

5 Ethernet Networking Applications

5.1 P2P Optical Access

Point-to-point (P2P) Ethernet optical access refers to the P2P FTTX access provided by the P2P Ethernet optical access board and the ONT, which meets the requirements for the application of the next generation access device under the integration of video, voice, and data services.

5.2 NE Cascading

NE cascading refers to a networking mode in which the MA5800 series are directly connected to each other through the ethernet port on the board. NE cascading saves the upstream optical fiber resources of the access node.

5.3 Ethernet OAM

Ethernet Operation, Administration, and Maintenance (OAM) is used to operate, administrate, and maintain Ethernet networks. It covers three features: connectivity fault management (CFM), Ethernet in the first mile (EFM), and performance monitoring (PM).

5.1 P2P Optical Access

Point-to-point (P2P) Ethernet optical access refers to the P2P FTTX access provided by the P2P Ethernet optical access board and the ONT, which meets the requirements for the application of the next generation access device under the integration of video, voice, and data services.

5.1.1 What Is P2P Optical Access

Definition

Point-to-point (P2P) Ethernet optical access is a mode in which P2P Ethernet optical access boards provide GE, 10GE and FE ports and coordinate with downstream devices to implement various optical access solutions for users. The solutions include FTTC/FTTB, FTTH, FTTO, FTTM.

Purpose

P2P Ethernet optical access is specially applicable to residential communities with optical fibers routed. It provides a more flexible FTTx solution, especially

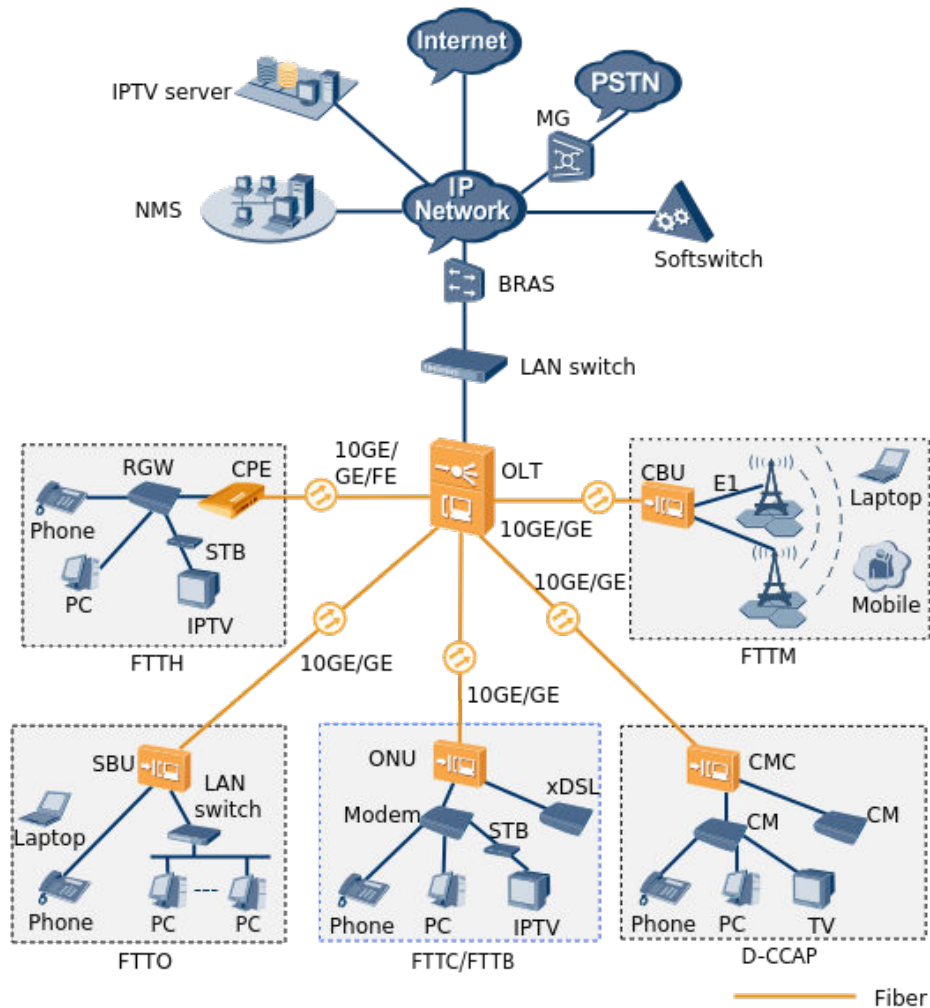
integrated services, including video, voice, and data for users. This feature has the following advantages:

- Higher bandwidth. The FTTH solution implemented through P2P optical access can provide a higher bandwidth for users, meeting the requirements of high-end users.
- Lower costs. P2P Ethernet optical access boards support more cascaded DSLAMs, reducing FTTC/FTTB networking costs.
- Higher reliability. P2P optical access allows higher reliability in the DSLAM cascading scenario through features such as inter-board aggregation, and ring check.
- More flexible scenarios. The P2P Ethernet optical access boards coordinate with a variety of downstream devices (such as the DSLAM, ONT, SBU, and CBU) to implement FTTC/FTTB, FTTH, FTTO, FTTM. An MA5800 configured with the P2P Ethernet optical access board cannot only be directly connected to access terminals but also cascade DSLAMs in order to converge a large number of users.

5.1.2 Networking Application

Figure 5-1 shows the network application in the P2P Ethernet optical access mode.

Figure 5-1 Network application in the P2P Ethernet optical access mode



To meet the requirements of different scenarios, the OLT works with ONUs of various types to implement network applications in multiple optical access modes, such as FTTC/FTTB, FTTH, FTTO, FTTM.

The FTTx network applications in P2P Ethernet optical access have the following in common: The data, voice, and video signals of terminal users are sent to ONUs, where the signals are converted into Ethernet packets and then transmitted over optical fibers to the OLT through the GE/FE upstream ports of the ONUs. Then, the Ethernet packets are forwarded to the upper-layer IP network through the upstream port of the OLT.

The differences between the networking applications of the P2P Ethernet optical access are as follows:

- **FTTH:** The OLT is connected to the CPEs at user premises through P2P Ethernet optical access. In this way, gigabit bandwidth is exclusively provided to each household. FTTH is applicable to new apartments or villas in loose distribution. In this scenario, FTTH provides services of higher bandwidth for high-end users.
- **FTTB/FTTC:** The OLT is connected to DSLAMs in corridors (FTTB) or by the curb (FTTC) through GE P2P Ethernet optical access. The DSLAMs are then

connected to user terminals through xDSL. With the aggregation provided by the DSLAMs, one port on the P2P interface board can be connected to a large number of users. FTTB/FTTC is applicable to densely-populated residential communities or office buildings. In this scenario, FTTB/FTTC provides services of certain bandwidth for common users.

- FTTO: The OLT is connected to enterprise SBUs through GE P2P Ethernet optical access. The SBUs are connected to user terminals through FE, POTS, or Wi-Fi. QinQ VLAN encapsulation is implemented on the SBUs and the OLT. In this way, transparent and secure data channels can be set up between the enterprise private networks located at different places, and thus the service data and BPDUs between the enterprise private networks can be transparently transmitted over the public network. FTTO is applicable to enterprise networks. In this scenario, FTTO implements TDM PBX, IP PBX, and private line service in the enterprise intranets.
- FTTM: The OLT is connected to CBUs through GE P2P Ethernet optical access. The CBUs are then connected to wireless base stations through E1. The OLT connects wireless base stations to the core IP bearer network through optical access technologies. This implementation mode is not only simpler than traditional SDH/ATM private line technologies, but also drives down the costs of base station backhaul. FTTM is applicable to reconstruction and capacity expansion of mobile bearer networks. In this scenario, FTTM converges the fixed network and the mobile network on the bearer plane.

5.1.3 Configuring MDUs Cascaded to an OLT

MDUs are cascaded to an OLT through the P2P board, thereby saving upstream optical fibers and simplifying the network and service configuration.

Service Requirements

- MDU_1 and MDU_2 are connected to an OLT through GE cascading, implementing the Internet access service.
- The Internet access service is provided in the PPPoE dialing mode.

Figure 5-2 Network of MDUs cascaded to an OLT

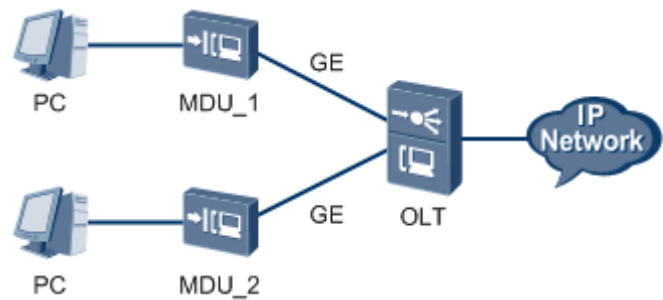


Table 5-1 Data plan

Item	Data
OLT	SVLAN ID: 100 SVLAN type: smart VLAN

Item	Data
	CVLAN ID: 200
	Upstream port: 0/9/0
MDU_1	SVLAN ID: 200 SVLAN type: smart VLAN
	Upstream port: 0/0/1 NOTE The upstream ports vary with MDU type.
MDU_2	SVLAN ID: 200 SVLAN type: smart VLAN
	Upstream port: 0/0/1

Procedure

- Configure the OLT.
 - a. Configure the port role.

Configure the port role of the P2P board as a cascading port. The port roles of the P2P board are user port and cascading port. By default, the port role is user port.

```
huawei(config)#interface eth 0/2
huawei(config-if-eth-0/2)#network-role cascade
huawei(config-if-eth-0/2)#quit
```
 - b. Create a VLAN and add an upstream port to the VLAN.

Create smart SVLAN 100. The upstream port is port 0/9/0.

```
huawei(config)#vlan 100 smart
huawei(config)#port vlan 100 0/9 0
```
 - c. Configure a service port.

Add the service port to the SVLAN by using default traffic profile 6. The CVLAN ID is 200, the same as the upstream VLAN ID of the MDU. MDU_1 and MDU_2 are connected to ports 0/2/0 and 0/2/1 of the OLT respectively.

```
huawei(config)#service-port vlan 100 eth 0/2/0 multi-service user-vlan 200 rx-cttr 6 tx-cttr 6
huawei(config)#service-port vlan 100 eth 0/2/1 multi-service user-vlan 200 rx-cttr 6 tx-cttr 6
```
 - d. Save the data.

```
huawei(config)#save
```
- Configure the MDUs.

The configurations of MDU_1 and MDU_2 are the same. The configuration of MDU_1 is used as an example.

 - a. Create a VLAN and add an upstream port to the VLAN.

Create smart SVLAN 200. The upstream port is port 0/0/1.

 NOTE

The SVLAN of the MDU must be the same as the CVLAN of the OLT.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/0 1
```

- b. Configure a service port.

According to actual conditions, an MDU supports multiple access modes. In this example, the ethernet port 0/3/1 is used. For other access modes, see the corresponding configuration guide of the MDU.

```
huawei(config)#service-port vlan 200 eth 0/3/1 multi-service user-vlan untagged rx-cttr 6
tx-cttr 6
```

- c. Save the data.

```
huawei(config)#save
```

----End

Result

On the PC, the Internet access service is provided in the PPPoE dialing mode.

Configuration File

Configure the OLT:

```
interface eth 0/2
network-role cascade
quit
vlan 100 smart
port vlan 100 0/9 0
service-port vlan 100 eth 0/2/0 multi-service user-vlan 200 rx-cttr 6 tx-cttr 6
service-port vlan 100 eth 0/2/1 multi-service user-vlan 200 rx-cttr 6 tx-cttr 6
save
```

Configure the MDU:

```
vlan 200 smart
port vlan 200 0/0 1
service-port vlan 200 eth 0/3/1 multi-service user-vlan untagged rx-cttr 6 tx-cttr 6
save
```

5.2 NE Cascading

NE cascading refers to a networking mode in which the MA5800 series are directly connected to each other through the ethernet port on the board. NE cascading saves the upstream optical fiber resources of the access node.

5.2.1 Introduction to NE Cascading

Definition

NE cascading refers to a networking mode in which the MA5800 series are directly connected to each other through the ethernet port on the board.

Purpose

NE cascading makes the networking of the MA5800s more flexible, and saves the upstream optical fiber resources of the access node. In addition, remote subtending saves the convergence devices at the central office (CO), simplifies topology, and facilitates service configuration.

5.2.2 Principle of NE Cascading

Cascade network configurations make the networking of the MA5800s more flexible, saving the upstream optical fiber resources of the access point. The remote cascade network configurations save the aggregation equipment resource, simplify the networking, and facilitates the service configuration.

According to the location, the NE-level cascade network supported by the MA5800 consists of the **local cascading** and **remote cascading**.

- Local cascading refers to the cascading of multiple MA5800 subracks in a cabinet or the cascading of multiple local cabinets.
- Remote cascading refers to the cascading of which the remote MA5800 subrack is cascaded by using the optical fiber.

According to the connection mode, the NE-level cascade network supported by the MA5800 consists of the **star cascading** and **daisy chain cascading**.

- In star cascading, multiple MA5800s form a star topology with the upstream device and connects to the upstream device through the MA5800. This networking features high reliability and simple network.
- In daisy chain cascading, multiple MA5800s form a chain topology with the upstream device and connects to the upstream device through one MA5800. This networking features low reliability, especially, if one device is faulty, all its downstream cascaded devices have upstream transmission failures.

Figure 5-3 Star cascading

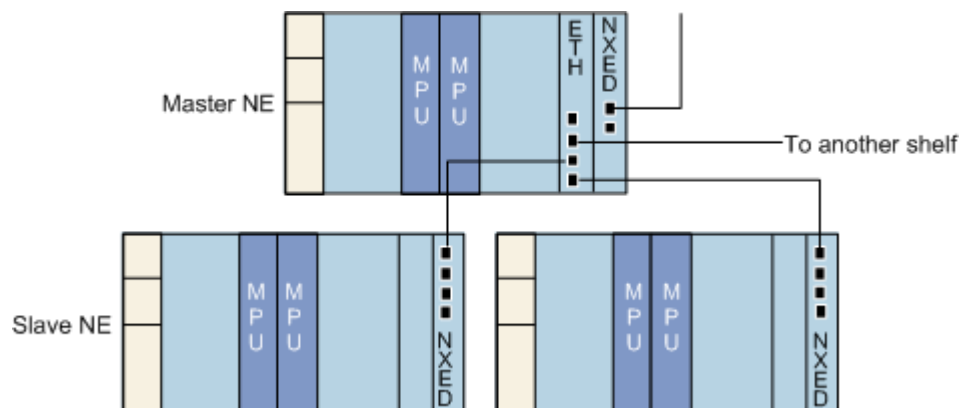
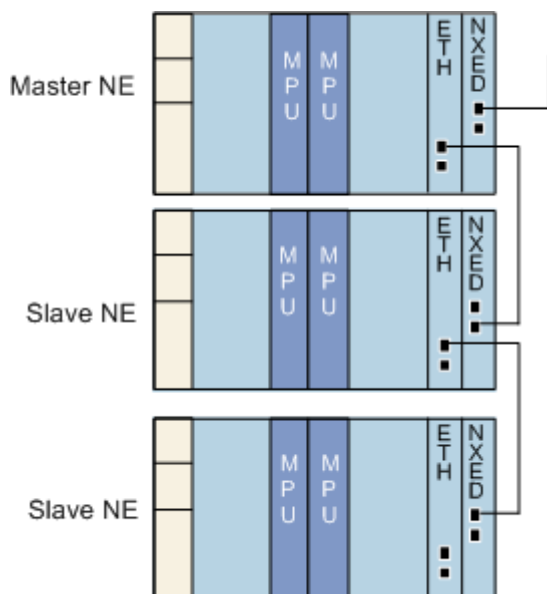


Figure 5-4 Daisy chain cascading

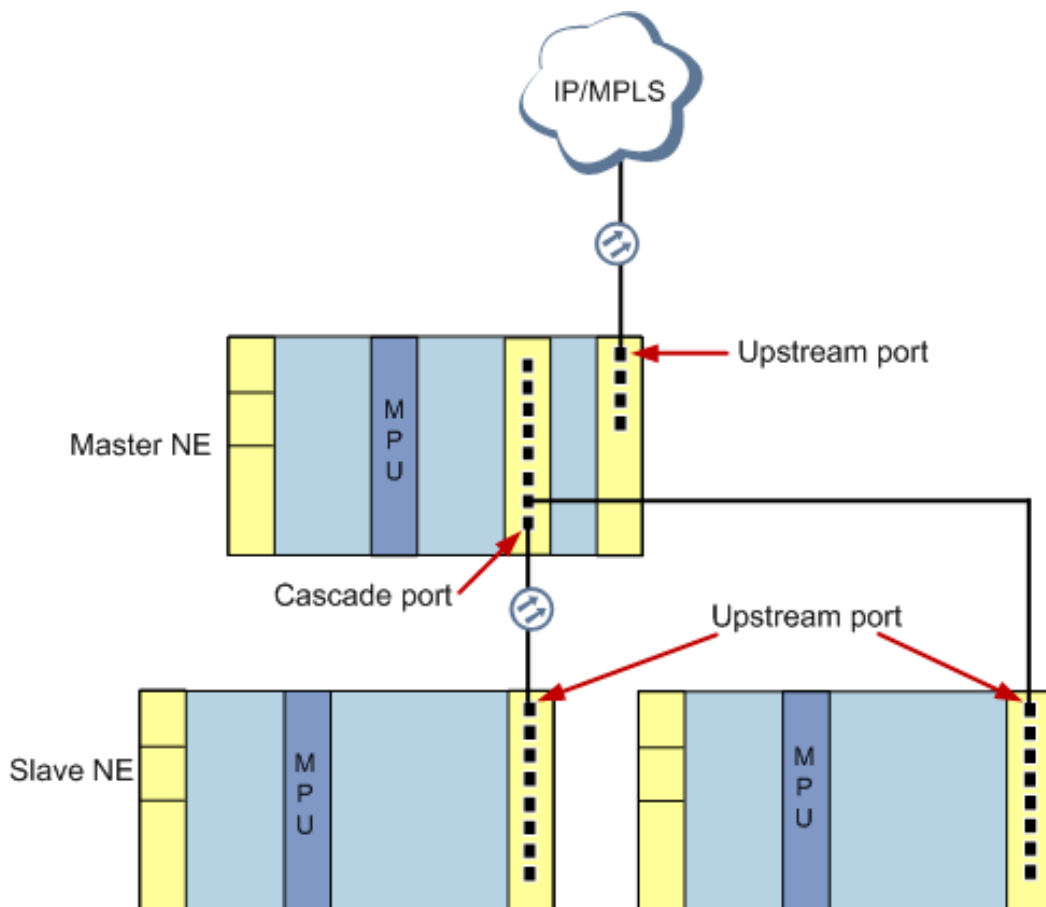
5.2.3 Configuring NE Cascade and Uplink Transmission

The MA5800s (NEs) can be directly connected to each other through the Ethernet port. Cascading saves the upstream optical fibers and simplifies networking and service configuration.

Context

The cascade ports on master NEs and upstream ports on slave NEs must have the same port type, port rate, and port duplex mode.

Figure 5-5 Cascading network



NOTE

Configure the network role of a board first. Otherwise, the network role may fail to be switched if other configurations have been performed.

Procedure

- Configure the master NE
 - a. Set the network role of the upstream board or port of the master NE.

Enter the specific board mode according to the upstream board types. Run the **network-role [port-id] uplink** command to set the network role of the board or port to upstream.
 - b. Set the network role of the cascade board or port of the master NE.

Enter the specific board mode according to the cascade board types. Run the **network-role [port-id] cascade** command to set the network role of the board or port to cascading.
 - c. Configure the VLAN of the master NE.

The VLAN type is smart, and the VLAN attribute is common. For details about the configuration, see **Configuring a VLAN**.
 - d. Add an upstream port to the VLAN of the master NE.

According to the upstream board types, run the **port vlan** command in global config mode to add the upstream port to the VLAN.

- e. Add a cascade port to the VLAN of the master NE.

According to the cascade board types, run the **port vlan** or **service-port** command in global config mode to add the cascade port to the VLAN.

NOTE

For boards OGHK and OXHD, run the **service-port** command to create service flows in Ethernet access.

- Configure the slave NE
 - a. Set the network role of the upstream board or port of the slave NE.

Enter the specific board mode according to the upstream board types. Run the **network-role [port-id] uplink** command to set the network role of the board or port to upstream.

- b. Configure the VLAN of the slave NE. The VLAN of the slave NE is the same as the VLAN of the master VLAN.

The VLAN type is smart, and the VLAN attribute is common. For details about the configuration, see **Configuring a VLAN**.

- c. Add an upstream port to the VLAN of the slave NE.

According to the upstream board types, run the **port vlan** command in global config mode to add the upstream port to the VLAN.

----End

Example

Assume that master NE huawei_A and slave NE huawei_B are cascaded through the OXHD board. To add upstream port 0/3/1 and cascade port 0/2/0 of huawei_A to VLAN 100, and add upstream port 0/3/1 of huawei_B to VLAN 100, do as follows:

