

19 Device Management

This topic covers the overview, general specifications, availability, and sub-features of device management security.

19.1 ANCP

The Access Node Control Protocol (ANCP) is used by the broadband network gateway (BNG) to manage the line parameters (including QoS and user) of the access node (AN).

19.2 ANCP Proxy

In ANCP proxy networking, an ANCP proxy device is located between the broadband network gateway (BNG) and access network (AN) device. This ANCP proxy device is responsible for proxy forwarding of ANCP packets exchanged between the BNG and AN device.

19.3 LLDP

Link Layer Discovery Protocol (LLDP) is a standard link layer discovery mode defined in IEEE 802.1ab. LLDP deployed on multi-vendor devices that are running in different networks and managed by the network management system (NMS) enables adjacent network devices to exchange device information with each other. By accessing the device information, the NMS obtains detailed information, such as topology of the whole network and physical connections between devices, in real time. As such, LLDP helps users monitor network status and locate network faults.

19.4 NETCONF

Network Configuration Protocol (NETCONF) is a network configuration and management protocol based on Extensible Markup Language (XML). NETCONF enables the network management system (NMS) to quickly configure and manage remote devices.

19.5 Telemetry

Telemetry is a remote measuring technology that can remotely collect data from physical or virtual devices at a high speed. The Telemetry feature provides real-time and high-speed data collection and improves the device and network usage during data collection.

19.6 Inband Management VPN

Inband management VPN is a means by which carriers use the virtual private network (VPN) to manage and maintain devices and the management protocol on the device can use virtual routers for route forwarding.

[19.7 Remote Software Commissioning \(Ethernet\)](#)

This section describes the implementation principles and configuration of remote software commissioning using Ethernet upstream transmission.

[19.8 OLT ZTD](#)

[19.9 Power Saving](#)

[19.10 Version and Data Management](#)

This topic provides an introduction to the version and data management feature, and describes the working principle of this sub feature.

[19.11 Anti-theft](#)

[19.12 Environment Monitoring](#)

This document describes the environment monitoring function of the MA5800 series products.

[19.13 RTU](#)

19.1 ANCP

The Access Node Control Protocol (ANCP) is used by the broadband network gateway (BNG) to manage the line parameters (including QoS and user) of the access node (AN).

19.1.1 ANCP Introduction

Definition

The Access Node Control Protocol (ANCP) is used by the broadband network gateway (BNG) to manage the line parameters (including QoS and user) of the access node (AN).

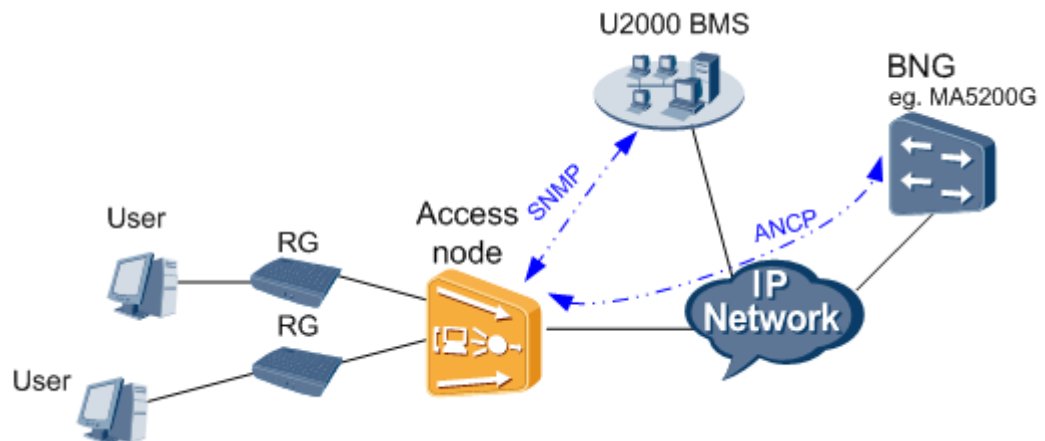
NOTE

A BNG can be a BRAS or a router, such as the MA5200G.

Figure 19-1 displays the NEs relevant to ANCP.

- The user powers on, disables, or connects the RG to change the line status.
- The BNG and the AN exchange ANCP messages.
- The network administrator manages the AN through the N2000 BMS by using SNMP.

Figure 19-1 ANCP network topology



Purpose

When ANCP is not used, if the BNG needs to manage the line parameters of an AN, the NMS is required. When the AN and the BNG use different NMSs, the line parameters are hard to be managed. Through ANCP, however, the BNG can directly manage such parameters without the NMS.

19.1.2 ANCP Principle

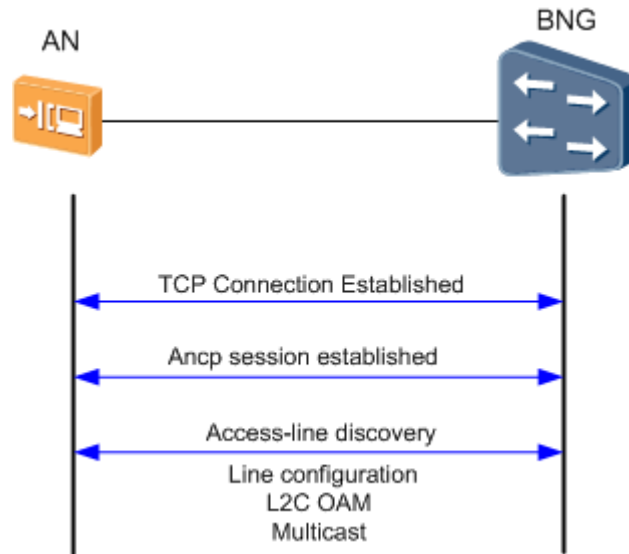
The ANCP supports the following functions:

- Line topology discovery
- L2C OAM
- Multiple partitions

Before the above-listed ANCP functions are implemented, an ANCP session needs to be set up between the BNG and the AN.

Setting Up an ANCP Session

[Figure 19-2](#) shows the process of setting up an ANCP session and negotiating the capabilities between the AN and the BNG.

Figure 19-2 Setting up an ANCP session

The process of setting up an ANCP session is as follows:

1. On the AN side, pre-configure the ANCP session IP address and TCP port ID of the BNG and enable ANCP through the CLI. Then, the AN actively sends a request to the BNG for establishing a TCP connection (the BNG is the server and the AN is the client).
2. After the TCP connection is successfully established, adjacency is formed between the AN and the corresponding BNG. After the capabilities are negotiated, the ANCP session is successfully set up. If the local end finds that the remote end does not support a certain capability, the local end disables this capability and negotiates with the remote end again until both ends have negotiated the capabilities supported by both ends.
3. Configure capability parameters. By default, the AN currently supports the capabilities of line topology discovery, line configuration, and L2C OAM. Multicast and unicast CAC can be added to the capabilities through configuration.

After the adjacency is set up, the ANCP protocol enters the maintaining stage. The AN handshakes with the BNG through the ACK message. The interval is the timeout time contained in the message exchanged during the adjacency setup process. If the AN does not receive the ACK message when the timeout time provided by the BNG expires for three times, the session between the AN and the BNG fails. The AN will then reset the adjacency and initiate a connection again.

Line Topology Discovery

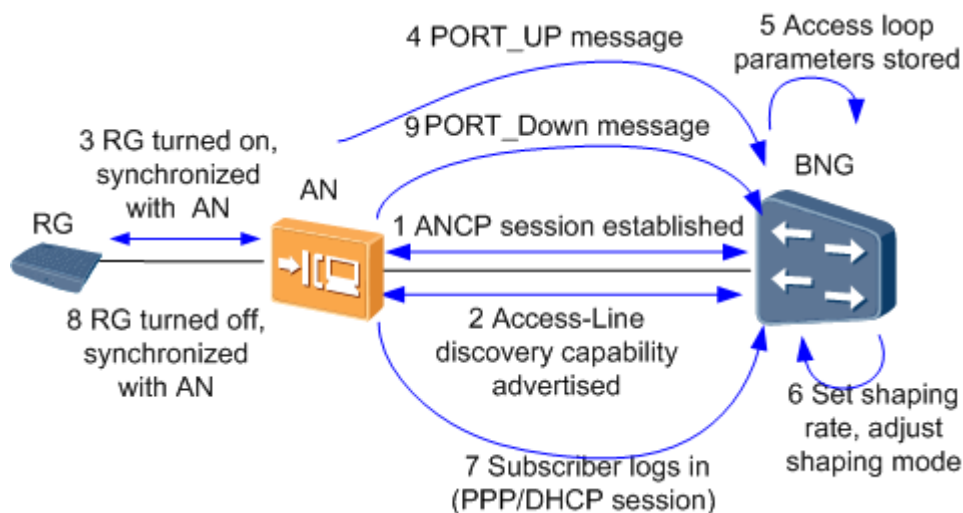
The BNG records the actual parameter information about user ports through line topology discovery and thus implements QoS control.

After a line is activated and the port rate stabilizes, the ANCP module of the AN queries the parameters (such as upstream/downstream activation rate) of the line and sends the port up message and line parameter information to the BNG. After

receiving the line information, the BNG saves the information to local and creates mapping to QoS control policies.

After the port is deactivated, the ANCP module sends the port down message to the BNG, as shown in [Figure 19-3](#).

Figure 19-3 Line topology discovery



[Table 19-1](#) lists the line parameters reported by the ANCP module.

Table 19-1 Reported line parameters

No.	Parameter
1	CID
2	RID
3	AGG-CID-ASCII
4	AGG-CID-BINARY
5	Actual-Net-Data-Rate-Upstream
6	Actual-Net-Data-Rate-Downstream
7	Line-State
8	Encapsulation
9	DSL Type

The port up or port down message is uniquely identified by the line ID. The format of the ANCP line ID is configurable. It is recommended to set the format of the ANCP line ID to be consistent with that of DHCP option 82 and PPPoE+ messages. At the same time, the format of the ANCP line ID must be the same as that on the BNG because the BNG creates mapping between user and line according to line ID and user name.

The ANCP module can report the port up or port down message in two modes: based on port or based on service stream.

- In the port-based mode, if SPLABEL (configured by running the **raio-format** command) is not configured in the line ID, the following information is reported when the port is up or down:
 - Message in the default format (VPI=0, VCI=32) if the PVC or CVLAN is not specified
 - Specified value if the PVC or CVLAN specified exists
- If the port-based mode, if SPLABEL (configured by running the **raio-format** command) is configured in the line ID, the following situations occur when the port is up or down:
 - The topology information is not reported if the PVC or CVLAN specified does not exist.
 - The specified value is reported if the PVC or CVLAN specified exists.
- In the service-stream-based mode, when a port goes up or down, messages are reported for all service streams of the port. When the status of a service stream changes, a message is reported for this service stream.

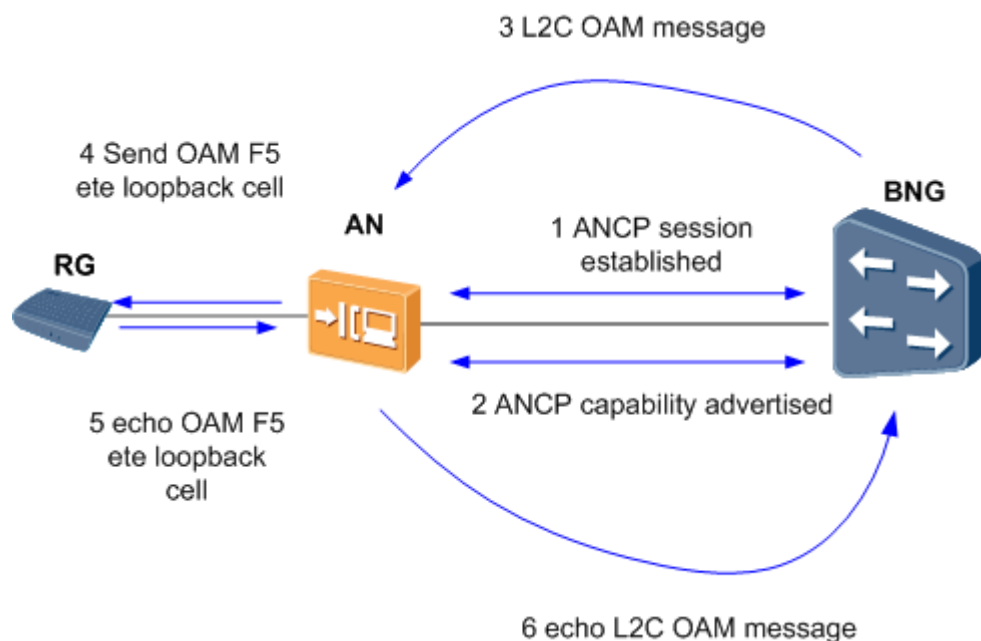
After the ANCP session fails and is re-established, the AN reports the stable line parameters and port status information, such as port UP or port DOWN, to the BNG.

L2C OAM

The ANCP L2C OAM function can implement the connectivity test between the BNG and the RG.

The implementation of the L2C OAM function mainly involves the RG, AN, and BNG, as shown in [Figure 19-4](#).

Figure 19-4 L2C OAM



L2C OAM implementation process:

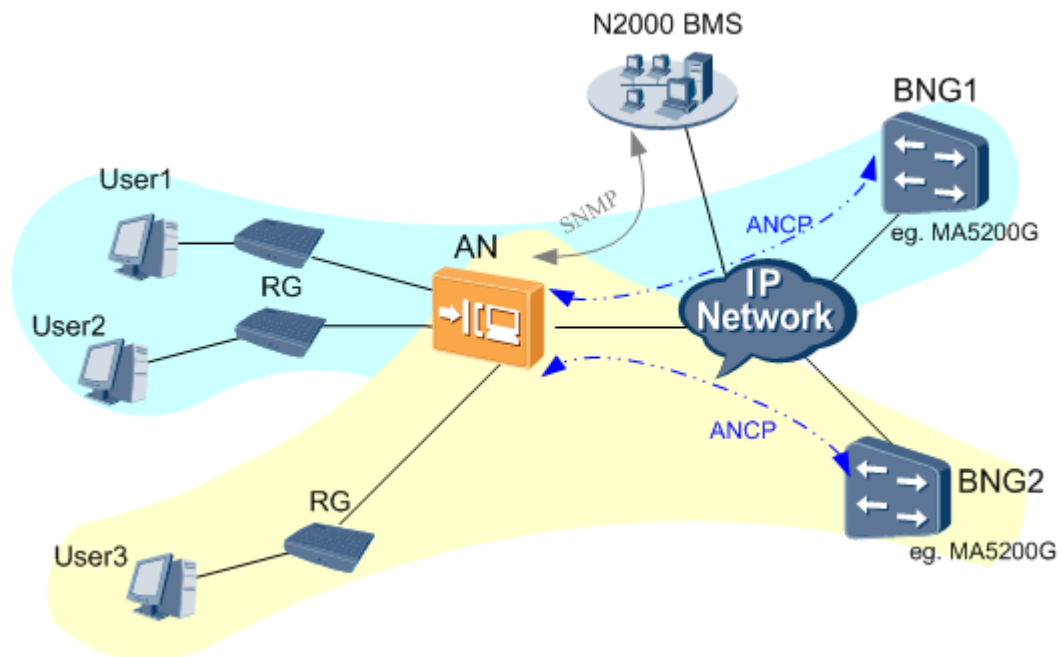
The AN sends response messages to the BNG according to the port status. If the port is up, the AN responds with a success message; if the port is down, the AN responds with a failure message.

Multiple Partitions

The ANCP multiple partitioning function enables different user ports to be grouped in different ANCP partitions. Different partitions are managed by different BNGs in order to support wholesale service. Generally, each BNG is managed by a respective ISP. One user port can belong to only one partition.

As shown in [Figure 19-5](#), user 1 and user 2 are managed by BNG 1, and user 3 by BNG 2. In other words, user 1 and user 2 belong to the same partition, and user 3 belongs to a different partition.

Figure 19-5 Network topology of ANCP with multiple partitions



19.1.3 Configuring ANCP

Access Node Control Protocol (ANCP) is used to implement the functions such as topology discovery, line configuration, and L2C OAM on the user ports. The MA5800 establishes an ANCP session according to the GSMP communication IP address configured in the network access server (NAS).

Prerequisites

- The system must work in the normal state.

- The system must be connected to the network access server in the normal state.

Context

- The MA5800 and the NAS use a TCP connection to carry an ANCP session. Therefore, before creating an ANCP session, you must create a TCP connection between the MA5800 and the NAS. The NAS functions as the server of the TCP connection, and the MA5800 functions as the client.
- After the TCP connection is created successfully between the MA5800 and the NAS, an ANCP session is created between the MA5800 and the NAS. After the ANCP session is created successfully, the MA5800 and the NAS need to use the ANCP ACK packets for heartbeat detection to maintain the ANCP session.
- The default values of the ANCP parameters are as follows:
 - GSMP address for an ANCP session: 0.0.0.0
 - ANCP session capability set: topology-discovery, line-config, and oam
 - ANCP packet sending priority: 6
 - GSMP TCP communication port number on the NAS side in an ANCP session: 6068
 - Interval for sending packets during the initial stage of an ANCP session: 10 (unit: 0.1s)
 - Interval for sending packets during the ANCP session stage: 250 (unit: 0.1s)

Procedure

Step 1 Run the **ancp partition enable** command to enable the ANCP partition function.

By default, the ANCP partition function is disabled.

Step 2 Run the **ancp port** command to enable the ANCP function of a port.

The ANCP function takes effect only when the ANCP function in the ANCP session mode and ANCP session function of a port are enabled.

Step 3 (Optional) Run the **ancp version** command to configure the ANCP version.

- The configured ANCP version must be the same as that on the NAS.
- By default, the ANCP version is draft-01.

Step 4 (Optional) Run the **raio-format ancp aggregation-circuit-id** command to customize the character string format for Access-Aggregation-Circuit-ID-ASCII TLV of the ANCP message.

NOTE

The system supports to customize the character string format for Access-Aggregation-Circuit-ID-ASCII TLV of the ANCP message only when the ANCP version is RFC6320.

Step 5 Run the **ancp session** command to create the ANCP session.

Step 6 (Optional) Run the **ancp partition** command to configure the ID of the partition associated with an ANCP session.

Step 7 Run the **ancp ip** command to configure the GSMP communication IP address for the ANCP session.

- The IP address configured here must be the same as the GSMP communication IP address configured on the NAS, but it should not be the same as the default IP address, multicast IP address, or broadcast IP address.
- When an ANCP session is enabled, the GSMP communication IP address of the NAS cannot be configured.

Step 8 (Optional) Run the **ancp capability** command to configure the capability set of the ANCP session.

- Supports topology discovery. When you select **topology-discovery** parameter, the MA5800 automatically reports the line parameters to the NAS.
- Supports line configuration. When you select **line-config** parameter, the MA5800 responds to the line configuration that is sent by the NAS.
- Supports the OAM. When you select **oam** parameter, the MA5800 responds to the line testing information that is sent by the NAS.
- Supports the preceding three types of capability.
- The default value is all, that is, the three capabilities (topology discovery, line configuration, and L2C OAM) are supported.

 NOTE

When the ANCP version is RFC6320, the system supports only topology-discovery, and does not support line-config or oam.

Step 9 (Optional) Run the **ancp ancp-8021p** command to set the priority for sending ANCP packets.

- After an ANCP session is enabled, the priority for sending the ANCP packet of the ANCP session cannot be configured.
- You can set the priority according to the actual requirements and network conditions, the higher the priority, the higher the reliability.

Step 10 (Optional) Run the **ancp nas-tcp-port** command to set the GSMP TCP communication port number for the ANCP session on the NAS.

- By default, the GSMP TCP communication port number is 6068.
- The GSMP TCP communication port number on the MA5800 must be the same as that on the NAS.
- Run the **ancp port begin** command to set the start port ID of the ANCP session. Make sure that the start port ID of the ANCP session is the same as the start ID of the ports on the service board. The default value is 0.

Step 11 (Optional) Run the **ancp init-interval** command to set the interval for sending packets during the establishment of the ANCP session.

- By default, the general query interval is 1s.
- After an ANCP session is enabled, the priority for sending the ANCP packet of the ANCP session cannot be configured.

Step 12 (Optional) Run the **ancp keep-alive** command to set the interval for sending packets during the ACNP session so that the handshake messages can be sent to the peer end at the preset interval.

- After an ANCP session is enabled, the priority for sending the ANCP packet of the ANCP session cannot be configured.
- By default, the interval is 10s.

Step 13 Run the **ancp enable** command to enable the ANCP session.

- Before an ANCP session is enabled, related parameters can be modified. After an ANCP session is enabled, related parameters cannot be modified.
- By default, the ANCP session is disabled.

Step 14 Run the **quit** command to quit the ANCP session mode.

Step 15 Run the **display ancp session** command to query the information about the ANCP session.

----End

Example

Consider configuring the ANCP topology discovery function of port 0/3/1 as an example. Configure the partition ID of the ANCP session to 1, ANCP version to rfc6320, the character string format for Access-Aggregation-Circuit-ID-ASCII TLV of the ANCP message is innervlanid and outervlanid, start port ID to 1, GSMP communication address of the ANCP session to 10.10.10.10, packet sending interval at the ANCP session creation phase to 2s, ANCP session capability set to topology-discovery, ANCP packet sending priority to 7, GSMP TCP communication port ID at the NSA side in the ANCP session to 6000, and packet sending interval at the ANCP session phase to 7s.

```
huawei(config)#ancp partition enable
huawei(config)#ancp port 0/3/1 partition 1
huawei(config)#ancp version rfc6320.
huawei(config)#raio-format ancp aggregation-circuit-id innervlanid.outervlanid
huawei(config)#ancp port begin 1
huawei(config)#ancp session 1
huawei(config-session-1)#ancp partition 1
huawei(config-session-1)#ancp ip 10.10.10.10
huawei(config-session-1)#ancp capability topology-discovery
huawei(config-session-1)#ancp ancp-8021p 7
huawei(config-session-1)#ancp nas-tcp-port 6000
huawei(config-session-1)#ancp init-interval 20
huawei(config-session-1)#ancp keep-alive 70
huawei(config-session-1)#ancp enable
huawei(config-session-1)#quit
huawei(config)#display ancp session 1
```

```
Session config status      : Enable
Session running status    : Before syn phase
Session diagnostic status  : -
GSMP version              : 3
GSMP sub version          : 1
AN name                   : -
NAS name                  : -
NAS IP                    : 10.10.10.10
Local IP                  : -
AN instance               : -
NAS instance              : -
Config capabilities       : TopologyDiscovery
Negotiate capabilities    : -
NAS TCP port              : 6000
Startup time(0.01s)      : -
Discontinuity time(0.01s) : -
Init interval(0.1s)      : 20
Keepalive interval(0.1s) : 70
PartitionID               : 1
Line config roll default  : Disable
OAM threshold(0.01)      : 100
Topology report shaper interval(0.1s) : 10
S-VLAN                    : -
```

S-VLAN priority	: 7
C-VLAN	: -
C-VLAN priority	: -
Session down send trap status	: Disable
Session up send trap status	: Disable

19.1.4 ANCP Reference Standards and Protocols

- draft-ooghe-ancp-framework-00
- draft-wadhwa-gsmp-l2control-configuration-00
- draft-wadhwa-gsmp-l2control-configuration-01
- draft-wadhwa-gsmp-l2control-configuration-02
- draft-decnodder-ancp-mib-an-01
- RFC3292
- RFC3293

19.2 ANCP Proxy

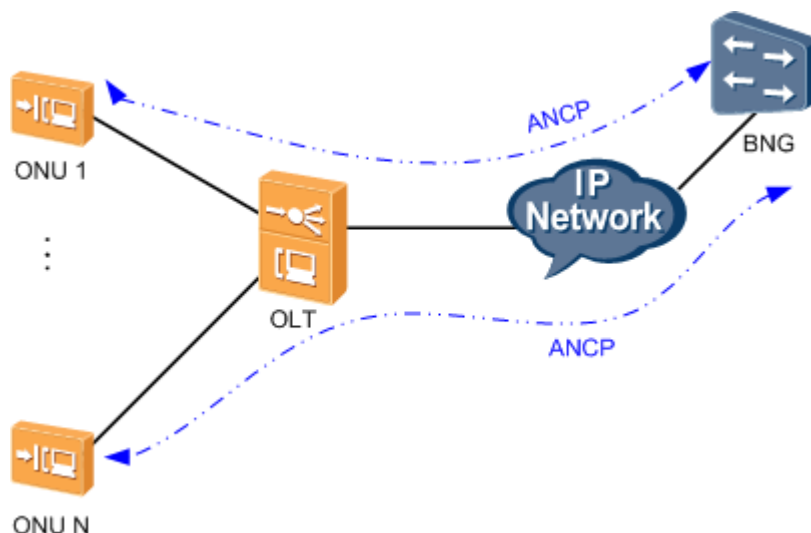
In ANCP proxy networking, an ANCP proxy device is located between the broadband network gateway (BNG) and access network (AN) device. This ANCP proxy device is responsible for proxy forwarding of ANCP packets exchanged between the BNG and AN device.

19.2.1 ANCP Proxy Introduction

Definition

In ANCP proxy networking, an ANCP proxy device is located between the broadband network gateway (BNG) and access network (AN) device. This ANCP proxy device is responsible for proxy forwarding of ANCP packets exchanged between the BNG and AN device.

According to the standard Access Node Control Protocol (ANCP), a BNG needs to set up an ANCP session with every ONU. [Figure 19-6](#) shows a standard ANCP networking.

