the **display monitor-link group** command to query the information about the monitor link group.

----End

Example

Assume the following configurations: The monitor link group ID is 1. The uplink is 0/9/0. The downlink with ID 0 is 0/9/1. The downlink with ID 1 is the Ethernet port

of ONT. The ONT ID is 0. The Ethernet port ID of ONT is 1. The recover time of monitor link is 10 seconds.

```
huawei(config)#monitor-link group 1
huawei(monitor-link-group-1)#member port 0/9/0 uplink
huawei(monitor-link-group-1)#member port 0/9/1 downlink 0
huawei(monitor-link-group-1)#member port 0/10/0 ont 0 eth-port 1 downlink 1
huawei(monitor-link-group-1)#recover-time 10
huawei(monitor-link-group-)#quit
huawei(config)#display monitor-link group 1
```

```
-----
Group ID      : 1
Recover Timer(s) : 10
Group State    : Normal
Downlink Number : 1
-----
Member      Role      Link  Last-up-time    Last-down-time
F/S/P  ONT Port
-----
0/9/0      Uplink      Online 2017-07-19      2017-07-19
              17:54:28+08:00  17:53:53+08:00
0/10/0  0  1 Downlink(0) Online -          -
0/9/1      Downlink(0) Online 2017-07-19      2017-07-19
              17:54:33+08:00  17:53:58+08:00
-----
```