```
huawei_A(config)#interface eth 0/2
huawei_A(config-if-eth-0/2)#network-role cascade
huawei_A(config-if-eth-0/2)#quit
huawei_A(config)#vlan 100 smart
huawei_A(config)#port vlan 100 0/3 1
huawei_A(config)#service-port vlan 100 eth 0/2/0 multi-service user-vlan 100

huawei_B(config)#vlan 100 smart
huawei_B(config)#port vlan 100 0/3 1
```

5.3 Ethernet OAM

Ethernet Operation, Administration, and Maintenance (OAM) is used to operate, administrate, and maintain Ethernet networks. It covers three features: connectivity fault management (CFM), Ethernet in the first mile (EFM), and performance monitoring (PM).

5.3.1 Introduction

Ethernet is a widely used local area network (LAN) technology featuring rich bandwidth and low cost. As the application of Ethernet is spanning from carrier networks to metropolitan area networks (MANs) and wide area networks (WANs), network administration and maintenance become increasingly important. However, traditional Ethernet is unable to provide end-to-end (E2E) service management, fault detection, or performance monitoring, which are instead implemented by IP-based mechanisms. These mechanisms (such as ping messages) at the IP layer are used to operate and manage the entire network, but they cannot meet operation and maintenance requirements of the Ethernet bottom layer that has no IP addresses. Against this backdrop, the IEEE and ITU-T have done a lot of researches and worked out their own Ethernet OAM standards.

Ethernet Operation, Administration, and Maintenance (OAM) covers three features: connectivity fault management (CFM), Ethernet in the first mile (EFM), and performance monitoring (PM). The following table describes the main functions of these features.

Feature	Description	Application Scenario
CFM	CFM is defined in the IEEE 802.1ag (802.1ag for short). It is an OAM feature for detecting and locating Ethernet connectivity faults by including the functions of continuity check (CC), loopback (LB), linktrace (LT), and so on. The ITU-T Y.1731 (Y.1731 for short) covers all the CFM functions defined in the 802.1ag and adds more information types to enhance the CFM capability.	CFM mainly applies to access and convergence nodes. It is used to monitor connectivity on the entire network and to locate connectivity faults for end-to-end (E2E) Ethernet links. For example, in IPTV services, CFM can be used to monitor network connectivity between a user terminal and the service provider's IPTV server and to determine the location of a fault.
EFM	EFM is defined in the IEEE 802.3ah (802.3ah for short). It is an OAM feature for detecting quality and connectivity of last-mile Ethernet links.	EFM packets cannot be forwarded across multiple hops. Therefore, EFM mainly applies to the user access network (that is, the last mile) and also to the Ethernet physical link that directly connects two devices. For example, EFM can be used to monitor the link between a user access board and a user terminal and to notify the system of link exceptions using Ethernet OAM link events. Link exceptions can be link interruptions or that the number of received error packets exceeds the preset threshold due to deteriorating link quality.

Feature	Description	Application Scenario
PM	PM is defined in the Y.1731. It is an OAM feature for measuring and testing Ethernet performance, including loss measurement (LM), delay measurement (DM), and throughput measurement.	PM is mainly used to evaluate the network performance and quality and to discover latent network defects (such as an increasing packet loss rate due to line aging), reducing user complaints and improving quality of service (QoS).

 NOTE

This chapter includes all the Ethernet OAM features that are supported by access devices. Some features and commands described in this chapter might be not supported by some specific devices. For details of which functions are supported by a specific device, refer to the specification list of the device.

5.3.2 Ethernet OAM Reference Standards and Protocols

Table 5-2 Reference standards and protocols of the Ethernet OAM feature

Ethernet OAM Type	Reference Standards and Protocols
CFM	- ITU-T Y.1731: OAM functions and mechanisms for Ethernet based networks - IEEE 802.1ag-2007 VLAN Amendment: 5 Connectivity Fault Management
EFM	IEEE 802.3ah: Operations, Administration, and Maintenance (OAM)
PM	ITU-T Y.1731: OAM functions and mechanisms for Ethernet based networks

 NOTE

Connectivity fault management (CFM) is implemented according to the formal IEEE 802.1ag-2007 and is not compatible with Draft6.0.

ITU-T Y.1731 mentioned in this document is of version 07/2011.

5.3.3 Differences in Implementing Y.1731 and 802.1ag on Access Device

The ETH OAM of the access device is implemented based on concepts defined by 802.1ag. For concepts defined by both 802.1ag and Y.1731, there is no difference in implementation. For concepts defined by Y.1731 but not defined in 802.1ag, the similar concepts in 802.1ag are used. The following table describes the differences

in implementing related concepts of Y.1731 and 802.1ag on the access device. The similar concepts of 802.1ag and Y.1731 are in the same row.

Concept of 802.1ag	Concept of Y.1731	Implementation of Differences Between Y.1731 and 802.1ag
Maintenance domain (MD)	No similar definition	For Y.1731, MD name is configured to no name .
Maintenance association (MA)	Maintenance entity group (MEG)	For Y.1731, ensure that the following requirements are met when configuring an MA. • MA ID is configured to MEG ID. • MA name must use the ICC-based format.
Maintenance point (MP)	MEG point (MP)	There is no difference in implementing MP in Y.1731 and 802.1ag.
Maintenance association end point (MEP)	MEG end point (MEP)	There is no difference in implementing MEP in Y.1731 and 802.1ag.
Maintenance association intermediate point (MIP)	MEG intermediate point (MIP)	There is no difference in implementing MIP in Y.1731 and 802.1ag.

5.3.4 CFM (802.1ag and Y.1731)

Connectivity fault management (CFM) is defined in the IEEE 802.1ag (802.1ag for short). It is an OAM feature for detecting and locating Ethernet connectivity faults. The ITU-T Y.1731 (Y.1731 for short) covers all the CFM functions defined in the 802.1ag and adds more information types to enhance the CFM capability.

5.3.4.1 CFM Introduction

The IEEE and ITU-T have worked out their own standards for monitoring Ethernet connectivity and identifying connectivity faults for E2E Ethernet links.

- The 802.1ag (also known as CFM) defines Ethernet Operations, Administration, and Maintenance (OAM) functions, which are used for detecting and identifying link connectivity faults on a network involving multiple independent maintenance organizations.
- The Y.1731 covers all functions defined in the 802.1ag and enhances some functions.

The access device supports CFM defined in the 802.1ag and Y.1731. [Table 5-3](#) describes functions of CFM.

Table 5-3 Functions of CFM

Function	Description
Continuity check (CC)	Monitors connectivity of Ethernet links in real time and reports link exceptions by alarms.
LinkTrace (LT)	- Obtains MAC addresses of intermediate devices along the Ethernet link between two devices. - Determines the location of a link fault.
Loopback (LB)	Unicast LB - Checks connectivity of the Ethernet link between two devices. - Determines the location of a link fault. Multicast LB - Checks connectivity of Ethernet links between one device and multiple other devices. - Obtains the MAC address of a remote device that has the same maintenance level as the local device. Bidirectional diagnostics test: Checks the packet loss rate and bit error rate of the bandwidth-specific bidirectional Ethernet link between two devices to determine whether the bandwidth meets user requirements.
AIS (Alarm Indication Signal)	- Suppress alarms. - Send link fault information to the peer with higher-level.
LLF (Link Loss Forwarding)	Upon link fault detection, the device sends information to the peer end which is still communicated with the device. Then the peer end can react such as shutting down the port automatically. LLF is often used in the FTTO scenarios of national broadband network. When the leased channel of the retail service provider (RSP) is faulty, LLF function makes it possible that the RSP and its users are informed by the operator immediately.

Y.1731 and 802.1ag have the following differences in implementing the CFM function.

- The continuity check (CC) function and principle defined by Y.1731 and 802.1ag are the same only with one difference in the format of the continuity check message (CCM). Because of the difference, there are some limitations in usage of the CFM function when the access device is interconnected with the peer end that only supports Y.1731.
 - When MD is being configured, configure **MD name** to no name.
 - When MA is being configured, MA ID is identical to MEG ID. **MA name** must use the ICC-based format.

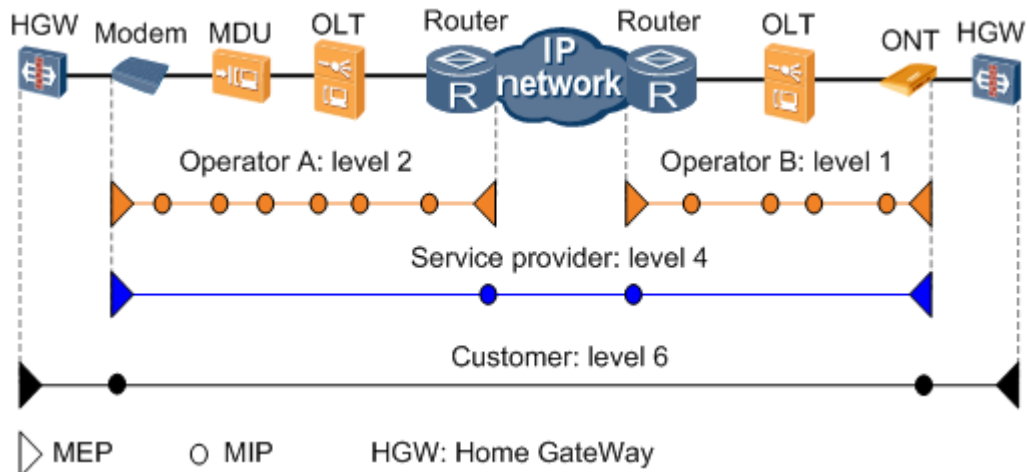
- 802.1ag defines the unicast LB. Y.1731 defines the unicast LB, multicast LB, and bidirectional diagnostics test. In addition, Y.1731 provides the extended loopback message (LBM), and the size and sending interval of LBMs can be set and disorder in the loopback reply (LBR) message returned by the peer end can be detected.
 - No matter whether the peer end device supports Y.1731 or 802.1ag, when implementing an LB (including the unicast LB, multicast LB, and bidirectional diagnostics test), the access device can receive the LBR message returned by its peer end. In addition, the test result does not vary with the protocol used at the peer end.
 - No matter whether the peer end device supports Y.1731 or 802.1ag, the access device can correctly reply with the LBR messages.
- Y.1731 and 802.1ag have no difference in implementing the LT function. No matter whether the peer end device supports Y.1731 or 802.1ag, the access device can implement the link trace (LT) and correctly reply with the linktrace reply (LTR) messages.
- ETH-AIS is only defined in Y.1731.
- LLF is a function defined by Huawei. It is implemented based on the information format defined in 802.1ag.

5.3.4.2 CFM Network Application

In carrier-class Ethernet networks, different organizations are required to provide different administration and maintenance scopes and contents. Therefore, carrier-class Ethernet needs to be maintained hierarchically. Three types of organizations are generally involved in carrier-class Ethernet services: customers (for example, private network users), service providers, and network operators. Customers purchase Ethernet services from service providers, service providers can use their own networks or leased networks to provide end-to-end (E2E) Ethernet services, while network operators provide networks for transmitting services.

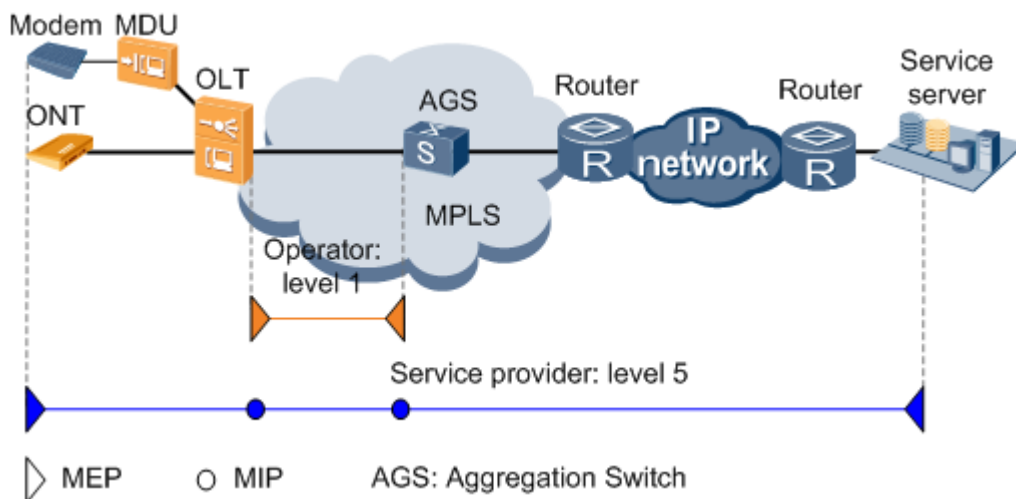
The following picture shows a typical CFM network. In the figure, locations of maintenance association end points (MEPs) and maintenance domain intermediate points (MIPs) are marked, and different maintenance domains (MDs) are configured for three maintenance levels (customer, service provider, and network operator).

Figure 5-6 Typical CFM network



CFM also applies to MPLS networks for connectivity diagnosis, as shown in the picture below.

Figure 5-7 Typical CFM network



5.3.4.3 CFM Basic Concepts

This topic describes some basic concepts of the connectivity fault management (CFM), such as the maintenance domain (MD), maintenance association (MA), maintenance association end point (MEP) and maintenance association intermediate point (MIP) that we need to understand before getting to know the working principle of the CFM function.

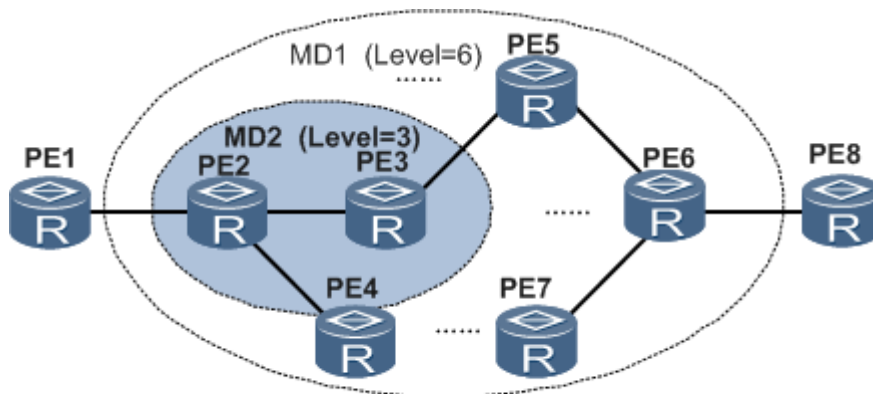
MD

A maintenance domain (MD) is used to divide the network covered by the connectivity fault test.

In order to locate a fault precisely, the concept of **level** is introduced in MD. An MD provides eight levels, represented by the integer number 0-7. A larger number indicates a higher level and a larger-range MD. An MD can be embedded into or neighbor on another MD but an MD cannot cross another. A low-level MD is embedded into a high-level MD, but a high-level MD cannot be embedded into a low-level MD.

The MD level makes the fault locating precise and easy. As shown in [Figure 5-8](#), MD2 is embedded into MD1. If MD1 detects a fault, it is suspected that the links or the devices from PE2 to PE6 are faulty. If MD2 does not detect any fault, PE2, PE3 and PE4 work properly. Therefore, the fault is narrowed down to the links between PE5, PE6, and PE7 or these devices.

In actual application, if an MD contains another small-range MD and the connectivity test is performed for the large-range MD, CFM packets need to traverse the small-range MD. To achieve that purpose, set the level of the large-range MD higher than that of the small-range MD. For example, in the network as shown in [Figure 5-8](#), MD1 contains MD2 and CFM packets of MD1 need to traverse MD2. The level of MD1 is set to 6 and the level of MD2 is set to 3. In this way, CFM packets of MD1 can traverse MD2 and CFM for the entire MD1 can be implemented. Moreover, CFM packets of MD2 will not spread to MD1.

Figure 5-8 MD levels

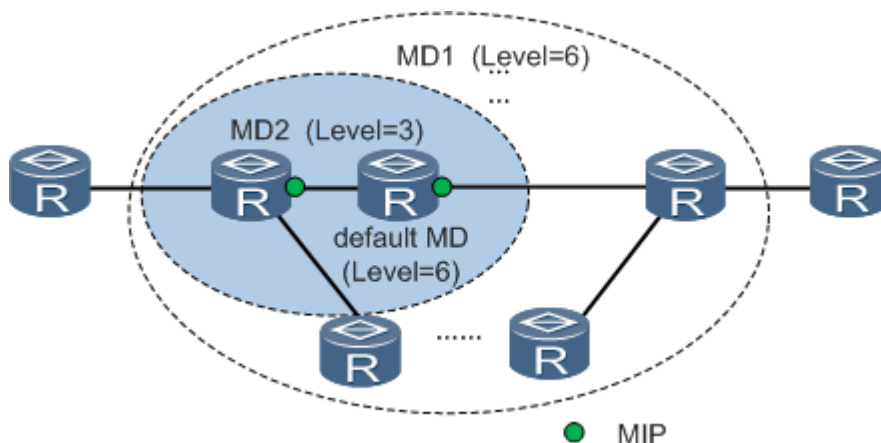
PE: Provider Edge

CFM packet interaction and basic CFM functions are implemented based on MDs. Proper MD planning can help network administrators locate faults quickly.

Default MD

The default MD is used for the high-level MD to sense the internal topology of the low-level MD.

As shown in [Figure 5-9](#), a low-level MD is embedded into a high-level MD, and devices in the high-level MD may be the edge and intermediate devices in the low-level MD. When CFM protocol packets of the high-level MD traverse the low-level MD, the packets are transmitted transparently. If the default MD is not configured and the high-level MD needs to sense the internal topology of the low-level MD, a maintenance association intermediate point (MIP) with a specific level needs to be created on the specific port of the device in the low-level MD and the MIP is used to reply to devices in the high-level MD with loopback reply (LBR) or linktrace reply (LTR) messages.

Figure 5-9 Default MD

If the default MD with the same level as the high-level MD is configured on the devices in the low-level MD, MIPs of corresponding levels based on default MDs are generated to reply to devices in the high-level MD with LBR or LTR messages.

In this way, the high-level MD can sense the topology changes in the low-level MD and CFM can be implemented in the entire MD1.

The level of the default MD is the same as that of the high-level MD but is higher than the levels of all MDs to which the MEPs configured on the device belong.

MA

An MA specifies the range a CCM can reach.

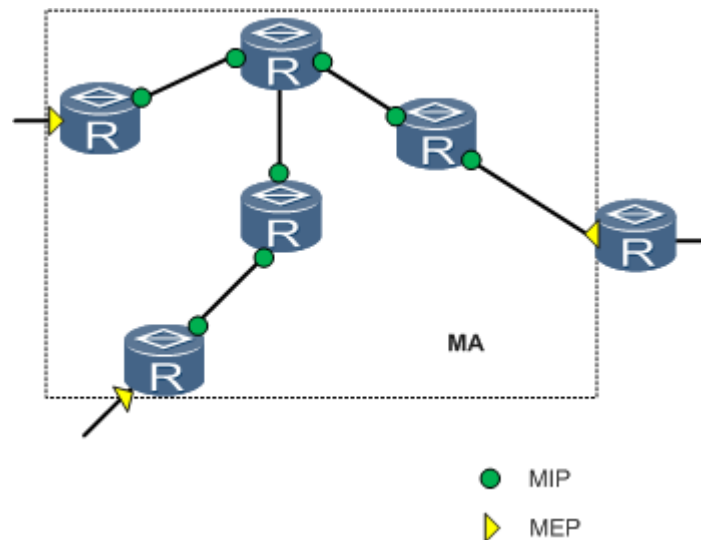
One or more MAs can be configured in an MD according to the actual needs. Each MA is a grouping of some maintenance points (MPs) in an MD. The level of an MA is the same as the level of the MD to which it belongs.

An MA serves a certain service (such as a VLAN): All packets sent by MPs in an MA carry the service tag, and an MP can receive packets sent by other MPs in the same MA.

MP

MPs are configured on ports and belong to a certain MA. There are two MPs: MEP and MIP. [Figure 5-10](#) shows the MPs.

Figure 5-10 MP



MEP

MEPs are end points of the MD and MA, and they specify the range and boundary of the MD and MA.

The level of an MEP is identical to the level of the MD to which it belongs. The level of an MEP determines the level of packets it can process.

- When an MEP receives a packet whose level is higher, it does not process this packet and forwards the packet along its original path so that the packet can traverse the MD.
- If an MEP receives a packet whose level is the same or lower, the MEP will process the packet.

The levels of packets sent by an MEP are the same as the level of the MEP.

MEPs are located on ports of devices and need to be created by users manually.

The MEP on any device that runs Ethernet CFM is called the local MEP. The MEPs on the other devices in the same MA are the remote maintenance association end points (RMEPs) to the local MEP.

MIP

MIPs are inside an MA. Network management can be improved by deploying multiple MIPs among MEPs. More MIPs bring about stronger control and improved management over networks. For profitable services that key accounts care about, carriers deploy much more MIPs.

MIPs are located on ports of devices, and they are generated automatically according to specific rules but cannot be created manually.

5.3.4.4 CFM Principles

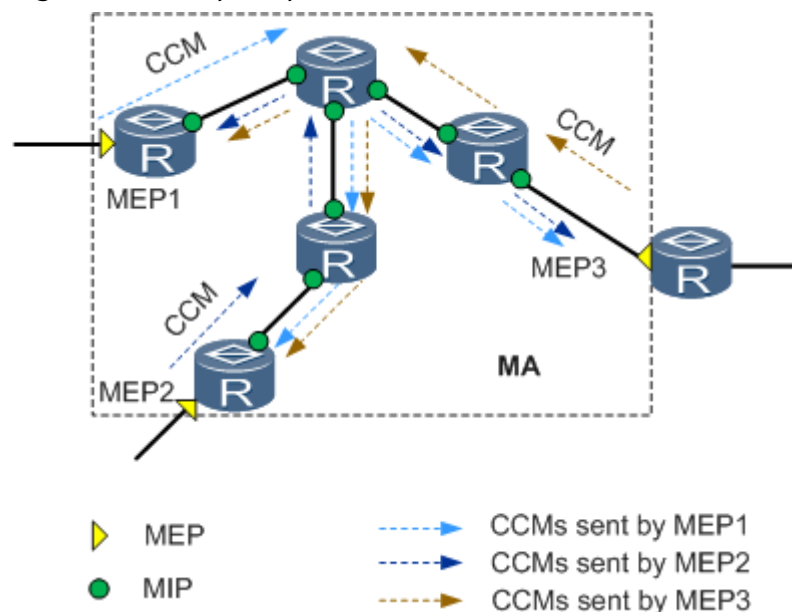
This topic describes the basic concepts and principles of CFM based on 802.1ag. Because the connectivity fault management (CFM) function defined by Y.1731 is similar to the one defined by 802.1ag, you can refer to the similar concepts of 802.1ag to get to know the mechanism of Y.1731 unless otherwise specified.

5.3.4.4.1 CC Principle

Continuity check (CC) is used to monitor connectivity of Ethernet links in real time and to report link exceptions by alarms.

A maintenance association end point (MEP) periodically sends multicast continuity check messages (CCMs) to other MEPs in the same maintenance association (MA). If an MEP fails to receive expected CCMs or receives unexpected CCMs within a certain period, the MEP considers that it has detected a connectivity fault in its MA. [Figure 5-11](#) illustrates the CC principle.

Figure 5-11 CC principle



1. MEP database setup
- Each device with Ethernet connectivity fault management (CFM) enabled has an MEP database. The database records the MEPs (local MEPs) configured on the local device and other devices' MEPs (that is, RMEPs) in the same MA. Local MEPs and RMEPs are manually configured but automatically recorded to the MEP database.
2. CCM generation
- An MEP generates and sends CCMs. As shown in [Figure 5-11](#), MEP1, MEP2, and MEP3 are in the same MA. After the function of sending CCMs is enabled, MEP1, MEP2, and MEP3 periodically multicast CCMs to each other at the same interval.
- All maintenance domain intermediate points (MIPs) and MEPs in an MA receive CCMs, with no need to send a reply.
- A CCM carries its maintenance level information. The level of a CCM is equal to the level of the MEP sending the CCM.
3. CCM termination
- An MEP terminates CCMs. If an MEP receives a CCM whose level is higher than the MEP's, the MEP forwards this CCM. If an MEP receives a CCM whose level is lower than or equal to the MEP's, the MEP does not forward this CCM, ensuring that CCMs in a lower-level maintenance domain (MD) are not sent to a higher-level MD.
4. Fault identification
- If an MEP fails to receive expected CCMs or receives unexpected CCMs within a certain period, the MEP considers that it has detected a connectivity fault in its MA and reports a link fault alarm. When multiple MEPs in an MD send CCMs, multipoint-to-multipoint (MP2MP) link connectivity is checked.

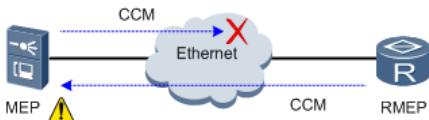
 NOTE

CC can determine whether a fault occurs but cannot identify the fault location. In this case, loopback (LB) and linktrace (LT) can be used to determine the fault location.

[Table 5-4](#) describes the alarms may be generated when link faults occur on a network.

Table 5-4 CC Alarm

Alarm Name	Principle	Troubleshooting
0x2f210001 Loss of Ethernet connectivity check message	If an MEP does not receive a CCM from an RMEP within a period equal to 3.5 times the CC interval, the MEP considers that the RMEP is lost, and the device on which the MEP is configured generates an alarm. The following figure shows how the alarm is generated. 	When the alarm is generated, the link from the RMEP to the MEP is faulty. In this case, LB or LT can be used on the MEP to determine the fault location.

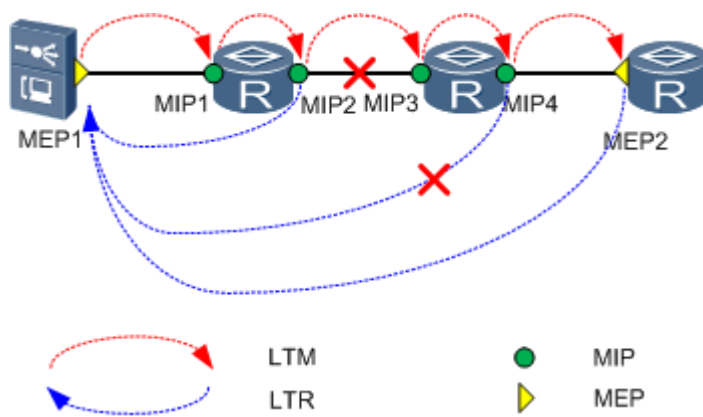
Alarm Name	Principle	Troubleshooting
0x2f210004 Reception of Ethernet connectivity check message with the RDI bit set	When an MEP receives CCMs from its RMEP but the RMEP fails to receive CCMs from the MEP within a period equal to 3.5 times the CC interval, the RMEP considers that the MEP is lost and sets the RDI bit in its CCMs to be sent to 1. If the MEP receives a CCM with the RDI bit set to 1, the device on which the MEP is configured generates an alarm. The following figure shows how the alarm is generated. 	When the alarm is generated, the link from the MEP to the RMEP is faulty but the link from the RMEP to the MEP is normal. That is, a unidirectional connectivity fault occurs on the link. In this case, LB or LT can be used on the MEP to determine the fault location.