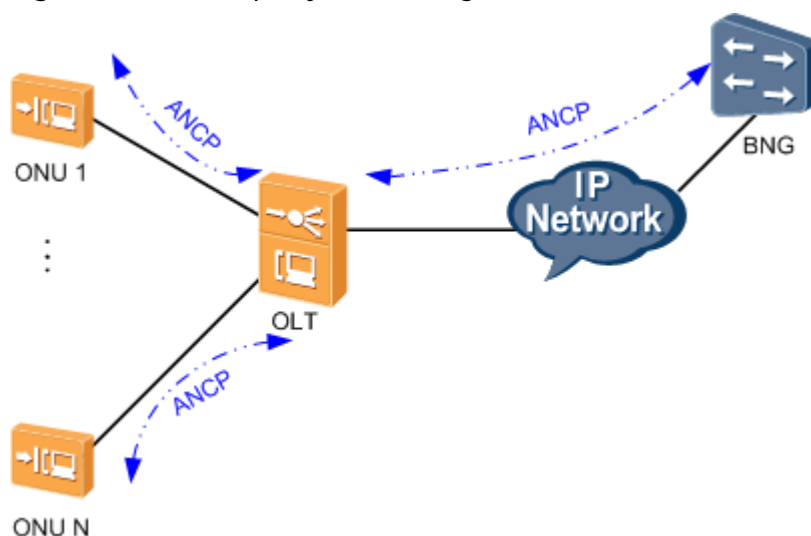
Figure 19-6 ANCP networking

Purpose

ANCP sessions require period handshaking and TCP connections in ANCP sessions occupy memory resources. If lots of ONUs are deployed in an ANCP proxy network, ANCP sessions consume lots of BNG resources.

In an ANCP proxy network, the OLT functions as an ANCP proxy and ONU functions as an AN device. In this network, the BNG sets up an ANCP session with the ANCP proxy, and the ANCP proxy then sets up ANCP sessions with AN devices. In this case, the OLT converges the number of ANCP sessions, reducing the number of ANCP sessions on the BNG.

Figure 19-7 shows ANCP proxy networking.

Figure 19-7 ANCP proxy networking

19.2.2 ANCP Proxy Principle

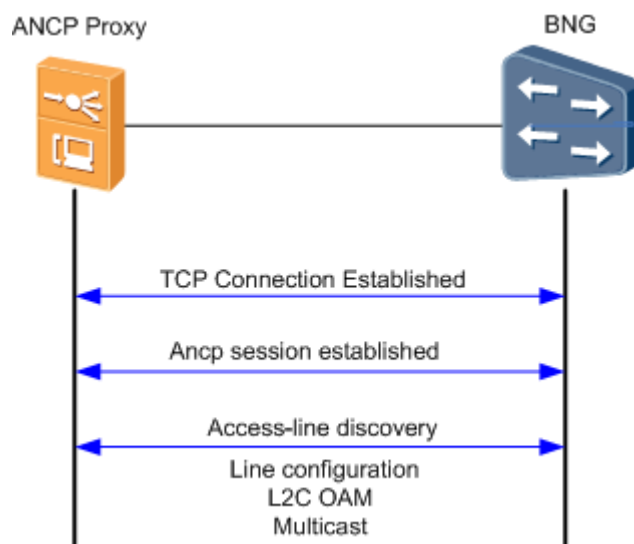
ANCP proxy is implemented by the following:

- Setting up a main ANCP session
- Setting up a sub ANCP session
- Setting up mapping between the main ANCP session and sub ANCP session
- Forwarding ANCP packets by proxy

Setting Up a Main ANCP Session

An ANCP session between the broadband network gateway (BNG) and ANCP proxy, that is, between OLTs, is called a main session. In the main ANCP session, ANCP proxy functions as the ANCP client. The main ANCP session negotiates capability sets between the BNG and ANCP proxy, as shown in [Figure 19-8](#).

Figure 19-8 Setting up an ANCP session



The process of setting up a main ANCP session is as follows:

1. On ANCP proxy, pre-configure the ANCP session IP address and TCP port ID of the BNG and enable ANCP through the CLI. Then, the AN actively sends a request to the BNG for establishing a TCP connection (the BNG is the server and the ANCP proxy is the client).
2. After a TCP connection is set up, ANCP proxy establishes adjacency with the corresponding BNG. After capability set negotiation, an ANCP session is set up successfully. If the peer end does not support a capability, the local end accordingly disables the same capability. This process continues till both ends have the same capability set.
3. Configure capability set parameters. By default, ANCP proxy currently supports the capability set of line topology discovery, line configuration, and L2C OAM.

After the adjacency is set up, the ANCP protocol enters the maintaining stage. The AN handshakes with the BNG through the ACK message. The interval is the

timeout time contained in the message exchanged during the adjacency setup process. If ANCP proxy does not receive the ACK message when the timeout time provided by the BNG expires for three times, the session between ANCP proxy and BNG fails. ANCP proxy will then reset the adjacency and initiate a connection again.

Setting Up a Sub ANCP Session

ANCP sessions between ANCP proxy and ONUs, that is, between the OLT and ANs, are sub ANCP sessions. In the main ANCP session, ANCP proxy functions as the ANCP client. When ANCP proxy and AN devices set up sub ANCP sessions, they negotiate about the capability set and ANCP partition ID on the AN device. The setup process of sub ANCP sessions is the same as that of the main ANCP session.

Only after the main ANCP session is set up can corresponding sub ANCP sessions be set up.

Setting Up Mapping Between the Main ANCP Session and Sub ANCP Session

ANCP proxy is used for establishing 1:N relationship between the main ANCP session and sub ANCP sessions so that the number of sessions can be reduced. Therefore, rules for mapping between the main ANCP session and sub ANCP sessions must be defined.

In mapping rules, the main ANCP session ID directly uses the existing ANCP session ID, and sub ANCP session IDs use AN IP addresses + partition IDs.

Forwarding ANCP Packets by Proxy

Proxy forwarding consists of the following 3 parts:

- Determination on upstream ANCP packet forwarding
- Determination on downstream ANCP packet forwarding
- Modification on ANCP packets

Determination on upstream ANCP packet forwarding

The main ANCP session has a 1:N relationship with sub ANCP sessions. After ANCP proxy receives upstream ANCP packets from a sub ANCP session, the unique main ANCP session can be determined. Then, ANCP packets are sent through this main session.

Determination on downstream ANCP packet forwarding

The main ANCP session has a 1:N relationship with sub ANCP sessions. After ANCP proxy receives downstream ANCP packets from the BNG, these packets can be forwarded according to other forwarding conditions.

- After receiving upstream ANCP packets, ANCP proxy extracts the AN ID (CID AN ID) from the packets and records the AN ID.
- After receiving downstream ANCP packets, ANCP proxy extracts the AN ID (CID AN ID) from the packets, and locates the corresponding sub ANCP session according to the AN ID and main session ID. Then, ANCP proxy sends these downstream ANCP packets.

Modification on ANCP packets

The main ANCP session and sub ANCP sessions may have different partitions. Therefore, the Partition ID field needs to be modified for ANCP packet forwarding.

- For upstream ANCP packets, the Partition ID is modified to the partition ID.
- For downstream ANCP packets, the Partition ID is modified to the partition ID.

19.2.3 Configuring ANCP Proxy

Prerequisites

- The system must work in the normal state.
- The system must be connected to the network access server in the normal state.

Context

- ANCP proxy configuration requires main ANCP session configuration and sub ANCP session configuration. Before sub ANCP session configuration, the main ANCP session must be configured. For details about main ANCP session configuration, see [19.1.3 Configuring ANCP](#). This topic describes how to configure a sub ANCP session.
- The MA5800 and the AN (ONU) use a TCP connection to carry an ANCP session. Therefore, before creating an ANCP session, you must create a TCP connection between the MA5800 and the AN. The MA5800 functions as the server of the TCP connection, and the AN functions as the client.
- After the TCP connection is created successfully between the MA5800 and the AN, an ANCP session is created between the MA5800 and the AN. After the ANCP session is created successfully, the MA5800 and the AN need to use the ANCP ACK packets for heartbeat detection to maintain the ANCP session.
- The default values of the ANCP parameters are as follows:
 - GSMP address for an ANCP sub session: 0.0.0.0
 - In an ANCP sub-session, the TCP communication port listened by the ANCP proxy is port 6068.
 - Interval for sending packets during the initial phase of an ANCP sub session: 10 (unit: 0.1s)
 - Interval for sending packets during the ANCP session phase: 250 (unit: 0.1s)

Procedure

Step 1 Run the **sysman server source ancp-proxy** command to bind a specified source port to the ANCP-Proxy service protocol.

 **NOTE**

Step 2 Run the **ancp proxy** command to enable ANCP Proxy function.

Step 3 (Optional) Run the **ancp tcp-listen-port** command to configure the number of the TCP communication port listened by the ANCP proxy in the ANCP sub-session.

- The default value is 6068.

- Step 4** Run the **ancp sub-session** command to create the ANCP sub session.
- Step 5** Run the **ancp partition** command to configure the ID of the partition associated with an ANCP sub session.
- Step 6** Run the **ancp ip** command to configure the IP address for the ANCP sub session.
- The IP address configured here must be the same as the AN GSMP communication address, but it must not be the default IP address, multicast IP address, or broadcast IP address.
 - When a session is enabled, the AN GSMP communication address cannot be configured.
- Step 7** (Optional) Run the **ancp init-interval** command to set the interval for sending packets during the establishment of the ANCP sub session.
- The default value is 10s.
 - After an ANCP sub session is enabled, the priority for sending the ANCP packet of the ANCP sub session cannot be configured.
- Step 8** (Optional) Run the **ancp keep-alive** command to set the interval for sending packets during the ANCP sub session so that the handshake messages can be sent to the peer end at the preset interval.
- The default value is 250s.
 - After an ANCP sub session is enabled, the priority for sending the ANCP packet of the ANCP sub session cannot be configured.
- Step 9** Run the **ancp_session** command to configure the ANCP session associated with an ANCP sub-session.
- Step 10** Run the **ancp enable** command to enable an ANCP sub session.
- Before an ANCP sub session is enabled, related parameters can be modified. After enabling, related parameters cannot be modified.
 - The default value is disabled.
- Step 11** Run the **quit** command to quit the ANCP sub-session mode.
- Step 12** Run the **display ancp sub-session** command to query the information about the ANCP sub session.
- End

Example

Example:

- Bind the ANCP proxy service protocol to a specified source port. Set the port type to loopback and the port index to 1.
- Configure an ANCP sub-session. Set the number of the TCP communication port listened by the ANCP proxy function to 6000, ID of the ANCP sub-session to 1, ID of the associated partition to 1, GSMP communication address of the ANCP session to 10.10.10.10, interval for sending packets in the ANCP session establishment phase to 2s, interval for sending packets in the ANCP session phase to 7s, and ID of the associated main ANCP session to 1.

```
huawei#sysman server source ancp-proxy loopback 1
huawei(config)#ancp proxy enable
```

```
huawei(config)#anclp tcp-listen-port 6000
huawei(config)#anclp sub-session 1
huawei(config-sub-session-1)#anclp partition 1
huawei(config-sub-session-1)#anclp ip 10.10.10.10
huawei(config-sub-session-1)#anclp init-interval 20
huawei(config-sub-session-1)#anclp keep-alive 70
huawei(config-sub-session-1)#anclp session 1
huawei(config-sub-session-1)#anclp enable
huawei(config-sub-session-1)#quit
huawei(config)#display anclp sub-session 1
```

19.3 LLDP

Link Layer Discovery Protocol (LLDP) is a standard link layer discovery mode defined in IEEE 802.1ab. LLDP deployed on multi-vendor devices that are running in different networks and managed by the network management system (NMS) enables adjacent network devices to exchange device information with each other. By accessing the device information, the NMS obtains detailed information, such as topology of the whole network and physical connections between devices, in real time. As such, LLDP helps users monitor network status and locate network faults.

19.3.1 Introduction

This topic describes the background and application values of LLDP.

As large-scale networking requirements keep emerging, a network is involving an increasingly large number of device types, each device having its own complicated configurations. In addition, higher requirements are posed on the NMS capabilities. For example, the NMS is required to automatically learn the topological status of connected devices, and to detect configuration conflicts between devices.

Most NMSs use the automated discovery function to follow network topology changes, but in this way the NMSs can analyse the topology to as deep as the network layer only. As such, operators can learn only the basic events, such as device addition or deletion, on a network, but cannot identify the specific location of a device. For example, operators cannot identify the ports through which a device connects to other devices. Though some vendors provide proprietary protocols for discovering adjacency between devices, there are still not sufficient means for generating the topology of an entire network.

LLDP well addresses the issues above. As a Layer 2 discovery protocol defined in IEEE 802.1ab, LLDP provides a standard link layer discovery method. Using this method, information such as the capabilities, management address, device ID, and port ID of a local device can be encapsulated in LLDP frames and transmitted to adjacent nodes. After receiving such information, the adjacent nodes save the information in a standard management information base (MIB), which can be queried by the NMS for determining the connectivity of links.

LLDP can precisely discover the ports of network devices and the interconnection between devices. By obtaining and integrating the LLDP local device information and neighbor device information on each network element (NE), the NMS can generate a clear topology of the entire network, along with detailed information such as the physical connections between devices. Such information helps network

operators monitor network status in real time and quickly locate network faults, effectively improving network security and stability.

19.3.2 LLDP Reference Standards and Protocols

This feature complies with the following standards and protocols:

- IEEE 802.1ab-2009
- IEEE 802.1ab-2005 (serves as the reference for the destination MAC address)

NOTE

IEEE 802.1ab-2009 provides a more complete definition of LLDP than IEEE 802.1ab-2005. Therefore, Huawei devices implement LLDP functions in compliance with IEEE 802.1ab-2009 by default. Specifically, LLDP IP addresses also comply with IEEE 802.1ab-2009.

19.3.3 Basic Concepts

This topic describes basic concepts related to the LLDP feature to help you better understand the working principles of LLDP.

LLDP MIB

MIB is a fundamental element for LLDP implementation. As defined in the LLDP protocol, each port on a device has four MIBs. Among them, the two most important MIBs are the LLDP local system MIB and the LLDP remote system MIB, which store the status information of the local device and the adjacent node, respectively. The status information includes device ID, port ID, system name, system description, port description, device capabilities, and network management address.

LLDP Agent

The LLDP protocol defines an LLDP agent for each port on a device for managing the LLDP operations regarding the device. The LLDP agent:

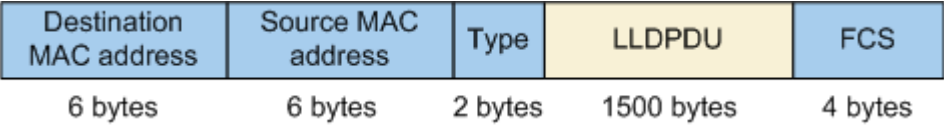
- Maintains the LLDP local system MIB information.
- Sends LLDP frames to the adjacent nodes, advertising the local system status information to the adjacent nodes.
- Recognizes and parses the LLDP frames sent from the adjacent nodes, and maintains the LLDP remote system MIB information.
- Sends LLDP alarms to the NMS when the LLDP local system MIB or LLDP remote system MIB information changes.

Compared with the IEEE 802.1ab-2009 specifications, Huawei's LLDP implementation supports one single port associated with one LLDP agent, but does not support one single port associated with multiple LLDP agents.

LLDP Frame

Ethernet frames in which LLDP data units (LLDPDUs) are encapsulated are called LLDP frames. The encapsulation has two formats: Ethernet II format and Subnetwork Access Protocol (SNAP) format. The MA5800 supports the Ethernet II encapsulation format. The following figure shows the structure of the LLDP frame encapsulated in this format.

Figure 19-9 LLDP frame structure



The following table explains the fields of the LLDP frame.

Field	Description
Destination MAC address	Set to a fixed multicast MAC address 0x0180-C200-000E, which is specified by IEEE 802.1ab-2005. The address is specified by IEEE 802.1ab-2005. Therefore, for the purpose of maximal compatibility (that is, considering all devices as common devices), the MA5800 uses 01-80-C2-00-00-0E as the destination MAC address. For the requirements of different types of devices on the reception and transmission of the destination MAC address, see IEEE 802.1ab-2009.
Source MAC address	The device MAC address serves as the source MAC address.
Type	Indicates the frame type, which is a fixed value 0x88CC.
LLDPDU	Indicates the LLDP data unit. LLDP information exchange is implemented through LLDPDUs.
FCS	Indicates the frame check sequence.

LLDPDU

LLDPDU is a data unit that is encapsulated in an LLDP frame. A device encapsulates the local information in the Type-Length-Value (TLV) format. Several such TLVs constitute an LLDPDU and are transmitted in an LLDP frame. Users can formulate LLDPDUs using different combinations of TLVs based on their requirements. Using these TLVs, the device advertises its status and learns the status of its adjacent nodes.

Figure 19-10 LLDPDU structure



The LLDP protocol stipulates four mandatory TLVs for an LLDPDU. Each LLDPDU must start with the Chassis ID TLV, Port ID TLV, and Time to Live TLV, and end with the End of LLDPDU TLV. Other TLVs are optional.

There are two types of LLDPDUs:

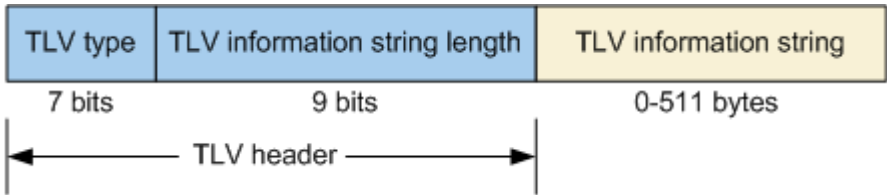
- Normal LLDPDU: contains the local device information and the adjacent node information.

- Shutdown LLDPDU: sent to disable the LLDP capability of a port. The shutdown LLDPDU is used to instruct the peer device to quickly clear the adjacent node information. The shutdown LLDPDU does not have optional TLVs, and the TTL TLV value is 0.

TLV

Indicating the type, length, and value of an object, TLV is the basic unit that forms an LLDPDU. Each TLV represents a type of device information, such as device ID, port ID, and management address, which correspond to fixed TLVs Chassis ID TLV, Port ID TLV, and Management Address TLV respectively.

Figure 19-11 TLV structure



LLDP supports two TLV formats: basic TLV and organizationally specific TLV. Organizationally specific TLVs include TLVs defined by 802.1 and 802.3, and may include more organizationally defined TLVs. The MA5800 supports only the basic TLV.

Table 19-2 TLV list

TLV Name	TLV Type	Description
End of LLDPDU TLV	0	Indicates the end of an LLDPDU.
Chassis ID TLV	1	Indicates the bridge MAC address of the device.
Port ID TLV	2	Indicates the name of the LLDPDU sending port. The value of this TLV uses the value of the ifName leaf of the IF-MIB.
Time To Live TLV	3	Indicates the time during which the local device information is valid on the adjacent node.
Port Description TLV	4	Indicates the port description. The value of this TLV uses the value of the ifDescr leaf in the iftable table of the IF-MIB.
System Name TLV	5	Indicates the device name, configurable using the sysname command.
System Description TLV	6	Indicates the device description, configurable using the system sys-info description command.

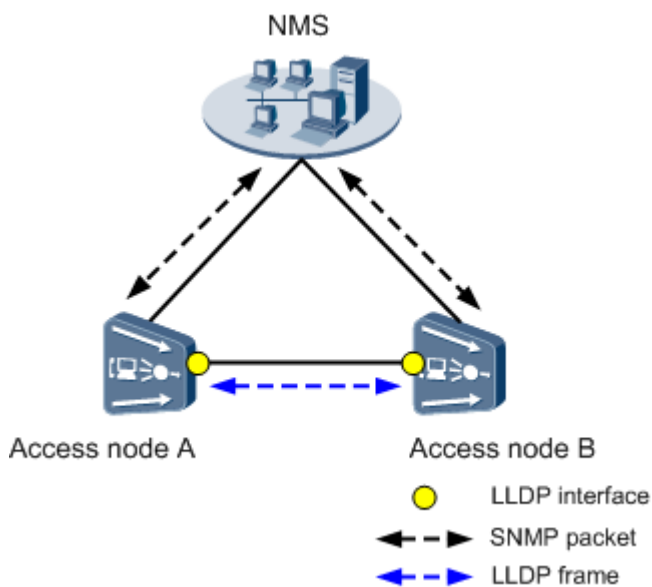
TLV Name	TLV Type	Description
System Capabilities TLV	7	Indicates the functions supported by the device and the functions that are enabled on the device.
Management Address TLV	8	Indicates the management address.
Reserved	9-126	Reserved for special application.
Organizationally Specific TLV	127	Each organization is represented by an organizationally unique identifier (OUI). For detailed description of this TLV and the OUI field, see the LLDP protocol.

19.3.4 Principles

Based on an LLDP basic network diagram, this topic describes how the NMS obtains device information and learns the network topology using the LLDP protocol.

LLDP Working Process

Figure 19-12 LLDP basic network diagram



As shown in the preceding figure, access node A and access node B support LLDP. The NMS collects device information in the following process:

1. Access node A encapsulates its local status information in an LLDP frame and sends the frame to its adjacent device, access node B.

2. Access node B receives and parses the LLDP frame, and stores the information about access node A in its LLDP remote system MIB. The information can be accessed by the NMS when the NMS extracts the topology information.
3. Similarly, access node B encapsulates its local status information in an LLDP frame and sends the frame to access node A.
4. Access node A receives and parses the LLDP frame, and stores the information about access node B in its LLDP remote system MIB. The information can be accessed by the NMS when the NMS extracts the topology information.
5. The NMS exchanges SNMP messages with access node A and access node B, and extracts the local device information and adjacent device information from their MIBs. By integrating and analyzing the information, the NMS discovers the topology of the whole network.

In the working process described above:

- To generate the topology of the entire network on the NMS, all devices managed by the NMS must support LLDP. LLDP is disabled on the MA5800 by default.
- Each device can discover the information about only the device that is directly connected to this device. Therefore, to generate a whole-network topology, the NMS needs to collect the local device information and adjacent device information reported by all devices on the network.

LLDP Port Working Modes

An LLDP port supports the following working modes:

- Tx/Rx: The port transmits and receives LLDP frames. This is the default mode on the MA5800.
- Tx: The port transmits but does not receive LLDP frames.
- Rx: The port receives but does not transmit LLDP frames.
- Disable: The port does not transmit or receive LLDP frames.

When the LLDP working mode of a port changes, the port initializes the protocol state machine. If the LLDP working mode of a port changes frequently, the port has to constantly perform re-initialization. To avoid this situation, the MA5800 supports configuration of a port initialization delay. A port performs re-initialization only when the delay expires after the port working mode changes.

LLDP Frame Transmission Mechanism

An LLDP-enabled device periodically transmits LLDP frames to its adjacent nodes. To make sure that it is detected by other devices as quickly as possible, the MA5800 supports a fast transmission mechanism. The MA5800 immediately transmits an LLDP frame in any of the following three conditions:

- The MA5800 discovers a new neighbor. In other words, the MA5800 receives a new LLDP frame and finds that the transmitting device information carried in the frame is not stored on the MA5800 yet.
- The LLDP status of the MA5800 changes from disabled to enabled.
- The port status of the MA5800 changes from Down to Up.

LLDP Frame Reception Mechanism

When receiving an LLDP frame, the device checks the validity of the frame and the TLV information carried in the frame. After the frame passes the validity check, the device stores the neighbor's information. According to the Time To Live (TLV) value carried in the LLDPDU, the device sets the aging time of the neighbor's information on this device. When receiving an LLDPDU whose Time To Live TLV value is 0, the device ages the information of the corresponding neighbor.

19.3.5 Network Application

The LLDP topology discovery function is usually used with the function of remote software commissioning (through GE upstream channel) to implement the plug-and-play (PnP) solution.

A general PnP solution is implemented in three steps:

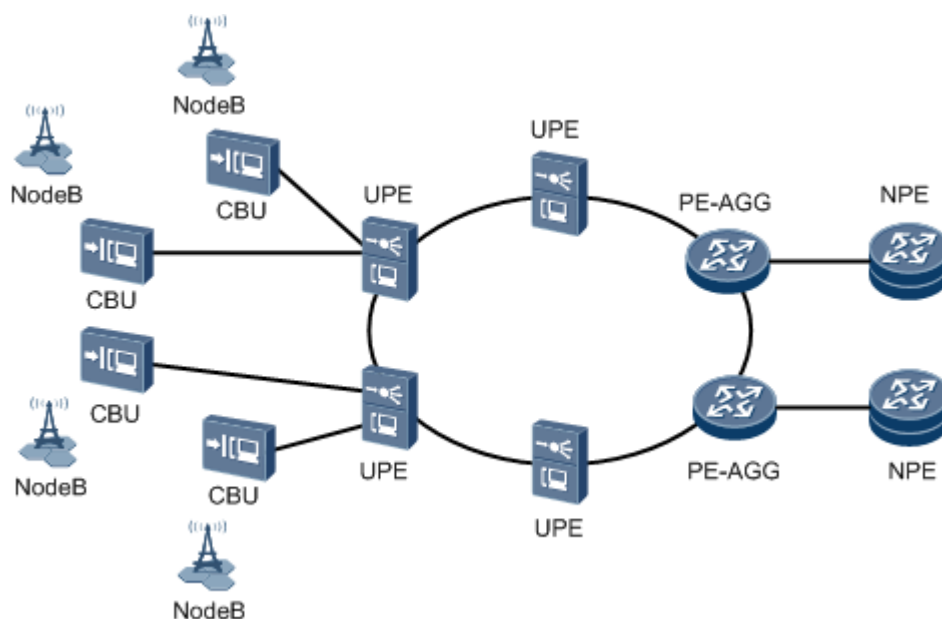
1. After a device (connected to the upstream through GE) is powered on, the device automatically obtains its IP address and management VLAN parameters. Such information is used for setting up the management channel for the device to enable remote management.
2. Service configurations of the device are automatically issued to the device; automatic upgrade of the device is pre-deployed.
3. The network topology is discovered on the NMS.

The first step is implemented using the function of remote software commissioning (through GE upstream channel). With this function, operators need not visit the sites to commission software, thereby reducing the costs for deploying a large number of devices. Steps 2 and 3 require coordination of the NMS. The LLDP function works with the NMS to implement step 3.