0x2f210002 Reception of invalid Ethernet connectivity check message	When an MEP receives CCMs with errors from its RMEP, the device on which the MEP is configured generates an alarm indicating reception of incorrect Ethernet OAM CCMs. Error types include: - Unexpected Periodicity defect (dUNP): The interval of sending CCMs is different from the CC interval of the MEP that receives the CCMs. - Unexpected MEP defect (dUNM): The MEP ID of CCMs is not included in the RMEP ID list of the MEP that receives the CCMs.	When the alarm is generated, the link between the MEP and the RMEP is not interrupted but the MEP receives incorrect CCMs. In this case, the network CFM data plan needs to be checked.
0x2f210003 Reception of Ethernet cross connect connectivity check message	When a CCM received by an MEP from its RMEP contains an item (MD name type, MD name, MA name type, or MA name) different from that configured on the MEP, the device on which the MEP is configured generates an alarm indicating reception of cross connect Ethernet OAM CCMs. The possible causes of the alarm are as follows: - The CCM with the level lowered than the local MEP is received. - When the CCM with the same level is received, the name or type of the peer MA or MD does not match the name of the local end.	When the alarm is generated, the link between the MEP and the RMEP is not interrupted but the MEP receives incorrect CCMs. In this case, the CFM data plan needs to be checked on the MEP and the RMEP.

5.3.4.4.2 LT Principle

Linktrace (LT) is used to obtain MAC addresses of intermediate devices along the Ethernet link between two devices and also determine the location of a link fault.

Along the link between the maintenance association end point (MEP) LT initiator and the target MEP, every device that generates a maintenance domain intermediate point (MIP) sends a linktrace reply (LTR) to the initiator and forwards the linktrace message (LTM) until the LTM reaches its target. The MEP LT initiator, through LTRs, obtains MAC addresses and locations of all in-between devices as well as the link section where a fault occurs. [Figure 5-12](#) illustrates the LT principle.

Figure 5-12 LT principle



1. When all links are functioning properly, MEP1 sends an LTM to MEP2.
2. After all devices along the link between MEP1 and MEP2 receive the LTM, egress points (MIP2 and MIP4) return an LTR to MEP1, and forward the LTM with the time to live (TTL) field decremented by 1 to the next hop. An LTR contains the MAC address of the device sending the LTR.
3. After receiving the LTM, MEP2 stops forwarding the LTM but directly returns an LTR to MEP1.
4. As shown in [Figure 5-12](#), when the link between MIP2 and MIP3 is faulty, MEP1 can receive an LTR from MIP2 but not from MIP4 after sending an LTM destined for MEP2. In this way, the fault location is determined.

5.3.4.4.3 LB Principle

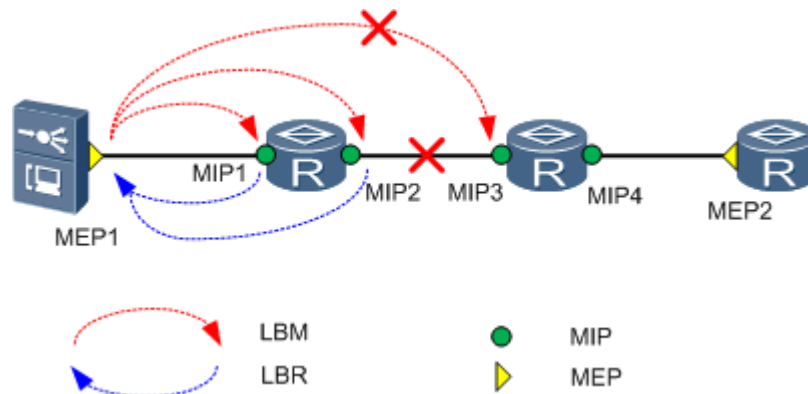
Loopback (LB) is used to check connectivity of end-to-end (E2E) Ethernet links between devices and also determine the location of a link fault.

Unicast LB

Unicast LB, similar to the ping operation at the IP layer, is mainly used to check the status of connection between a local device and a remote device.

[Figure 5-13](#) illustrates the principle of unicast LB.

Figure 5-13 Unicast LB principle



1. MEP1 sends a loopback message (LBM) to MIP1.
2. MEP1 receives a loopback reply (LBR) from MIP1.

NOTE

A maintenance domain intermediate point (MIP) only responds to the received LBM but does not forward the LBM to the next-hop MIP or the target maintenance association end point (MEP).

3. MEP1 sends an LBM to the next hop of MIP1, that is, MIP2.
4. MEP1 receives an LBR from MIP2.
5. MEP1 sends an LBM to the next hop of MIP2, that is, MIP3.
6. MEP1 fails to receive an LBR from MIP3 because the link between MIP2 and MIP3 is faulty.
7. MEP1 determines that the link between MIP2 and MIP3 is faulty.

In unicast LB, the destination MAC address of an LBM is a unicast MAC address. Therefore, before using unicast LB, ensure that:

- The MAC address or MEP index of MEP2 and the MAC addresses of all MIPs along the link between MEP1 and MEP2 are obtained if the connection status of all links between MEP1 and MEP2 is required for accurately determining the fault location. LT can be performed on MEP1 to obtain the MAC addresses of all MIPs along the link between MEP1 and MEP2.
- The MAC address or MEP index of MEP2 is obtained if only the connection status between MEP1 and MEP2 is required.

MEP1 can send multiple LBMs and, based on the number of received LBRs, determine whether packet loss occurs on the network.

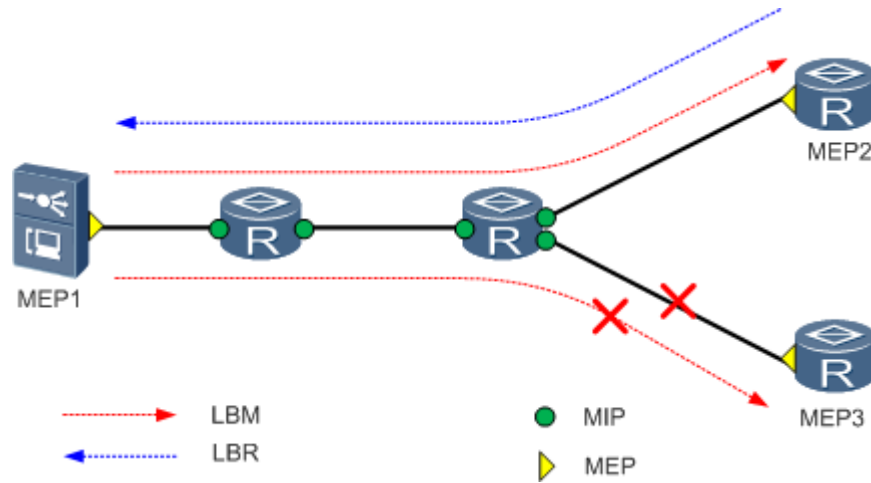
Multicast LB

Multicast LB is used to check connectivity between an MEP and its peer MEPs and to obtain MAC addresses of those MEPs.

Multicast LB generally applies to scenarios in which multiple MEPs are deployed. In multicast LB, the MAC address of an LBM is a multicast MAC address in format of 01-80-C2-00-00-3x, where x is the level of the MEP initiating multicast LB. When the level of a peer MEP is equal to the level of the received multicast LBM,

the peer MEP returns an LBR to the MEP initiating multicast LB. **Figure 5-14** illustrates the principle of multicast LB.

Figure 5-14 Multicast LB principle



1. MEP1 multicasts an LBM.
2. MEP2 returns an LBR after receiving the LBM.
3. MEP3 fails to receive the LBM and therefore does not return an LBR because the link between MEP3 and MEP1 is interrupted.
4. MEP1, according to the received LBR, determines that the link between MEP1 and MEP2 is functioning properly but the link between MEP1 and MEP3 is faulty.

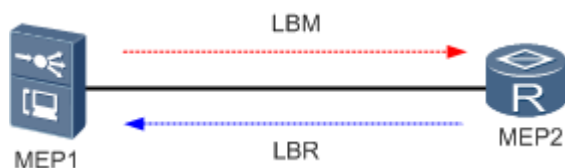
An LBR contains the MAC address of the remote MEP (RMEP) sending this LBR; therefore, multicast LB can also be used to obtain the MAC address of an RMEP.

As defined in the Y.1731, only one multicast LBM can be sent at a time. However, for compatibility with LB defined in the 802.1ag, the system supports a configurable number of multicast LBMs to be sent. An RMEP has a delay in responding to the received LBM. Therefore, an MEP may receive disordered LBRs in response to multiple LBMs it sends. That is, the serial numbers (SNs) of LBRs returned by an RMEP may not be consecutive. Therefore, it is recommended that the number of LBMs that can be sent at a time be set to 1 before multicast LB is performed.

Bidirectional diagnostics test

Bidirectional diagnostics test is used to check the packet loss rate and bit error rate of a bandwidth-specific bidirectional link between two MEPs to determine whether the bandwidth meets user requirements.

Figure 5-15 illustrates the principle of bidirectional diagnostics test.

Figure 5-15 Bidirectional diagnostics test principle

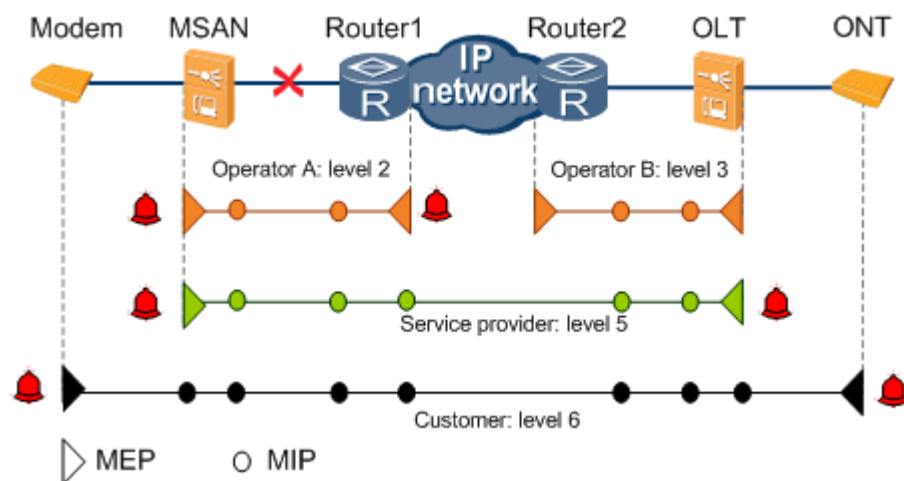
In bidirectional diagnostics test, an LBM and an LBR both carry a testing code, which is used for pseudo random binary sequence (PRBS) check. The following describes the process of bidirectional diagnostics test:

1. MEP1 sends a unicast LBM to MEP2.
2. MEP2 modifies the received LBM to an LBR and returns it to MEP1.
3. MEP1 analyzes the received LBR and determines whether packet loss and bit errors occur over the bidirectional link between MEP1 and MEP2.

5.3.4.4.4 AIS Principles

Alarm indication signal (AIS) is a dedicated function of Y.1731 and is not supported by 802.1ag. AIS is used to send link fault notifications to the client. AIS also suppresses redundant alarms.

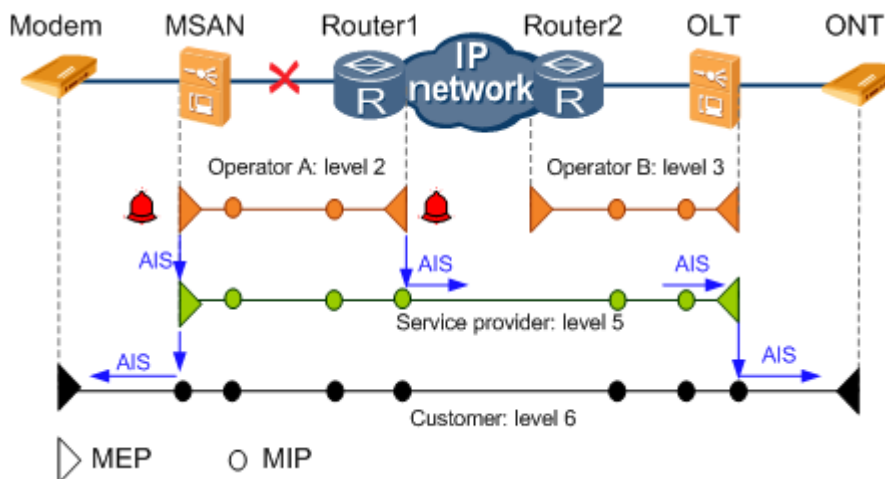
As shown in [Figure 5-16](#), when lower-level services encounter continuity check (CC) faults, maintenance association end points (MEPs) at each level detect CC faults through ETH CC and report fault alarms. Alarms generated in this scenario are mostly redundant alarms. Actually, the OAM engineer can locate the section of the link where the fault has occurred according to the alarm reported by the lowest-level MEP. For example, if the network of Operator A encounters a fault, the fault can be identified within this network, and there is no need to locate the fault in maintenance domains (MDs) owned by the service provider and customer.

Figure 5-16 Before AIS Is Enabled

Alarm suppression can be performed through AIS. Specifically, after a lower-level MEP detects a CC fault, this MEP periodically sends AIS packets to the client MEP level in the reverse direction. After receiving these AIS packets, the client-level

MEP no longer reports an alarm when detecting a CC fault. For example, MDs owned by the service provider and customer do not report any alarms.

Figure 5-17 After AIS Is Enabled



Fault types triggering AIS alarms include connection loss, crossed connection, errored MEP ID, errored period, and MAC status fault.

5.3.4.4.5 LLF Principles

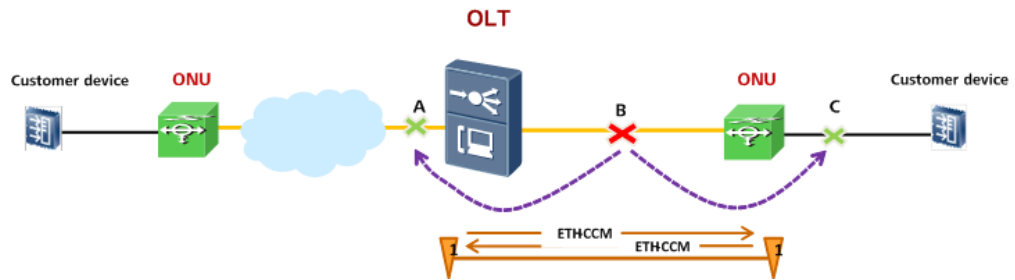
Link loss forwarding (LLF) is a Huawei-defined Ethernet OAM function. It transmits fault information about Ethernet links according to message types defined in the 802.1ag protocol.

Usually, LLF is used in open access networks for national broadband programs. In fiber to the office (FTTO) scenarios, retail service providers (RSPs) set up networks of their own and rent access pipelines and device ports from operators. If pipelines rent to RSPs encounter faults, LLF can be used to notify RSPs and the RSPs' affected enterprise users so that they can know about the faults and take corresponding measures more responsively.

LLF sends the interface status TLV (defined in 802.1ag) carried in the continuity check messages (CCMs) to the peer maintenance end point (MEP). Then, the peer MEP judges whether to generate a fault alarm or fault clear alarm according to the received interface status TLV.

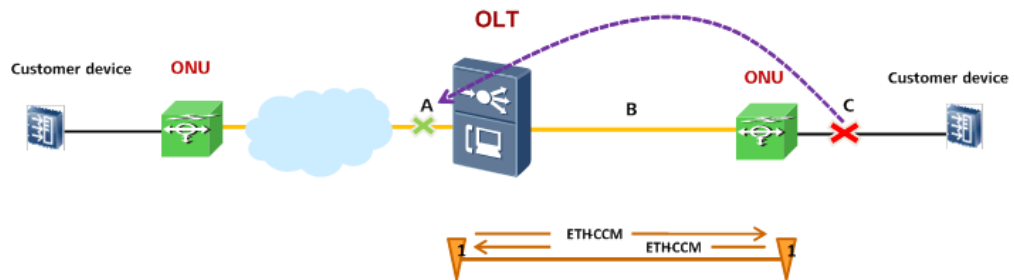
1. Maintenance scenario 1: The network is disconnected and the network-side port and user-side port are disabled. The network continuity is checked using the continuity check (CC) function of the MEP. Specifically, if the MEP on port A or port C detects a CC failure, port A or port C will be disabled; if the MEP on port A or port C detects a CC failure recovery, port A or port C will be enabled. [Figure 5-18](#) shows this scenario.

Figure 5-18 Disabling the network-side port and user-side port when the network is disconnected



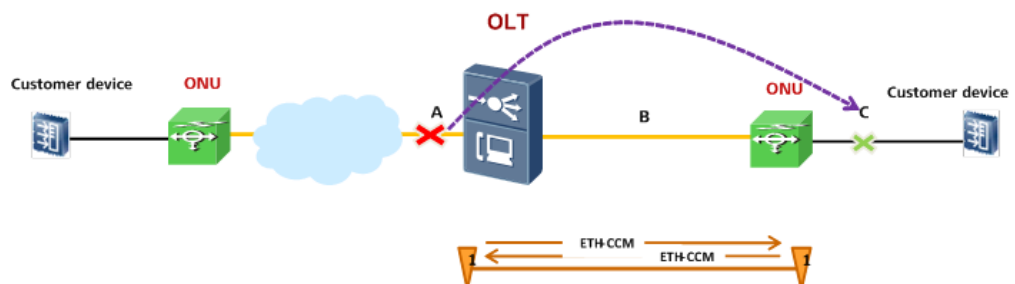
- Maintenance scenario 2: The user-side port is disconnected and the corresponding network-side port is disabled. Specifically, when the user-side port C is disconnected, interface status TLV carried in the CCM is used to indicate whether the local port is faulty. If the MEP on port A receives a CCM carrying interface status TLV 2, the MEP will be notified that the user-side port C is faulty and will disable port A; if the MEP on port A receives a CCM carrying interface status TLV 1, the MEP will be notified that the user-side port C has recovered and will enable port A. [Figure 5-19](#) shows this scenario.

Figure 5-19 Disabling the corresponding network-side port when the user-side port is disconnected



- Maintenance scenario 3: The network-side port is disconnected and the corresponding user-side port is disabled. Specifically, when the network-side port A is disconnected, interface status TLV carried in the CCM is used to indicate whether the local port is faulty. If the MEP on port C receives a CCM carrying interface status TLV 2, the MEP will be notified that the network-side port A is faulty and will disable port C; if the MEP on port C receives a CCM carrying interface status TLV 1, the MEP will be notified that the network-side port A has recovered and will enable port C. [Figure 5-20](#) shows this scenario.

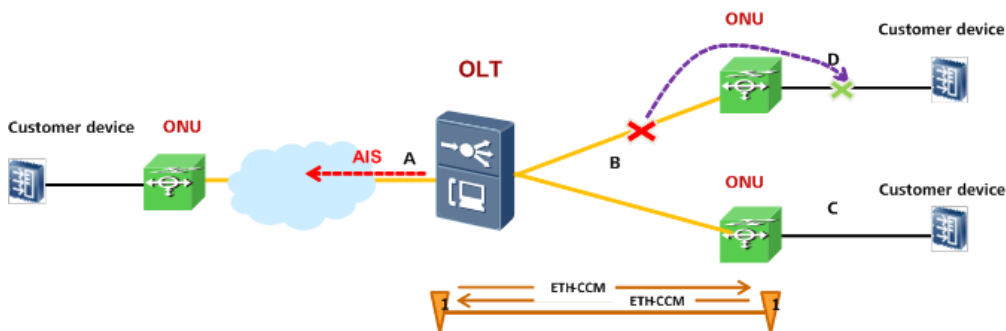
Figure 5-20 Disabling the corresponding user-side port when the network-side port is disconnected



- Maintenance scenario 4: In the aggregation scenario, the network is disconnected and the alarm indication signal (AIS) is sent. Specifically, in the

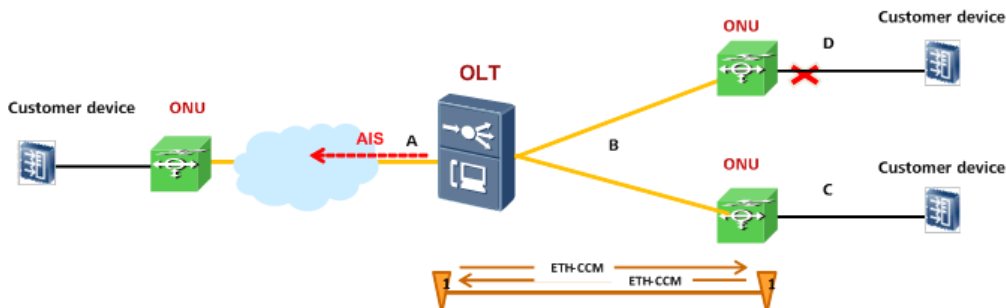
aggregation scenario, when services of a user in the network are interrupted, the network-side port cannot be disabled because services of the other users are still normal. In this case, the OLT sends the AIS to the normal ONU to notify a link abnormality. If link B is disconnected, the MEP on port A detects a failure and notifies the ONU of this failure; if the MEP on port D detects a CC failure, port D is disabled. After the fault is rectified, if the MEP on port D detects a CC failure recovery, port D will be enabled; if the MEP on port A detects a CC failure recovery, it stops sending AISs. [Figure 5-21](#) shows this scenario.

Figure 5-21 Sending AISs when the network is disconnected in the aggregation scenario



- Maintenance scenario 5: In the aggregation scenario, the user-side port is disconnected and the AIS is sent. Specifically, in the aggregation scenario, when the user-side link is disconnected, the network-side port cannot be disabled because the other user-side links are still normal. In this case, the AIS is sent to notify the ONU of a link abnormality. When user-side port D is disconnected, interface status TLV carried in the CCM is used to indicate whether the local port is faulty. If the MEP on port A receives a CCM carrying interface status TLV 2, the MEP will be notified that the user-side port D is faulty and will send the AIS to notify the ONU of a failure; if the MEP on port A receives a CCM carrying interface status TLV 1, the MEP will be notified that the user-side port D has recovered and will stop sending the AIS. [Figure 5-22](#) shows this scenario.

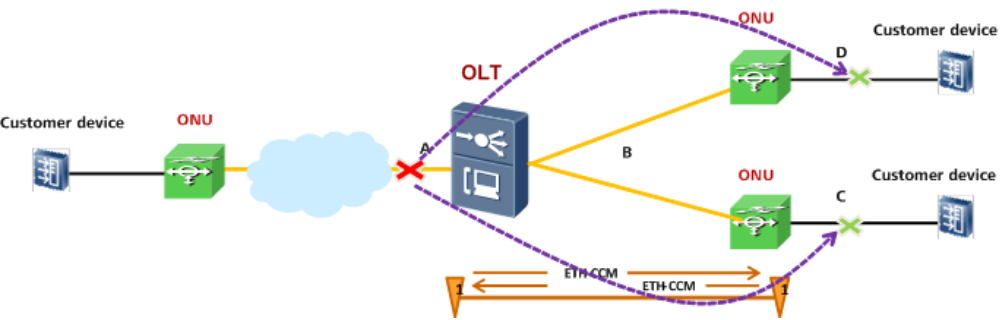
Figure 5-22 Sending AISs when the user-side port is disconnected in the aggregation scenario



- Maintenance scenario 6: In the aggregation scenario, the network-side port is disconnected and all the user-side ports are disabled. Specifically, in the aggregation scenario, when the network-side port A is disconnected, interface status TLV carried in the CCM is used to indicate whether the local port is faulty. If the MEP on port C or port D receives a CCM carrying interface status

TLV 2, the MEP will be notified that the port C or port D is faulty and will disable port C or port D; If the MEP on port C or port D receives a CCM carrying interface status TLV 1, the MEP will be notified that port C or port D has recovered and will enable port C or port D. **Figure 5-23** shows this scenario.

Figure 5-23 Disabling all the user-side ports when the network-side port is disconnected in the aggregation scenario



The preceding scenarios which are achieved under the guideline of the following LLF principles:

- 1. The local MEP adds interface status TLV to the CCM according to the port link status and then sends the CCM.
- 2. The peer MEP determines to generate or not to generate a someMACstatusDefect alarm according to the interface status TLV carried in the CCM.

The someMACstatusDefect alarm is generated by complying with the 802.1ag protocol. Specifically, when the port on a remote MEP is not UP, the MEP generates the someMACstatusDefect alarm. Alternatively, when none of the ports on the remote MEPs are in the forwarding state, the MEPs generate the someMACstatusDefect alarm.

Defect		Priority	
Variable	highestDefect (20.33.9)	highestDefectPri (20.33.8)	Importance
xconCCMdefect (20.23.3)	DefXconCCM	5	Most
errorCCMdefect (20.21.3)	DefErrorCCM	4	
someRMEPCCMdefect (20.33.5)	DefRemoteCCM	3	
someMACstatusDefect (20.33.6)	DefMACstatus	2	Least
someRDIddefect (20.33.7)	DefRDICCM	1	

- 3. When an MEP detects a CC alarm that has a higher severity than the associated alarm severity, the port connected to the MEP is automatically shut down. When the alarm is cleared, the port status recovers. A port can also be

shut down through the CLI. Therefore, before performing configuration, know the relationships between the associated port shutdown function and the CLI-configured port shutdown function, as listed in the following table.

Associated Status	CLI-configured Status	Final Status
Shutdown	Shutdown	Shutdown
Shutdown	Undo shutdown	Shutdown
Undo shutdown	Shutdown	Shutdown
Undo shutdown	Undo shutdown	Undo shutdown
Associated port shutdown function disabled	Shutdown	Shutdown
Associated port shutdown function disabled	Undo shutdown	Undo shutdown

NOTE

Triggering the associated port shutdown function means to associate the MEP CC alarm status with the activation status of the port where the MEP resides. In other words, the port is automatically disabled or enabled according to the CC status. When association is enabled, the lowest CC alarm severity (2 by default) needs to be configured. Association is triggered when the severity of the CC alarm generated by the MEP is higher than or equal to the configured association alarm severity. When association is disabled, the port status is irrelevant to the CC status.

5.3.4.5 Configuring the Ethernet CFM OAM

CFM OAM is an OAM at the network level. It supports connectivity check, loopback testing and link tracking, and applies to the end-to-end fault detection in large-scale network.

Prerequisites

- ONT or Modem must support the 802.1ag protocol.
- Service configurations (VLAN configuration and service port configuration, for example) are finished, and the customer services are normal.

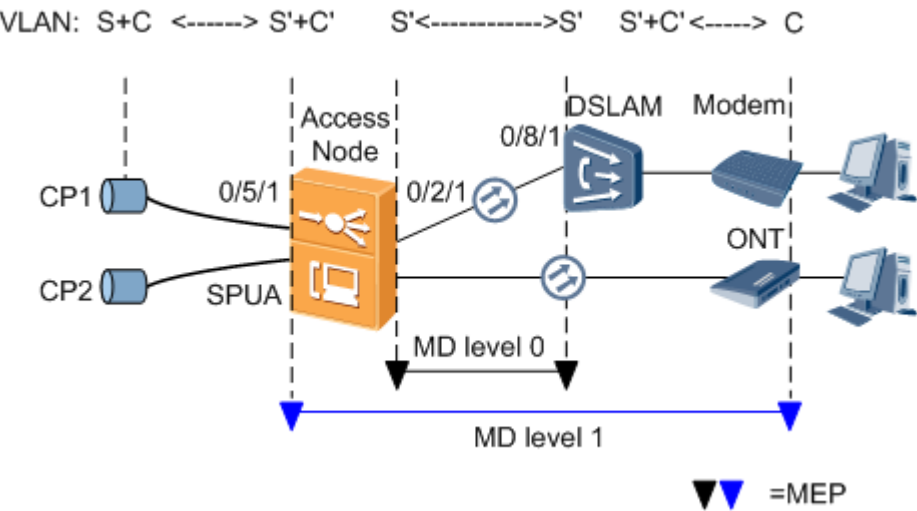
Networking

Figure 5-24 shows a typical FTTx integrated networking. Through the deployment of CFM OAM, service providers can detect connectivity between any two devices based on their needs. When there is a connectivity problem, the system generates an alarm reporting the fault location. Assume that the access node is an OLT.

- The OLT cascades to the DSLAM through a cascade board. An MD is deployed for the management channel between the cascading port (0/2/1) of OLT and the upstream port (0/8/1) of DSLAM.

- The OLT is connected to the ONT through a PON board. An MD is deployed for the service channel between the upstream port (0/5/1) of OLT and the user port of ONT (or modem). The MD has a higher level than that of the previous MD.
- The DSLAM connects to the DSL modem to provide various services to users.

Figure 5-24 Typical networking of CFM OAM



Data Plan

Table 5-5 shows the key data plan for deploying the MD for management channel between cascading port on OLT and upstream port on DSLAM.

Table 5-5 Data plan for the Ethernet CFM OAM - MD level 0

Item	Data
OLT	• MD ID: 0. MD name: fttc_md0 • MD level: 0 • MA ID: 0. MA name: fttc_ma0 • MA VLAN: 100 (Management VLAN for the OLT) • MEP ID: 1. MEP port: 0/2/1 • MEP VLAN tag: 8 (Management VLAN for the DSLAM). MEP direction: Down • Remote MEP ID: 2 • CC-interval: 10 minutes

Item	Data
DSLAM	• MD ID: 0. MD name: fttc_md0 • MD level: 0 • MA ID: 0. MA name: fttc_ma0 • MA VLAN: 8 (Management VLAN for the DSLAM) • MEP ID: 2. MEP port: 0/8/1 • MEP direction: Down • Remote MEP ID: 1 • CC-interval: 10 minutes

Table 5-6 shows the key data plan for deploying another MD for service channel between upstream port on OLT and UNI port of ONT (or modem).

Table 5-6 Data plan for the Ethernet CFM OAM - MD level 1

Item	Data
OLT	• MD ID: 1; MD name: fttc_md1 • MD level: 1 • MA ID: 1; MA name: fttc_ma1 • MA VLAN: 10 • MEP ID: 1; MEP port: 0/5/1 • MEP VLAN tag1: 10 (VLAN for Internet access services on the upstream port of the upstream board) • MEP direction: Up • Remote MEP ID: 2 • CC-interval: 10 minutes • MAC address: 00e0-fc00-0001
UNI interface of the ONT (or Modem)	• MD ID: 1; MD name: fttc_md1 • MD level: 1 • MA ID: 1; MA name: fttc_ma1 • MA VLAN: 10 • MEP ID: 2; MEP port: 0/1/0 • ONT ID: 0; Ethernet port: 2 • MEP VLAN tag1: 10 • MEP direction: Up • Remote MEP ID: 1 • CC-interval: 10 minutes

Procedure

- Configure the MD for management channel on the OLT (MD index 0 and MD level 0).

Pay attention to the following:

- The MD name and MA name configured on OLT must be the same as that of on DSLAM.
- Local MEP on OLT corresponds to the remote MEP on the DSLAM, and remote MEP on OLT corresponds to the local MEP on the DSLAM.

a. Configure the MD.

Configure MD 0 with name `fttc_md0` (character string type), and MD level 0.

- MDs with the same index or level cannot be created.
- The name type and the name of an MD must be unique.
- The total length of the names of an MD and its MAs cannot be longer than 44 characters.
- The MD name type, the MD name and the MD level must be consistent at both ends.