According to how the access device is connected to upstream devices, topology discovery of the access device includes the following scenarios.

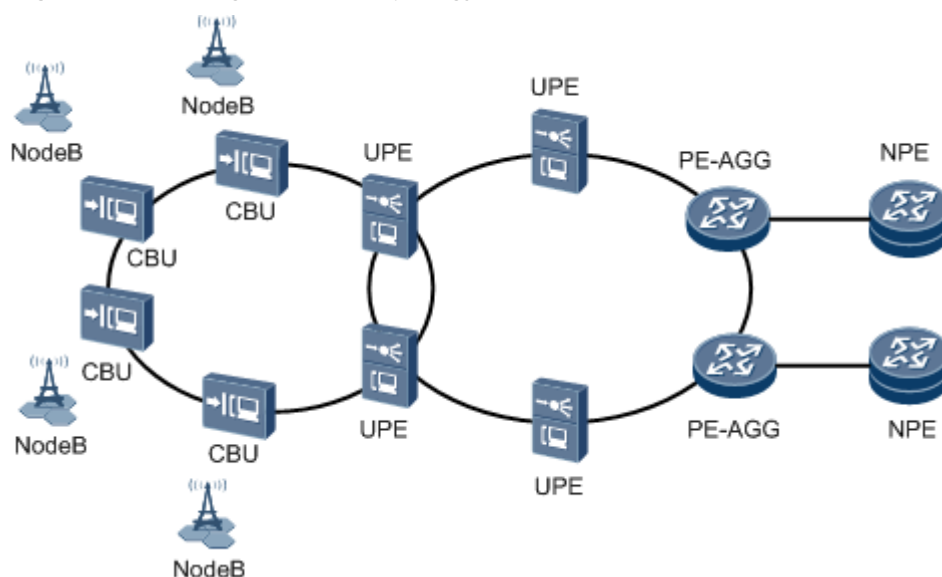
Point-to-Point Connection

As shown in [Figure 19-13](#), the access node MxU works as the CBU, and an OLT or a switch works as the UPE. The MxU connects to the upstream device through FE/GE. The IP address is obtained using DHCP, and the device location is identified by DHCP option 82. Specifically, DHCP relay or DHCP proxy is enabled on the upper-layer device, and the device reports the MxU location information to the NMS through DHCP option 82. The topology of this type of network can be discovered using LLDP.

Figure 19-13 Network of point-to-point connection

Ring or Chain Network Topology

For a network topology shown in [Figure 19-14](#), the device location cannot be identified using DHCP option 82. This is because DHCP option 82 does not apply to the scenario in which MxUs are cascaded. For such a network, LLDP can be used for topology discovery. Specifically, LLDP is used for discovering and creating the link topology information of adjacent devices. The NMS scans the link topology MIBs of all MxUs and their upper-layer devices, and builds the topology of the entire network. The location of an MxU can be identified through the connections between MxUs and their upper-layer devices. In this network scenario, the IP address is also obtained using DHCP. This network scenario applies to OLTs as well.

Figure 19-14 Ring network topology

19.3.6 Configuring LLDP

If you need to manage devices of different vendors and networks, you can configure Link Layer Discovery Protocol (LLDP) on all the devices to obtain the detailed information, such as connections between network topologies and devices. This section describes how to configure LLDP on one device.

Prerequisites

All devices on a network support LLDP so that the network topology can be set up on the NMS.

Procedure

Step 1 Run the **lldp enable** command to enable the global LLDP function.

Step 2 Run the **lldp enable port** command to enable the port LLDP function.

LLDP must be enabled on all ports that are connected to devices. All LLDP-related configurations take effect only when both global LLDP and port LLDP are enabled.

Step 3 Run the **lldp management address** command to configure the LLDP management address.

Generally, the interface IP address for NMS management is set as the LLDP management address so the management interface IP addresses of devices can be queried using the LLDP topology.

Step 4 (Optional) Configure LLDP parameters.

NOTE

You are advised to configure the same LLDP parameters on all devices.

- Run the **lldp message-transmission interval** command to configure the interval between sending LLDP notification packets.
- Run the **lldp message-transmission hold-multiplier** command to configure the message hold multiplier. The message hold multiplier is used to calculate the TTL value of a sent packet. The system compares 65535 with hold-value x interval-value + 1, the smaller one is used as the TTL value.
- Run the **lldp restart-delay** command to configure the delay for switching the global or port LLDP status. The delay controls the minimum interval for switching the global or port LLDP status so that the system burden does not increase due to frequently changes of the status.

Step 5 (Optional) Configure LLDP trap function.

- Run the **lldp trap enable** command to enable the LLDP trap sending function.
- Run the **lldp trap interval** command to configure the interval for a port enabled with Link Layer Discovery Protocol (LLDP) to send traps. After the interval is configured, the device will not send a large number of traps to trouble the NMS or subscribers.

Step 6 Query the LLDP information.

- Run the **display lldp local** command to query the local LLDP information, including the system information, LLDP configuration, number of remote neighbors, and ports enabled with LLDP.

- Run the **display lldp neighbor [port frameid/slotid/portid]** command to query the detailed neighbor information about the local device and port relationship between the neighbor device and local device.
- Run the **display lldp neighbor brief** command to query the brief neighbor information.
- Run the **display lldp statistics** command to query LLDP packet statistics.

Step 7 (Optional) Reset the LLDP information.

- Run the **reset lldp statistics** command to clear the packet statistics of all the ports or a specific port.
- Run the **clear lldp neighbor** command to clear the neighbor information about of all the ports or a specific port.

----End

Example

Set the management IP address to 10.10.10.2, set the interfaces connected to other devices to 0/9/0 and 0/9/1, use default values for other parameters. To configure LLDP and enable LLDP alarming, do as follows:

```
huawei(config)#lldp enable
huawei(config)#lldp enable port 0/9 0,1
huawei(config)#lldp management-address 10.10.10.2
huawei(config)#lldp trap enable
huawei(config)#display lldp local
{ <cr>|port<K>||<K> }:
```

Command:
display lldp local

System information:

ChassisId subtype	: macAddress
ChassisId	: 00e0-fc00-0000
System name	: MA5800
System description	: Huawei Integrated Access Software
System capabilities supported	: bridge
System capabilities enabled	: bridge
LLDP up time	: 2021-08-21 20:39:03+08:00

System configuration:

LLDP status	: enabled
LLDP message TX interval	: 30s
LLDP message TX hold multiplier	: 4
LLDP restart delay	: 2s
LLDP trap interval	: 30s
LLDP trap enable	: enabled
Management address	: 10.10.10.2

Remote neighbors statistics:

Remote neighbors last change time	: 0 day(s), 0h: 0m: 0s
Remote neighbors added	: 0
Remote neighbors deleted	: 0
Remote neighbors dropped	: 0
Remote neighbors aged	: 0
Total remote neighbors	: 0

Port information:

Port	: 0/9/0
PortId subtype	: interfaceName
PortId	: ethernet0/9/0
Port description	: Huawei-MA5800-ETHERNET
LLDP enable status	: enabled TX-RX

```
Total remote neighbors      : 0
Port                        : 0/9/1
PortId subtype             : interfaceName
PortId                     : ethernet0/9/1
Port description           : Huawei-ETHERNET
LLDP enable status         : enabled TX-RX
Total remote neighbors      : 0
Total port number          : 2
```

19.4 NETCONF

Network Configuration Protocol (NETCONF) is a network configuration and management protocol based on Extensible Markup Language (XML). NETCONF enables the network management system (NMS) to quickly configure and manage remote devices.

19.4.1 Feature Updates

Version	Description
V100R019C1X and later versions	First version to support this feature.

19.4.2 Introduction

Network Configuration Protocol (NETCONF) is a key technology that simplifies complex network configuration.

Background

With the development of networks, the types and number of communication devices increase rapidly. Traditional Command Line Interface (CLI) or Simple Network Management Protocol (SNMP) configuration methods cannot adapt to the management of complex networks. Especially when devices from multiple vendors exist on the same network, the management methods of devices from different vendors are independent of each other, and the operations are complex. Therefore, automatic configuration is difficult to implement. To resolve this issue, the NETCONF protocol based on Extensible Markup Language (XML) and structured data model defined based on YANG are developed.

Definition

- **NETCONF** provides mechanisms to add, modify, delete, and query the configurations of network devices, and obtain the network device status. With NETCONF, network devices can provide standard application programming interfaces (APIs). Applications can directly use these APIs to send configurations to or obtain configurations from network devices. NETCONF can directly use the existing functional modules of devices. This reduces the development cost of NETCONF and allows users to use new features supported by the devices at any time.

- **YANG** defines a structured data model. It is a machine-oriented model interface, and defines the data structure and constraints to describe data more flexibly and completely.

Value

NETCONF complies with YANG model constraints to implement communication between clients and servers. With standardized deployment, network administrators can use NETCONF to uniformly manage, configure, and monitor various network devices that support YANG, simplifying O&M and reducing O&M costs.

Compared with traditional configuration protocols, NETCONF is more convenient on man-machine interfaces and machine-to-machine interfaces. [Table 19-3](#) shows the comparison between SNMP and NETCONF.

Table 19-3 Comparison between NETCONF and SNMP

Comparison Item	SNMP	NETCONF
Configuration management	Does not provide the protection lock mechanism when multiple users perform operations on the same configuration.	Provides the protection lock mechanism to prevent conflicts caused by multi-user operations.
Query	Supports the query for one or more records in a table but requires multiple interactions.	Supports the direct query for the configuration data of the system, and supports filtering on data query.
Scalability	Poor expansibility	Good expansibility • SNMP models are defined by layer and each layer is independent of each other. Extensions to one layer have little effect on the other layers. • NETCONF is in the XML encoding format. This expands the management capability and system compatibility of NETCONF.

Comparison Item	SNMP	NETCONF
Security	The SNMPv3 security protocol has no room for expansion.	NETCONF uses existing security protocols to ensure network security, and is not specific to any security protocols. This enables users to flexibly select a security protocol.

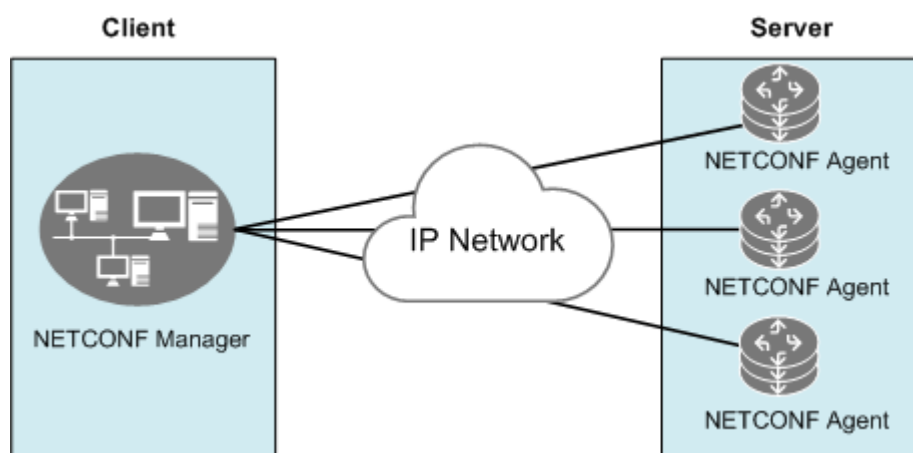
19.4.3 Principles

Network Configuration Protocol (NETCONF) uses a hierarchical structure. A lower layer provides services for the upper layer. The hierarchical structure enables each layer to focus only on a single aspect of NETCONF and reduces the dependencies between different layers.

NETCONF Network Architecture

NETCONF uses the Client/Server structure. [Figure 19-15](#) shows the basic network architecture.

Figure 19-15 NETCONF network architecture



The NETCONF network architecture comprises the following components:

- **NETCONF Manager:** serves as a client on the network and runs on the NMS/EMS. It works with the NETCONF Agent to implement device management. The network administrator uses the NETCONF Manager to send a **<rpc>** request in XML format to the NETCONF Agent.
- **NETCONF Agent:** serves as the server on the network. During device configuration, the NETCONF Manager sends a configuration management request to the NETCONF Agent. The NETCONF Agent parses the request and manages the device configuration and sends a response to the NETCONF manager in XML format.

- **YANG:** NETCONF data modeling language, which is used to design configuration data and status data models, remote invocation models, and notification mechanisms for NETCONF operations.

NETCONF Framework Layers

NETCONF consists of four layers: content layer, operation layer, remote procedure call (RPC) layer, and application protocol layer. For details, see [Table 19-4](#).

Table 19-4

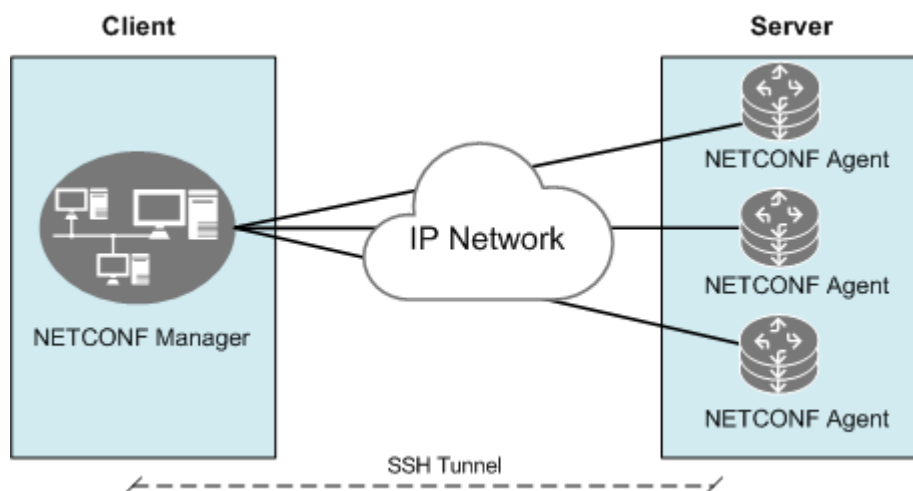
Protocol Layer	Example	Description
Content layer	Configuration data	Describes the configuration data related to network management. The data varies depending on vendors' devices. The data modeling language is YANG.
Operation layer	<get-config>, <edit-config>, <notification>	Defines basic operations for applications in the RPC and calls these operations using XML encoding parameters.
RPC layer	<rpc>, <rpc-reply>	Provides a simple RPC request and response mechanism that does not depend on the transport protocol. • The client encapsulates the RPC request into an <rpc> element and sends the <rpc> element to the server. • The server encapsulates the request processing result in an <rpc-reply> element and sends the <rpc-reply> element to the client.

Protocol Layer	Example	Description
Application protocol layer	BEEP, SSH, SSL	Provides the communication path between the NETCONF client and NETCONF server. Any transport protocol that meets the basic requirements can be used. The basic requirements for the transport protocol are as follows: • Connection-oriented. A persistent connection must be established between the NETCONF Manager and the NETCONF Agent. After the connection is established, reliable and serialized data transmission services must be provided. • Provides user authentication, data integrity, and security encryption for NETCONF. • The transport protocol provides a mechanism for distinguishing the session type (client or server) for NETCONF.

19.4.4 Networking Scenario

Network Configuration Protocol (NETCONF) ensures security and expansibility. When the NMS is used to manage network devices, you can use NETCONF to ensure communication between the NMS and the devices.

On a communications network, devices usually come from different vendors, and each vendor provides a unique device management method (for example, using different commands). In this scenario, configuring and managing these devices using traditional methods will be costly and ineffective. To resolve this issue, use NETCONF to remotely configure, manage, and monitor devices. The specified YANG file can be used to perform unified configuration. [Figure 19-16](#) shows the networking.

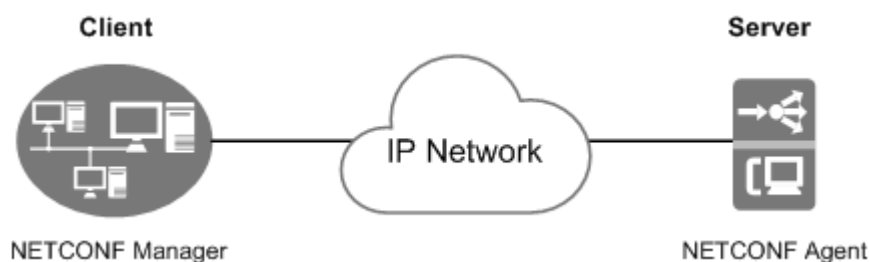
Figure 19-16 NETCONF networking scenario

19.4.5 Configuring NETCONF

Configure Network Configuration Protocol (NETCONF) to implement remote communication between the network management system (NMS) and devices.

Networking Diagram

As shown in [Figure 19-17](#), when NETCONF is configured, the NETCONF Manager functions as the client and the NMS is deployed. The NETCONF Agent functions as the SSH server and receives the connection from the NETCONF Manager that functions as the SSH client. In this way, the configuration file can be managed through NETCONF.

Figure 19-17 NETCONF Scenario

Procedure

Step 1 Run the **sysman server source** command to bind a specified source interface.

```
huawei(config)#sysman server source netconf vlanif 100
```

NOTE

In V100R020C00 and later versions and later versions, you must perform this step for the NETCONF function to take effect.

Step 2 Run the **sysman service netconf enable** command to enable NETCONF on the NETCONF agent and create a device user.

```
huawei(config)#sysman service netconf enable
```

The netconf administrator user already exists, are you sure to create another?

```
(y/n)[n]:y
User Name(length<6,15>):user123
User Password(length<12,128>):
Confirm Password(length<12,128>):
The operation is being processed. Please wait...
The operation is successful
```

- Step 3** Deploy the NMS on the NETCONF Manager.
- Step 4** Log in to the NETCONF Agent from the NETCONF Manager using the NMS.
- Step 5** Run the **display sysman server source netconf** command to check the configuration of the source interface.

```
huawei(config)#display sysman server source netconf
{ <cr>|ipv6<K>||<K> }:
```

Command:

```
display sysman server source netconf
```

No.	InterfaceType	InterfaceNum	IPv4 Address	VPN Instance
1	vlanif	-	-	-

 NOTE

V100R020C00 and later versions support this command.

- Step 6** Run the **display sysman service state** command to check the NETCONF configuration result.

```
huawei(config)#
display sysman service state
{ <cr>||<K> }:
```

Command:

```
display sysman service state
```

Network service	Port	State
telnet	23	disable
trace	1026	disable
ssh	22	enable
snmp	161	enable
ftp-client	----	----
sftp-client	----	----
ntp	123	enable
radius	----	enable
dhcp-relay	67	disable
dhcpv6-relay	547	disable
ntp6	123	disable
ipdr	4737	enable
twamp	862	enable
netconf	830	enable
telnetv6	23	disable
sshv6	22	disable
snmpv6	161	disable
web-proxy	8024	disable
portal	2000	disable
capwap	5246	disable

----End

19.4.6 NETCONF Reference Standards and Protocols

Table 19-5 Main reference standards of NETCONF

Standard No.	Description
RFC 4741	NETCONF Configuration Protocol
RFC 4742	NETCONF Configuration Protocol over Secure Shell (SSH)
RFC 6241	Network Configuration Protocol (NETCONF)
RFC 6242	Using the NETCONF Protocol over Secure Shell (SSH)
RFC 5277	NETCONF Event Notifications
RFC 6536	Network Configuration Protocol (NETCONF) Access Control Model

19.5 Telemetry

Telemetry is a remote measuring technology that can remotely collect data from physical or virtual devices at a high speed. The Telemetry feature provides real-time and high-speed data collection and improves the device and network usage during data collection.

NOTICE

According to industry practices, Telemetry data collection may involve obtaining personal data and personal communication content (the product does not store, parse, or process such data) for the purpose of ensuring network operation and services. Huawei alone is unable to collect or save the personal data of and user communication content. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the personal data of users and the content of users' communications are fully protected when the personal data and the content are being used and saved.

19.5.1 Telemetry Feature Updates

Product Version	Change Description
V100R020C00	First version to support this feature.

19.5.2 Introduction to Telemetry

Context

As the network expands, more and more services are carried. The intelligent network O&M system poses higher requirements on the number, performance, and precision of network monitoring devices.

Traditional network monitoring (SNMP and syslog) uses the pull mode to periodically poll each device on the network to obtain device data, resulting in high pressure on devices and low query efficiency when massive data needs to be queried. In addition, different vendors have different data formats and unstructured data, making it difficult to adapt analysis tools. Therefore, a new network monitoring mode is urgently needed.

Definition

Telemetry, as a mainstream performance collection mechanism for the future, is a network monitoring mode in push mode. That is, sampled devices on the network proactively push the interface traffic data to the NMS periodically. The push mode of Telemetry can achieve second-level or subsecond-level sampling precision.

Benefits

The Telemetry network monitoring mode enables the intelligent network O&M system to monitor more devices with higher precision. In addition, the monitoring process has little impact on the functions and performance of devices.

Compared with traditional SNMP query, Telemetry has higher collection efficiency. [Table 19-6](#) describes the advantages of Telemetry sampling compared with SNMP query.

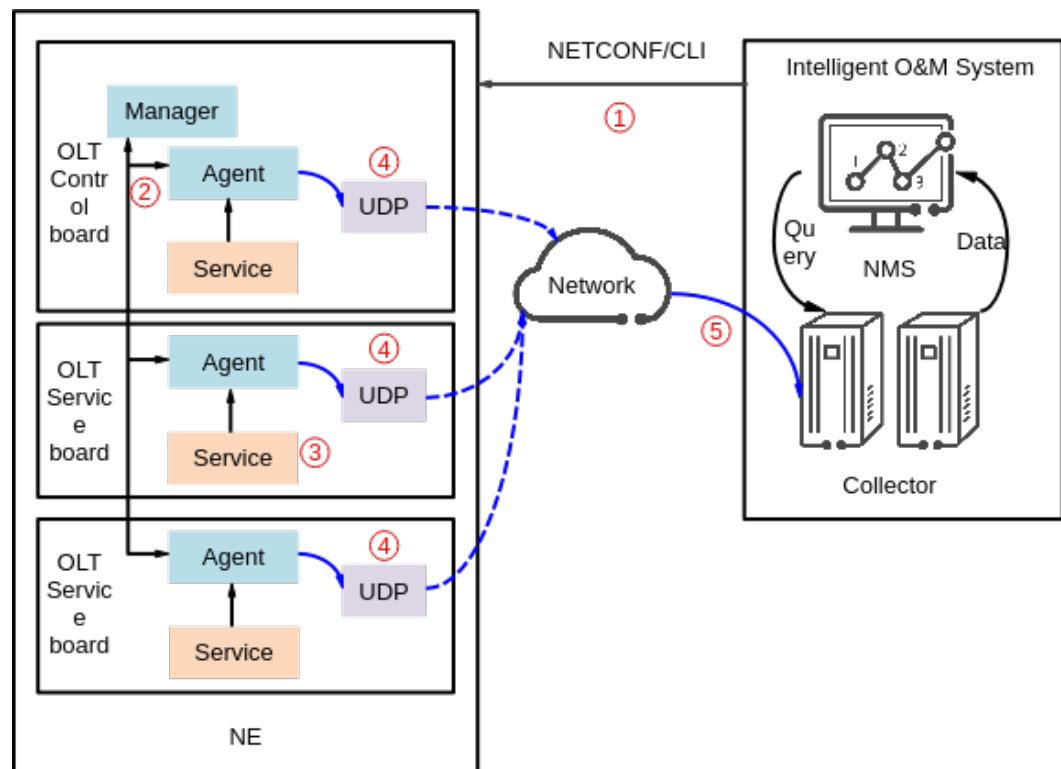
Table 19-6 Comparison between the SNMP query and telemetry sampling

Telemetry		SNMP	
Push collection	NEs continuously push collected data after one subscription.	Pull collection	The NMS needs to send a query request each time data is collected.
Distributed collection	Interface boards send data directly.	Centralized collection	The collected data is aggregated to the control board.
Hardware collection	Hardware-based data collection allows data to be collected within milliseconds.	Software collection	Software-based data collection has a long collection time.
Google Protocol Buffer (GPB)	Improves storage and transmission efficiency.	Unstructured data	Low information processing efficiency

19.5.3 Telemetry Data Collection and Reporting Process

In the application scenario where access network devices support the Telemetry interface-based collection function, the Telemetry collection system can be divided into the intelligent O&M system and OLT. The intelligent O&M system makes collection configurations, receives data collected by the OLT through Telemetry, and processes and analyzes the data. The OLT reports data collected through Telemetry based on the collection configurations.

Figure 19-18 Data collection process



1. The intelligent O&M system uses NETCONF/CLI static configurations to deliver the collection model to NEs that support Telemetry. Collection models include:
 - Data source type
 - Sampling frequency
 - Upstream transmission channel
 - Data format
2. The OLT control board delivers the collection and subscription information to specific service boards.
3. Service boards sample data (such as interface traffic) or monitor alarms and events and store the data.
4. Upload the collected data through UDP.
5. The collector collects sampled data.

 NOTE

- The collector is a big data analysis system that is capable of receiving, storing, and processing sampled data reported by devices on the network.
- The intelligent O&M system processes services based on the analysis results from the big data analysis system, for example, checking the network status and optimizing the network promptly. After an optimization instruction takes effect, newly sampled data is sent to the collector. The intelligent O&M system can analyze whether the optimization effect meets expectations.

19.5.4 Telemetry Data Model

The collection controller consists of the control module and collection module. The control module must support the NETCONF protocol and configurations based on the openconfig-telemetry.yang and xxx-openconfig-telemetry-ext.yang data models. The OLT can function as a UDP agent and encapsulate and report data based on xxx-telemetry.proto and the data collection model.

Table 19-7 NETCONF configuration protocol data model

Layer	Description
Content layer	Includes the collection configuration data. The openconfig-telemetry.yang and xxx-openconfig-telemetry-ext.yang YANG models are used to model the collection configuration data, and the sensor-path contained in the models is used to specify collection items. The configuration must comply with IETF RFC 7950.
Operation layer	Supports NETCONF. NETCONF implementation must comply with IETF RFC 6241.
Messages layer	Supports NETCONF. NETCONF implementation must comply with IETF RFC 6241.
Communication protocol layer	Supports NETCONF. NETCONF implementation must comply with IETF RFC 6241.

The collected packets reported by the OLT to the collection module must comply with the UDP protocol. The following table lists the protocol layers and requirements.

Table 19-8 Protocol data model for packet collection in UDP reporting mode

Layer		Description
Data model layer NOTE The data model layer is divided into two layers, which are defined in different .proto files.	Service data layer	Complies with the definition of the sensor_path field in the xxx-telemetry.proto file. The value of this field is obtained from different service data .proto files. 0 is meaningful data and should be reported. All Fs indicate data that cannot be reported due to device faults.
	Telemetry layer	The value must comply with the definition in the xxx-telemetry.proto file.
Message header layer		(Optional) Fragmentation and coding format indication can be implemented through the message header layer. In the message header layer, bit 4 is the S bit, and bits 5 to 8 are ET bits. When S is set to 1 and ET is set to 0, the encoding format is GPB. For details, see IETF draft-ietf-netconf-udp-pub-channel-05.
UDP layer		Supports the UDP protocol and complies with IETF RFC768 when implementing UDP.

The collection items supported by the OLT, collection performance requirements on a single collection item, and collection data model are defined in the service proto file.

 NOTE

The sensor path format in the collection configuration must meet the following requirements:

- Data model file name at the service data layer: message name/.../message name
- message name/message name/message name indicates the node path in the data model. Set this parameter based on the site requirements.
- When a single collection object needs to be collected, the filter needs to be configured in the huaweiopencon-telemetry-ext.yang file.

Example: The message QueueKpiRecords of the an-bb-quene-kpi.proto model is used to collect queue traffic, and the sensor path is an-bb-quene-kpi:QueueKpiRecords.

19.5.5 Key Telemetry Technologies

19.5.5.1 UDP Transport Protocol

UDP is a simple datagram-oriented transport layer protocol that does not provide reliability, flow control, or error recovery functions for IP. UDP applies to networks that have low reliability requirements but require economical transmission.

Telemetry uses UDP to report the data encapsulated in an encoding format to the collector.

 NOTE

For the definition of the UPC message header, see draft-ietf-netconf-udp-pub-channel-05.

Figure 2 shows the layers of the UDP protocol stack.

Figure 2 UDP protocol stack layers

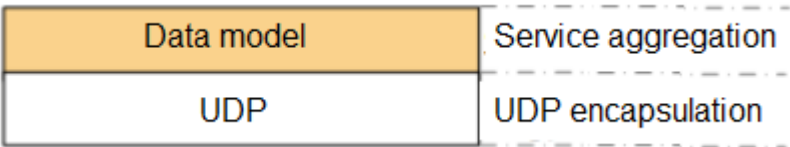


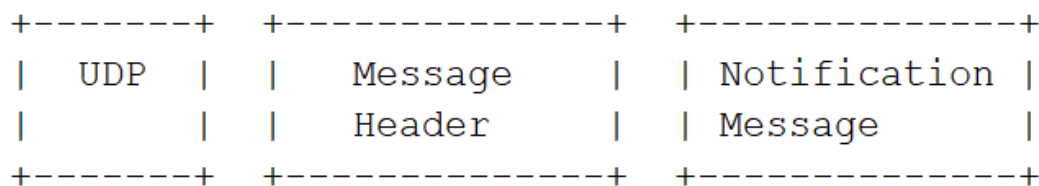
Table 19-9 describes the layers.

Table 19-9 Table 2 Description of each layer

Layer	Description	Remark
UDP layer	Communication protocol based on the UDP connection.	-
Message header layer	For the structure definition of the message header layer, see UPC Message Header .	The data model layer is divided into three layers. Except the message header layer, the other two layers are defined in different .proto files.To establish a UDP connection between the collector and a network device, use the .proto files for interconnection. The .proto files on the two ends must be the same to facilitate decoding.
Telemetry layer	When the encoding format of the data to be sent is GPB, it is defined in the huawei-telemetry.proto file.	
Service data layer	When the encoding format of the data to be sent is GPB, the value of the encoding field in the huawei-telemetry.proto file is Encoding_GPB (0), the data_gpb field carries sampled data in GPB format, and the data_str field is empty. NOTE The data_gpb field needs to be decoded using the .proto file of the corresponding service, which is determined by the sensor_path field in the huawei-telemetry.proto file. For example, if the value of the sensor_path field is huawei-ifm:ifm/interfaces/interface , the .proto file is huawei-ifm.proto .	

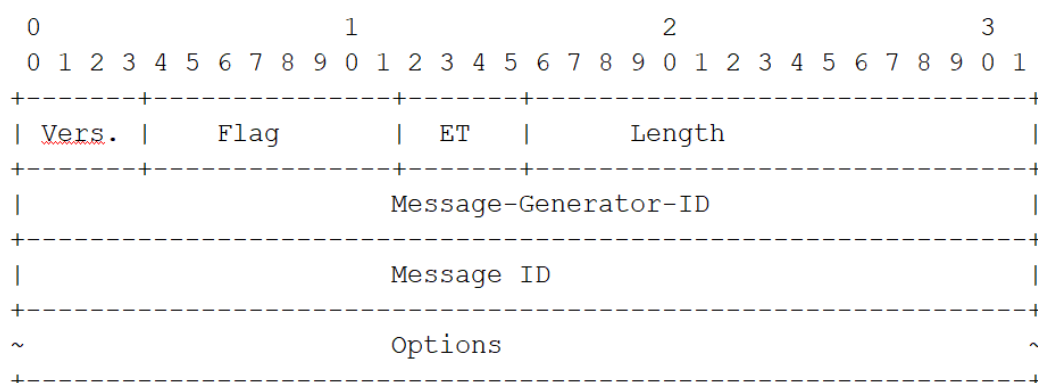
UPC Message Header

Figure 19-19 describes the typical UPC message structure.

Figure 19-19 UDP release message description

- A message header packet includes information that can facilitate message transmission before deserializing a notification message.
- A notification message is the encoded content transmitted through a release channel. Common encoding methods include GPB, CBOR [RFC7049], JSON, and XML.

Figure 19-20 describes the data format of the UPC message header.

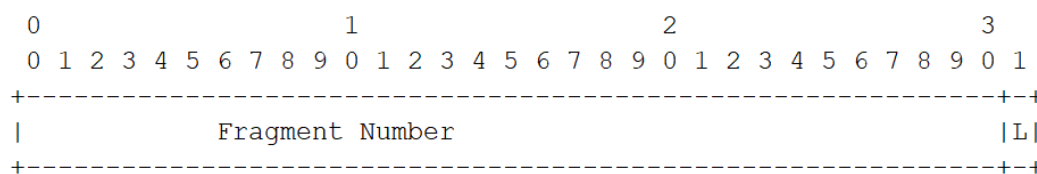
Figure 19-20 Data format of the UPC message header

- A UPC message header occupies only 12 bytes, excluding the Options field, if the message is not fragmented.
- Vers.: indicates the encoding version of the protocol data unit (PDU). The initial value is 0.
- Flag: a bitmap that indicates the functions and additional options of a data packet. Each bit is associated with a function and an option data. When a bit is set to 1, the associated function is enabled and option data is added. The order in which options exist follows the bit order of the bitmap. In this document, the flags are specified as follows.
 - bit 0, the reliability flag;
 - bit 1, the fragmentation flag;
 - Other bits are reserved.
- ET: a 4-bit identifier that indicates the encoding type used for the notification message. 16 encoding types can be expressed.
 - 0: GPB
 - 1: CBOR
 - 2: JSON

- 3: XML
- Others are reserved
- Length: indicates the total length of a message, in octets, including the message header.
- Message-Generator-ID: 32-bit identifier of the process that creates the notification message. This allows ambiguity to be removed from the source of information, such as identifying different line cards that send notification messages. The source IP address of the UDP datagram should not be interpreted as the identifier of the host initiating the UPC message. The entity that sends a UPC message may be only a relay.
- Message ID: It is generated by the message generator consecutively. Different users share the same notification ID sequence.
- Options: variable-length field. Details about options are described in the following sections.

The following figure shows the format of the option part. When the fragment flag is set to 1, the fragment option is available in the message header.

Figure 19-21 Fragment option format



- Fragment Number: indicates the sequence number of the current fragment.
- L: a flag used to indicate whether the current fragment is the last fragment. When this parameter is set to 0, the current fragment is not the last fragment. Therefore, more fragments are expected. If this parameter is set to 1, the current fragment is the last fragment.

UDP Message Example

Figure 19-22 UPC message header example

0000	45 00 05 44 5a 41 00 00	f9 11 37 bd 06 03 11 14	E..DZA..7.....
0010	06 0f 0d 85 4e 20 04 d2	05 30 4f 98 00 00 05 28	...N..00... (
0020	27 a8 e8 d6 00 00 00 43	0a 03 49 41 53 12 05 73	'.....C..IAS..s

- The content in the red box is the content of the UPC message header.
- First uint32:
 - vers = 0
 - flag = 0: no option, that is, no fragment.
 - ET = 0: The reported content is in GPB coding format.
 - length = 0x0528 = 1320: same as the UDP payload length parsed by the Wireshark. Figure 1-6
- Second uint32:

- Message-Generator-ID = 0x27a8e8d6: reported process ID. The MA5800 reports the 1970s timestamp.
- Third uint32:
 - Message ID = 0x43: message sequence number. The value is incremented by 1 each time a packet is sent.
- All bytes following 0x0a starting from the 0x28 address are GPB codes.

19.5.5.2 GPB Encoding Format

Telemetry uses the GPB encoding format (the file name extension of a file encoded in GPB format is .proto) and provides a mechanism for serializing structured data flexibly, efficiently, and automatically. The GPB format is binary encoding and has good performance and high efficiency.

- GPB encoding depends on the information about the data structure. The message data structure used by the GPB is defined in the proto file. The message definition in the proto file can be converted from a yang file or manually compiled. Each field in the message data structure definition has a unique index. Once the proto is released, the index of each field in the message data structure should not be changed.
- GPB encoding uses a series of key-value pairs to represent fields in a message data structure.
- The key is obtained by combining the field index and data type of each field in each message, for example, key = (index<<3) | type.
- In GPB encoding, seven bits in a byte indicate valid data, and the most significant bit indicates whether the current byte is the last byte.
- Because the type in the key occupies 3 bits, if the index value is large, more bytes are required to represent the key.
- For example, a field index ranging from 1 to 15 requires only one byte for GPB encoding, including the field index and type (you can find more information in Protocol Buffer Encoding). A field index ranging from 16 to 2047 occupies two bytes, and a larger index requires more bytes. Because of this GPB encoding representation, indexes 1 to 15 should be reserved for message elements that appear very frequently. GPB allows indexes ranging from 1 to $2^{29} - 1$ (536,870,911). Indexes 19000 to 19999 are reserved for GPB and cannot be used.

Types Supported by GPB Encoding

Table 19-10 Types supported by GPB encoding

Type	Meaning	Used For
0	Varint	int32, int64, uint32, uint64, sint32, sint64, bool, enum
1	64-bit	fixed64, sfixed64, double
2	Length-delimited	string, bytes, embedded messages, packed repeated fields

Type	Meaning	Used For
3	Start group	groups(deprecated)
4	End group	groups(deprecated)
5	32-bit	fixed32, sfixed32, float

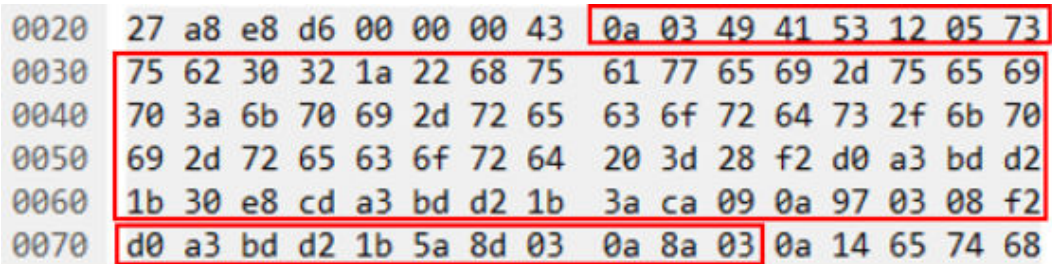
- The preceding types 3 and 4 are obsolete.
- The remaining types 0, 1, and 5 are all numeric types in the format of key-value.
- The remaining type 2 is a variable-length type, and is used to indicate string, bytes, message nesting, and the like in the format of key-length-value. If the value is a string, \0 at the end is not included.

Base 128 Varints encoding (compression algorithm) is used for keys, numeric values, or lengths: A compact method for representing numbers based on the assumption that smaller numbers are more frequently used. In this encoding method, the most significant bit of each byte has a special meaning. If the most significant bit is 1, it indicates that the subsequent bytes are also a part of the number. If the most significant bit is 0, it indicates that the number ends. That is, only seven bits of each byte are valid data, and the most significant bit is a flag, indicating whether the current byte is the last byte. If the bit width of a number is greater than 7 bits, multiple bytes are required to represent the number. In addition, the number is in big-endian order, and the least significant digit is the first byte.

GPB Parsing Example of the Proto File Header

The following figure shows a GPB parsing example of a proto file.

Figure 19-23 .proto file header packet



- 0A 03 49 41 53: field index 1, string, node_id_str = IAS
- 12 05 73 75 62 30 32: field index 2, string, subscription_id_str = sub02
- 1A 22 68 75... 63 6F 72 64: field index 3, string, sensor_path = huawei-ueip:kpi-records/kpi-recor
- 20 3D: field index 4, uint, collection_id = 0x3d
- 28 F2 D0 A3 BD D2 1B: field index 5, uint, collection_start_time

- 30 E8 CD A3 BD D2 1B: field index 6, uint, msg_timestamp
- 3A CA 09: field index 7, variable length, length = 0xCA09=0x4ca = 1226. The data_gpb field is a variable of the TelemetryGPBTable structure and its length is uncertain at this layer. Therefore, the length of this field is variable.
- 0A 97 03: field index 1, variable length, length = 0x9703 = 0x197 = 407. Note that the field index changes to 1 again because the first variable row of the corresponding structure TelemetryGPBTable is repeated before the row defined by proto, indicating that the row is an array. Therefore, it indicates the total data length of the row[] array.
- 08 F2 D0 A3 BD D2 1B: field index 1, int, TelemetryRowGPB.timestamp. The field index is 1, which is the first field of the TelemetryRowGPB structure.
- 5A 8D 03: field index 11, variable length, length=0x8D03=0x18D=397, TelemetryRowGPB.content. This field is followed by the reported service data. It is defined by bytes and is variable-length data. The length is the total number of bytes of the subsequent service data.
- The subsequent field content does not belong to the Telemetry header, but belongs to the service data Telemetry.
- 0A 8A 03: field index 1, variable length, length=0x8A03=0x18A=394, corresponding to the outermost repeated KpiRecord kpi_record of proto of the service data. Note that this is a variable definition with repeated annotations. It is also an array. Therefore, 394 is the length of the kpi_record[] array.

19.5.6 Telemetry Configurations

The control module of the collector uses NETCONF to deliver data collection configurations based on the configured YANG data model.

NOTE

Before configuring Telemetry, use the Telemetry packet parsing tool to start server monitoring, start the NETCONF server, and import the YANG file.

Perform the following steps to configure Telemetry static subscription:

1. Enable NETCONF.
2. Configure the data to be sampled.
3. Configure a destination collector.
4. Create a subscription.

19.5.6.1 Enabling NETCONF

Procedure

1. Run the **sysman server source netconf** command to bind a source port to the NETCONF service protocol.
2. Run the **sysman service netconf enable** command to enable the NETCONF service and create a NETCONF user.

Example

- Bind the NETCONF service protocol to a specified source port. Set the port type to vlanif and the port index to 300.

- Enable NETCONF and set the user name and password. Here, V100R021C0x is used as an example. For other versions, the actual display prevails.
huawei#sysman server source netconf vlanif 300
huawei(config)#sysman service netconf enable
Please enter the username and password to create a netconf administrator
user
User Name(length<6,15>):Test-
user1
User
Password(length<12,128>):
Confirm
Password(length<12,128>):
Adding user successfully

19.5.6.2 Configuring the Data to Be Sampled

Create a sampling sensor group and specify a sampling path.

Table 19-11 Elements for configuring data to be sampled

Element	Description	Parameter
sensor-group-id	Indicates the ID of a sampling sensor group.	The value is a string of 1–63 characters, including uppercase letters, lowercase letters, and digits (0–9).
path	Indicates the sampling path.	The value is a string of 1–254 characters.

Set sensor-group-id to sen01 and path to huawei-gpon-pm-ont-line-quality:gpon-pm-ont-line-qualitys/gpon-pm-ont-line-quality. The following is a YANG configuration example. If the configuration is successful, OK is returned.

- Request example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1581665858050">
  <edit-config>
    <target>
      <running />
    </target>
    <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
      <telemetry-system xmlns="http://openconfig.net/yang/telemetry">
        <sensor-groups>
          <sensor-group>
            <sensor-group-id>sen01</sensor-group-id>
            <config>
              <sensor-group-id>sen01</sensor-group-id>
            </config>
            <sensor-paths>
              <sensor-path xc:operation="create">
                <path>huawei-gpon-pm-ont-line-quality:gpon-pm-ont-line-qualitys/gpon-pm-ont-line-quality</path>
              </sensor-path>
              <sensor-path>
                <config>
                  <path>huawei-gpon-pm-ont-line-quality:gpon-pm-ont-line-qualitys/gpon-pm-ont-line-quality</path>
                </config>
              </sensor-path>
            </sensor-paths>
          </sensor-group>
        </sensor-groups>
      </telemetry-system>
    </config>
  </edit-config>
</rpc>
```

```
</sensor-groups>
</telemetry-system>
</config>
</edit-config>
</rpc>
```

- Response example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1581665858050">
  <ok />
</rpc-reply>
```

Query the configured data to be sampled. The following is an example:

- Request example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1581665858121">
  <get>
    <filter type="subtree">
      <telemetry-system xmlns="http://openconfig.net/yang/telemetry" xmlns:hw-telemetry-ext="urn:huawei:yang:huawei-openconfig-telemetry-ext">
        <sensor-groups>
          <sensor-group>
            <sensor-paths>
              <sensor-path />
            </sensor-paths>
          </sensor-group>
        </sensor-groups>
      </telemetry-system>
    </filter>
  </get>
</rpc>
```

- Response example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1581665858121">
  <data>
    <telemetry-system xmlns="http://openconfig.net/yang/telemetry">
      <sensor-groups>
        <sensor-group>
          <sensor-group-id>sen01</sensor-group-id>
          <sensor-paths>
            <sensor-path>
              <path>huawei-gpon-pm-ont-line-quality:gpon-pm-ont-line-qualitys/gpon-pm-ont-line-quality</path>
              <config>
                <path>huawei-gpon-pm-ont-line-quality:gpon-pm-ont-line-qualitys/gpon-pm-ont-line-quality</path>
              </config>
              <state>
                <path>huawei-gpon-pm-ont-line-quality:gpon-pm-ont-line-qualitys/gpon-pm-ont-line-quality</path>
              </state>
            </sensor-path>
          </sensor-paths>
        </sensor-group>
      </sensor-groups>
    </telemetry-system>
  </data>
</rpc-reply>
```

19.5.6.3 Configuring a Destination Collector

Create a destination collector group and specify the destination collector to which the sampled data is sent.

Table 19-12 Elements for configuring a destination collector

Element	Description	Parameter
group-id	Indicates the ID of a destination collector group.	The value is a string of 1–63 characters, including uppercase letters, lowercase letters, and digits (0–9).
destination-address	Indicates a destination IP address.	Loopback IP addresses, all-0 IP addresses, all-f IP addresses, and IPv6 addresses are not supported.
destination-port	Indicates a destination port.	The value is an integer ranging from 1 to 65535.

Set group-id to dest01, destination-address to 192.168.1.1, and destination-port to 20001. The following is a YANG configuration example. If the configuration is successful, OK is returned.

- Request example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1579172235104">
  <edit-config>
    <target>
      <running />
    </target>
    <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
      <telemetry-system xmlns="http://openconfig.net/yang/telemetry">
        <destination-groups>
          <destination-group>
            <group-id>dest01</group-id>
            <config>
              <group-id>dest01</group-id>
            </config>
          </destination-group>
          <destinations>
            <destination xc:operation="create">
              <destination-address>192.168.1.1</destination-address>
              <destination-port>20001</destination-port>
            </destination>
            <config>
              <destination-address>192.168.1.1</destination-address>
              <destination-port>20001</destination-port>
            </config>
          </destinations>
        </destination-group>
      </destination-groups>
    </telemetry-system>
  </config>
</edit-config>
</rpc>
```

- Response example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1579172235104">
  <ok />
</rpc-reply>
```

Query information about the configured destination collector. The following is an example:

- Request example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1581665858129">
  <get>
    <filter type="subtree">
      <telemetry-system xmlns="http://openconfig.net/yang/telemetry">
        <destination-groups>
          <destination-group>
            <destinations>
              <destination />
            </destinations>
          </destination-group>
        </destination-groups>
      </telemetry-system>
    </filter>
  </get>
</rpc>
```
- Response example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1581665858129">
  <data>
    <telemetry-system xmlns="http://openconfig.net/yang/telemetry">
      <destination-groups>
        <destination-group>
          <group-id>dest01</group-id>
          <destinations>
            <destination>
              <destination-address>192.168.1.1</destination-address>
              <destination-port>20001</destination-port>
              <config>
                <destination-address>192.168.1.1</destination-address>
                <destination-port>20001</destination-port>
              </config>
              <state>
                <destination-address>192.168.1.1</destination-address>
                <destination-port>20001</destination-port>
              </state>
            </destination>
          </destinations>
        </destination-group>
      </destination-groups>
    </telemetry-system>
  </data>
</rpc-reply>
```

19.5.6.4 Creating a Subscription

Create a subscription, associate the configured destination group with the sampling sensor group, and establish a data sending channel to complete data sending. Data can be sent through UDP.

Table 19-13 Elements for creating a subscription

Element	Description	Parameter
subscription-name	Indicates the subscription name.	The value is a string of 1–63 characters, including uppercase letters, lowercase letters, and digits (0–9).

Element	Description	Parameter
local-source-address	Indicates a source IP address.	The value is an IPv4 address.
protocol	Indicates the protocol.	The STREAM_UDP type is supported.
encoding	Indicates the encoding format.	The ENC_PROTO3 type is supported.
local-source-port	Indicates a source port.	The value is an integer ranging from 1 to 65535.
sensor-group	Indicates the sampling sensor group to be associated with the subscription.	The value is a string of 1–63 characters, including uppercase letters, lowercase letters, and digits (0–9). The sensor-group must have been created.
sample-interval	Indicates the sampling interval.	The value is an integer ranging from 1 to 86400000, in milliseconds.
group-id	Indicates the destination collector group to be associated with the subscription.	The value is a string of 1–63 characters, including uppercase letters, lowercase letters, and digits (0–9). The destination-group must have been created.

Set subscription-name to sub01, local-source-address to 10.71.214.35, protocol to STREAM_UDP, encoding to ENC_PROTO3, local-source-port to 55, sensor-group to sen01, sample-interval to 60000, and group-id to dest01. The following is a YANG configuration example. If the configuration is successful, OK is returned.

- Request example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1579172235116">
  <edit-config>
    <target>
      <running />
    </target>
    <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
      <telemetry-system xmlns="http://openconfig.net/yang/telemetry" xmlns:hw-telemetry-ext="urn:huawei:yang:huawei-openconfig-telemetry-ext">
        <subscriptions>
          <persistent>
            <subscription xc:operation="create">
              <subscription-name>sub01</subscription-name>
            <config>
              <subscription-name>sub01</subscription-name>
              <local-source-address>10.71.214.35</local-source-address>
```

```
<protocol>STREAM_UDP</protocol>
<encoding>ENC_PROTO3</encoding>
<hw-telemetry-ext:local-source-port>55</hw-telemetry-ext:local-source-port>
</config>
<sensor-profiles>
  <sensor-profile>
    <sensor-group>sen01</sensor-group>
    <config>
      <sensor-group>sen01</sensor-group>
      <sample-interval>60000</sample-interval>
    </config>
  </sensor-profile>
</sensor-profiles>
<destination-groups>
  <destination-group>
    <group-id>dest01</group-id>
    <config>
      <group-id>dest01</group-id>
    </config>
  </destination-group>
</destination-groups>
</subscription>
</persistent>
</subscriptions>
</telemetry-system>
</config>
</edit-config>
</rpc>
```

- **Response example:**

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1579172235116">
  <ok />
</rpc-reply>
```

Query the created subscription information. The following is an example:

- **Request example:**

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1579172235130">
  <get>
    <filter type="subtree">
      <telemetry-system xmlns="http://openconfig.net/yang/telemetry">
        <subscriptions>
          <persistent>
            <subscription />
          </persistent>
        </subscriptions>
      </telemetry-system>
    </filter>
  </get>
</rpc>
```

- **Response example:**

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="1579172235130">
  <data>
    <telemetry-system xmlns="http://openconfig.net/yang/telemetry">
      <subscriptions>
        <persistent>
          <subscription>
            <subscription-name>sub01</subscription-name>
            <config>
              <subscription-name>sub01</subscription-name>
              <local-source-address>10.71.214.35</local-source-address>
              <protocol xmlns:hw-telemetry-ext="urn:huawei:yang:huawei-openconfig-telemetry-ext">hw-
telemetry-ext:STREAM_UDP</protocol>
              <encoding xmlns:oc-telemetry-types="http://openconfig.net/yang/telemetry-types">oc-
telemetry-types:ENC_PROTO3</encoding>
              <local-source-port xmlns="urn:huawei:yang:huawei-openconfig-telemetry-ext">55</local-
```

```
source-port>
  </config>
  <state>
    <subscription-name>sub01</subscription-name>
    <local-source-address>10.71.214.35</local-source-address>
    <protocol xmlns:hw-telemetry-ext="urn:huawei:yang:huawei-openconfig-telemetry-ext">hw-
telemetry-ext:STREAM_UDP</protocol>
    <encoding xmlns:oc-telemetry-types="http://openconfig.net/yang/telemetry-types">oc-
telemetry-types:ENC_PROTO3</encoding>
    <local-source-port xmlns="urn:huawei:yang:huawei-openconfig-telemetry-ext">55</local-
source-port>
  </state>
  <sensor-profiles>
    <sensor-profile>
      <sensor-group>sen01</sensor-group>
      <config>
        <sensor-group>sen01</sensor-group>
        <sample-interval>60000</sample-interval>
      </config>
      <state>
        <sensor-group>sen01</sensor-group>
        <sample-interval>60000</sample-interval>
      </state>
    </sensor-profile>
  </sensor-profiles>
  <destination-groups>
    <destination-group>
      <group-id>dest01</group-id>
      <config>
        <group-id>dest01</group-id>
      </config>
      <state>
        <group-id>dest01</group-id>
      </state>
    </destination-group>
  </destination-groups>
</subscription>
</persistent>
</subscriptions>
</telemetry-system>
</data>
</rpc-reply>
```

19.6 Inband Management VPN

Inband management VPN is a means by which carriers use the virtual private network (VPN) to manage and maintain devices and the management protocol on the device can use virtual routers for route forwarding.