```
huawei(config)#cfm md 0 name-format string fttc_md0 level 0 mhf-creation no-mhf
```

b. Configure the MA.

- The system supports up to 4096 MAs. That is, if an MD is configured with 4096 MAs, the other MDs in the system cannot be configured with any MA.
- An MD must be available for creating an MA.
- An existing MA cannot be created again.
- The total length of the names of an MD and its MAs cannot be longer than 44 characters.
- The MA name type, the MA name and the sending period of CC packets must be consistent at both ends.

Create an MA with the index 0/0. The name is `fttc_ma0` (character string type). The sending period of CC packets is 10 minutes (the sending period of CC packets is 1 minute by default).

```
huawei(config)#cfm ma 0/0 name-format string fttc_ma0 cc-interval 10m
```

Set the VLAN associated to the MA to 100, it is the management VLAN of the OLT.

```
huawei(config)#cfm ma 0/0 vlan 100
```

Set the ID of MEP contained by the MA to 1 and 2. The number of local MEPs and remote MEPs supported by an MA depends on the type of the service board. Furthermore, all these MEP IDs must be unique. MEP ID 2 needs to be configured on the peer DSLAM.

```
huawei(config)#cfm ma 0/0 meplist 1 //local end MEP
```

```
huawei(config)#cfm ma 0/0 meplist 2 //remote end MEP on the DSLAM
```

c. Configure the MEP.

- MEP refers to a maintenance association end points. Ethernet CFM OAM is used to test the link connectivity by using the MEPs at the two ends of a maintenance channel.
- By default, the MEP management function is enabled, the priority of sending CFM packets is 7, and the function of sending CC packets is enabled.
- There are two kinds of MEPs: UP MEP and DOWN MEP. An UP MEP indicates that the MEP transmits packets to the bridge trunk direction. A DOWN MEP indicates that the MEP transmits packets to the physical medium direction.
- **vlantag1** or **vlantag2** must be configured, when you add an MEP is added for a port with service streams. **vlantag1** is the outer VLAN of the port carrying the service link for the MEP. **vlantag2** is the inner VLAN of the port carrying the service link for the MEP.
- The MEP priority must be consistent at both ends.

```
huawei(config)#cfm mep 0/0/1 direction down port 0/2/1 vlantag1 8 priority 7
```

d. Enable the remote MEP detection function.

The system can check the remote MEPs of an MA and report alarms for loss of CCM and RDI only when the following functions are enabled: the global CFM function, the global function of checking remote MEPs, and the function of checking the remote MEPs of the MA.

By default, the remote MEP detection function of the MA is enabled, while the global remote MEP detection function is disabled.

i. Enable the remote MEP detection function of the MA.

```
huawei(config)#cfm ma 0/0 remote-mep-detect enable
```

ii. Enable the continuity check function of the MEP.

```
huawei(config)#cfm mep 0/0/1 cc enable
```

iii. Enable the global remote MEP detection function.

```
huawei(config)#cfm remote-mep-detect enable
```

e. Enable the global CFM function.

```
huawei(config)#cfm enable
```

- Configure the MD for management channel on the DSLAM (MD index 0 and MD level 0).

a. Configure the MD.

```
huawei(config)#cfm md 0 name-format string ftc_md0 level 0 mhfc-creation no-mhf
```

b. Configure the MA.

```
huawei(config)#cfm ma 0/0 name-format string ftc_ma0 cc-interval 10m
```

Set the VLAN associated to the MA to 8, it is the management VLAN of the DSLAM.

```
huawei(config)#cfm ma 0/0 vlan 8
```

Set the ID of MEP contained by the MA to 2 and 1. The number of local MEPs and remote MEPs supported by an MA depends on the type of the service board. Furthermore, all these MEP IDs must be unique. MEP ID 1 needs to be configured on the peer OLT.

```
huawei(config)#cfm ma 0/0 meplist 2 //local end MEP on the DSLAM
huawei(config)#cfm ma 0/0 meplist 1 // remote end MEP on the OLT
```

c. Configure the MEP.

```
huawei(config)#cfm mep 0/0/2 direction down port 0/8/1 vlantag1 8 priority 7
```

d. Enable the remote MEP detection function.

i. Enable the remote MEP detection function of the MA.

```
huawei(config)#cfm ma 0/0 remote-mep-detect enable
```

ii. Enable the continuity check function of the MEP.

```
huawei(config)#cfm mep 0/0/2 cc enable
```

iii. Enable the global remote MEP detection function.

```
huawei(config)#cfm remote-mep-detect enable
```

e. Enable the global CFM function.

```
huawei(config)#cfm enable
```

- Configure the MD for service channel on the OLT (MD ID 1 and MD level 1).

a. Configure the MD.

Configure MD 1 with name fttc_md1 (character string type), and MD level 1.

```
huawei(config)#cfm md 1 name-format string fttc_md1 level 1 mhf-creation no-mhf
```

b. Configure the MA.

Create an MA with the index 1/1. The name is fttc_ma1 (character string type). The sending period of CC packets is 10 minutes (the sending period of CC packets is 1 minute by default).

```
huawei(config)#cfm ma 1/1 name-format string fttc_ma1 cc-interval 10m
```

Set the VLAN associated to the MA to 10, it is the service VLAN of the OLT.

```
huawei(config)#cfm ma 1/1 vlan 10
```

Set the ID of MEP contained by the MA to 1 and 2. The number of local MEPs and remote MEPs supported by an MA depends on the type of the service board. Furthermore, all these MEP IDs must be unique. MEP ID 2 needs to be configured on the peer device.

```
huawei(config)#cfm ma 1/1 meplist 1 //local end MEP
```

```
huawei(config)#cfm ma 1/1 meplist 2 //remote end MEP on the ONT (or Modem)
```

c. Configure the MEP.

Configure the MEP (direction: up) on a specified port of the upstream board. This port is connected to the user port (SVLAN: 10) of an ONT or modem. If the MEP alarm priority is higher than 1, alarms are reported.