19.6.1 Introduction to Inband Management VPN

Definition

In inband management VPN (Virtual Private Network), associated inband management protocols on the device support the specified VPN instances so that management packets can be received and forwarded using multiple virtual routes. In this way, carriers can use the private network IP address to remotely manage and maintain devices. This method saves public network IP addresses and isolates the management network from the public network.

To achieve inband management VPN, both the inband management server and client must be able to receive the connection requests and data packets from VPN.

Constraints

- The outband management interface belongs to the public network but not VPN. Therefore, only the inband interface but not the outband management interface supports VPN management.
- The servers that can receive VPN requests include:
 - Telnet server
 - SSH server
 - SNMP AGENT
 - TRACE server

NOTE

SSH server is recommended.

- The clients that can receive VPN requests include:
 - FTP client
 - TFTP client
 - SFTP client
 - SNMP TRAP
 - SYSLOG
 - Telnet client
 - SSH client

NOTE

SFTP client is recommended.

19.6.2 Principles to Inband Management VPN

Basic Concepts

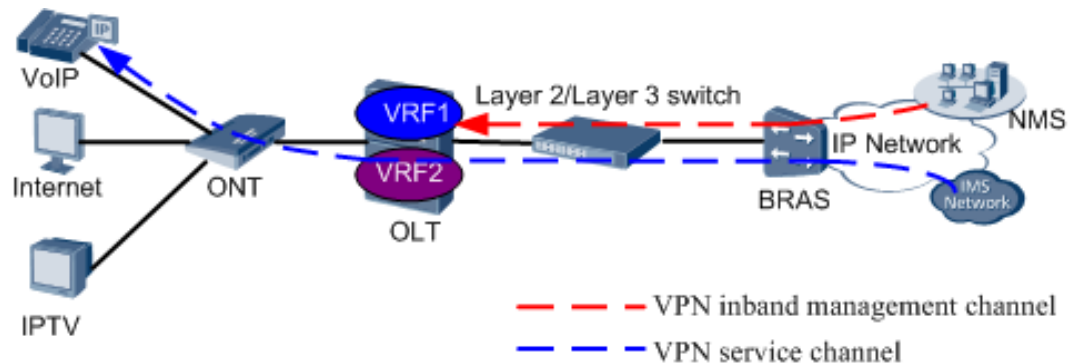
Virtual private network (VPN) is a network technology for encapsulating or encrypting private data and then transmitting the data over the public network. With this technology, the security level of the private network can be provided for the transmitted data and a private network can be constructed based on the public network. VPN is a logical private network that provides the functions of the private network. The network itself, however, is not an independent physical network. In the IP bearer network, VPN is an important measure for logically isolating services, preventing attacks, and helping implement QoS control.

A VPN instance is also called a VPN routing and forwarding table (VRF). Each router is logically divided into multiple virtual routers, that is, multiple VRFs. Each VRF corresponds to a VPN and has its own routing table, forwarding table, and interface. In other words, a router shared by various VPNs is simulated as multiple private routers, thereby isolating VPN routes. Devices that are grouped into a private route exchange routing information of only the private route. After VPN maintenance and management instances are configured, the server end protocols of the device, that is, telnet server ends (SSH and CLI), SNMP, and TRACE, accept connection requests of only the specified management and maintenance VPN networks and do not accept those of other VPNs or of the public network.

Inband Management VPN

Inband management VPN uses the VRF function to add the remote NMS and the OLT to the same VPN while on the OLT classifying the management address and VoIP address to different VRFs. In this way, carriers can use the private network IP address to remotely manage and maintain devices. This method saves public network IP addresses and isolates the management network from the public network.

Figure 19-24 Network diagram of inband management VPN



In [Figure 19-24](#), two VRFs (VRF1 and VRF2) are defined on the OLT. VRF2 is the VoIP service channel and VRF1 is the VPN inband management channel.

On the OLT, if a system-level VPN instance for management and maintenance is configured, all related management protocols by default use this VPN instance to connect to or send data to the remote server. In addition, if a user specifies the VPN instance of a single server when configuring the trap destination server or running the telnet command, these two management protocols (for trap and telnet) do not use the system-level VPN instance but instead use the specified VPN instance to connect to the remote server.

19.7 Remote Software Commissioning (Ethernet)

This section describes the implementation principles and configuration of remote software commissioning using Ethernet upstream transmission.

19.7.1 Introduction

During the deployment of the multi-dwelling unit (MDU) in the Ethernet upstream networking or the deployment of the OLT, you need to configure management channel parameters after installing the device so that the device can be managed. To avoid onsite commissioning and reduce the engineering deployment cost, the MDU and OLT provide the remote software commissioning function for Ethernet upstream transmission. After a device is powered on, management data and service data can be automatically configured.

Remote software commissioning for Ethernet upstream transmission can be implemented based on Dynamic Host Configuration Protocol (DHCP) or neighbor automatic communication (NAC).

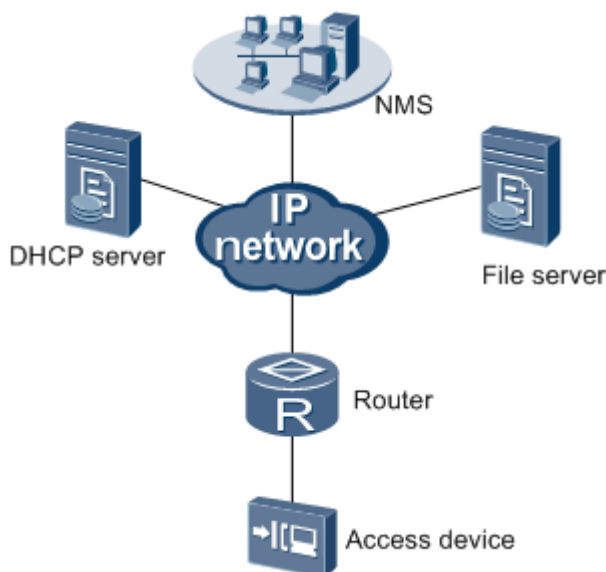
 NOTE

Run the **sysman server source** command to bind a specified source port to the SNMP/SSH/NETCONF service protocol first in V100R020C00 and later versions.

DHCP-based Remote Software Commissioning for Ethernet Upstream Transmission

Figure 19-25 shows the networking diagram for this solution.

Figure 19-25 Networking of DHCP-based remote software commissioning for Ethernet upstream transmission



1. Bind the IP address and MAC address of the access device (MDU or OLT) according to the network planning, and configure the data on the DHCP server.
2. After the access device is powered on, it automatically sends a DHCP request to the DHCP server. The DHCP server allocates an IP address to the access device based on the mapping between the IP address and the MAC address

NOTICE

If you log in to the device when the DHCP remote software commissioning function is enabled, the remote software commissioning process may be interrupted. To restart the remote software commissioning function, clear the database and reset the device.

3. The access device requests the policy file from the FTP server and loads the policy file for remote commissioning.

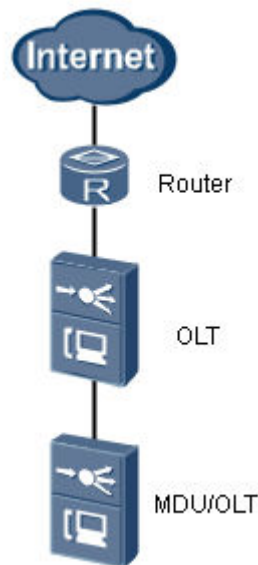
NOTICE

- DHCP-based Remote Software Commissioning packets are not encrypted. Ensure that the DHCP-based Remote Software Commissioning networking environment is secure. NETCONF ZTP software commissioning-free mode that supports identity authentication and encrypted transmission is recommended in V100R020C10 and later versions.
- Before V100R020C10 version, the SFTP protocol is not supported in DHCP-based Remote Software Commissioning. FTP and TFTP have security risks due to protocol restrictions, and can be used only in a secure environment.
- SFTP is recommended in DHCP-based Remote Software Commissioning with a higher security in V100R020C10 and later versions.

NAC-based Remote Software Commissioning for Ethernet Upstream Transmission

Figure2 Networking of NAC-based remote software commissioning for Ethernet upstream transmission show the networking diagrams for this solution.

Figure 19-26 Networking of NAC-based remote software commissioning for Ethernet upstream transmission



The NAC-based remote software commissioning solution for Ethernet upstream transmission applies two scenarios: The database of the cascaded device is empty, or the database of the cascaded device is not empty.

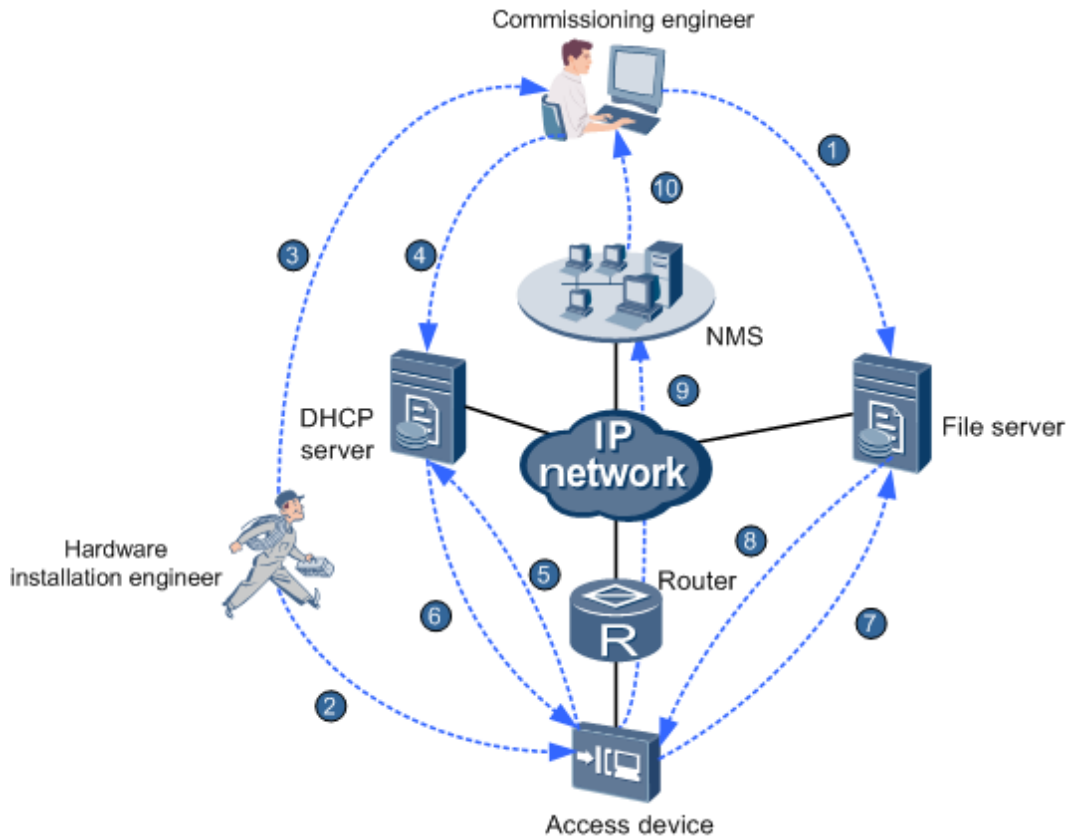
- If the database of the cascaded device is empty, the NAC protocol is used to implement remote software commissioning for Ethernet upstream transmission. In this scenario, the upper layer of the Internet can also be connected to the NMS to configure management channel parameters.
- If the database of the cascaded device is not empty, you need to log in to the cascaded device on the CLI of the transparent channel and perform

operations to implement the remote software commissioning for Ethernet upstream transmission.

19.7.2 Principles (Based on DHCP)

Figure 19-27 shows the implementation of DHCP-based remote software commissioning for Ethernet upstream transmission.

Figure 19-27 Implementation of DHCP-based remote software commissioning for Ethernet upstream transmission



NOTE

DHCP-based remote software commissioning for Ethernet upstream transmission is configured on the upper-layer devices instead of on access devices.

Before R019C20 version, the DHCP packets sent to the upper-layer device are untagged. A port default VLAN ID (PVID) must be configured on the upper-layer device to transparently transmit these DHCP packets; in R019C20 and later versions, the access device updates the VLAN (VLAN 1 to VLAN 16) and upstream ports one by one and attempts to obtain an IP address through DHCP.

The process is as follows:

1. A commissioning engineer prepares the pre-configuration policy file and policy description file and uploads them to the FTP server.

For a policy file:

- If different devices require different policy files, the policy files can be named in the [IP]_stFile.txt or [MAC]_stFile.txt format. If the policy file is

in the [IP]_stFile.txt format, ensure that the IP address of the device does not conflict with those of other devices. You can bind the IP address of a device to a MAC address to avoid IP address conflict.

- If devices of same type use the same policy file, the name of the configuration file can be a common string.
 - IP indicates the IP address planned for a device. For example, if the IP address of a device is 192.168.10.10, the policy file of the device is named 192.168.10.10_stFile.txt.
 - MAC indicates the actual MAC address of a device. For example, if the MAC address of a device is 00E0FC11ABEE, the policy file of the device is named 00-E0-FC-11-AB-EE_stFile.txt.
 - The policy file name is a common character string, for example, OLTxxxstFile.txt (*example*). All devices of the same type use the policy file.

For a policy description file:

- The name of a policy description file must be in the format of xxx.ini. The file content includes the path for storing the policy file and the name of the policy file.
- The format and content of a policy description file must be correct. Otherwise, the remote software commissioning flow may be interrupted. If this happens, operators must remotely log in to the device using the IP address allocated by the DHCP server and reset the device. Alternatively, operators can reset the device onsite. Then, the remote software commissioning flow can be restarted.
- One site requires only one policy description file.
- For example, the policy file for a site is named by an IP address. The content of the policy description file is as follows (the following is only an example, and the file name must be consistent with the actual plan):

```
[OLT]                               //Device type
TargetVersion=OLT Vx00RxxxCxx      //Device version
[HxxxXXXX]                         //Control board type (example)
PacketFile="Dir\xxxx_packetfile.bin" //Package file to be loaded to the control board
(Example)
CfgFile="Dir\[IP]_stFile.txt"       //Policy file to be loaded to the control board, in the
IP_stFile.txt naming format
```

2. A hardware installation engineer obtains the device, transports the device from the warehouse to a site, and installs, connects, and powers on the device.

NOTICE

Do not remove or insert a board when the device is starting. Otherwise, the device data may be abnormal.

3. The hardware installation engineer records the MAC address and site information of the access device and reports the information to the commissioning engineer.
4. The commissioning engineer creates a mapping between the MAC address, management IP address, and physical location of the access device, binds the

IP and MAC addresses of the device, and configures the device data on the DHCP server.

5. After the upstream optical path of the access device is normal (the LINK indicator is steady on), the access device automatically initiates a DHCP request to the DHCP server.
6. The DHCP server allocates the IP address to the access device based on the IP address configuration, writes the FTP information (including the FTP server address, FTP user name, password, and policy description file name) in an option packet, and sends the option packet to the access device.
7. After receiving the Option packet from the DHCP server, the access device configures the IP address and gateway and sends a request to the FTP server.
8. The FTP server delivers a policy file to the access device.
9. The access device downloads the policy file from the FTP server and automatically loads the file to complete automatic device configuration. The configuration takes effect after the device restarts. At the same time, a trap is reported to the NMS, indicating that an access device goes online.

 NOTE

If the loading fails, the system automatically retries for about 24 hours. If the loading still fails, the loading is stopped.

10. The commissioning engineer receives the access device online trap on the NMS.

When an access device online trap is received, a network management channel has been created, and the access device can be remotely managed on the NMS.

19.7.3 Configuring NAC-based Remote Software Commissioning for Ethernet Upstream Transmission

When devices are cascaded to an OLT that supports the NAC protocol, management channels to these devices can be automatically enabled without the need for a commissioning engineers to go onsite.

Prerequisites

Management parameters, including the inband management VLAN ID, management IP address, and SNMP profile parameters, have been configured on the cascading device for cascaded devices. (SNMP profile parameters are required if the cascaded devices needs to be managed on the NMS.)

Context

This section uses the scenario of connecting an MDU to an existing OLT as an example to describe the configuration process. For the scenario where an OLT is cascaded to an OLT, the configuration process is the same as that used in scenario where an MDU is cascaded to an OLT, except that the former scenario does not support automatic deployment of policy files.

 NOTE

- The MDU does not save the management parameters delivered through NAC. To save the parameters, run the **save** command. After saving the parameters, the NAC function will be disabled automatically.

In V100R021C00 and later versions, you are advised to run the **nac authentication-mode** command to configure the authentication mode for the NAC channel. By default, the authentication mode of an NAC channel is certificate authentication. If the authentication mode of the NAC channel is certificate authentication, you need to bind the PKI domain to the NAC channel for normal authentication. You can run the **nac bind pki-domain** command to bind a PKI domain.

NOTICE

Huawei devices are delivered with preconfigured certificates which are applied for and managed using the Huawei PKI platform. To improve system security, you are advised to replace the preconfigured certificates and keys with your own certificates and keys and periodically update the certificates and keys.

Pay attention to the validity period of the certificates. Generally, the start time of a certificate is the time when the certificate is issued, and the end time is the time when the certificate expires. You can run the **display pki certificate** command to query the validity period of a certificate.

When a certificate is about to expire or has expired, the system reports an alarm indicating that the certificate is about to expire or has expired, prompting users to promptly update the certificate.

Device certificates can be updated using the following methods:

- **Method 1: Apply for a certificate online using CMPv2.**
 - a. Run the **rsa pki local-key-pair create** command to create a local RSA (Ron Rivest, Adi Shamirh, Leonard Adleman) key pair.
 - b. Run the **pki entity** command to create a PKI entity.
 - c. Run the **pki domain** command to create a PKI domain and run the **pki import-certificate** command to import a certificate file.
 - d. Run the **ssl policy** command to create an SSL policy and run the **pki-domain** command to bind a PKI domain.
 - e. Run the **pki cmp session** command to create a Certificate Management Protocol (CMP) session and enter CMP session mode.
 - f. Run the **cmp request** command to configure a local certificate, CA certificate, and URL of the CMP server.
 - g. Run the **pki domain** command to enter PKI domain mode, and run the **certificate request** command to specify the local RSA key pair, PKI entity information, and CMP session information for certificate application.
 - h. In PKI domain mode, run the **cmp initial-request** command to apply for a certificate online.
- **Method 2: Apply for a certificate offline and import it to the device.**

- a. Apply for a certificate outside the device.
- b. Run the **load pki certificate** command to load the obtained certificate to the device.

Procedure

- The MDU database is empty.
 - a. Enable NAC on the OLT.

The OLT port connected to the MDU is 0/2/0.

```
huawei(config)#nac enable master security 0/2 0
```

 NOTE

When enabling NAC on the OLT, you are advised to select **security** to enable the security mode. Then, the master node encrypts remote software commissioning parameters before sending them to a slave node. This improves parameter security.

- b. Pre-configure remote software commissioning parameters for the MDU on the OLT and check whether the pre-configuration is successful.

The MDU inband management VLAN ID is 8, the management IP address is 192.168.50.2, the IP address of the gateway is 192.168.50.254, and the SNMP profile ID is 64. These parameters can be configured in two ways:

 NOTE

When both NAC and RN configuration commands are executed, the latter overrides the previous one.

Configure and query parameters using NAC commands:

```
huawei(config)#nac config master 0/2/0 slave vlan 8 priority 3 ip-address 192.168.50.2  
mask 255.255.255.0 gateway 192.168.50.254 snmp-profile-id 64
```

```
huawei(config)#display nac configuration master  
{ <cr>|frameid/slotid/portid<S><Length 5-18>|frameid/slotid<S><Length 3-15> }:
```

Command:
display nac configuration master

```
-----  
Frame ID/Slot ID/Port ID : 0/2/0  
VLAN : 8  
VLAN priority : 3  
IP address : 192.168.50.2  
Mask : 255.255.255.0  
Gateway : 192.168.50.254  
Snmp-profile-id : 64  
Snmp-profile-name : snmp-profile_64  
-----
```

Total: 1

Configure and query parameters using RN commands:

```
huawei(config)#rn ipconfig 0/2/0 ip-address 192.168.50.2 mask 255.255.255.0 gateway  
192.168.50.254 vlan 8 priority 3  
huawei(config)#rn snmp-config 0/2/0 snmp-index 0 profile-id 64
```

```
huawei(config)#display rn info 0/2/0
```

Command:
display rn info 0/2/0

```
-----  
F/S/P : 0/2/0  
Equipment ID : XXXXXX // "XXXXXX" is the MDU name.  
Uplink type : ETH  
MAC/SN : xxxx-xxxx-xxxx  
-----
```

```

Run state      : Offline
Config state   : -
IP             : 192.168.50.2
Subnet mask    : 255.255.255.0
Gateway        : 192.168.50.254
Manage VLAN    : 8
Manage priority : 3
Deploy profile ID : -
Deploy profile name : -
-----
Index  SNMP      SNMP      Effective
      Profile ID Profile name      Flag
-----
0     64      snmp-profile_64      No
1     -       -              -
-----

```

- c. Configure an automatic deployment policy profile (applicable only to the scenario when the OLT is cascaded with an MDU).

The profile name is `deploy-profile_1`, the policy file name of the MDU is `stfile`, the IP address is `10.10.10.10`, the file transfer protocol is FTP, the user name is `user1`, and the password is `user123` (the system does not display the entered password).

```

huawei(config)#rn deploy-profile add profile-id 1 profile-name deploy-profile_1 filename
stfile ip 10.10.10.10 ftp user user1

```

- d. Bind the automatic deployment policy profile to the MDU (applicable only to the scenario when the OLT is cascaded with an MDU).

Bind the profile based on ports:

```

huawei(config)#rn deploy-config 0/2/0 profile-id 1

```

Bind the profile based on device types:

```

huawei(config)#rn deploy-policy MAXXXX profile-id 1 //Change MAXXXX to the actual MDU
type.

```

NOTE

The port-based profile binding takes precedence over the device type-based profile binding.

- e. After the MDU is powered on, it exchanges data with the OLT to obtain the MDU device management parameters and service configuration parameters. Wait for 2 minutes. Then, run the `ssh` command to remotely log in to the MDU.
- f. Query the devices connected to the OLT cascading port.

The query can be performed in two ways:

Using NAC commands:

```

huawei(config)#display nac slave info detail
-----
NAC master port      : 0/2/0
NAC auto-find fsm state : Established
NAC auto-find result  : Found
Multiple slave node exist : No
Slave node device type : XXXXXX // "XXXXXX" is the MDU name.
Slave node mac-address : 00-E0-FC-01-00-52
NAC slave port       : 0/0/1
NAC config fsm state  : INIT
NAC config result     : Added successfully
NAC config fail reason : -
-----

```

Using RN commands:

```
huawei(config)#display rn info 0/2/0
Command:
display rn info 0/2/0
-----
F/S/P      : 0/2/0
Equipment ID : XXXXXX // "XXXXXX" is the MDU name.
Uplink type  : ETH
MAC/SN      : xxxx-xxxx-xxxx
Run state    : Online
Config state : Normal
IP           : 192.168.50.2
Subnet mask  : 255.255.255.0
Gateway      : 192.168.50.254
Manage VLAN  : 8
Manage priority : 3
Deploy profile ID : 1
Deploy profile name : deploy-profile_1
-----
Index  SNMP      SNMP      Effective
      Profile ID Profile name      Flag
-----
0      64      snmp-profile_64      Yes
1      -       -              -
-----
```

- g. (Optional) Disable NAC on the OLT.
- Perform this operation after the MDU obtains the device management parameters. This prevents the OLT from delivering the planned data to a substitute MDU.

```
huawei(config)#nac master 0/2 0 lock
```

- The MDU database is not empty.

NOTICE

The packets transmitted through a transparent channel are not encrypted and involves risks. Exercise caution when performing this operation.

The following describes only the configuration process if the MDU database must be erased. The configuration is simple if the MDU database does not need to be erased because you only need to perform the operations in **b** to log in to the MDU and configure device management parameters on the MDU.

 NOTE

The transparent channel is enabled on the MDU by default. To ensure system security or if the transparent channel is not used, run the **transparent remote disable** command to disable it.