```
huawei(config)#cfm mep 1/1/1 direction up port 0/5/1 vlantag1 10 lowest-alarm-pri 1
```

d. Enable the remote MEP detection function.

The system can check the remote MEPs of an MA and report alarms for loss of CCM and RDI only when the following functions are enabled: the global CFM function, the global function of checking remote MEPs, and the function of checking the remote MEPs of the MA.

By default, the remote MEP detection function of the MA is enabled, while the global remote MEP detection function is disabled.

- i. Enable the global CFM function.
`huawei(config)#cfm enable`
 - ii. Enable the remote MEP detection function of the MA.
`huawei(config)#cfm ma 1/1 remote-mep-detect enable`
 - iii. Enable the continuity check function of the MEP.
`huawei(config)#cfm mep 1/1/1 cc enable`
 - iv. Enable the global remote MEP detection function.
`huawei(config)#cfm remote-mep-detect enable`
- e. Configure the alarm indication signal (AIS) function. (Optional.)
 - i. Set the client level of MA 1/1 to 2.
`huawei(config)#cfm ma 1/1 client-level 2`
 - ii. Enable AIS transmission on MEP 1/1/1.
`huawei(config)#cfm mep 1/1/1 ais enable`
 - iii. Set the interval at which AIS packets of MA 1/1 are sent to 1 minute.
`huawei(config)#cfm ma 1/1 ais-interval 1m`
- f. Configure the link loss forwarding (LLF) function. (Optional.)

Set CC alarm severity to 3 at which port status association of MEP 1/1/1 is triggered.

`huawei(config)#cfm mep 1/1/1 trigger if-down 3`
- Configure the MD for service channel on the ONT (MD ID 1 and MD level 1). ETHOAM CFM configurations of the ONT are completed on the OLT by running commands and are issued to the ONT through the optical network terminal management and control interface (OMCI).
 - a. Enter the ONT ETHOAM mode.
`huawei(config)#ont-ethoam`
 - b. Configure the MD.

Configure MD 1 with name `fttc_md1` (character string type), and MD level 1.

`huawei(config-ont-ethoam)#cfm md 1 name-format string fttc_md1 level 1`
 - c. Configure the MA.

Create an MA with the index 1/1. The name is `fttc_ma1` (character string type). The sending period of CC packets is 10 minutes (the sending period of CC packets is 1 minute by default). Set the client level of the MA to 2.

`huawei(config-ont-ethoam)#cfm ma 1/1 name-format string fttc_ma1 cc-interval 10m`
`huawei(config-ont-ethoam)#cfm ma 1/1 client-level 2`
 - d. Configure the MEP.

Configure the MEP (direction: up) on a specified port of the upstream board. This port is connected to the user port (SVLAN: 10) of an ONT or modem.

`huawei(config-ont-ethoam)#cfm mep 1/1/2 0/1/0 0 eth 2 direction up vlan 10 remote-mep 1`
 - e. Enable the remote MEP detection function.

The system can check the remote MEPs of an MA and report alarms for loss of CCM and RDI only when the following functions are enabled: the global CFM function, the global function of checking remote MEPs, and the function of checking the remote MEPs of the MA.

By default, the remote MEP detection function of the MA is enabled, while the global remote MEP detection function is disabled.

- i. Enable the global CFM function.
huawei(config-ont-ethoam)#**cfm 0/1/0 0 enable**
 - ii. Enable the remote MEP detection function of the MA.
huawei(config-ont-ethoam)#**cfm ma 1/1 remote-mep-detect enable**
 - iii. Enable the continuity check function of the MEP.
huawei(config-ont-ethoam)#**cfm mep 1/1/2 cc enable**
 - iv. Enable AIS transmission on the MEP.
huawei(config-ont-ethoam)#**cfm mep 1/1/2 ais enable**
 - v. Enable the remote MEP detection function of the ONT.
huawei(config-ont-ethoam)#**cfm 0/1/0 0 remote-mep-detect enable**
- f. Configure the link LLF function. (Optional)
- Set CC alarm severity to 3 at which port status association of MEP 1/1/2 is triggered.
- ```
huawei(config-ont-ethoam)# cfm mep 1/1/2 trigger if-down 3
```
- g. Configure the LB function. (Optional)
- Enable the LB test for MEP 1/1/2, set the MAC address of the remote MEP (OLT) to 00e0-fc00-0001, and send 5 LBM packets (data length: 20; priority: 6) at an interval of 1s.
- ```
huawei(config-ont-ethoam)#cfm loopback mep 1/1/2 dst-mac-address 00e0-fc00-0001 interval 1 count 5 data-length 20 priority 6
```
- h. Configure the LT function. (Optional)
- Configure the LT function on the link between MEP 1/1/2 and remote destination MEP 1 (OLT).
- ```
huawei(config-ont-ethoam)#cfm link-trace mep 1/1/2 mepid 1
```

----End

## Result

After the configuration is finished,

- OLT or DSLAM is able to learn the MEP ID and MAC address from its remote peer automatically. You can run the **display cfm mep** command to query MEP configuration.
- On the OLT or DSLAM, run the **display cfm mep** command to query the MEP configurations of a specified ONT in the ONT-ETHOAM mode.
- Disconnect OLT and DSLAM, the system will generate CFM OAM alarm automatically, reporting the fault location and cause.
- Run the **cfm loopback** command on the OLT to start a remote loopback test. Under normal circumstances, the number of packets sent and received must be the same.

## Configuration File

Configure the MD for management channel on the OLT (MD index 0 and MD level 0).

```
cfm md 0 name-format string fttc_md0 level 0 mhf-creation no-mhf
cfm ma 0/0 name-format string fttc_ma0 cc-interval 10m
```

```
cfm ma 0/0 vlan 100
cfm ma 0/0 meplist 1 //local end MEP
cfm ma 0/0 meplist 2 //remote end MEP on the DSLAM
cfm mep 0/0/1 direction down port 0/2/1 vlantag1 8 priority 7
cfm ma 0/0 remote-mep-detect enable
cfm mep 0/0/1 cc enable
cfm remote-mep-detect enable
cfm enable
```

Configure the MD for management channel on the DSLAM (MD index 0 and MD level 0).

```
cfm md 0 name-format string fttc_md0 level 0 mhf-creation no-mhf
cfm ma 0/0 name-format string fttc_ma0 cc-interval 10m
cfm ma 0/0 vlan 8
cfm ma 0/0 meplist 2 //local end MEP
cfm ma 0/0 meplist 1 //remote end MEP on the OLT
cfm mep 0/0/2 direction down port 0/8/1 vlantag1 8 priority 7
cfm ma 0/0 remote-mep-detect enable
cfm mep 0/0/2 cc enable
cfm remote-mep-detect enable
cfm enable
```

Configure the MD for service channel on the OLT (MD ID 1 and MD level 1).

```
cfm md 1 name-format string fttc_md1 level 1 mhf-creation no-mhf
cfm ma 1/1 name-format string fttc_ma1 cc-interval 10m
cfm ma 1/1 vlan 10
cfm ma 1/1 meplist 1 //Indicates the local MEP.
cfm ma 1/1 meplist 2 //Indicates the remote MEP on the DSLAM.
cfm mep 1/1/1 direction up port 0/5/1 vlantag1 10 lowest-alarm-pri 1
cfm enable
cfm ma 1/1 remote-mep-detect enable
cfm mep 1/1/1 cc enable
cfm remote-mep-detect enable
cfm ma 1/1 client-level 2
cfm mep 1/1/1 ais enable
cfm ma 1/1 ais-interval 1m
cfm mep 1/1/1 trigger if-down 3
```

Configure the MD for service channel on the ONT (MD ID 1 and MD level 1).

```
ont-ethoam
cfm md 1 name-format string fttc_md1 level 1
cfm ma 1/1 name-format string fttc_ma1 cc-interval 10m
cfm ma 1/1 client-level 2
cfm mep 1/1/2 0/1/0 0 eth 2 direction up vlan 10 remote-mep 1
cfm 0/1/0 0 enable
cfm ma 1/1 remote-mep-detect enable
cfm mep 1/1/2 cc enable
cfm mep 1/1/2 ais enable
cfm 0/1/0 0 remote-mep-detect enable
cfm mep 1/1/2 trigger if-down 3
cfm loopback mep 1/1/2 dst-mac-address 00e0-fc00-0001 interval 1 count 5 data-length 20 priority 6
cfm link-trace mep 1/1/2 mepid 1
```

### 5.3.5 EFM (802.3ah)

EFM is defined in the IEEE 802.3ah (802.3ah for short). It is an OAM feature for detecting quality and connectivity of last-mile Ethernet links.

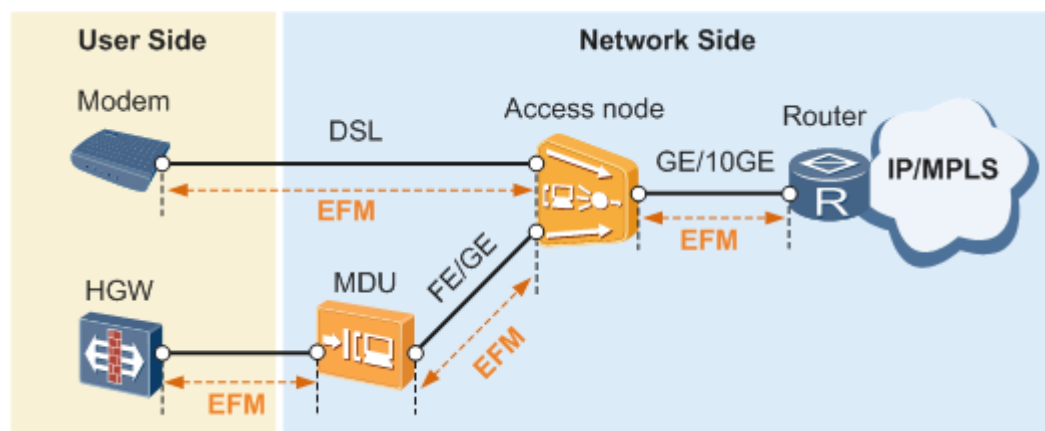
#### 5.3.5.1 EFM Introduction

As an OAM mechanism, EFM monitors the link status, quickly locates a faulty link, and identifies the fault type in real time for carriers.

Among Ethernet applications, high-end users, such as banks and financial companies, demand high reliability. They expect carriers to monitor both carrier networks and last-mile links that connect users to those carrier networks. However, this is a difficulty for carriers because user devices are out of control of carriers.

Ethernet in the First Mile (EFM) can be used to satisfy these demands. As an OAM mechanism, EFM monitors the link status, quickly locates a faulty link, and identifies the fault type in real time for carriers. EFM mainly applies to the user access network and also to the Ethernet physical link that directly connects two devices. The following example illustrates EFM implementation on the network shown in [Figure 5-25](#).

**Figure 5-25** Typical EFM network



The router and access node are placed in the CO, MDU is in the corridor or curb, modem and home gateway (HGW) are in users' home. By deploying EFM between the devices shown in [Figure 5-25](#), network maintenance engineers can remotely check connectivity and quality of links between these devices.

[Table 5-7](#) lists the main functions of EFM supported by access device.

**Table 5-7** Main functions of EFM

| Function                                  | Purpose                                                                                                                                                                                               |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">OAM discovery</a>             | Negotiates EFM capabilities of the connected two ends and obtains the EFM status of the remote end.                                                                                                   |
| <a href="#">Remote failure indication</a> | Sends a remote failure indication to the remote end when traffic is interrupted because the device is faulty or is invalid to monitor the link connectivity.                                          |
| <a href="#">Remote loopback</a>           | Loops back the packets sent to the remote end to the local end and tests the link by comparing the received and transmitted packets to obtain the link performance data (including packet loss rate). |
| <a href="#">Link monitoring</a>           | Monitor the link quality by sending a link deterioration event to the network maintenance engineer.                                                                                                   |

### 5.3.5.2 EFM Basic Concept

Basic concepts of EFM, such as DTE and OAMPDU.

The following concepts are used a lot in the [Principle of EFM](#). If you are not familiar with EFM, it is recommended to have a rough understanding of these basic concepts.

#### DTE

The data terminating entity (DTE) is the basic object on which EFM feature takes effect. A DTE is associated with a port.

- If the port is on the local device, it is a local DTE.
- If the port is on the remote device, it is a remote DTE.

#### OAMPDUs

EFM works at the data link layer and uses protocol packets called OAM Protocol Data Units (PDUs). EFM DTEs periodically exchange OAMPDUs to report link status, helping network administrators effectively manage networks. [Figure 5-26](#) shows the OAMPDU format and common types of OAMPDUs. [Table 5-8](#) lists and describes fields in an OAMPDU.

Figure 5-26 OAMPDU format

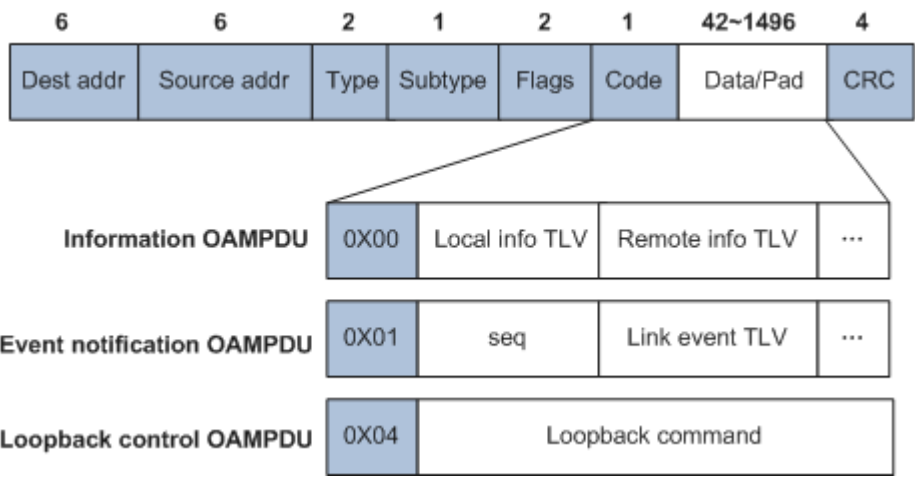


Table 5-8 Fields and descriptions in an OAMPDU

| Field       | Description                                                                                                                                                                                            |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dest addr   | Destination MAC address, which is a slow-protocol multicast address 0x0180-C200-0002. Network bridges cannot forward slow-protocol packets thus EFM OAMPDUs cannot be forwarded over multiple devices. |
| Source addr | Source address, which is a unicast MAC address of a port on the transmit end. If no port MAC address is specified on the transmit end, the bridge MAC address of the transmit end is used.             |

| Field   | Description                                                                                                                                                                                                                        |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type    | Slow protocol type, which has a fixed value of 0x8809.                                                                                                                                                                             |
| Subtype | Subtype of a slow protocol. The value is 0x03, which means that the slow sub-protocol is EFM.                                                                                                                                      |
| Flags   | Status of a DTE: <ul style="list-style-type: none"><li>• Remote Stable</li><li>• Remote Evaluating</li><li>• Local Stable</li><li>• Local Evaluating</li><li>• Critical Event</li><li>• Dying Gasp</li><li>• Link Fault</li></ul>  |
| Code    | OAMPDU type: <ul style="list-style-type: none"><li>• 0X00: Information OAMPDU</li><li>• 0X01: Event Notification OAMPDU</li><li>• 0X04: Loopback Control OAMPDU</li></ul> <a href="#">Table 5-9</a> lists common types of OAMPDUs. |

**Table 5-9** OAMPDU types

| OAMPDU Type               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Information OAMPDU        | <ul style="list-style-type: none"><li>• Used to discover a remote DTE, initiate a handshake process, and establish an EFM connection. After the EFM connection is established, both EFM DTEs periodically exchange Information OAMPDUs to monitor link connectivity.</li><li>• Used to advertise fault information. If the local DTE detects a fault, an event is generated on the local device and an Information OAMPDU is sent to the remote DTE. When the remote DTE receives the Information OAMPDU, an event is generated on the remote device.</li></ul> |
| Event Notification OAMPDU | Used to monitor links. If a local DTE detects an errored frame event, errored symbol period event, or errored frame second summary event, an event is generated on the local device and an Event Notification OAMPDU is sent to the remote DTE. When the remote DTE receives the Event Notification OAMPDU, an event is generated on the remote device.                                                                                                                                                                                                         |
| Loopback Control OAMPDU   | Used to enable or disable the remote loopback function.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Modes

EFM supports two modes: active and passive. [Table 5-10](#) lists capabilities for processing OAMPDUs in the two modes.

**Table 5-10** Capabilities for processing OAMPDUs in active and passive modes

| Capability                                                                                  | Active Mode                                          | Passive Mode  |
|---------------------------------------------------------------------------------------------|------------------------------------------------------|---------------|
| Initiate a connection request by sending an Information OAMPDU during the discovery process | Supported                                            | Not supported |
| Respond to a connection request during the discovery process                                | Supported                                            | Supported     |
| Send Information OAMPDUs                                                                    | Supported                                            | Supported     |
| Send Event Notification OAMPDUs                                                             | Supported                                            | Supported     |
| Send Loopback Control OAMPDUs                                                               | Supported                                            | Not supported |
| Respond to Loopback Control OAMPDUs                                                         | Supported (The remote DTE must work in active mode.) | Supported     |

 **NOTE**

- Two DTEs on both ends of an EFM link work in active mode by default.
- An EFM connection can only be initiated by a DTE working in active mode. A DTE working in passive mode waits to receive a connection request from its remote DTE. Two DTEs both working in passive mode cannot establish an EFM connection between them.
- A loopback request can only be initiated by a DTE working in active mode.

### 5.3.5.3 EFM Principle

EFM functions are defined in section 57 of the IEEE 802.3ah protocol. This topic describes only functions supported by the access device.

 **NOTE**

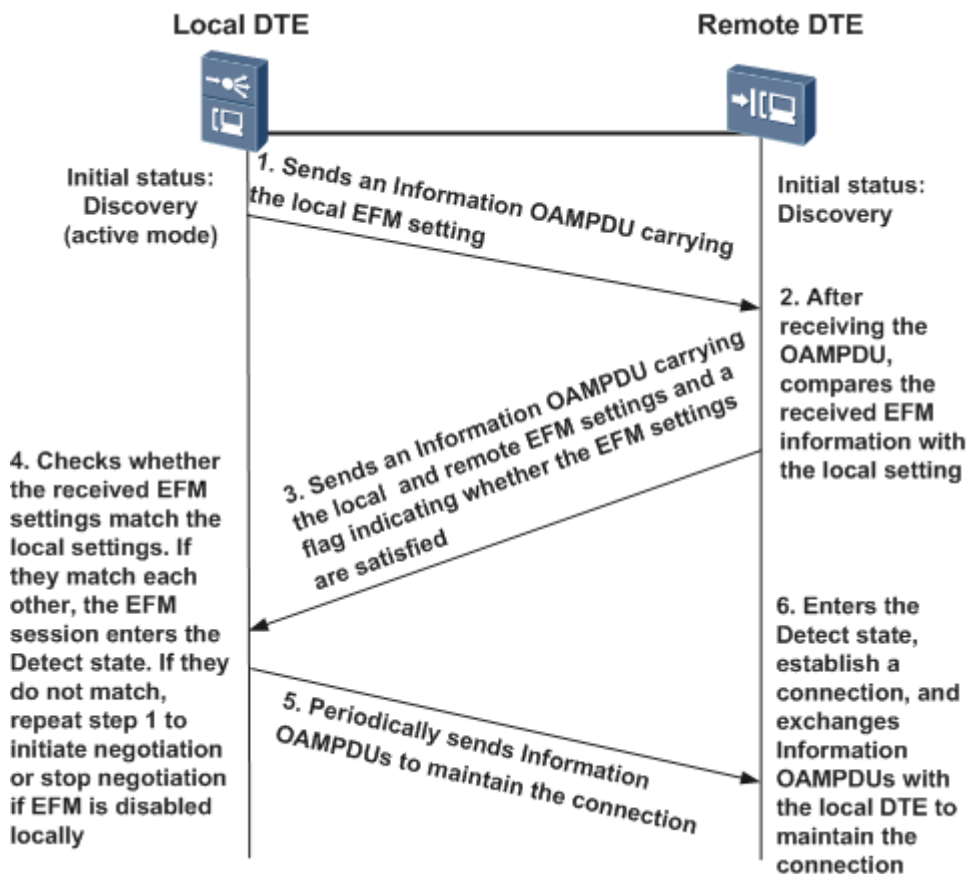
The following principles are for the access device. Different devices support different functions. For details, see "Feature Specifications and Limitations."

## OAM Discovery

After being enabled with EFM, the local DTE initiates the Discovery negotiation. During the Discovery phase, a local DTE discovers and establishes a stable EFM connection with a remote DTE. If both the local and remote DTEs are satisfactory

for EFM functions, the EFM connection is established. [Figure 5-27](#) shows this process.

**Figure 5-27** Schematic diagram for OAM discovery



After the EFM connection is established, DTEs at both ends of an EFM connection periodically exchange Information OAMPDUs to monitor link connectivity. The interval at which Information OAMPDUs are sent is also known as an interval between handshakes. If a DTE does not receive Information OAMPDUs from the remote DTE within the connection timeout period, the DTE considers the connection interrupted and generates an event. Establishing an EFM connection is a way to monitor physical link connectivity automatically.

## Remote Failure Indication

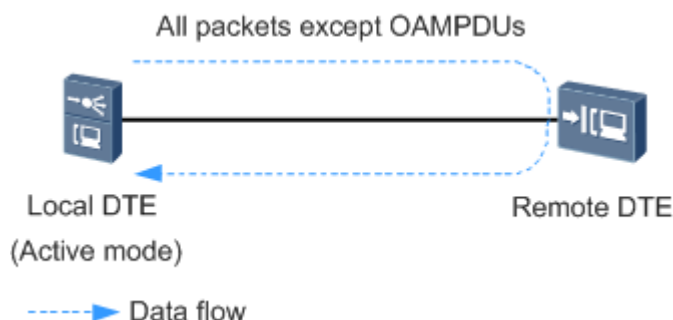
After the OAM discovery phase finishes, two DTEs at both ends of an EFM connection exchange Information OAMPDUs to monitor link connectivity. If traffic is interrupted due to a remote device failure, the remote DTE sends an Information OAMPDU carrying an event listed in [Table 5-11](#) to the local DTE. After receiving the notification, the local DTE generates the Ethernet OAM link event. An administrator can determine link status based on the event and take measures to rectify the fault.

**Table 5-11** Critical link events

| Type           | Description                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------------------|
| Link Fault     | A loss of signal (LoS) error occurs because the interval at which OAMPDUs are sent elapses or a physical link fails. |
| Dying Gasp     | An unexpected status changes or event occurs because a remote device is powered off or a board is reset.             |
| Critical Event | An unidentified critical event occurs.                                                                               |

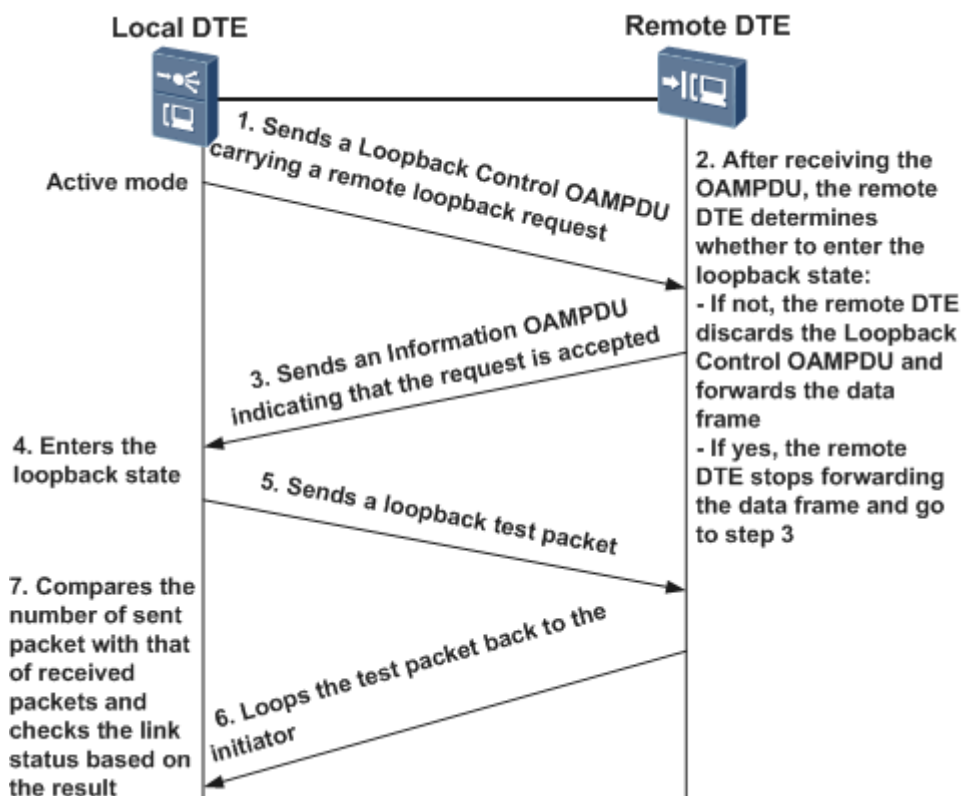
## Remote Loopback

**Figure 5-28** demonstrates the principles of remote loopback. When a local DTE sends non-OAMPDUs to a remote DTE, the remote DTE loops the non-OAMPDUs back to the local DTE, not to the destination addresses of the non-OAMPDUs. This is remote loopback. It helps to obtain the link performance data (including packet loss rate) by comparing the received and transmitted packets.

**Figure 5-28** Principles of EFM remote loopback

To implement remote loopback, an EFM connection must be established first. After remote loopback is enabled, all data frames forwarding except OAMPDUs are stopped and services will be interrupted. This function can be used to detect the link quality before a new network is deployed or after a link fault is rectified to prevent services from being affected.

In remote loopback mode, the local DTE sends testing packets to the remote DTE. The local DTE then computes communication quality parameters, such as the packet loss ratio, of the current link according to the numbers of sent packets and received packets. If the local DTE attempts to stop remote loopback, it sends a message to instruct the remote DTE to disable remote loopback. After receiving the message, the remote DTE disables remote loopback. **Figure 5-29** shows the remote loopback process.

**Figure 5-29** Remote loopback process

## Link Monitoring

Monitoring Ethernet links is difficult if network performance deteriorates while traffic is being transmitted over physical links. To resolve this problem, the EFM link monitoring function can be used. It can detect data link layer faults in various environments. DTEs that are enabled with link monitoring exchange Event Notification OAMPDUs to monitor links.

After monitoring common link events listed in [Table 5-12](#), the DTE at an end sends OAMPDUs carrying corresponding events to the other end and generates Ethernet OAM link events at local. When the other end receives the OAMPDUs, it generates an event. This facilitates real-time network monitoring and effective network management for maintenance engineers.

**Table 5-12** Common link events

| Type                        | Description                                                             | Purpose                                                                         |
|-----------------------------|-------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Errored Symbol Period Event | The number of errored symbols during a period reaches the threshold.    | To detect code errors during data transmission at the physical layer.           |
| Errored Frame Event         | The number of frames during the unit time reaches the preset threshold. | To detect frame errors that occur during data transmission at the MAC sublayer. |

| Type                                | Description                                                                                                                                                                                         | Purpose                                                                                  |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Errored Frame Period Event          | The number of errored frames in the latest N frames reaches the threshold.                                                                                                                          |                                                                                          |
| Errored Frame Seconds Summary Event | <p>The number of errored frames in the latest M seconds reaches the threshold.</p> <p><b>NOTE</b><br/>If an errored frame is generated at a second, this second is called errored frame second.</p> | To detect errored frame seconds that occur during data transmission at the MAC sublayer. |

### 5.3.5.4 EFM Configuration

#### 5.3.5.4.1 Configuring an EFM Remote Loopback

In an Ethernet in the first mile (EFM) remote loopback, all non-OAM protocol data units (PDUs) sent from the local data terminating entity (DTE) to the remote DTE are looped back to the local DTE. The link performance data (such as packet loss rate) can be obtained by comparing the sent and received non-OAM PDUs on the local DTE. This helps to evaluate Ethernet link quality and locate faults.

#### Context

Before the EFM remote loopback starts, the EFM feature must be enabled on the local DTE and the remote DTE. After the EFM feature is enabled, the EFM mode and the response mode of EFM remote loopback cannot be modified on the port. If these two modes need to be modified, disable the EFM feature.

An EFM remote loopback results in service interruption. Therefore, stop the loopback right after the link performance data is collected.

The following describes how to configure an EFM remote loopback by assuming that the local DTE initiates an EFM remote loopback and the remote DTE responds to the EFM remote loopback.

#### Procedure

##### Step 1 Configure the remote DTE.

1. Run the **efm loopback frameid/slotid/portid process** command to set the response mode of EFM remote loopback on a port. By default, the response mode of EFM remote loopback on a network-side port is set to process, while the response mode of EFM remote loopback on a user-side port is set to ignore.

 NOTE

Only a few boards can respond to an EFM remote loopback. For these boards, run the above command to set the response mode to process or ignore, that is, to respond to or ignore the EFM remote loopback initiated by the peer DTE. For boards that cannot respond to an EFM remote loopback, the response mode is defaulted to ignore and cannot be modified.

2. Run the **efm oam frameid/slotid/portid enable** command to enable the EFM feature for the port. By default, the EFM feature is disabled.

**Step 2** Configure the local DTE.

1. Run the **efm oam mode frameid/slotid/portid active** command to set the EFM mode of a port to the default value active.
2. Run the **efm oam frameid/slotid/portid enable** command to enable the EFM feature for the port. By default, the EFM feature is disabled.
3. Run the **efm loopback frameid/slotid/portid start** command to start the EFM remote loopback. By default, the EFM remote loopback stops.

 NOTE

If you want the EFM remote loopback to automatically stop after a period of time, configure the **timeout** parameter to set the loopback timeout period when running the **efm loopback frameid/slotid/portid start** command.

----End

## Result

All packets except OAM PDUs sent from the local DTE to the remote DTE are looped back to the local DTE.

## Example

Assume that Ethernet cascade port 0/2/0 on the OLT is connected to upstream port 0/0/1 on the MDU, Ethernet cascade port on the OLT initiates an EFM remote loopback, and upstream port on the MDU responds to the EFM remote loopback. To configure an EFM remote loopback on the two ports, do as follows:

1. Configure MDU.  
MDU(config)#**efm oam 0/0/1 enable**
2. Configure OLT.  
OLT(config)#**efm oam 0/2/0 enable**  
OLT(config)#**efm loopback 0/2/0 start**

## Follow-up Procedure

After the link performance data is collected, run the **efm loopback frameid/slotid/portid stop** command on the local DTE to stop the EFM remote loopback.

 NOTE

If the timeout period has been set, the EFM remote loopback will automatically stop after the timeout period expires.

### 5.3.5.4.2 Configuring EFM Ethernet Link Monitoring

The Ethernet in the First Mile (EFM) is an operation, administration and maintenance (OAM) feature which provides a real-time link monitoring mechanism. Using this mechanism, events are reported in the case of traffic interruption or link quality degradation so that the network maintenance engineers can monitor Ethernet link quality in real time.

## Context

EFM events can be classified into two types: local EFM events and remote EFM events. Local EFM events are detected by the local DTE; remote EFM events are detected by the remote DTE and sent to the local DTE.

- All remote EFM events will be reported as long as the EFM feature is enabled. There is no command that can be used to configure the event reporting function for the remote EFM events.
- For some local EFM events, you need to enable the event reporting function so that the local EFM events can be reported. As listed in the [Table 5-13](#), the local DTE reports the related EFM events and notifies the remote DTE only when the EFM feature and the event reporting function are enabled. If the EFM feature is enabled but the event reporting function is disabled, you can run the **display efm oam event current frameid/slotid/portid local** command to query the EFM events detected by the local DTE.

**Table 5-13** Conditions for detecting and reporting local EFM events

| EFM Feature | Event Reporting Function | Detect Local EFM Events or Not | Report Local EFM Events or Not |
|-------------|--------------------------|--------------------------------|--------------------------------|
| Enabled     | Enabled                  | Yes                            | Yes                            |
|             | Disabled                 | Yes                            | No                             |
| Disabled    | Enabled                  | No                             | No                             |
|             | Disabled                 | No                             | No                             |

The local DTE detects only three types of EFM events: link fault event, errored frame event, and errored frame seconds summary event.

- For the errored frame event and errored frame seconds summary event, the event reporting function is disabled by default. You need to run some commands to enable this function. For the specific commands, see the following configuration steps.
- For the link fault event, the event reporting function is enabled by default and cannot be modified.

## Procedure

- Step 1** Run the **efm oam frameid/slotid/portid enable** command to enable the EFM feature for the port. By default, the EFM feature is disabled.

**Step 2** (Optional) Configure the event reporting function and related parameters on the local DTE.

When the local DTE needs to report the errored frame event or the errored frame seconds summary event and notify the remote DTE, perform this step by running the **efm error-frame** command or **efm error-frame-second** command respectively.

**Step 3** Query the configuration results. The following table lists the query commands related to EFM Ethernet link monitoring.

| Item                                                                                 | Command                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Querying the status of the EFM feature on the local DTE                              | <b>display efm oam status frameid/slotid/portid local</b><br><b>NOTE</b><br>In the command output, the <b>Admin Status</b> parameter indicates whether the EFM feature is enabled on the local DTE.                                                                |
| Querying the status of the remote DTE                                                | <b>display efm oam status frameid/slotid/portid remote</b><br><b>NOTE</b><br>In the command output, the <b>Event Support</b> parameter indicates whether the remote DTE supports sending a notification to the local DTE when the remote DTE detects an EFM event. |
| Querying the event reporting function and related parameters of different EFM events | <b>display efm oam event config</b>                                                                                                                                                                                                                                |
| Querying the latest EFM event                                                        | <b>display efm oam event current</b>                                                                                                                                                                                                                               |
| Querying the number of EFM events                                                    | <b>display statistics performance</b>                                                                                                                                                                                                                              |

----End

## Result

In the case of traffic interruption or link quality degradation, the access device (local DTE) reports events based on the configurations.

## Example

Assume that Ethernet cascade port 0/2/0 on the OLT is connected to upstream port 0/0/1 on the MDU, both OLT and MDU can receive the EFM events sent by each other and can detect EFM events, and the detection interval and other thresholds are defaulted. To monitor the quality of this Ethernet link section, do as follows:

- OLT configurations:  
OLT(config)#**efm oam 0/2/0 enable**  
OLT(config)#**efm error-frame 0/2/0 notification enable**  
OLT(config)#**efm error-frame-second 0/2/0 notification enable**

- MDU configurations:  
MDU(config)#efm oam 0/0/1 enable  
MDU(config)#efm error-frame 0/0/1 notification enable  
MDU(config)#efm error-frame-second 0/0/1 notification enable  
MDU(config)#efm error-frame-period 0/0/1 notification enable

#### NOTE

Of the OLT and MDU, only the MDU can detect the errored frame period event, and only MDUs of some models can detect this event. For details, see the *Feature Specifications* in related MDU product documents.

### 5.3.5.5 EFM Maintenance and Diagnosis

After EFM is enabled, the access device uses **0x2f00000a Ethernet OAM Link Events** to implement **remote failure indication** and **link monitoring**. According to event parameters, the event type (such as link fault and errored frame) and location (local or remote) can be determined.

- The access device can receive all types of EFM events sent by the remote device and then report **0x2f00000a Ethernet OAM Link Events** at local.
- The access device can only detect some types of EFM events, report **0x2f00000a Ethernet OAM Link Events** at local, and uses the OAMPDU to notify the remote end. Types of EFM events can be detected at local are related to the hardware. For the hardware supported, see "Specifications."

After the EFM connection is established, the remote DTE status can be queried by the **display efm oam status** command.

The statistics of EFM OAM packets that are received and sent by local TDE can be queried by the **display efm oam statistics** command.

### 5.3.6 PM (Y.1731)

Performance monitoring (PM) is defined in ITU-T Y.1731. PM, as an OAM feature, is used to test the performance of Ethernet links and evaluate the network quality.

#### 5.3.6.1 PM Introduction

This topic describes the benefits and functions of performance monitoring (PM) defined in ITU-T Y.1731.

#### Benefits

As the multi-play service (for example, IPTV) prevails, more and more difficulties in Ethernet OAM emerge. The following uses the triple-play service as an example to explain the difficulties facing carriers.

- IPTV: Video streams are sensitive to packet loss and delay. The loss of a packet affects dozens of pictures, causing frame freezing and impairing user experience.
- VoIP: Audio streams are sensitive to packet loss and delay. Packet loss or overlong delay results in intermittent voices; delay variations result in vague voices, which are intolerable to users.

- High-speed Internet (HSI): Packet loss or delay occurring in the data streams may cause user authentication failures or user connection failures, which increases user complaints.

As a result, minimizing user complaints (caused by network quality degradation) and improving fault locating efficiency have become carriers' top concerns.

Besides, in the case of national broadband, carriers charge retail service providers (RSPs) based on the level of network quality when selling bandwidth to the RSPs. Some carriers even charge end users based on the level of network quality. Therefore, carriers need to monitor the network quality and provide the service level agreement (SLA) as the accounting basis.

ITU-T Y.1731 defines a series of methods for monitoring Ethernet link performance. These methods help carriers collect link performance data in real time and fast diagnose the network performance faults. ITU-T Y.1731 also provides carriers with technical means for outputting the SLA reports.

## Functions

The following table lists the three PM functions supported by access devices.

| Function             | Description                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Single-ended ETH-LM  | Single-ended Ethernet loss measurement (ETH-LM) is used to collect the packet loss rate of an Ethernet link based on a count of transmitted and received data frames between a pair of MEPs.                                                                                                                                                                                 |
| Two-way ETH-DM       | Two-way Ethernet delay measurement (ETH-DM) is used to collect the delay, delay variation of an Ethernet link.                                                                                                                                                                                                                                                               |
| Single-ended ETH-SLM | Single-ended Ethernet synthetic loss measurement (ETH-SLM) is a mechanism to measure frame loss using synthetic frames, rather than data traffic. A number of synthetic frames are sent and received, and the number of those that are lost is hence calculated. This can be treated as a statistical sample, and used to approximate the frame loss ratio of data traffic . |

Both single-ended ETH-LM, two-way ETH-DM and single-ended ETH-SLM support the following modes:

- On-demand mode: In this mode, performance data is collected in real time. On-demand single-ended ETH-LM and two-way ETH-DM are used for diagnosing network quality faults. They can be started through the CLI or NMS, and related measurement results are displayed on the CLI or NMS.
- Periodic mode: In this mode, performance data is collected and reported periodically. Periodic single-ended ETH-LM and two-way ETH-DM are used by carriers to output periodic SLA reports. They can be started only through the NMS.

### 5.3.6.2 PM Networking Application

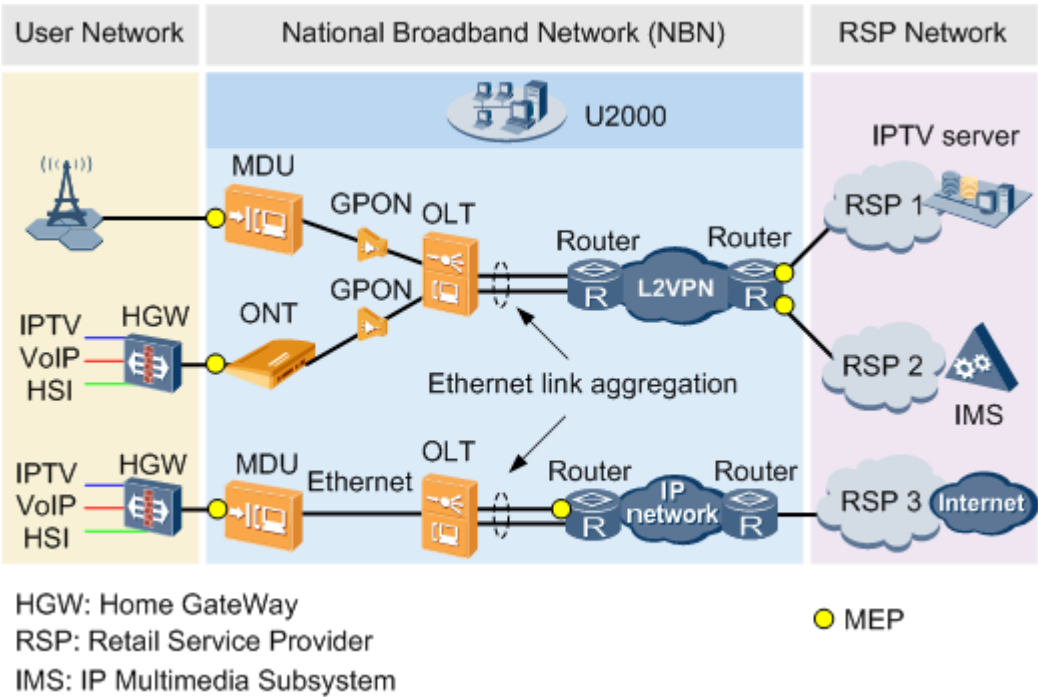
Performance monitoring (PM) is mainly used on the national broadband (NBB) network to monitor and evaluate carriers' service quality. In addition, some carriers deploy maintenance association end points (MEPs) on their networks. These MEPs help carriers test link performance section by section along a network link, achieving fast fault demarcation and fault locating.

The following describes the typical MEP deployment on common networks.

#### NBB Network

**Figure 5-30** shows the typical MEP deployment on the NBB network to implement PM according to ITU-T Y.1731. The user ports on the MDUs and ONTs mark the boundary between the NBB network and the user network; the network-side ports on routers mark the boundary between the NBB network and the retail service provider (RSP) network. MEPs deployed on the boundaries of the NBB network collect the performance data about the Ethernet links between 2 MEPs. The collected performance data is used for network quality evaluation. ITU-T Y.1731 is a Layer 2 network protocol, and the Ethernet protocol packets defined by ITU-T Y.1731 cannot traverse an IP network. If MEPs need to be deployed on the network-side ports on the routers at the boundary of the NBB network, a Layer 2 VPN tunnel needs to be established between the routers.

**Figure 5-30** Typical MEP deployment on the NBB network



**NOTE**

Currently, no ONT supports Ethernet synthetic loss measurement (ETH-SLM) defined in ITU-T Y.1731.