- a. Perform steps **a-d**.
- b. After the MDU is powered on, enable the transparent channel on the OLT port, and log in to the MDU.

The OLT port connected to the MDU is 0/2/0.

```
huawei(config)#diagnose
huawei(diagnose)%%transparent on 0/2/0
>>User name:huawei //Enter the user name of the MDU.
>>User password: //Enter the user password.
```

```
Huawei Integrated Access Software (huawei).  
Copyright(C) Huawei Technologies Co., Ltd. 2002-2013. All rights reserved.
```

```
-----  
User last login information:  
-----
```

```
Access Type : Serial  
IP-Address : --  
Login Time : 2013-07-21 01:04:17+08:00  
Logout Time : 2013-07-21 05:19:35+08:00  
-----
```

```
User root has used a default password. Change the password in time.
```

c. Erase the MDU database.

 NOTE

The default command mode of **erase flash data** varies with the software version.
The following configuration is for reference only.

```
huawei>enable  
huawei#erase flash data  
This command will clear the active board data that has been loaded or saved  
Please remember to backup the system  
configuration data  
Are you sure to continue? (y/n)[n]:y  
Command executes successfully, and will take effect after active board  
rebooted
```

d. Reset the MDU.

```
huawei#reboot system  
Please check whether data has saved, the unsaved data will lose if reboot  
system, are you sure to reboot system? (y/n)[n]:y
```

e. After the MDU is reset, OLT commands are displayed. Wait for 2 minutes, then check the remote software commissioning result.

The query can be performed in two ways:

Using NAC commands:

```
huawei(diagnose)%%quit  
huawei#display nac slave info detail  
-----  
NAC master port      : 0/2/0  
NAC auto-find fsm state : Established  
NAC auto-find result  : Found  
Multiple slave node exist : No  
Slave node device type : XXXXXX // "XXXXXX" is the MDU name.  
Slave node mac-address : 00-E0-FC-01-00-52  
NAC slave port       : 0/0/1  
NAC config fsm state  : INIT  
NAC config result     : Added successfully  
NAC config fail reason : -  
-----  
Total: 1
```

Using RN commands:

```
huawei(config)#display rn info 0/2/0  
Command:  
display rn info 0/2/0  
-----  
F/S/P      : 0/2/0  
Equipment ID : XXXXXX // "XXXXXX" is the MDU name.  
Uplink type  : ETH  
MAC/SN      : xxxx-xxxx-xxxx  
Run state    : Online  
Config state : Normal
```

```
IP          : 192.168.50.2
Subnet mask : 255.255.255.0
Gateway     : 192.168.50.254
Manage VLAN : 8
Manage priority : 3
Deploy profile ID : 1
Deploy profile name : deploy-profile_1
-----
Index  SNMP      SNMP      Effective
      Profile ID Profile name   Flag
-----
0     64      snmp-profile_64    Yes
1     -       -                -
-----
```

- f. Run the **ssh** command to remotely log in to the MDU.

 NOTE

The transparent channel commands for logging in to a device are diagnostic commands. After Layer 3 communication is set up, log in to and configure the MDU in remote mode in priority.

----End

19.7.4 Remote Software Commissioning (Ethernet) Reference Standards and Protocols

The following table lists the reference standards and protocols of remote software commissioning using Ethernet upstream transmission.

Standard	Description
IETF RFC 2131	Dynamic Host Configuration Protocol
IETF RFC 1533	DHCP Options and BOOTP Vendor Extensions
IEEE 802.3ah-2004	IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks

19.8 OLT ZTD

With the zero touch deployment (ZTD) feature, OLTs are plug-and-play and can be automatically deployed.

19.8.1 Feature Updates

Table 19-14 Feature Updates

Product Version	Change Description
V100R019C2X and later versions	The first version to support this feature

19.8.2 Why the OLT Needs to Support ZTD

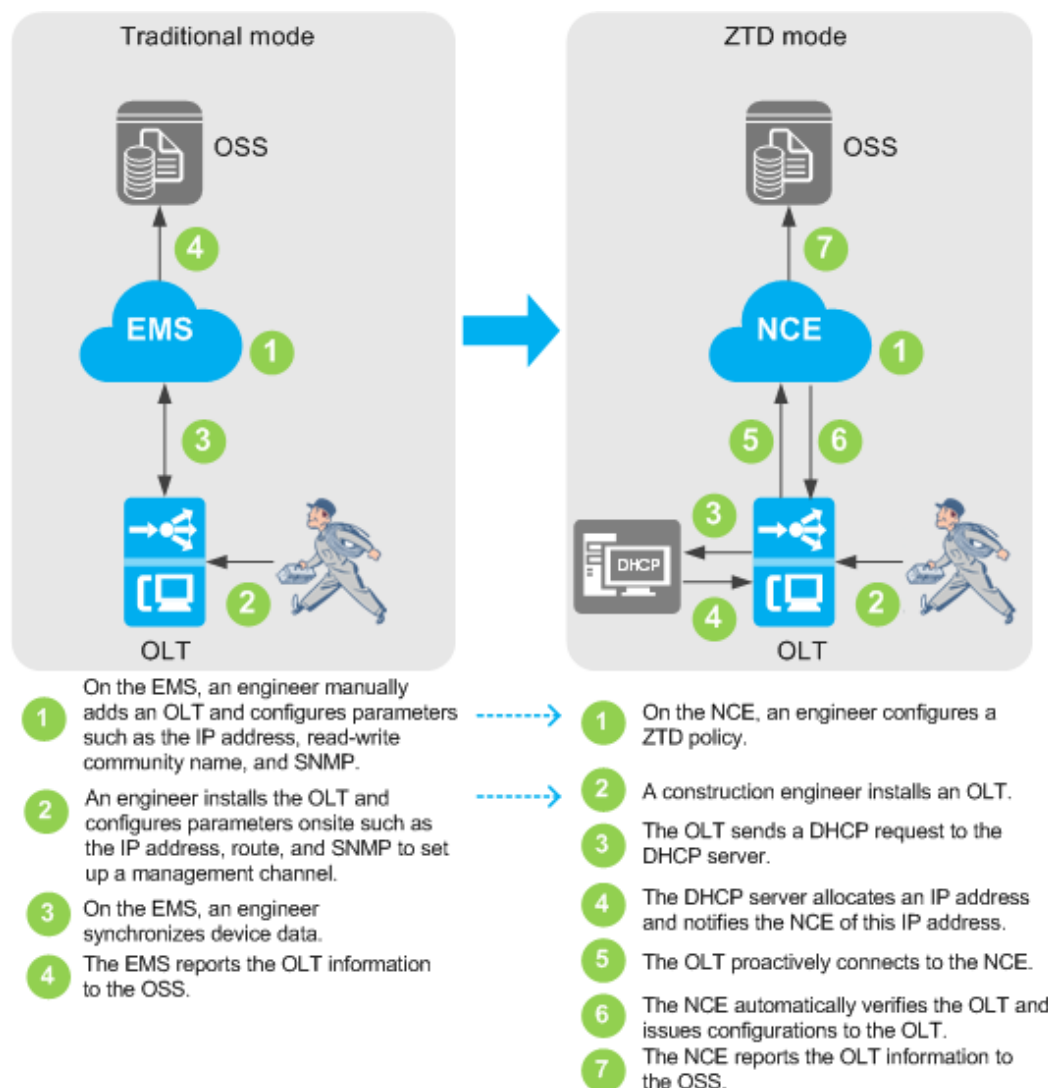
When devices are deployed in traditional mode, the following problems exist:

- OLT configuration parameters need to be manually added, which is prone to errors.
- Each OLT needs to be configured separately, which is time-consuming.
- Onsite software commissioning requires a technical foundation for onsite construction personnel and multiple site visits. In this case, plug-and-play is not supported.

As shown in the following figure, a ZTD network can be constructed to implement plug-and-play and automatic deployment of network devices. The ZTD feature improves the service rollout efficiency of network devices and reduces operating costs.

- Unified ZTD configuration policy, verification in advance, zero-error delivery, one-time configuration, and process-based running
- Automatic setup of a management channel without the need of secondary site visits, improving the OLT deployment efficiency and reducing the workload of installation and maintenance personnel

Figure 19-28 Comparison between the traditional configuration mode and the ZTD configuration mode



The OLT works with the Network Cloud Engine (NCE) to implement the plug-and-play function. The OLT supports the NETCONF CALL HOME feature (described in RFC 8071). After an OLT is connected to the NCE, the NCE reports the OLT information to the upper-layer equipment serial number (ESN) whitelist system for authentication. An NE supports plug-and-play after it passes the whitelist authentication.

NOTE

After the CALL HOME service is enabled, the system automatically creates a default NETCONF administrator (user name: ncroot; password: NFRoot.123).

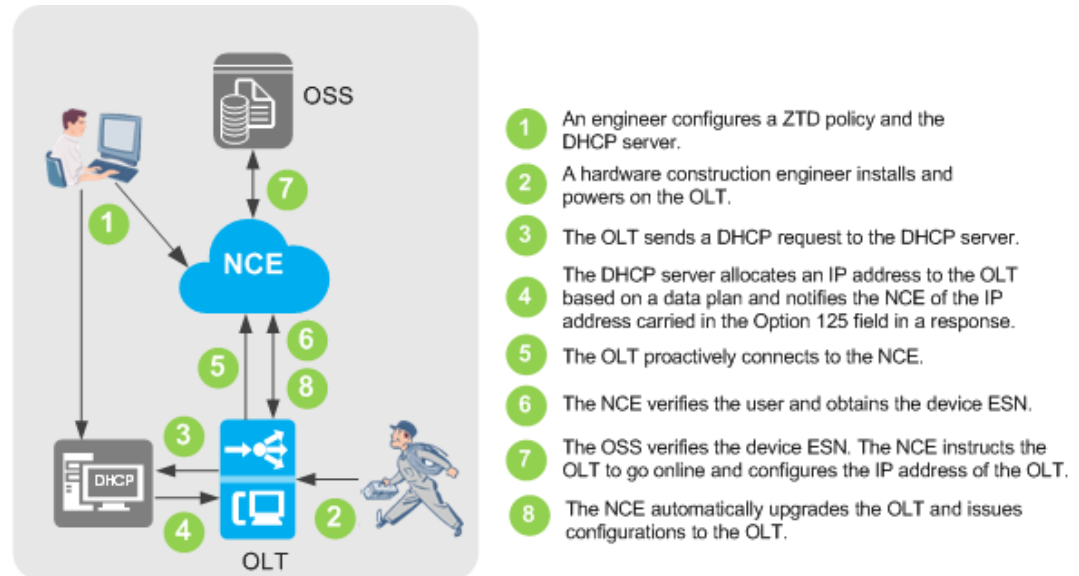
19.8.3 OLT ZTD Application Scenarios

OLT Initial Installation Without the Need of commissioning

After an OLT is powered on and passes cloud-based verification, the NCE automatically upgrades the OLT and issues configurations to the OLT based on a

preconfigured process. After configuring basic NE communication parameters on the NCE, an installation and maintenance engineer only needs to install and power on the OLT to provision services and does not need to perform onsite software commissioning.

Figure 19-29 Process of OLT initial installation without the need of commissioning

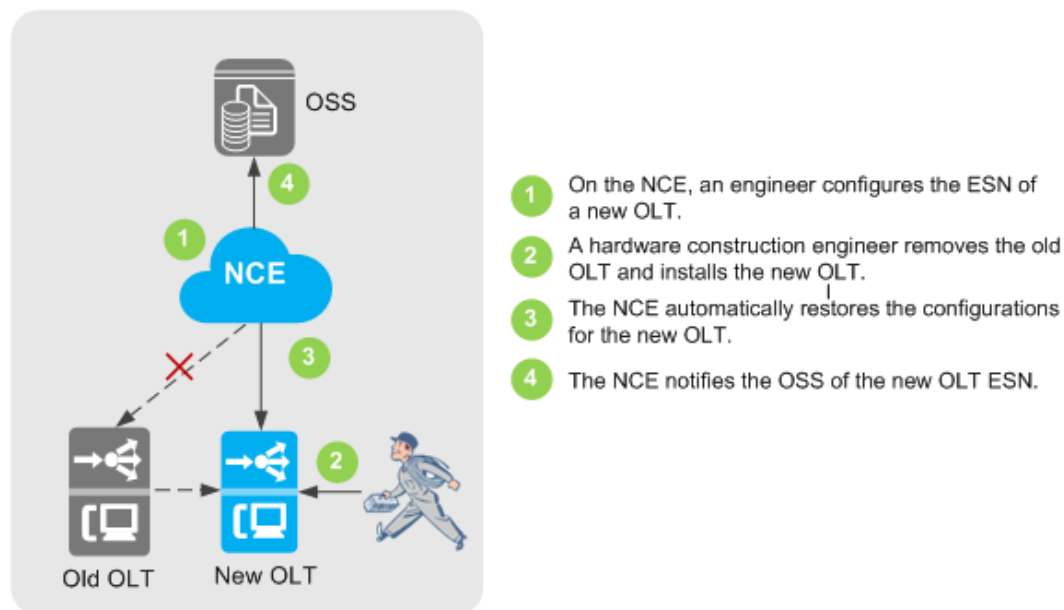


OLT Replacement Due to a Fault

When an OLT needs to be completely replaced because of a subrack fault or when the backplane needs to be replaced, it is required that the software version and data remain the same after the replacement is complete.

On the NCE interface, enter the equipment serial number (ESN) of the old and new OLTs. Replace the correct OLT at the site directly. Then services can be restored through the Call Home power-on process.

Figure 19-30 OLT replacement process

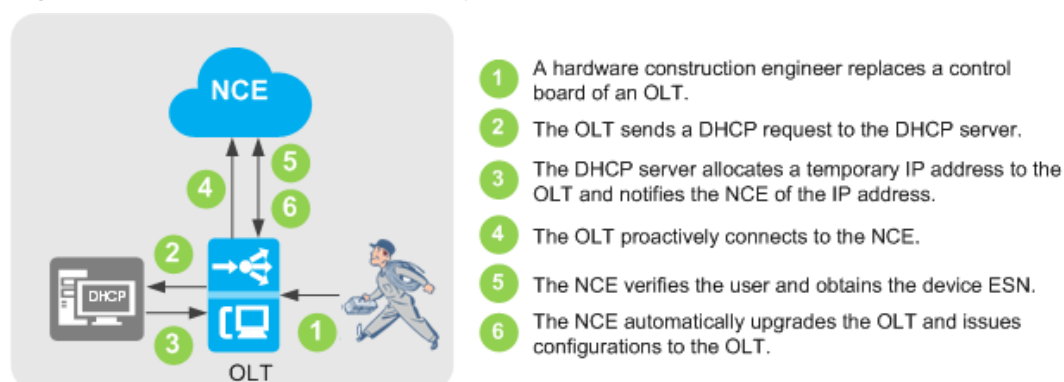


OLT Control Board Replacement Due to a Fault

If control board replacement is required when both the active and standby control boards of an OLT are faulty or when the only control board of an OLT is faulty, the software version and data must remain the same after the replacement is complete.

After a control board is replaced, the NCE applies the original configurations to the OLT based on the same ESN to recover services.

Figure 19-31 OLT Control Board Replacement Process



19.9 Power Saving

19.9.1 Introduction to Energy Saving

Definition

The energy saving technology enables the system to automatically detect the usage or service load of each functional module, board, and interface unit of a device. When a module is idle or the load is light, the system automatically disables the module or enables the module to enter low energy consumption mode to reduce the energy consumption of the device.

Purpose

With the surge of bandwidth requirements of broadband users, fiber-in copper-out has accelerated and FTTH, as the current and future mainstream fixed broadband access mode, has a substantial market space. As a result, optical access devices consume significantly more power than other fixed access devices. To reduce such energy consumption and carbon emission, and build a greener ultra-broadband access network, the FTTH energy saving solution is developed.

Benefits

The solution aims to reduce the energy consumption and carbon emission of devices, thereby reducing device use costs.

19.9.2 Energy Saving Principles

19.9.2.1 Energy Saving Principles

To simplify the application and management of the energy saving solution and as different energy saving measures have different impacts on service quality and O&M, an OLT supports five device-level energy saving modes: standard mode, basic mode (default), deep mode, optimal mode, and custom mode. The standard mode supports the fewest energy saving measures but does not have any impact on products. The optimal mode prioritizes energy saving but may affect product service quality and O&M. The custom mode supports flexible configuration of various energy saving measures as required by customers.

Mode	Function Description	Impact on Services
Standard mode	An OLT supports dynamic speed adjustment only for fans. For other hardware components, an OLT supports only static energy saving measures. For example, during device or board initialization, an OLT permanently disables the redundant interfaces and function units of the chips.	This mode does not have any adverse impact on the product. It will not be perceived by users and does not affect user experience.

Mode	Function Description	Impact on Services
Basic mode	In addition to the measures supported by the standard mode, the basic mode supports configuration-based dynamic energy saving. For example: • 19.9.2.2.1 Automatic Shutdown of Unused High-speed Interfaces • 19.9.2.2.2 Automatic Zone-based Fan Speed Adjustment	This mode does not have any adverse impact on the product. It will not be perceived by users and does not affect user experience.
Deep mode	In addition to the measures supported by the basic mode, the deep mode supports application-based dynamic energy saving. For example: • 19.9.2.2.3 Automatic Shutdown of Unused Ports • 19.9.2.2.4 Automatic Shutdown of Unused Boards	This mode has certain impact on the O&M. For example: it will take 2 to 3 minutes to restart a disabled board, and 1 to 2 seconds to enable a disabled port. The electronic label of a disabled board cannot be queried. The mode does not have adverse impact on service quality, but affects new service rollout time due to board and port restart and energy saving configuration check and execution. Port level: The time for new service rollout on a disabled port is prolonged. (by about 1 to 20 seconds). Board level: The time for new service rollout on a disabled board is prolonged (by about 2 to 3 minutes). The electronic label of a disabled board cannot be queried.

Mode	Function Description	Impact on Services
Optimal mode	In addition to the measures supported by the deep mode, the optimal mode supports service load-based dynamic energy saving. See 19.9.2.2.6 Dynamic Frequency Adjustment .	The optimal mode enables a device to run with optimal energy efficiency, but may decrease service performance and quality. For example, in the case of burst traffic, the mode may cause momentary packet loss or bit errors. NOTE The mode is not recommended for normal situations and is suitable only for scenarios where energy efficiency is a top priority.
Custom mode	In this mode, in addition to some default energy saving measures (such as automatic fan speed adjustment), users can customize other measures, such as: • 19.9.2.2.3 Automatic Shutdown of Unused Ports • 19.9.2.2.4 Automatic Shutdown of Unused Boards • 19.9.2.2.5 Automatic Shutdown of Unused Channels • 19.9.2.2.7 Intelligent Board Scheduling	The impact of the mode is determined by customized measures. Disabling unused ports: This measure does not have adverse impact on existing services, but affects the time of new service rollout on disabled ports (by about 1 to 20 seconds). Disabling unused boards: This measure does not have adverse impact on existing services, but affects the time of new service rollout on disabled boards (by about 2 to 3 minutes). The electronic label of a disabled board cannot be queried. Disabling unused channels: This measure does not have adverse impact on existing services, but affects the time of new service rollout in disabled channels (by about 1 to 20 seconds). Intelligent board scheduling: in the case of burst traffic, the mode may slightly increase the latency. NOTE The custom mode can be configured only after the corresponding license is applied for on the NMS, and cannot be directly configured on the CLI.

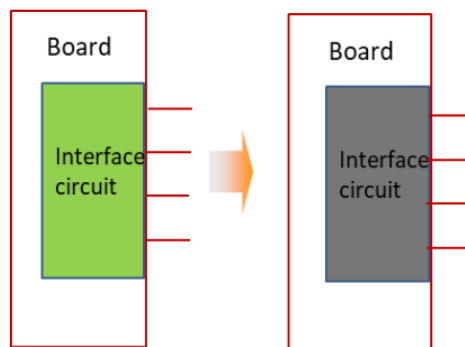
19.9.2.2 Energy Saving Technology Description

19.9.2.2.1 Automatic Shutdown of Unused High-speed Interfaces

An OLT working in basic energy saving mode can detect the usage of high-speed interfaces. When a high-speed interface is not in use, the device automatically shuts down the interface to reduce energy consumption. When the interface needs to be used, the device automatically wakes it up. This does not affect the use of the product. For example:

- When detecting that a service board is not installed in a slot, the system automatically disables the control board high-speed interface that connects to this slot, thereby reducing energy consumption of the control board.
- When detecting that an optical module is not installed on a PON port, the system automatically disconnects the interface circuit of the PON port.

Take a control board for example. The energy saving technology can save 40% energy consumption of a control board in idle state.



Detection scope: all service board slots of a subrack

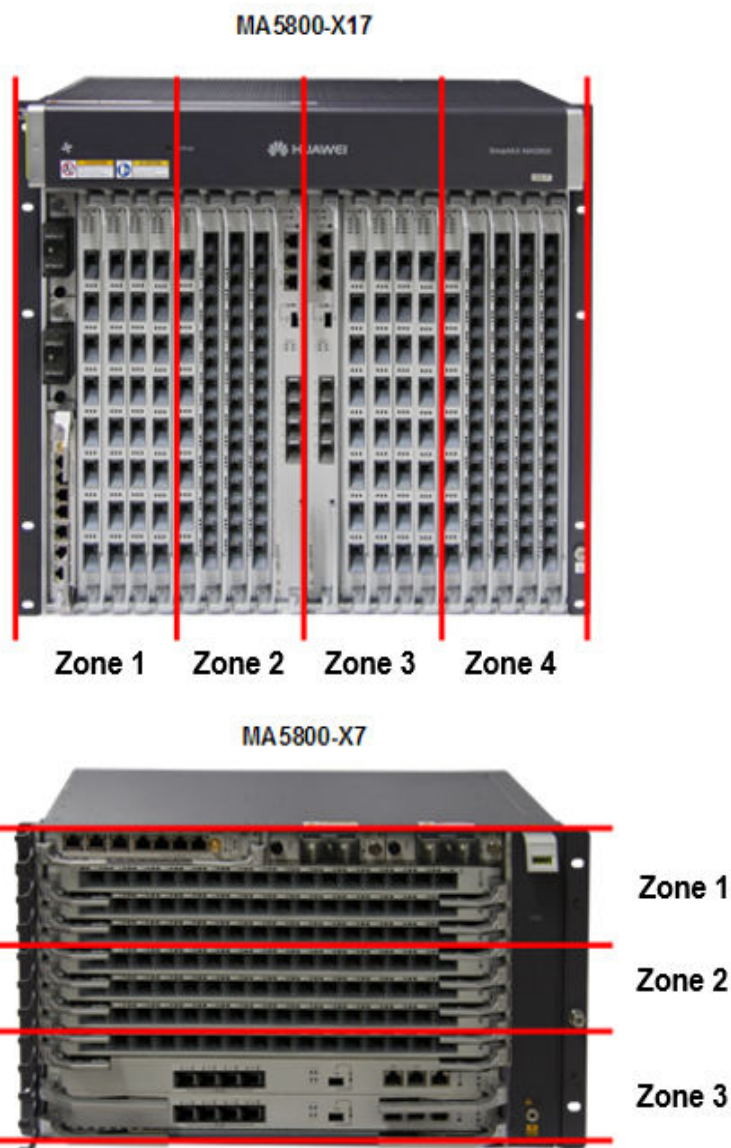
Detection mechanism:

1. The system checks all slots every several seconds. When detecting that a service board is not installed in a slot or powered off, the system disables the control board high-speed interface that connects to the slot service board.
2. After the board is inserted, the board registration process automatically enables the high-speed interface.
3. During board configuration restoration, if the system detects that an optical module is not installed, it disables the high-speed interface circuit on the board.
4. After the optical module is removed or inserted, the system detects the installation status change of the optical module and automatically disables or enables the high-speed interface on the board.

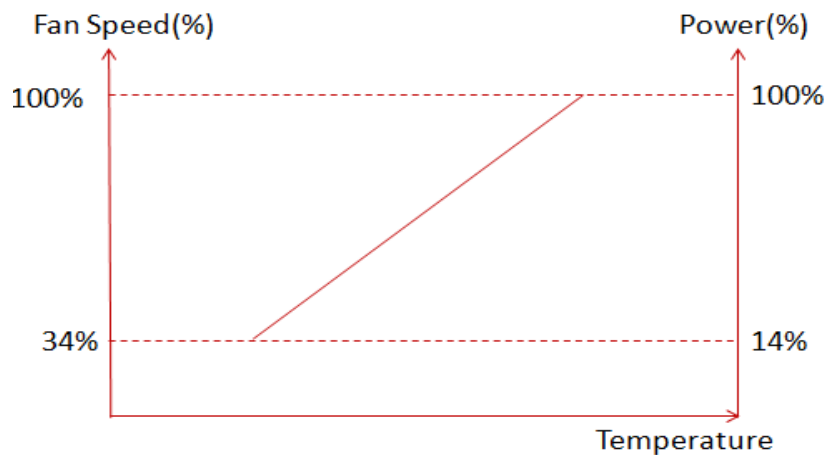
19.9.2.2.2 Automatic Zone-based Fan Speed Adjustment

Fans in the subrack of an OLT do not run at a monotonous speed. Instead, an OLT working in basic energy saving mode collects information through the control

board about service board temperatures and zones where the service boards reside. According to the current and target temperatures of each board, the device implements stepless speed adjustment by zone (as shown in the following figure). In this way, fan noises and energy consumption are minimized without affecting reliable running of the device.



The following figure shows the relationships between the fan speed, temperature, and energy consumption.