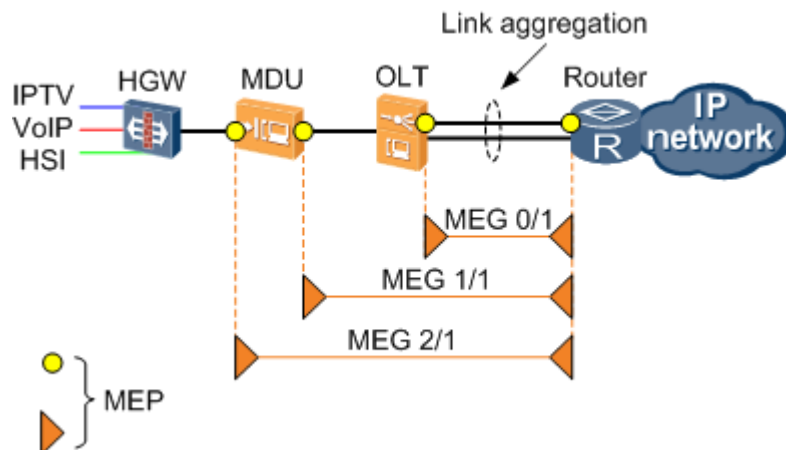
## FTTB/FTTC Network

**Figure 5-31** shows the MEPs deployed on the user port and upstream port on the MDU, upstream link aggregation group of the OLT, and downstream link aggregation group of the router on a fiber to the building (FTTB) or a fiber to the curb (FTTC) network. These MEPs help test the link performance in each maintenance entity group (MEG).

For example, if a user reports that the voice is intermittent during the call, maintenance engineers perform single-ended Ethernet loss measurement (ETH-LM) section by section along the network link to diagnose the specific network section in which the user's voice service stream encounters packet loss. As shown in **Figure 5-31**, maintenance engineers check whether packets are lost in MEG 2/1. If no packet is lost, the link between the user port on the MDU and the router runs normally. If packets are lost, maintenance engineers continue to check whether packets are lost in MEG 1/1.

- If packets are lost in MEG 1/1, maintenance engineers check whether packets are lost in MEG 0/1.
- If no packet is lost in MEG 1/1 but packets are lost in MEG 2/1, it indicates that packets are lost on the MDU.

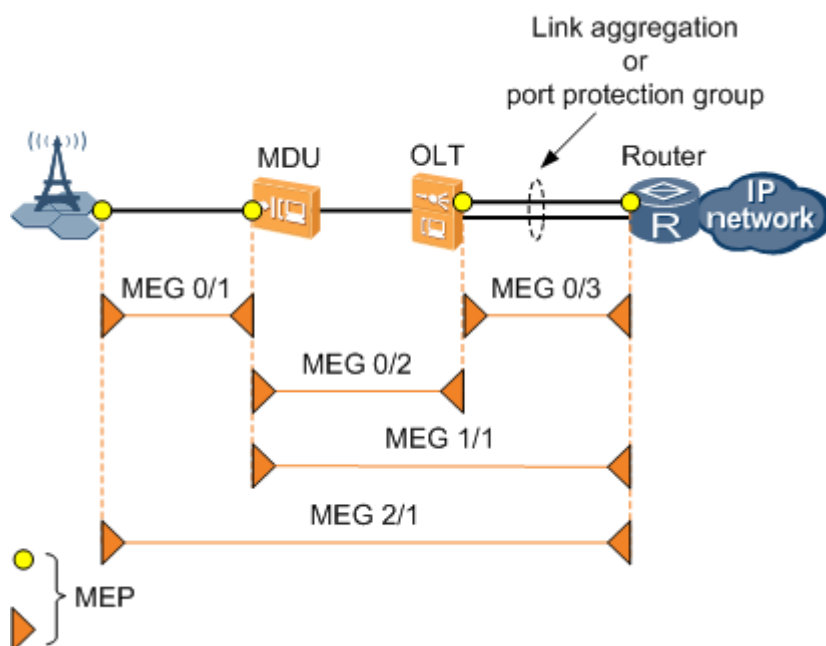
**Figure 5-31** Typical MEP deployment on an FTTB/FTTC network



## FTTM Network

Fiber to the mobile base station (FTTM) networks have a high requirement on link reliability. Therefore, port protection groups or link aggregation groups (active/standby mode) are created on the links between the OLT and router on an FTTM network. **Figure 5-32** shows the MEPs deployed on the upstream port on the mobile base station, user port on the MDU, upstream port protection group or link aggregation group of the OLT, and user-side port protection group or downstream link aggregation group of the router. These MEPs help test the link performance in each MEG.

**Figure 5-32** Typical MEP deployment on an FTTM network



## FTTH Network

The MEP is deployed on the LAN port or the WAN port on the ONT, upstream link aggregation group of the OLT, and downstream link aggregation group of the router. These MEPs help test the link performance in each MEG.

- **Figure 5-33** shows the up MEP deployed on the LAN port of a bridging ONT.
- **Figure 5-34** shows the down MEP deployed on the WAN port of a routing ONT.

**Figure 5-33** Typical MEP deployment on an FTTH network with bridging ONT

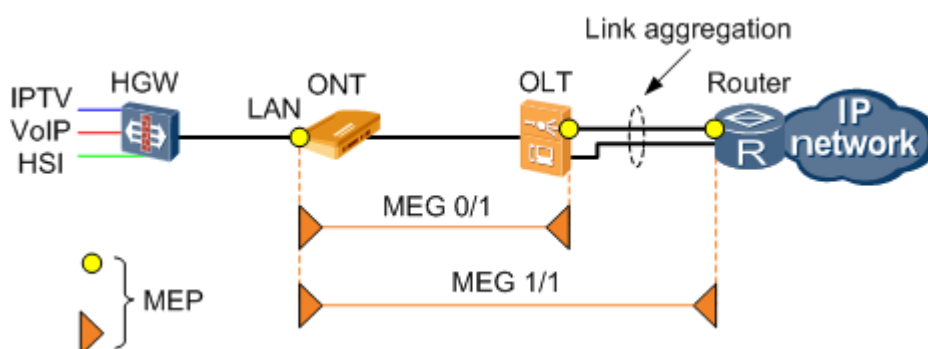
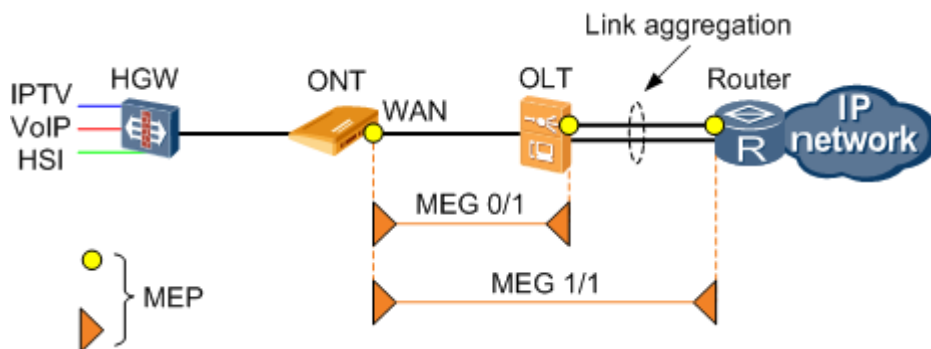


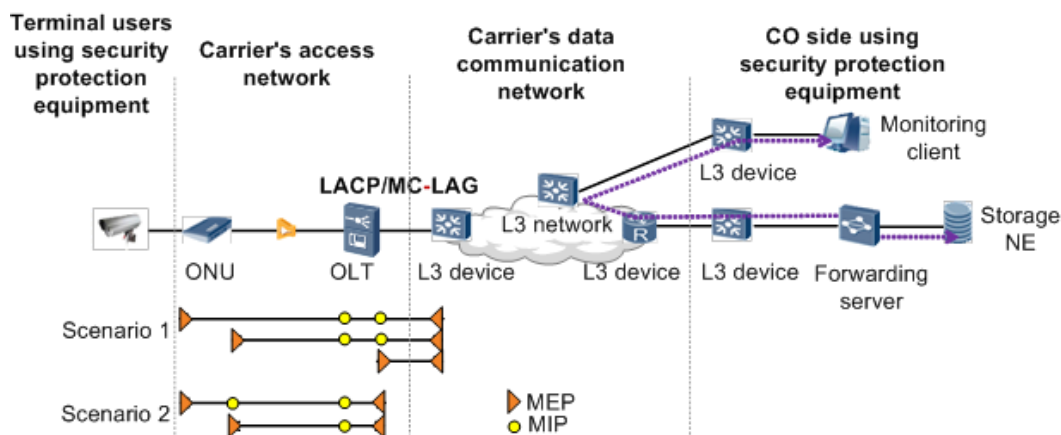
**Figure 5-34** Typical MEP deployment on an FTTH network with routing ONT

In FTTH scenario, the performance monitoring function of ONT is configured through the CLI of OLT. Then OLT issues the configuration to ONT through the optical network terminal management and control interface (OMCI) channel. ONT can only function as the responding end.

## FTTO Video Monitoring Network

On-demand video monitoring is preferred for fault demarcation, as shown in [Figure 5-35](#).

- Scenario 1. MEGs are deployed on the Layer 3 UNI and ONU UNI to check continuity and check packet loss, delay, and jitter in one direction. In this scenario, the protection network between the upstream port on the OLT and Layer 3 device needs to be considered, including single-homing Link Aggregation Control Protocol (LACP) protection and dual-homing multi-chassis link aggregation group (MC-LAG) protection.
- Scenario 2. MEGs are deployed on the OLT NNI and ONU UNI to check continuity and check packet loss, delay, and jitter in one direction.

**Figure 5-35** Typical MEP deployment on an FTTO video surveillance network

### 5.3.6.3 PM Basic Concepts

This topic introduces the basic concepts of performance monitoring (PM) defined in ITU-T Y.1731.

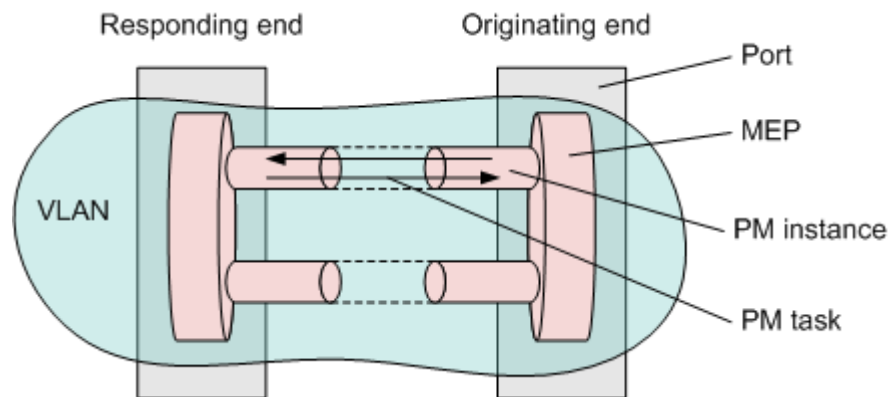
Some concepts are detailed in ITU-T Y.1731 and IEEE 802.1ag. When access devices implement PM, some concepts, such as the maintenance association end

point (MEP) and maintenance association (MA) are used. For details, see [5.3.4.3 CFM Basic Concepts](#) and [5.3.3 Differences in Implementing Y.1731 and 802.1ag on Access Device](#).

Besides, Huawei introduces some concepts (such as the PM instance and PM task) that are not defined in the protocols. The following table lists the items that need to be configured during PM deployment. The relationships between the configured items are shown in [Figure 5-36](#).

| Item | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MEP  | <p>Used to demarcate the Ethernet link to be monitored. MEPs can be divided into originating and responding ends based on the type of Ethernet protocol packets sent by them.</p> <ul style="list-style-type: none"><li>• Originating end: sends the Ethernet protocol request packets and receives the Ethernet protocol response packets sent by the responding end. By comparing the request and response packets, the system calculates the packet loss rate, number of lost packets, and the delay occurring on the link between the 2 MEPs.</li><li>• Responding end: replies to the originating end with Ethernet protocol response packets. The responding end does not calculate or save the performance test results.</li></ul> |

| Item        | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PM instance | <p>Used to select the PM object on the Ethernet link between 2 MEPs. PM instances are identified by the test ID. The following parameters are provided to differentiate between different PM instances.</p> <ul style="list-style-type: none"> <li>• <b>mep</b>, <b>remote-mep</b>, and <b>remote-mep-mac</b>: specify the two ends of the Ethernet link to be monitored. Two MEPs exchange Ethernet protocol packets with each other to collect performance data.</li> <li>• <b>receive-8021p</b> and <b>send-8021p</b>: specify the priority of Ethernet protocol packets sent and received by the MEP. The priority of the Ethernet protocol packets must be the same as that of the to-be-monitored service flow. In <b>Multi-priority Convergence</b> scenario, to calculate all the packets received by or sent from the MEP according to Huawei's proprietary protocol, set these parameters to <b>unaware</b>. Parameter value <b>unaware</b> is valid to Ethernet loss measurement (ETH-LM), Ethernet delay measurement (ETH-DM), and Ethernet synthetic loss measurement (ETH-SLM).</li> <li>• <b>backward-mac</b>, <b>onward-mac</b>, <b>update-backward-mac</b>, and <b>update-onward-mac</b>: defined by Huawei's proprietary protocol. These 4 parameters are used to differentiate between service flows when an ETH-LM or ETH-DM test is performed in the <b>point-to-multipoint connection (N:1 VLAN)</b> scenario. These 4 parameters do not need to be configured when an Ethernet synthetic loss measurement ETH-SLM is performed or when an ETH-LM or ETH-DM test is performed in the <b>point-to-point connection (1:1 VLAN)</b> scenario.</li> </ul> |
| PM task     | <p>Used to select one of the PM instances configured in the system for an LM or delay measurement (DM) test. PM instances are configured manually and do not trigger the Ethernet protocol packet exchange between the MEPs at both ends of the link. The 2 MEPs normally exchange Ethernet protocol packets only when the originating and responding ends use the same PM instance for performing the same PM task.</p> <ul style="list-style-type: none"> <li>• <b>pm lm send</b> and <b>pm dm send</b>: used to configure the interval for sending Ethernet protocol packets (used for LM and DM tests) and configure the number of Ethernet protocol packet sending attempts on the originating end. After these 2 parameters are configured, the originating end starts to send Ethernet protocol request packets.</li> <li>• <b>pm lm receive</b>, <b>pm dm receive</b>, and <b>pm slm receive</b>: used to configure whether the responding end responds to the requests initiated by the originating end.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

**Figure 5-36** Items that need to be configured during PM deployment

### 5.3.6.4 PM Principles

Performance monitoring (PM) defined in ITU-T Y.1731 cannot be used in some application scenarios. Therefore, Huawei broadens the PM application scenarios based on Huawei's proprietary protocol. The following introduces how to implement Ethernet link PM on an FTTB/FTTC network with typical VLAN and QoS planning.

Access devices implement single-ended Ethernet loss measurement (ETH-LM), two-way Ethernet delay measurement (ETH-DM) and single-ended Ethernet synthetic loss measurement (ETH-SLM) according to ITU-T Y.1731. For basic implementation principles, see ITU-T Y.1731.

#### 5.3.6.4.1 Performance Monitoring with Typical VLAN Planning

Single-ended Ethernet loss measurement (ETH-LM) and two-way Ethernet delay measurement (ETH-DM) defined in ITU-T Y.1731 are based on the point-to-point (P2P) connection. That is, a maintenance association end point (MEP) receives packets only from a remote MEP. However, in actual networking applications, the VLAN planning is very flexible, which means that a MEP receives packets from multiple remote MEPs. This networking mode is a type of point-to-multipoint (P2MP) connection mode. The following introduces how to implement single-ended Ethernet loss measurement (ETH-LM) and two-way Ethernet delay measurement (ETH-DM) in P2P and P2MP connection scenarios with typical VLAN planning.

## P2P Connection (1:1 VLAN Scenario)

**Figure 5-37** P2P network for enterprise users

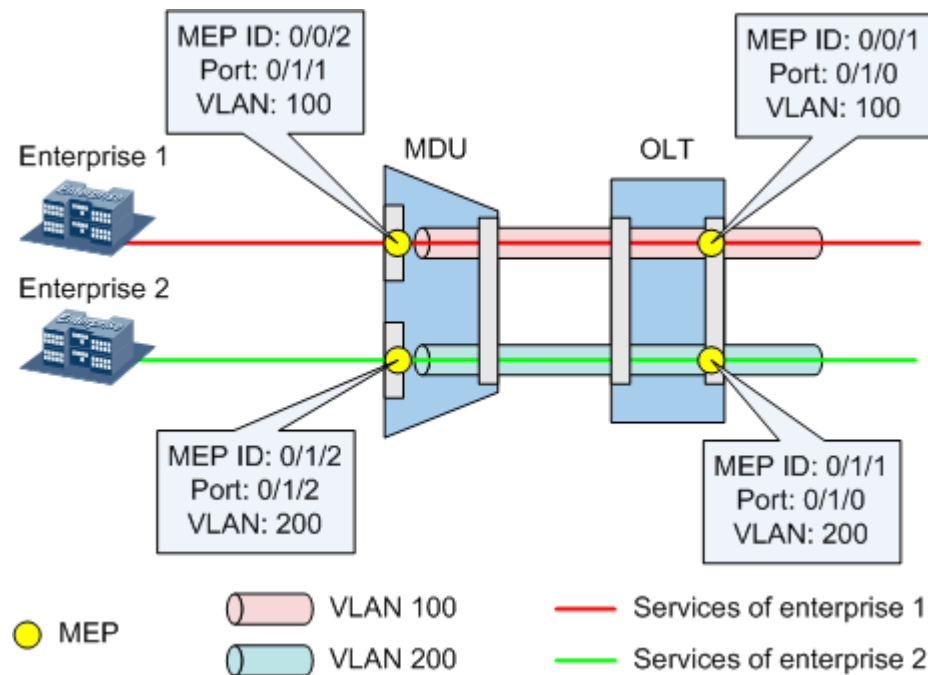


**Figure 5-37** shows the typical 1:1 VLAN planning. The MDU translates the VLAN of the enterprise user's service flow to the service VLAN (S-VLAN). Then the OLT transparently transmits the VLAN. The following conditions must be met during the S-VLAN planning.

- Different enterprise users connected to the same OLT must be configured with different S-VLANs.
- Packets sent by any 2 MDUs connected to the same OLT cannot carry the same S-VLAN tag.

Assume that enterprise users' services in **Figure 5-37** are transmitted upstream by the upstream interface board on the OLT. If maintenance engineers need to check the performance of the link between the MDU user port and the OLT upstream port, deploy the MEPs on the MDU user port and the OLT upstream port as shown in **Figure 5-37**. All the packets received on MEP 0/0/1 are sent from MEP 0/0/2. Such a connection is a P2P connection. For a P2P connection, when a PM instance is added, the MEPs at both ends of the link and the priorities of to-be-test services must be specified.

## P2MP Connection (N:1 VLAN Scenario)

Figure 5-38 P2MP network for home users

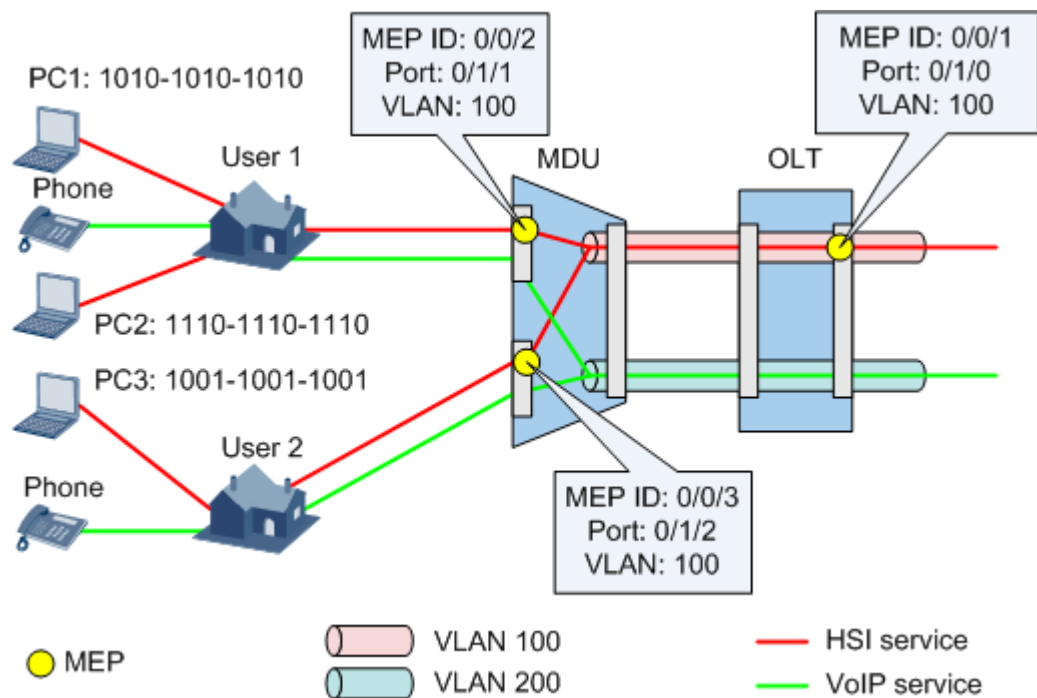


Figure 5-38 shows the typical N:1 VLAN planning. The MDU translates the VLAN of the home user's service flow to the S-VLAN. Then the OLT transparently transmits the VLAN. The following conditions must be met during the VLAN planning.

- Customer VLANs (C-VLANs) are used to differentiate between home users' service flows.
- The MDU translates C-VLANs to S-VLANs. Packets of the same type are transmitted upstream through the same S-VLAN.

Assume that home users' services in Figure 5-38 are transmitted upstream through the upstream interface board on the OLT. If maintenance engineers need to measure the packet loss rate of user 1's HSI services on an FTTx network, deploy the MEPs on the MDU user port and the OLT upstream port as shown in Figure 5-38. All data services on the MDU are transmitted upstream through the same S-VLAN. All the packets received on MEP 0/0/1 are sent from MEP 0/0/2 and MEP 0/0/3. Such a connection is a P2MP connection. In this case, MEP 0/0/1 cannot differentiate between packets from MEP 0/0/2 and those from MEP 0/0/3. Therefore, the packet loss rate cannot be accurately measured on the link between MEP 0/0/1 and MEP 0/0/2. To solve this issue, Huawei defines 2 concepts, onward MAC and backward MAC, in its proprietary protocol. Onward MAC and backward MAC are used to identify P2P service flows on a P2MP connection network.

Essentially, onward MAC and backward MAC are MAC addresses of user terminals. Each MAC address is globally unique. Therefore, the MEP where service flows converge can identify the source of the packets based on the MAC address.

- Backward MAC: used to configure the PM instance at the access end (for example, the MDU user port in Figure 5-38) of the service flows.

- Onward MAC: used to configure the PM instance at the convergence end (for example, the OLT upstream port in [Figure 5-38](#)) of the service flows.

Onward MAC and backward MAC can be manually specified or randomly selected by the device.

- When maintenance engineers need to measure the packet loss rate of a specific user's service flows on a link, use the **onward-mac** and **backward-mac** parameters to manually specify the MAC address of the user terminal.
- When maintenance engineers need to measure the packet loss rate of the whole links, use the **update-onward-mac** and **update-backward-mac** parameters to make the device randomly select the service flows from a user terminal as the test sample.

Assume that, in [Figure 5-38](#), the priority of the upstream and downstream packets of user 1's and user 2's HSI services is 0; the MEP on the OLT functions as an originating end; the MEP on the MDU functions as a responding end. The following table lists PM instance configurations (using [Figure 5-38](#) as an example).

| Test Object             | PM Instance Configuration on the MDU                                                                       | PM Instance Configuration on the OLT                                                                     |
|-------------------------|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Data services of user 1 | <b>pm instance mep 0/0/2<br/>remote-mep 1 receive-8021p<br/>0 send-8021p 0 backward-mac 00e0-fc00-1010</b> | <b>pm instance mep 0/0/1<br/>remote-mep 2 receive-8021p<br/>0 send-8021p 0 onward-mac 00e0-fc00-1010</b> |
| HSI services of user 1  | <b>pm instance mep 0/0/2<br/>remote-mep 1 receive-8021p<br/>0 send-8021p 0 update-backward-mac</b>         | <b>pm instance mep 0/0/1<br/>remote-mep 2 receive-8021p<br/>0 send-8021p 0 update-onward-mac</b>         |
| HSI services of user 2  | <b>pm instance mep 0/0/3<br/>remote-mep 1 receive-8021p<br/>0 send-8021p 0 update-backward-mac</b>         | <b>pm instance mep 0/0/1<br/>remote-mep 3 receive-8021p<br/>0 send-8021p 0 update-onward-mac</b>         |

On a P2MP connection network, the access device differentiates between service flows according to the MAC addresses of user terminals. The following requirements must be met during PM instance deployment.

- The MAC address learning function is not disabled at the access end (for example, the MDU in [Figure 5-38](#)).
- The maximum number of learnable dynamic MAC addresses on the service port must be greater than or equal to the actual number of MAC addresses on the service port to ensure that all the source MAC addresses of packets sent by user terminals can be learnt by the access device. Otherwise, the access device may regard the user packets as unknown unicast packets and discard them. Therefore, the test results may be inaccurate.
- On an FTTB/FTTC network, if an up MEP is configured on the MDU service board, 1:1 VMAC can be enabled on the MDU, while N:1 VMAC address cannot.

- In an FTTH network, 1:1 VMAC or N:1 VMAC cannot be enabled on the OLT.
- The access device implements single-ended Ethernet loss measurement (ETH-LM) on a P2MP connection network according to Huawei's proprietary protocol, and therefore the access devices interconnect only with Huawei devices. When the peer MEP is on a device which is not manufactured by Huawei, ETH-SLM can be used to collect the packet loss rate on a P2MP connection network.
- If the performance of the service flow needs to be monitored, the traffic classification parameter of the **service-port** must be created based on user-vlan instead of **user-8021p**, **user-8021p-list** or **user-encap**.

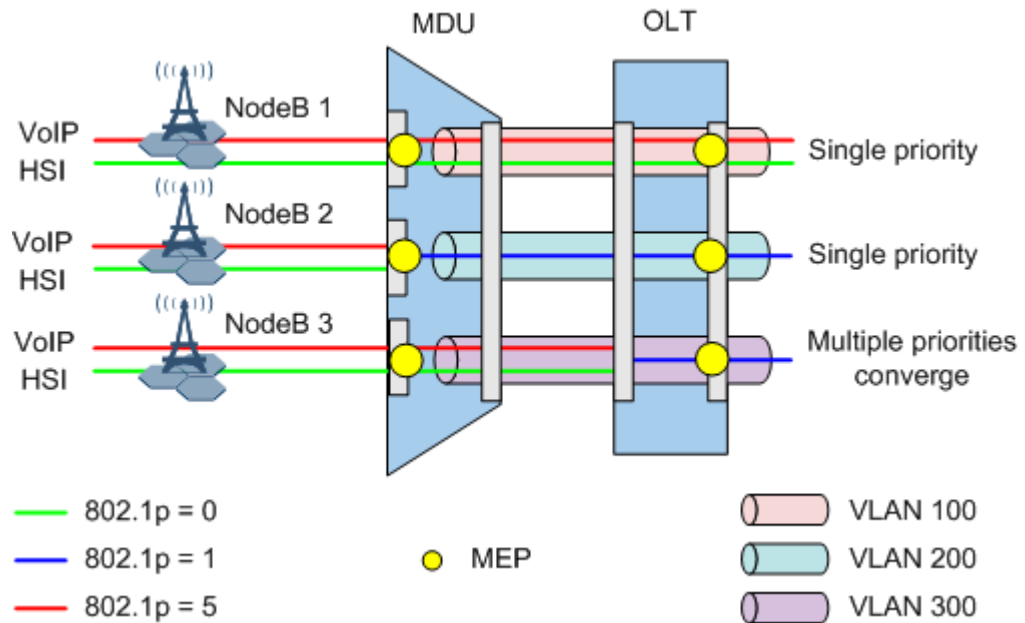
#### 5.3.6.4.2 Performance Monitoring with Typical QoS Planning

As defined in ITU-T Y.1731, the priority of Ethernet protocol packets used for single-ended Ethernet loss measurement (ETH-LM), two-way Ethernet delay measurement (ETH-DM) and single-ended Ethernet synthetic loss measurement (ETH-SLM) must be configurable to make the priority of Ethernet protocol packets equal to that of to-be-tested packets. If the priority of to-be-tested packets changes during packet forwarding, the priority of Ethernet protocol packets must be changed accordingly. The following describes the PM configuration and implementation principles on an FTTM point-to-point (P2P) network with different QoS plans.

#### Single Priority and Multi-priority Convergence

A service flow may contain packets with different priorities. Generally, the system chooses packets with the same priority for PM tests. This belongs to the single priority scenario (for example, NodeB 1 and NodeB 2 in [Figure 5-39](#)). However, in actual networking applications, carriers may modify packet priorities based on the QoS planning. Therefore, a service flow on a MEP may contain packets with different priorities, but this service flow on another MEP contains packets with the same priority. This belongs to the multi-priority convergence scenario (for example, NodeB 3 in the [Figure 5-39](#)).

**Figure 5-39** Single priority and multi-priority convergence



Assume that the 802.1p field is used to differentiate between service flows. Carriers configure different priority processing policies for different NodeBs, as shown in [Figure 5-39](#).

- NodeB 1: The MDU and OLT copy the 802.1p priority of user-side packets as the priority of upstream packets and copy the 802.1p priority of network-side packets as the priority of downstream packets.
- NodeB 2: The MDU specifies the 802.1p priority of upstream packets to 1, and the OLT copies the 802.1p priority of user-side packets as the priority of upstream packets. The MDU and OLT copy the 802.1p priority of network-side packets as the priority of downstream packets.
- NodeB 3: The MDU copies the 802.1p priority of user-side packets as the priority of upstream packets, and the OLT specifies the 802.1p priority of upstream packets to 1. The MDU and OLT copy the 802.1p priority of network-side packets as the priority of downstream packets.

As shown in [Figure 5-39](#), MEPs are deployed on the MDU user port and the OLT upstream port to monitor the performance of Ethernet links.

- For NodeB 1 and NodeB 2, MEPs at both ends of a link perform PM tests based on packets with the same priority in upstream and downstream directions. This belongs to the single priority scenario.
- For NodeB 3, a service flow on the MEP of the MDU contains packets with different priorities, while the service flow on the MEP of the OLT contains packets with the same priority. This belongs to the multi-priority convergence scenario. However, this scenario is not defined in ITU-T Y.1731. Therefore, the access device implements ETH-LM, ETH-DM and ETH-SLM of the multi-priority convergence scenario based on the Huawei's proprietary protocol. As defined in Huawei's proprietary protocol, the priority of Ethernet protocol packets on the MEP containing packets with different priorities is set to **unaware** so that all the packets sent to or received by the MEP are counted during statistics measurement. For example, to perform LM between the user

port of the MDU and the upstream port of the OLT, set the priority of Ethernet protocol packets of the PM instance corresponding to NodeB 3 to **unaware** on the MDU.

Assume that the 802.1p priority of downstream packets is set to 0; the MEP on the OLT functions as an originating end; the MEP on the MDU functions as a responding end. The following table lists the priority configurations of Ethernet packets in PM instances. The priorities of services on NodeB 2 and NodeB 3 are modified to the same priority. Therefore, the system can monitor only the performance of all the services, but cannot monitor the performance of a specific service.

| Test Object              | Priority Configurations on the MDU    | Priority Configurations on the OLT |
|--------------------------|---------------------------------------|------------------------------------|
| VoIP services of NodeB 1 | receive-8021p 0<br>send-8021p 5       | receive-8021p 5<br>send-8021p 0    |
| HSI services of NodeB 1  | receive-8021p 0<br>send-8021p 0       | receive-8021p 0<br>send-8021p 0    |
| Services of NodeB 2      | receive-8021p 0<br>send-8021p 1       | receive-8021p 1<br>send-8021p 0    |
| Services of NodeB 3      | receive-8021p 0<br>send-8021p unaware | receive-8021p 1<br>send-8021p 0    |

In the multi-priority convergence scenario, the priority after multiple priorities converge is used as the priority of Ethernet protocol packets, which is different from the priority of the service flow. Therefore, PM results may be incorrect.

For example, if PM is performed on NodeB 3 in [Figure 5-39](#), service packets forwarded by the MDU to the upstream direction are with different priorities, and the 802.1p priority of Ethernet protocol packets sent by the MEP on the MDU is 1. The priority of the Ethernet protocol packets is not the same as that of any service packets. In this case, the sequence of Ethernet protocol packets and service packets received on the OLT may change, which may be different from that of Ethernet protocol packets and service packets sent by the MDU. Consequently, the PM results may be inaccurate.

In the multi-priority convergence scenario, to ensure accurate PM results, ensure that the originating end, responding end, and devices in between map packets with different priorities into the same queue for scheduling so that the sequence of Ethernet protocol packets and service packets is not changed during scheduling.



MDU functions as a responding end. The following table lists the priority configurations of Ethernet packets in PM instances.

| Test Object         | Priority Configurations on the MDU | Priority Configurations on the OLT |
|---------------------|------------------------------------|------------------------------------|
| Services of NodeB 1 | receive-8021p 0<br>send-8021p 1    | receive-8021p 1<br>send-8021p 0    |
| Services of NodeB 2 | Not supported                      | Not supported                      |

### 5.3.6.5 PM Configuration

This topic describes how to configure ITU-T Y.1731-defined performance monitoring (PM) using the CLI. The CLI supports only the configuration of on-demand PM tests, such as Ethernet loss measurement (ETH-LM), Ethernet delay measurement (ETH-DM) and Ethernet synthetic loss measurement (ETH-SLM). Periodic PM tests are configured only on the NMS. For the detailed operations, see the NMS configuration guide.

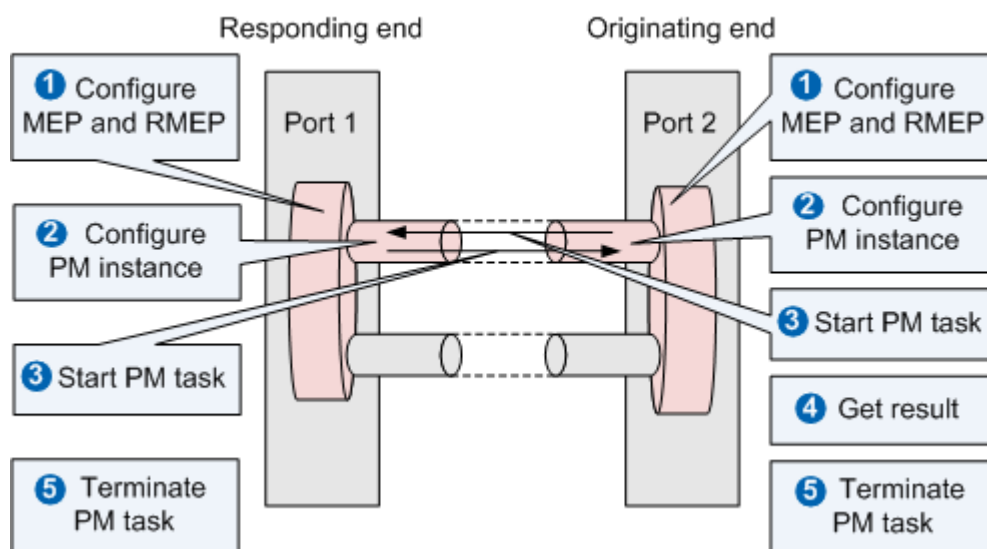
#### Prerequisites

Service configurations (such as VLAN and service flow configurations) are completed, and user-side services run normally.

#### Configuration Procedure

**Figure 5-41** shows the overall procedure of configuring and performing a PM task on the originating and responding ends.

**Figure 5-41** PM configuration procedure



As shown in [Figure 5-41](#), the configuration items and steps on the originating end are similar to those on the responding end. The following table lists the related configuration commands and precautions.

| Step                                                       | Command               | Precautions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.<br>Configure maintenance association end points (MEPs). | <b>cfm md</b>         | Parameter <b>name-format</b> must be set to <b>no-name</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                                                            | <b>cfm ma</b>         | The maintenance association (MA) ID must be the same as the maintenance entity group (MEG) ID, and parameter <b>name-format</b> must be set to <b>icc-based</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                                                            | <b>cfm ma vlan</b>    | If the MEP is configured on the NXED board, the VLAN associated with the MA must be the same as that configured in <b>vlantag1</b> of the MEP in the MA.<br><b>NOTE</b><br>For a MEP on the ONT, do not configure this command.                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                                                            | <b>cfm ma meplist</b> | The MEP list must contain the MEP and RMEP.<br><b>NOTE</b><br>For a MEP on the ONT, do not configure this command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                                                            | <b>cfm mep</b>        | For detailed limitations on MEP configurations, see Feature Dependency and Limitation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 2.<br>Configure PM instances.                              | <b>pm instance</b>    | <ul style="list-style-type: none"><li>The parameters that need to be configured varies with the VLAN and QoS planning. For details, see <a href="#">5.3.6.4.1 Performance Monitoring with Typical VLAN Planning</a> and <a href="#">5.3.6.4.2 Performance Monitoring with Typical QoS Planning</a>.</li><li>You are advised to set the test ID on the originating end to be the same as that on the responding end to facilitate future management and maintenance if these 2 test IDs belong to the same PM instance.</li><li>The <b>display pm instance</b> command can be used to query the configured PM instances in the system.</li></ul> |

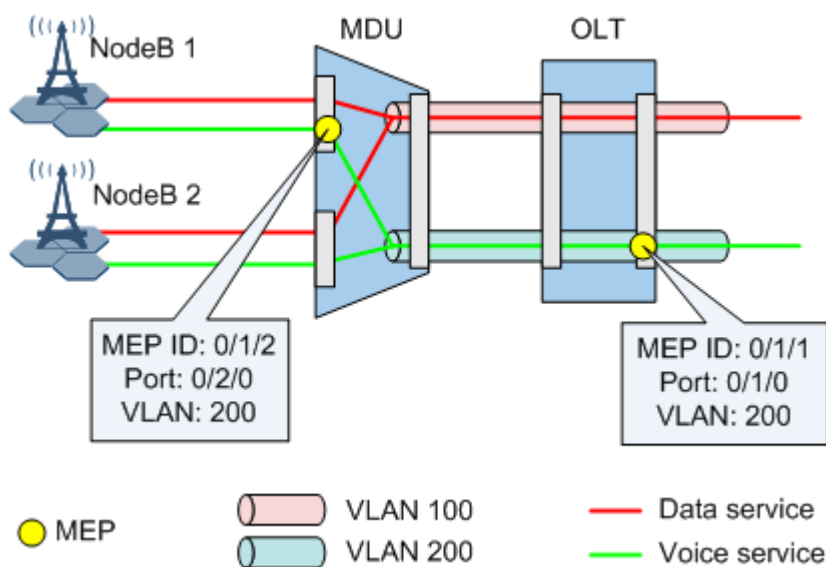
| Step                        | Command                                                                                                                                                                                                                                         | Precautions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3. Start PM tasks.          | ETH-LM<br>1. Responding end: <b>pm lm receive</b><br>2. Originating end: <b>pm lm send</b><br>ETH-DM<br>1. Responding end: <b>pm dm receive</b><br>2. Originating end: <b>pm dm send</b><br>ETH-SLM<br>1. Responding end: <b>pm slm receive</b> | <ul style="list-style-type: none"> <li>The number of started PM tasks must comply with that of PM tasks that can be supported by the devices where the originating and responding ends are configured.</li> <li>For an LM test, if one of the 2 MEPs (belonging to the same PM instance) is set as the originating end on a device, the other MEP cannot be set as the responding end on the same device. Similarly, if one of the 2 MEPs is set as the responding end on a device, the other MEP cannot be set as the originating end on the same device.</li> <li>After a PM task is started on the responding end, the responding end sends the response packets to the peer MEP only when the test ID configured for the PM task on the responding end matches the MEP configured on the originating end.</li> <li>The <b>display pm task</b> command can be used to query the started PM tasks on the device. If a PM task is interrupted abnormally, but the timeout interval for the PM task does not expire, this PM task can be queried by running the <b>display pm task</b> command.</li> <li>The <b>display pm oam pdu statistics</b> command can be used to query the Ethernet protocol packets that are transmitted and received by the device.</li> </ul> |
| 4. Obtain the test results. | <b>display pm statistics</b>                                                                                                                                                                                                                    | <p>You can use any of the following methods to obtain the test results on the originating end.</p> <ul style="list-style-type: none"> <li>The test results will be displayed on the CLI in real time after a PM task is started.</li> <li>You can run the <b>display pm statistics</b> command to query the test results after the test is completed.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Step               | Command                                                                                                                                                                                                                                                                                                                                                                                                | Precautions                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5. Stop a PM task. | <p>ETH-LM</p> <ol style="list-style-type: none"> <li>1. Originating end: -</li> <li>2. Responding end: <b>undo pm lm receive</b></li> </ol> <p>ETH-DM</p> <ol style="list-style-type: none"> <li>1. Originating end: -</li> <li>2. Responding end: <b>undo pm dm receive</b></li> </ol> <p>ETH-SLM</p> <ol style="list-style-type: none"> <li>1. Responding end: <b>undo pm slm receive</b></li> </ol> | <p>A PM task on the originating end will be stopped if any of the following conditions is met.</p> <ul style="list-style-type: none"> <li>• The maintenance engineer presses <b>Ctrl+C</b> to manually stop the PM task.</li> <li>• The PM task is completed successfully, or the timeout interval for a PM task has expired so that the system automatically stops the PM task.</li> </ul> |

## PM Instance and Data Planning

The following describes how to configure PM on a fiber to the mobile base station (FTTM) network.

**Figure 5-42** LM on an FTTM network



Assume that mobile services in **Figure 5-42** are transmitted upstream through the NXED board on the OLT. If maintenance engineers need to perform an LM test on

NodeB 1's voice services on an FTTM network, deploy the MEPs on the MDU user port and the OLT upstream port as shown in [Figure 5-42](#). The MEP on the OLT functions as the originating end, and the MEP on the MDU functions as the responding end. The following table lists the data planning.

| Item        | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MEP         | <p>The MEP ID and the port where the MEP is configured are shown in <a href="#">Figure 5-42</a>.</p> <p>MEP level: 0</p> <p>VLAN planning of the MEP: N:1 VLAN (as listed in the following)</p> <ul style="list-style-type: none"><li>• Customer VLANs (C-VLANs) are used to differentiate between upstream service flows of a NodeB.</li><li>• The MDU translates C-VLANs to service VLANs (S-VLANs). Packets of the same type are transmitted upstream through the same S-VLAN. S-VLAN 100 is intended for data services, while S-VLAN 200 is intended for voice services.</li><li>• The OLT transparently transmits VLANs.</li></ul>                                                                                                                        |
| PM instance | <p>Test ID planning:</p> <ul style="list-style-type: none"><li>• Data services: test ID 100</li><li>• Voice services: test ID 200</li></ul> <p>QoS planning: The MDU and OLT copy the priority of user-side packets as the priority of upstream packets, and copy the priority of network-side packets as the priority of downstream packets.</p> <ul style="list-style-type: none"><li>• Data services: The priority of upstream packets is 0 and that of downstream packets is 1.</li><li>• Voice services: The priority of both upstream and downstream packets is 5.</li></ul> <p>Onward MAC and backward MAC: The device randomly chooses the source MAC addresses of the service packets sent from a NodeB as the onward and backward MAC addresses.</p> |
| PM task     | <p>The Ethernet protocol packets used for an LM test are sent every 1s and for 4 times.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Procedure

### Step 1 Configure MEPs.

MDU configurations:

```
MDU (config) #cfm md 0 name-format no-name level 0
MDU (config) #cfm ma 0/1 name-format icc-based FTTM_VOICE
MDU (config) #cfm ma 0/1 vlan 200
MDU (config) #cfm ma 0/1 meplist 1
MDU (config) #cfm ma 0/1 meplist 2
MDU (config) #cfm mep 0/1/2 direction up port 0/2/0 vlantag1 200
```

OLT configurations:

```
OLT(config)#cfm md 0 name-format no-name level 0
OLT(config)#cfm ma 0/1 name-format icc-based FTTM_VOICE
OLT(config)#cfm ma 0/1 vlan 200
OLT(config)#cfm ma 0/1 meplist 1
OLT(config)#cfm ma 0/1 meplist 2
OLT(config)#cfm mep 0/1/1 direction up port 0/1/0 vlantag1 200
```

## Step 2 Configure PM instances.

MDU configurations:

```
MDU(config)#pm instance test-id 200 mep 0/1/2 remote-mep 1 receive-8021p 5 send-8021p 5 update-backward-mac
```

OLT configurations:

```
OLT(config)#pm instance test-id 200 mep 0/1/1 remote-mep 2 receive-8021p 5 send-8021p 5 update-onward-mac
```

## Step 3 Start a PM task and obtain the test results.

MDU configurations:

```
MDU(config)#pm lm receive single-ended test-id 200
```

OLT configurations:

```
OLT(config)#pm lm send single-ended test-id 200 interval 1000 count 4
```

Command:

```
pm lm send single-ended test-id 100 interval 1000 count 4
Press CTRL_C to break
```

| Index | Near-loss<br>ratio | Near-loss | Far-loss<br>ratio | Far-loss | ERR |
|-------|--------------------|-----------|-------------------|----------|-----|
| 1     | 0                  | 0         | 8                 | 7407407  | 1   |
| 2     | 0                  | 0         | 100               | 1000000  | 0   |
| 3     | 8000               | 80000000  | 900               | 90000000 | 0   |

|                          |                                    |
|--------------------------|------------------------------------|
| Maximum near-loss : 8000 | Maximum near-loss ratio : 80000000 |
| Minimum near-loss : 0    | Minimum near-loss ratio : 0        |
| Average near-loss : 2666 | Average near-loss ratio : -        |
| Total near-loss : -      |                                    |
| Maximum far-loss : 900   | Maximum far-loss ratio : 90000000  |
| Minimum far-loss : 8     | Minimum far-loss ratio : 1000000   |
| Average far-loss : 336   | Average far-loss ratio : 9074540   |
| Total far-loss : 1008    |                                    |

Note:

Ratio unit: 10<sup>^</sup>(-8)

ERR:

0: No error

1: Statistics for single-ended LM are incorrect

2: Statistics for average single-ended LM ratio are incorrect

3: Statistics for two-way DM are incorrect

4: A value exceeds the threshold and therefore a reverse occurs

## Step 4 Stop a PM task.

In this test, the PM task is completed on the originating end. Maintenance engineers only need to run the following command to stop the PM task on the responding end. MDU configurations:

```
MDU(config)#undo pm lm receive single-ended test-id 200
```

----End

## Result

The LM test result (including the number of lost packets on the local and remote ends and packet loss rate) will be displayed on the CLI, as listed in step 3. ITU-T Y.1731 provides the detailed explanation about the parameters in the test results.

## Follow-up Procedure

Maintenance engineers diagnose whether the link between the 2 MEPs is faulty based on the test results.