Detection scope: subracks divided into multiple zones

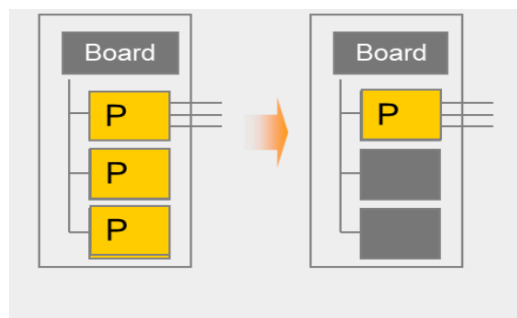
Detection mechanism: The system collects information about temperatures of all normal boards every several seconds and sends it to the fans. Then the fans implement stepless speed adjustment by zone based on the current and target temperatures of each board.

Exceptions:

1. Some subracks only have one zone and do not support this function.

19.9.2.2.3 Automatic Shutdown of Unused Ports

An OLT working in deep energy saving mode can detect the usage of PON board ports. When detecting an unused port, the device automatically shuts down the interface circuits and optical module of the port to reduce energy consumption. When the port needs to be used, the device automatically enables the port and restores it to the normal running state. This does not have any impact on existing service, but may affect new service rollout time on the port (by about 1 to 20 seconds). This technology saves energy consumption by 1.1 W per port for GPON and 1 W per port for Combo PON.



Definition of an unused port:

If ONT auto-discovery check is enabled, a port is considered an unused port when the following conditions are met.

1. No ONT is added to the port.
2. The port does not belong to a Type B or Type C dual-homing protection group.

3. The port is not configured with ONT auto-discovery.

If ONT auto-discovery check is disabled (**ont autofind energy-saving enable**), a port is considered an unused port when the following conditions are met:

1. No ONT is added to the port.
2. The port does not belong to a Type B or Type C dual-homing protection group.

Detection scope: GPON or EPON ports only

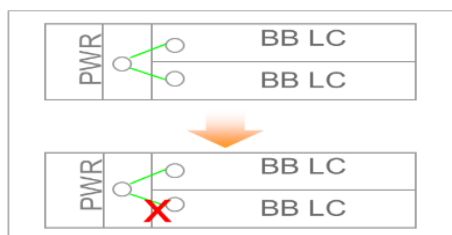
Detection mechanism: Generally, when users enable automatic shutdown of unused ports or switch to the deep or optimal energy saving mode, the system checks all GPON and EPON ports on each normal board every several seconds. When detecting an unused port, the system disables it. When detecting that a port that needs to be used is shut down for energy saving, the system enables it.

Exceptions:

1. If a user disables automatic shutdown for a specific port (**system energy-saving disable f/s/p**), the port will not be automatically disabled for energy saving.
2. If the energy saving mode of a port is switched to manual shutdown (**system energy-saving mode [deep| optimal | custom] method unused-port-shutdown shutdown-operator manual**), the port will not be automatically disabled for energy saving.
3. An L-type board does not support this function.

19.9.2.2.4 Automatic Shutdown of Unused Boards

An OLT working in deep energy saving mode can detect the usage of boards. When detecting an unused board, the OLT automatically shuts down power supply of the board to ensure zero energy consumption. When the board needs to be used, the OLT automatically powers on the board and restores it to the normal running state. This does not have any impact on existing service, but restarting a board may affect the new service rollout time on the board (by about 2 to 3 minutes). This technology can reduce the energy consumption by 100%.



Definition of an unused board:

An ETH access board is considered an unused board when the following conditions are met:

1. The board is not configured with a protection group.
2. There is no service flow on the board.

A PON access board is considered an unused board when the following conditions are met:

1. The board is not configured with a protection group.
2. There is no service flow on the board.
3. All ports are unused ports (see the definition of unused port), that is, no ONT is added to any port, no Type B or Type C dual-homing protection group is configured on any port, and ONT auto-discovery is not configured or checked.

Detection scope: PON boards and ETH access boards

Detection mechanism:

The system checks all service boards every several seconds. When detecting that all ports on an idle board without any configuration change in 2 minutes have been disabled for more than 15 minutes, the system shuts down the board. When detecting that the board service configurations change, the system powers on the board immediately.

Exceptions:

1. If a user disables automatic shutdown for a specific board (**system energy-saving disable f/s**), the board will not be automatically disabled for energy saving.
2. If the energy saving mode of a board is switched to manual shutdown (**system energy-saving mode [deep | optimal | custom] method unused-board-shutdown shutdown-operator manual**), the board will not be automatically disabled for energy saving.
3. An L-type board does not support this function.

19.9.2.2.5 Automatic Shutdown of Unused Channels

If automatic shutdown of unused channels is enabled on an OLT working in custom energy saving mode, the OLT detects boards with multiple channels. When detecting an unused channel, the device automatically shuts down the laser of the channel to reduce energy consumption. When detecting that the channel needs to be used, the device automatically enables the channel and restores it to the normal running state. This does not affect the use of the board. This technology can reduce the energy consumption by 0.3 W per channel.

Definition of an unused channel:

If the port where the channel resides is not configured with a protection group and no ONT is added to the channel, the channel is considered an unused channel.

If the port where the channel resides is configured with a protection group and no ONT is added to the channel of the master port, the channel is considered an unused channel.

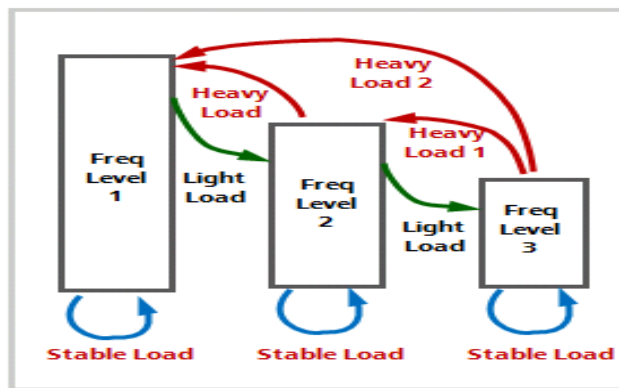
Detection scope: boards with multiple channels

Detection mechanism: When a user switches to the custom mode and enables automatic shutdown of unused channels, the system checks all channels of each

normal board every several seconds. When detecting an unused channel, the system shuts it down. When detecting that a channel that needs to be used is shut down for energy saving, the system enables it.

19.9.2.2.6 Dynamic Frequency Adjustment

An OLT working in optimal energy saving mode can detect the service load of some service boards. When detecting that a service board is carrying a small service load, the device automatically reduces the working frequency of the service processing module of the board to reduce energy consumption. When the service load of the board increases, the device automatically increases the working frequency of the service processing module to meet service needs. This technology can reduce the energy consumption by 2 to 3 W per board.



⚠ CAUTION

In the case of burst traffic, this function may cause momentary packet loss or bit errors.

19.9.2.2.7 Intelligent Board Scheduling

An OLT working in custom energy saving mode can detect the service load of some service boards. When detecting that a service board is carrying a small service load, the device automatically reduces the working frequency of the service processing module of the board to reduce energy consumption. When the service load of the board increases, the device automatically increases the working frequency of the service processing module to meet service needs.

This technology can reduce the energy consumption by 2 to 3 W per board.

⚠ CAUTION

In the case of burst traffic, this function will not cause packet loss but may increase the latency for a short time.

19.9.3 Energy Saving Modes and Constraints

- The following technologies can be used to configure the custom energy-saving mode: automatic shutdown of unused ports, automatic shutdown of unused boards, intelligent board scheduling, and automatic shutdown of unused channels.
- Automatic shutdown of unused high-speed interfaces and automatic fan speed adjustment by zone are enabled in custom mode and cannot be disabled.
- The dynamic frequency adjustment technology may cause packet loss in the case of burst traffic.
- After an optical module is removed and re-inserted, the board does not report an alarm indicating that the optical module is not in position if board energy saving is enabled.
- If an alarm indicating that the optical module is not in position needs to be reported after port energy saving is enabled, you need to run the **xpon alarm optical-module-alarm control disable** command.

19.9.4 Principles of Power Savings and Power Estimation

1. Principles for Estimating OLT Power Savings

Estimated power savings = Power saved by shutting down boards + Power saved by shutting down ports + Power saved by shutting down channels

- **Shutdown of unused boards:** Calculate the difference between the power before and after a board is shut down. For example, if the total power is 300 W before a board is shut down and 250 W after the board is shut down, the power saved by shutting down the board is 50 W (with a power fluctuation error).
- **Shutdown of unused ports:** Based on different combinations of the board type, port mode, and optical module in-position status, the typical value tested in the lab is used for estimation. For example, for the H908CGHF board, if the port mode is XG/G PON and the optical module is in position, shutting down one port saves 1.1 W (lab test data) and shutting down five ports saves 5.5 W.
- **Shutdown of unused channels:** Based on different combinations of the board type, port mode, channel type, and optical module in-position status, the typical value tested in the lab is used for estimation. For example, for the H908CGHF board, if port mode is XG/G PON and the optical module is in position, shutting down one 10G PON channel saves 0.8 W (lab test data) and shutting down one GPON channel saves 0.2 W (lab test data).

2. Description of OLT power saving errors

- **The error in power saved by shutting down unused boards comes from the current collection precision of the power board.**

The power saved for the entire subrack is calculated by subtraction, which depends on the precision of the current collected by the power board. The collection precision meets the ETSI 202 336-12 standard.

Power board load at 25%–100%: ±3%

Power board load at 5%–25%: ±5%

- **The error in power saved by shutting down unused ports comes from optical modules.**

Data source of the typical power of optical modules: The data of each type of optical modules is the average value of 16 optical modules of the same type selected from mainstream vendors and versions in the lab under the normal temperature of 25°C.

The power of an optical module is affected by the following factors:

- Tx optical power:** The power varies with the optical power of optical modules (Class B+, Class C+, and Class D).
- Process:** The power of optical modules varies with the process control (such as the processing precision, temperature, and humidity of the production line) of different vendors and batches.
- Temperature:** The power of an optical module varies with the temperature. Generally, the higher the temperature, the larger the leakage current and the higher the power.

19.9.5 Energy Saving Configuration Description

19.9.5.1 Energy Saving Configuration

There are two ways to configure energy saving. One is to configure the 4 energy saving modes (standard, basic, deep, and optimal modes) on an OLT, and the other is to configure the custom mode and specific energy saving measures on the network management system (NMS) through the network cloud engine (NCE).

19.9.5.1.1 Configuring an Energy Saving Mode

Run the **system energy-saving mode** command to set the energy saving mode of the system.

Run the **undo system energy-saving mode** command to restore the energy saving mode of the system to the default value (basic mode).

Run the **display system energy-saving mode** command to query the current energy saving mode of the system.

To set the current energy saving mode of the system to deep mode, do as follows:

```
huawei(config)#system energy-saving mode deep
{ <cr>|method<K> }:  
Command:  
    system energy-saving mode deep  
Command is being executed, please wait for a moment...  
Set the energy-saving mode successfully
```

Table 19-15 The following table lists the energy saving measures corresponding to each mode.

Energy Saving Mode	Measures
Standard mode	19.9.2.2.1 Automatic Shutdown of Unused High-speed Interfaces

Energy Saving Mode	Measures
Basic mode	• 19.9.2.2.1 Automatic Shutdown of Unused High-speed Interfaces • 19.9.2.2.2 Automatic Zone-based Fan Speed Adjustment
Deep mode	• 19.9.2.2.1 Automatic Shutdown of Unused High-speed Interfaces • 19.9.2.2.2 Automatic Zone-based Fan Speed Adjustment • 19.9.2.2.3 Automatic Shutdown of Unused Ports • 19.9.2.2.4 Automatic Shutdown of Unused Boards
Optimal mode	• 19.9.2.2.1 Automatic Shutdown of Unused High-speed Interfaces • 19.9.2.2.2 Automatic Zone-based Fan Speed Adjustment • 19.9.2.2.3 Automatic Shutdown of Unused Ports • 19.9.2.2.4 Automatic Shutdown of Unused Boards • 19.9.2.2.6 Dynamic Frequency Adjustment
Custom mode	Measures that take effect by default: • 19.9.2.2.1 Automatic Shutdown of Unused High-speed Interfaces • 19.9.2.2.2 Automatic Zone-based Fan Speed Adjustment Measures that are enabled manually: • 19.9.2.2.3 Automatic Shutdown of Unused Ports • 19.9.2.2.4 Automatic Shutdown of Unused Boards • 19.9.2.2.5 Automatic Shutdown of Unused Channels • 19.9.2.2.7 Intelligent Board Scheduling CAUTION You need to apply for a license and then configure the energy saving mode on the NCE. It cannot be directly configured on the CLI.

19.9.5.1.2 Configuring Custom Energy Saving Measures

Users can run the **system energy-saving mode custom method** method-name { **enable** | **disable** } command to enable or disable energy saving measures in custom mode.

Table 19-16 Description of the *method-name* parameters

Parameter	Measure Name
unused-board-shutdown	Indicates that a board is shut down when not in use to save energy.
unused-port-shutdown	Indicates that a port is shut down when not in use to save energy.
intelligent-board-scheduling	Indicates intelligent board scheduling to save energy.
unused-channel-shutdown	Indicates that a channel is shut down when not in use to save energy.

Configuring Shutdown of Unused Boards

To enable shutdown of unused boards in custom energy saving mode, do as follows:

```
huawei(config)#system energy-saving mode custom method unused-board-shutdown enable
Set the energy-saving method successfully
```

Configuring Shutdown of Unused Ports

To enable shutdown of unused ports in custom energy saving mode, do as follows:

```
huawei(config)#system energy-saving mode custom method unused-port-shutdown enable
Set the energy-saving method successfully
```

Configuring Parameters for Unused Port Shutdown: Disabling ONT Auto-Discovery Check

Generally, ONT auto-discovery is regarded as a port configuration. After ONT auto-discovery is configured (**port ont-auto-find**) on a port, the port cannot be shut down for energy saving even though it is not configured with any other services. To enable both ONT auto-discovery and port shutdown when not in use, run the **ont autofind energy-saving enable** command to disable ONT auto-discovery check.

You can run the **display ont global-config** or **display xpon global-config** command to query whether ONT auto-discovery check is enabled.

To enable unused port shutdown in custom energy saving mode and disable ONT auto-discovery check, do as follows:

```
huawei(config)#system energy-saving mode custom method unused-port-shutdown enable
Set the energy-saving method successfully

huawei(config)#ont autofind energy-saving enable
```

To disable ONT auto-discovery check in deep energy saving mode, do as follows:

```
huawei(config)#system energy-saving mode deep
{ <cr>|method<K> }:
```

```
Command:
system energy-saving mode deep
Command is being executed, please wait for a moment...
Set the energy-saving mode successfully
```

```
huawei(config)#ont autofind energy-saving enable
```

Enable deep energy saving for an optical module. This function is supported only in V100R022C10SPH211 version.

```
huawei(config)#xpon global-config switch optical-deep-energy-saving enable
```

Configuring Shutdown of Unused Channels

To enable unused channel shutdown in custom energy saving mode, do as follows:

```
huawei(config)#system energy-saving mode custom method unused-channel-shutdown enable
Set the energy-saving method successfully
```

Configuring Intelligent Board Scheduling

To enable intelligent board scheduling in custom energy saving mode, do as follows:

```
huawei(config)#system energy-saving mode custom method intelligent-board-scheduling enable
Set the energy-saving method successfully
```

19.9.5.1.3 Querying Energy Saving Configurations

1. Run the **display system energy-saving mode** command to query the current energy saving mode.

```
huawei#display system energy-saving mode
{ <cr>|<K> }:
Command:
display system energy-saving mode
Energy-saving mode: basic
```

2. Run the **display system energy-saving method custom** command to query energy saving measures in custom mode.

```
huawei#display system energy-saving method custom
{ <cr>|<K> }:
Command:
display system energy-saving method custom
```

Method	Custom
zone-based-fan-speed-adjustment	Y
unused-high-speed-interface-shutdown	Y
unused-board-shutdown	N
unused-port-shutdown	N
unused-channel-shutdown	N
intelligent-board-scheduling	N

3. Run the **display system energy-saving parameter** command to query parameters of a specified measure.

```
huawei#display system energy-saving parameter
{ <cr>|<K> }:
```

```
Command:
display system energy-saving parameter
-----
Mode:Deep
-----
Method          Parameter          Value
-----
unused-board-shutdown  shutdown-operator  auto
unused-port-shutdown   shutdown-operator  auto
-----
Mode:Optimal
-----
Method          Parameter          Value
-----
unused-board-shutdown  shutdown-operator  auto
unused-port-shutdown   shutdown-operator  auto
-----
Mode:Custom
-----
Method          Parameter          Value
-----
unused-board-shutdown  shutdown-operator  auto
unused-port-shutdown   shutdown-operator  auto
-----
```

Run the **display ont global-config** or **display xpon global-config** command to query whether ONT auto-discovery check is enabled.

```
huawei#display ont global-config
{ <cr>||<K> }:
Command:
display ont global-config
-----
ONT autofind aging time(s)          : 300
ONT autofind conflict check switch   : disable
ONT autofind distance time(only for GPON)(s) : 5
ONT autofind energy-saving           : enable
ONT CATV port current default operational state : on
ONT auto-migration switch            : disable
ONT auto-aging time(day)             : no-aging
ONT authentication conflict check by-sn : enable
ONT authentication conflict check by-loid : enable
ONT autofind additional notice switch : disable
ONT autofind additional notice times   : -
ONT autofind additional notice interval(s) : -
ONT online rate control              : disable
-----
huawei#display xpon global-config
{ <cr>||<K> }:

Command:
display xpon global-config
-----
Current configuration mode           : distributing-mode
-----
xPON rogue ONT auto detection switch : off
xPON alarm clear-on-shutdown switch  : disable
xPON group power off alarm switch     : disable
xPON LOS alarm control switch         : disable
xPON LOS alarm control DGi threshold ratio(%) : 20
xPON LOS alarm control DGi threshold time(s) : 10
xPON suppress initial alarm switch    : enable
xPON suppress optical initial alarm switch : disable
xPON optical module alarm control switch : disable
xPON distribute fiber LOS alarm switch : disable
xPON modify bound profile switch      : enable
xPON protect group different range switch : disable
xPON port color sensitive switch      : disable
-----
```

```
xPON ONT power reduction switch          : enable
xPON ONT offline monitor switch          : disable
xPON ONT offline monitor alarm threshold(%) : 70
xPON ONT offline monitor restore threshold(%) : 80
xPON auto-alloc GEM port encrypt         : off
xPON virtual system ONT ID alloc policy   : independent
xPON optical-alarm auto-monitor port switch : standard-threshold
xPON optical-alarm auto-monitor ont switch : disable
xPON ONT IPv6 multicast switch in CTC     : disable
xPON ONT optical-ddm quick-query switch   : disable
xPON ONT distance variation threshold(m)   : Unlimited
xPON rogue ONT detect-rssi-threshold(dBm) : -28.00
xPON rogue ONT clear-rssi-threshold(dBm)   : -28.00
xPON bandwidth combine switch             : disable
xPON default OMCC encrypt switch          : enable
xPON default GEM port encrypt switch      : enable
xPON OLT RX ONT power mode                : high-precision
xPON ONT type check strict switch         : disable
xPON channel rogue onu check switch       : enable
xPON optical-module info mode             : normal
xPON SIP URI format                       : TEL
xPON operator check CLI switch            : enable
xPON mode2 time sync switch               : disable
xPON optical module deep-energy-saving switch : enable
-----
ONT autofind aging time(s)                : 300
ONT autofind conflict check switch         : disable
ONT autofind distance time(only for GPON)(s) : 5
ONT autofind energy-saving                 : enable
ONT CATV port current default operational state : on
ONT auto-migration switch                 : enable
ONT auto-aging time(day)                  : 15
ONT authentication conflict check by-sn    : enable
ONT authentication conflict check by-loid  : enable
ONT autofind additional notice switch      : enable
ONT autofind additional notice times       : 5
ONT autofind additional notice interval(s) : 100
ONT online rate control                   : disable
-----
GPON DBA bandwidth type                   : GPON
GPON DBA bandwidth assignment mode        : min-loop-delay
GPON multicast GEM port                   : 4095
XG-PON multicast GEM port                 : 65532
GPON ONT password renew interval(min)     : -
GPON T-CONT auto-create switch            : disable
GPON interoperability standard             : ITU-T
GPON interoperability multicast authentication : ONT control
GPON interoperability T-CONT PQ priority reverse: disable
GPON interoperability ONT WAN config mode  : set-by-create
GPON ONT home gateway config method       : default
GPON anti-dos PLOAM switch                : enable
GPON ONT SN format                       : vendor-prefix
GPON ONT vlan tag operation mode           : modify single tag
GPON ONT multicast vlan filter             : default
XGS-PON RTU allocation priority policy     : Bandwidth RTU first
GPON broadcast GEM port                   : disable
Extended VLAN tagging operation            : enable
ONT ETH layer-2 service switch             : enable
-----
```

NOTE

```
xPON SIP URI format          : TEL
xPON operator check CLI switch : enable
xPON mode2 time sync switch   : disable
xPON optical module deep-energy-saving switch : enable
```

Supported only in V100R022C10SPH211 version.

19.9.5.1.4 Powering Off an Unused Port/Board

The **system energy-saving power-off** { frameid/slotid / frameid/slotid/portid } command is used to power off a board or port. When you need to shut down a board or port that does not carry any services to save energy, run this command.

The **system energy-saving power-on** { frameid/slotid / frameid/slotid/portid } command is used to power on a board or port that has been powered off for energy saving. When you need to configure services for a board or port that has been shut down for energy saving, run this command.

To power off board 0/1 for energy saving, do as follows:

```
huawei(diagnose)%%system energy-saving power-off 0/1
Are you sure to power off the board?(y/n)[n]:y
Energy saving shutdown successfully
```

19.9.5.2 Querying Energy Saving Results

19.9.5.2.1 Querying Energy Saving Status

The **display system energy-saving info** { frameid | frameid/slotid } command is used to query the energy saving running status of a specified subrack or board.

The **display system energy-saving info detail** { frameid/slotid | frameid/slotid/portid } command is used to query detailed energy saving information about a specified board or port.

Parameter	Description
Frame/Slot	Indicates the subrack ID and slot ID of a board.
Frame/Slot/Port	Indicates the subrack ID, slot ID, and port ID of a port.
Enabled	Indicates the enabling status of the energy-saving function of a board or port. You can run the system energy-saving command to set this parameter.
EnergySavingOperStatus	Indicates the energy saving running status of a board or port. Options: • NoEnergySaving: no energy saving state. • Deactivated: deactivated state. • PartialEnergySaving: partial energy saving state. • ESavingStandby: shutdown when no service is running. When a board or port is in this state, you can run the system energy-saving power-off command to configure shutdown measures for energy saving. • ESavingShutdown: energy saving shutdown state. You can run the system energy-saving power-off command to set this parameter. • ManualShutdown: manual shutdown state. You can run the board power-off command to set this parameter.

Parameter	Description
Channel x EnergySavingOperSta- tus	Indicates the energy saving running status of a channel. Options: • NoEnergySaving: no energy saving state. • ESavingShutdown: energy saving shutdown state. • ManualShutdown: manual shutdown state. You can run the port laser-select(gpon) or port laser-select(epon) command to set this parameter. This information is displayed only when the detailed information about the energy-saving function of a port is queried on a board that supports dual channels. Replace <i>x</i> with 0 or 1.

19.9.5.2.2 Querying the Shutdown Status of a Board

The **display system energy-saving info { frameid | frameid/slotid }** command is used to query the energy saving running status of a specified board or port.

To query the brief information about the energy-saving function of all boards in subrack 0, do as follows:

```
huawei#display systeEm energy-saving info 0
{ <cr>||<K> }:
Command:
    display system energy-saving info 0
-----
Frame/Slot      Enabled  EnergySavingOperStatus
-----
0/0              Enable   NoEnergySaving
0/1              Enable   NoEnergySaving
0/2              Enable   NoEnergySaving
0/3              Enable   ESavingShutdown
0/4              Enable   ESavingShutdown
0/5              Enable   NoEnergySaving
0/9              Enable   NoEnergySaving
0/10             Enable   NoEnergySaving
-----
```

As shown in the command output, subracks 0/3 and 0/4 are shut down for energy saving.

19.9.5.2.3 Querying the Shutdown Status of a Port

To query the brief information about the energy-saving function of all ports on board 0/1, do as follows:

```
huawei#display system energy-saving info 0/1
{ <cr>||<K> }:
Command:
    display system energy-saving info 0/1
-----
Frame/Slot/Port  Enabled  EnergySavingOperStatus
-----
0/1/0            Enable   NoEnergySaving
0/1/1            Enable   NoEnergySaving
0/1/2            Enable   ESavingShutdown
0/1/3            Enable   ESavingShutdown
-----
```

0/1/4	Enable	NoEnergySaving
0/1/5	Enable	NoEnergySaving

As shown in the command output, ports 0/1/2 and 0/1/3 are shut down for energy saving.

19.9.5.2.4 Querying the Shutdown Status of a Channel

To query the detailed information about the energy-saving function of port 0/1/0, do as follows:

```
huawei#display system energy-saving info detail 0/1/0
{ <cr>||<K> }:
Command:
    display system energy-saving info detail 0/1/0
-----
Enabled: Enable
EnergySavingOperStatus: PartialEnergySaving
Channel 0 EnergySavingOperStatus: ESavingShutdown
Channel 1 EnergySavingOperStatus: ESavingShutdown
-----
```

As shown in the command output, port 0/1/0 on the board is shut down for energy saving.

19.9.5.2.5 Querying Zone-based Fan Speed Adjustment Results

Run the **display fan speed** command to query the speed of each fan. When board temperature differences are large between zones, the fan speeds change.

To query the current fan speeds, do as follows:

```
huawei(config-if-fan-1)%%display fan speed
Fan 0 Real-time speed: 1470times/minute, Fan speed Occupy: 32%
Fan 1 Real-time speed: 1530times/minute, Fan speed Occupy: 34%
Fan 2 Real-time speed: 1530times/minute, Fan speed Occupy: 34%
Fan 3 Real-time speed: 1530times/minute, Fan speed Occupy: 34%
Fan 4 Real-time speed: 1500times/minute, Fan speed Occupy: 33%
Fan 5 Real-time speed: 1500times/minute, Fan speed Occupy: 33%
Fan 6 Real-time speed: 1500times/minute, Fan speed Occupy: 33%
Fan 7 Real-time speed: 1500times/minute, Fan speed Occupy: 33%
```

As shown in the command output, when board temperature differences are large between zones, the fan speeds change.

19.9.5.2.6 Querying Dynamic Frequency Adjustment Results

For a board that supports dynamic frequency adjustment, if the board version is V100R023C1xSPC200 or earlier, you can only run the expert maintenance command to enter the board CLI through the transparent channel and then run the **asic freq get** command to query the adjustment status.

For example:

In privilege mode or global config mode, run the **diagnose** command to enter diagnose mode.

In diagnose mode, run the **su** command to enter SU mode.

Run the **transparent on 0/1** command to enter the transparent channel of slot 1, and then run the **asic freq get** command.

```
huawei(su)%%asic freq get
atom: 850
rp : 425
eqm : 425
bac : 533.33
ifb : 300
pa : 533.33
pe : 533.33
pba : 400
```

You can obtain the dynamic frequency adjustment result based on the *atom* frequency change in the command output.

The following table describes the parameters in response to this command:

Parameter	Description
atom	Indicates the ATOM clock frequency.
rp	Indicates the RP clock frequency.
eqm	Indicates the EQM clock frequency.
bac	Indicates the BAC clock frequency.
ifb	Indicates the IFB clock frequency.
pa	Indicates the PA clock frequency.
pe	Indicates the PE clock frequency.
pba	Indicates the PBA clock frequency.

In addition, when dynamic frequency adjustment takes effect for a board, the board is in the partial energy saving state. You can run the **display system energy-saving info detail 0/1** command to query the information.

```
huawei#display system energy-saving info detail 0/1
<cr>||<K> }:
Command:
    display system energy-saving info detail 0/1
-----
Enabled: Enable
EnergySavingOperStatus: PartialEnergySaving
-----
```

As shown in the command output, when dynamic frequency adjustment takes effect, the board in subrack 0/1 is in the partial energy saving state.

19.9.5.2.7 Querying Intelligent Board Scheduling Results

For a board that supports intelligent board scheduling, if the board version is V100R023C1xSPC200 or earlier, you can only run the expert maintenance command to enter the board CLI through the transparent channel and then run the **asic power display np-dynamic-freq-info** command to query the intelligent board scheduling status.

For example:

In privilege mode or global config mode, run the **diagnose** command to enter diagnose mode.

In diagnose mode, run the **su** command to enter SU mode.

Run the **transparent on 0/2** command to enter the transparent channel of slot 2, and then run the **asic power display np-dynamic-freq-info** command.

```
huawei(su)%%asic power display
{ freq<K>|pll-power-down-en<K>|sds-power-down-en<K>|np-dynamic-freq-info<K>|tm-
dynamic-freq-info<K> } :np-dynamic-freq-info
en up-th down-th freq
disable 950M 425M 950M
Command execute success!
```

You can obtain the intelligent board scheduling result based on the *freq* frequency change in the command output.

The following table describes the parameters in response to this command:

Parameter	Description
en	Indicates the NP dynamic frequency adjustment status. - enable - disable
up-th	Indicates the highest frequency.
down-th	Indicates the lowest frequency.
freq	Indicates the current frequency.

In addition, when intelligent board scheduling takes effect for a board, the board is in the partial energy saving state. You can run the **display system energy-saving info detail 0/2** command to query the information.

```
huawei#display system energy-saving info detail 0/2
<cr>||<K> } :
Command:
display system energy-saving info detail 0/2
-----
Enabled: Enable
EnergySavingOperStatus: PartialEnergySaving
-----
```

As shown in the command output, when intelligent board scheduling takes effect, the board in subrack 0/2 is in the partial energy saving state.

19.9.5.3 Energy Saving Configuration Examples

19.9.5.3.1 Configuring the Deep Energy Saving Mode on an OLT

Step 1 Set the current energy saving mode of the system to deep mode.

```
huawei(config)#system energy-saving mode deep
{ <cr>|method<K> } :
Command:
system energy-saving mode deep
Command is being executed, please wait for a moment...
Set the energy-saving mode successfully
```

Step 2 Check whether the current energy-saving mode takes effect.

```
huawei#display system energy-saving mode
{ <cr>||<K> }:
Command:
    display system energy-saving mode
Energy-saving mode: deep
```

Step 3 If there are unused boards or ports in the environment, they will be detected after a certain period of time and shut down for energy saving. You can run the **display system energy-saving info** command to query the energy saving result.

```
huawei#display system energy-saving info 0/1
{ <cr>||<K> }:
Command:
    display system energy-saving info 0/1
-----
Frame/Slot/Port   Enabled   EnergySavingOperStatus
-----
0/1/0             Enable    ESavingShutdown
0/1/1             Enable    ESavingShutdown
0/1/2             Enable    ESavingShutdown
0/1/3             Enable    ESavingShutdown
0/1/4             Enable    ESavingShutdown
0/1/5             Enable    ESavingShutdown
-----
```

Step 4 Run the **undo system energy-saving mode** command to exit the deep energy saving mode.

```
Huawei(config)#undo system energy-saving mode
{ <cr>||<K> }:
Command:
    undo system energy-saving mode
Command is being executed, please wait for a moment...
Set the energy-saving mode successfully
```

----End

19.9.5.3.2 Configuring the Deep Energy Saving Mode on the NMS

NMS Version Requirements

- For NEs of V100R022C00 and earlier versions, ONU auto-discovery check disabling is not supported.
- For NEs of V100R022C10SPC200 and earlier versions:

Only the energy saving measures automatic shutdown of unused boards and automatic shutdown of unused ports are supported. The association relationships between the measures are as follows:

When either of automatic shutdown of unused boards and automatic shutdown of unused ports is enabled, the other measure is automatically enabled on same device.

A union set of effective periods of associated energy saving measures is used. As long as one measure is within its energy saving period, the others take effect as well.

- For NEs of V100R022C10SPH203 and later versions, all energy saving functions are supported and there are no associations between them.

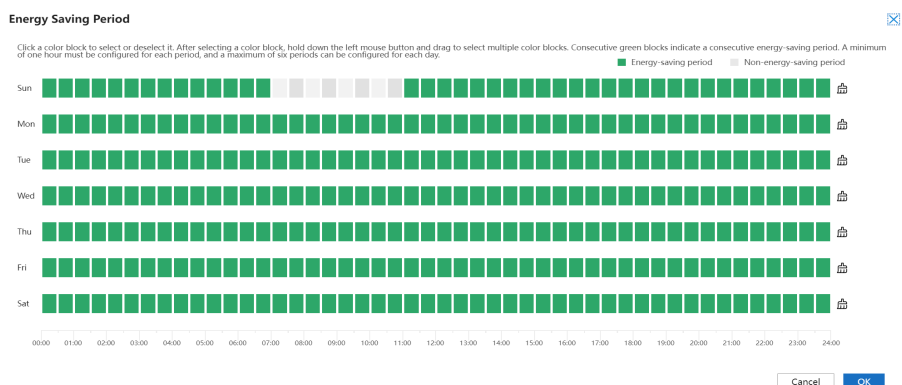
Procedure

- Step 1** Open the Access Controller app and choose **Automation Control Center** from the main menu.
- Step 2** In the **Automation Control Center** area, click **Energy Consumption Management**.
- Step 3** Click the **Energy Saving Model Management** tab.
- Step 4** Use either of the following methods to create an energy saving model.
- **Configuring an Energy Saving Model**
 - a. Click **Create**. In the displayed dialog box, set the energy-saving model name, and enable or disable energy-saving measures and ONU auto-discovery check.

Parameter	Description
Automatic shutdown of unused boards	When a board is not in use, it is automatically powered off. When the system detects that the board needs to be used, it automatically powers on the board and restores it to the normal running state. NOTE This does not affect service quality but has certain impact on the O&M. It takes about 2 to 3 minutes to restart a board that is shut down.
Automatic shutdown of unused ports	When a PON port is not in use, the corresponding interface circuit and optical module are automatically shut down. When the system detects that the port needs to be used, it automatically enables the port and restores it to the normal running state. NOTE This does not affect service quality but has certain impact on the O&M. It takes about 1 to 2 seconds to restart a port that is shut down.
Automatic shutdown of unused channels	When there is an unused channel of a Combo PON port, the channel is automatically shut down. When the system detects that the channel needs to be used, it automatically enables the channel and restores it to the normal running state. NOTE This does not affect service quality but has certain impact on the O&M. It takes about 1 to 2 seconds to restart a channel that is shut down.

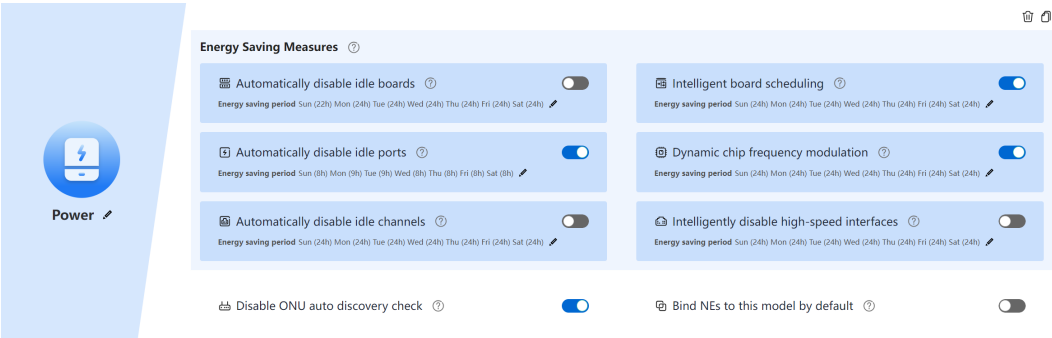
Parameter	Description
Intelligent board scheduling	A board intelligently schedules internal forwarding resources based on the service load. When the service load decreases, a board automatically disables some forwarding resources or reduces the working frequency of forwarding resources. When the service load increases, the board enables the forwarding resources that have been disabled or improves the working frequency of forwarding resources. NOTE In the case of burst traffic, packet forwarding may have latency, but no packets will be lost.
ONU auto-discovery check disabling	After this function is enabled, the system does not check the ONU auto-discovery configuration for energy saving measures, that is, automatic shutdown of unused boards, ports, and channels, to take effect. The ONU auto-discovery function is not available when energy saving measures are effective.

- b. Click  corresponding to an energy saving measure to set the energy saving period.



- c. Click **OK**.
- Copying an Energy Saving Model
 - a. Click  corresponding to an energy saving model. In the displayed dialogue box, set the energy saving model name, enable or disable energy saving measures and ONU auto-discovery check, and set the energy saving period.
 - b. Click **OK**.

Step 5 After an energy saving model is created, you can modify the model name, energy saving measure, and energy saving period. To enable an NE to be automatically bound to the energy saving model when it goes online, enable **Bind NEs to this model by default**.



----End

19.9.6 Energy Saving Conditions

19.9.6.1 Function Conditions

19.9.6.1.1 Energy Saving Mode Conditions

Energy Saving Mode	Supported Versions (Replace <i>x</i> in the Version Number with 0, 1, or 2.)	NMS Start Version
Standard mode	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions	V100R022C10SPC101
Basic mode	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions	V100R022C10SPC101
Deep mode	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions	V100R022C10SPC101
Optimal mode	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions	V100R022C10SPC101
Custom mode	V100R022C1xSPH203and later versions	V100R022C10SPC101

19.9.6.1.2 Energy Saving Measure Conditions

Energy Saving Mode	Energy Saving Measure	Supported Versions (Replace <i>x</i> in the Version Number with 0, 1, or 2.)
Standard mode	Zone-based automatic fan speed adjustment	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions
Basic mode	Zone-based automatic fan speed adjustment	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions
	Automatic shutdown of unused high-speed interfaces	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions
Deep mode	Zone-based automatic fan speed adjustment	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions
	Automatic shutdown of unused high-speed interfaces	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions
	Automatic shutdown of unused ports	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions
	Automatic shutdown of unused boards	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions
Optimal mode	Zone-based automatic fan speed adjustment	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions
	Automatic shutdown of unused high-speed interfaces	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions

Energy Saving Mode	Energy Saving Measure	Supported Versions (Replace <i>x</i> in the Version Number with 0, 1, or 2.)
	Automatic shutdown of unused ports	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions
	Automatic shutdown of unused boards	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions
	Dynamic frequency adjustment	V100R018C00SPC500, V100R019C1xSPC200, and respective later versions
Custom mode	Zone-based automatic fan speed adjustment	V100R022C1xSPH203 and later versions
	Automatic shutdown of unused high-speed interfaces	V100R022C1xSPH203 and later versions
	Automatic shutdown of unused ports	V100R022C1xSPH203 and later versions
	Automatic shutdown of unused boards	V100R022C1xSPH203 and later versions
	Automatic shutdown of unused channels	V100R022C1xSPH203 and later versions
	Intelligent board scheduling	V100R022C1xSPH203 and later versions

19.9.6.1.3 Energy Saving Parameter Conditions

Energy Saving Measure	Energy Saving Parameter	Supported Versions (Replace <i>x</i> in the Version Number with 0, 1, or 2.)
Automatic shutdown of unused boards	Manual shutdown	V100R022C1xSPC200 and later versions
	ONT auto-discovery check disabling	V100R022C1xSPC200 and later versions
Automatic shutdown of unused ports	Manual shutdown	V100R022C1xSPC200 and later versions

19.9.6.2 Board Conditions

19.9.6.2.1 Energy Saving Configuration Conditions

Due to board and subrack model differences, each energy saving measure only takes effect for certain boards. The following figure shows the conditions:

Energy Saving Measure	Applicable Hardware
Zone-based fan speed adjustment	All multi-zone subracks such as X17 and X7 (X15, X2, and X1 are single-zone subrack.)
Shutdown of unused high-speed interfaces	All service boards
Shutdown of unused boards	Supported by EPON/GPON/ETH boards Not supported by control, power, interface, or AEC boards Not supported by upstream or L-type boards Not supported by X1 subrack boards
Shutdown of unused ports	Supported by ports on EPON/GPON boards; not supported by upstream ports Only GPON, EPON, and Flex-PON boards in V100R022C10SPH211 version support power-off of optical modules; other boards do not support this function
Shutdown of unused channels	Supported by dual-channel boards such as Combo boards and 10E PON boards; not supported by L-type boards

Energy Saving Measure	Applicable Hardware
Dynamic frequency adjustment	Boards using 5121 chips
Intelligent board scheduling	Boards using 5122 chips

You can query detailed board conditions through the following specification query tools:

Operators: [\(Operator\) Huawei Optical Product Info-Finder \(huawei.com\)](#)

Enterprise customers: [\(Enterprise\) Huawei Optical Product Info-Finder \(huawei.com\)](#)

19.9.6.2.2 Support for Energy Consumption Visualization

After enabling the energy saving function, you can enable the energy saving visualization function on the network management system (NMS). The energy saving visualization function depends on the capability of the power board. The following table lists the power boards that support energy saving visualization.

Subrack	Power Board Name	Whether Supporting Energy Saving Visualization	Start Version
X17/X15/X7	H901PILA	N	-
X17/X15/X7	H901PILB	N	-
X17/X15/X7	H901PIMA	N	-
X17/X15/X7	H902PILA	N	-
X17/X15/X7	H903PILA	Y	R22C01 R22C02
X17/X15/X7	H905PILA	Y	R22C01 R22C02
X2	H901PISA	N	-
X2	H901PISB	Y	R22C01 R22C02
X2	H901PISC	Y	R22C01 R22C02

Subrack	Power Board Name	Whether Supporting Energy Saving Visualization	Start Version
X2	H902PISB	Y	R22C01 R22C02
X2	H903PISB	Y	R22C01 R22C02
X1	H931PICA	Y	R24C01 R24C02
X1	H931PICB	Y	R24C00 R24C01 R24C02
X1	PAC300S12	Y	R24C01 R24C02
X1	PDC300S12	Y	R24C01 R24C02

 CAUTION

1. All power boards on a device must support the energy saving visualization function for the NMS to support energy saving visualization.

2. If a power board on a device is faulty, the energy saving visualization function may be abnormal.

19.9.7 FAQ

19.9.7.1 Can the Custom Energy Saving Mode Be Configured on a Device?

You need to apply for a license before configuring the custom energy saving mode. Currently, you can only switch to the custom mode on the NMS. The CLI does not support this operation.

19.9.7.2 Does a Custom Energy Saving Measure Take Effect Immediately After Configuration?

A custom energy saving measure only takes effect in custom mode. There are two scenarios:

1. If the system runs in non-custom mode (for example, the basic mode), a configured custom energy saving measure does not take effect. You need to switch to the custom mode for the measures to take effect.

2. If the system runs in custom mode, a configured custom energy saving measure immediately takes effect after configuration.

19.9.7.3 Link for the Manual of Configuring Custom Energy Saving Measures on the NMS

Path: **iMaster NCE-FAN Product Documentation > NCE-FAN Application Operation and Maintenance > Access Controller > Energy Consumption Management**

V100R022C10 version link: https://support.huawei.com/hedex/hdx.do?docid=DOC1101081994&id=EN-US_TOPIC_0000001321356616

19.10 Version and Data Management

This topic provides an introduction to the version and data management feature, and describes the working principle of this sub feature.

NOTICE

After saving the data, keep the data properly to avoid security risks.

19.10.1 Introduction

Definition

Version and data management includes patch management, rollback function, configuration data management, and version upgrade.

Purpose

This sub feature facilitates carriers in version upgrade and maintenance.

Benefits

Benefits to carriers: The carriers' operating expenditure (OPEX) is saved considerably, and the customer satisfaction is increased.

19.10.2 Principle

Patch Management

The flash memory (storage medium in the system) has a patch area to store the loaded patches.

A patch can be a hot patch or cold patch. The system needs to be restarted for a cold patch to take effect or stop functioning. Nevertheless, in the case of a hot patch, the system need not be restarted for the same purpose. A hot patch supports the rollback function; therefore, the hot patch can be rolled back to the status before the latest hot patch is loaded.

In addition, a patch can be activated, deactivated, run, or deleted. The loaded patch is deactivated by default; therefore, to make the loaded patch take effect, activate it. To make the patch take effect after the system restart, activate and run the patch before the system is restarted.

The system supports the following four types of patches:

- HP refers to the host hot patch. It takes effect after being loaded and then activated. For a user, this type of patches, after being loaded, is displayed as HPXXX.
- SPH is the set of HP patches. It takes effect after being loaded and activated. For a user, this type of patches, after being loaded, is displayed as SPHXXX, without displaying the status of HP patches
- CP refers to the host cold patch. It takes effect after it is loaded and the system is restarted. For a user, this type of patches, after being loaded, is displayed as CPXXX.
- SPC is the set of CP patches. It takes effect after being loaded and activated. For a user, this type of patches, after being loaded, is displayed as SPCXXX, without displaying the status of CP patches.

Rollback Function

The flash memory of the control board is divided into two same storage areas (namely, active storage area and standby storage area) to store the program, database, and extended BIOS. The storage area that is operating currently is the active storage area. When the program, database, and extended BIOS are upgraded, the new program, database, and extended BIOS are loaded to the standby storage area. After the system is restarted, the system automatically loads the new program, database, and extended BIOS. The rollback function is implemented based on two sets of program, database, and extended BIOS in both the active and standby storage areas.

By default, after upgrade, the system saves the pre-upgrade host program and database for 48 hours. 48 hours later, the system automatically cancels the rollback function. That is, 48 hours later, the system duplicates the program, database, and extended BIOS in the operating area to the standby storage area. In this way, the versions in both the active and standby storage areas are the same. You can run the **set norollback time** command to set the time for canceling the rollback function.

The system supports automatic rollback and manual rollback. After version upgrade, if the system fails to start up, the system is automatically rolled back to the version before upgrade. After version upgrade, if the system becomes abnormal during the running and cannot recover, you can run the **rollback** command to roll back the system to the version before upgrade.

Configuration Data Management

- Saving the configuration data manually: The current configuration data can be saved manually through the **save** commands. If the configuration data is not saved before the system is reset or restarted, it will be lost after the system reset or restart. Therefore, manually save the configuration data once before the system is reset or restarted.

- Saving the configuration data after any changes to the configuration data: After the configuration data is changed, the system will save the changed configuration data automatically at a preset interval. You can run the **autosave interval** command to set the interval.
- Saving the configuration data at a preset time or interval: In the system, the configuration data can be saved automatically at a preset time or interval. This time or interval is user-defined. For example, the time or interval can be set to 23:00 or two hours respectively. In this case, the configuration data is saved at an interval of two hours or at 23:00.

The data erasure operation can be performed to restore the configuration data of the device to the default settings.

The system also supports backing up the current configuration data manually or at a preset time to a specified file server.

Version Upgrade

Software version in the system can be upgraded through the CLI or the NMS by using FTP/TFTP/XMODEM/SFTP.

NOTE

FTP, TFTP and XMODEM have security risks due to protocol restrictions. SFTP is recommended.

19.10.3 ISSU

Definition

In-service software upgrade (ISSU) is an upgrade mode in which services are not interrupted or interrupted for only a short period of time.

Benefits

With the development of fiber to the mobile base station (FTTM), fiber to the office (FTTO), and large-capacity fiber to the home (FTTH) services, customers require shorter or zero service interruption during an upgrade. The previous generation of OLT supports ISSU, but has the following problems:

- When control boards work in active/standby mode and service boards are not configured with inter-board type X protection switching, services are not interrupted during control board upgrade, but are interrupted when the service boards are reset.
- When control boards work in active/standby mode and service boards and upstream boards are configured with inter-board type X protection switching, services are interrupted for less than 200 ms during an upgrade. In this scenario, all these boards are in dual configurations, which increases operation costs.

The MA5800 enhances the ISSU feature. Specifically, when control boards work in active/standby mode and service boards are not configured with inter-board type X protection switching, ONUs remain online and services are interrupted for less than 10s during an upgrade. The enhanced ISSU feature improves system reliability and helps reduce operation costs.

Principles

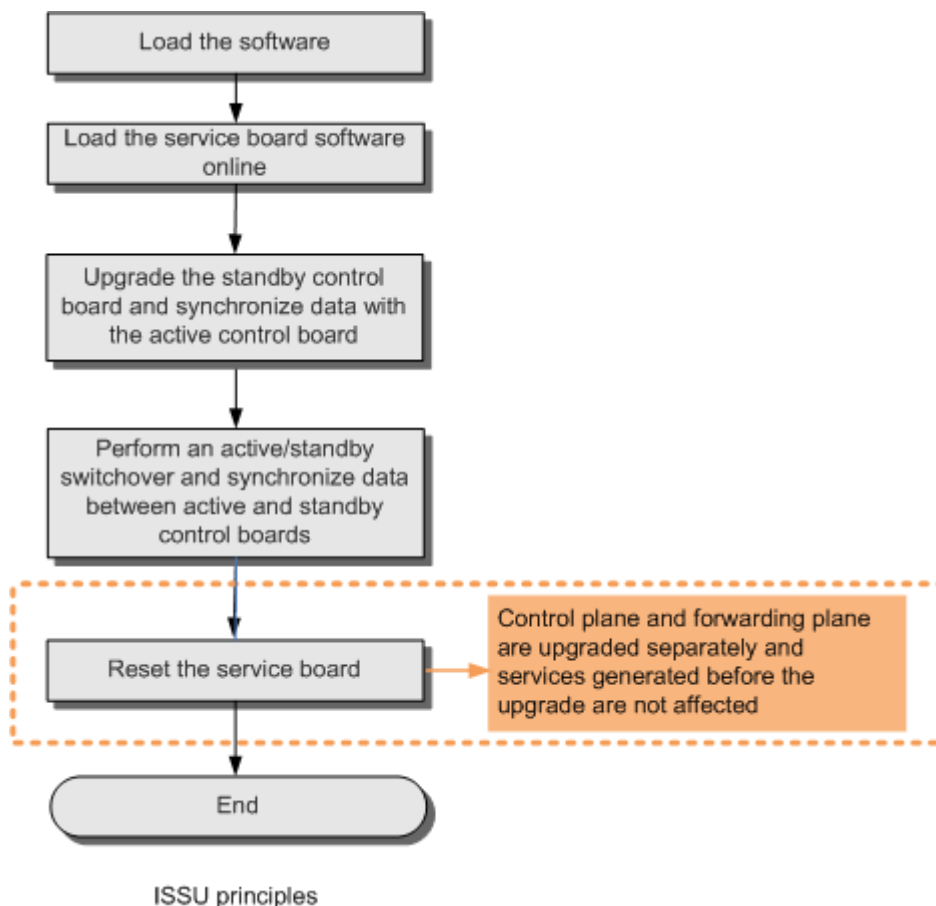
Prerequisite

- Control boards working in active/standby mode are configured.
- The upstream port is provided by the control board or a backup upstream board is configured, and inter-board protection or aggregation is configured.

Working Principles

The following figure shows the principles of MA5800 ISSU.

Figure 19-32 Working principles



Boards of the MA5800 support decoupling of the control plane and forwarding plane, that is, the control plane and forwarding plane can be upgraded separately.

- When the control plane is being upgraded, the forwarding plane works continuously and therefore services generated before the upgrade are not affected.
- When forwarding entries of the forwarding plane are upgraded, services are interrupted for about 10s.

Through the separate upgrade of the control plane and forwarding plane, boards of the MA5800 ensure that ONUs are continuously connected, services generated

before the upgrade are affected for only about 10s, and services generated during the upgrade are affected for about 2 minutes.

NOTE

Existing services refer to the services that have been provisioned before the ISSU upgrade. New services refer to the newly configured services that have not been provisioned before the ISSU upgrade.

ISSU Upgrade

An MA5800 ISSU upgrade consists of the following operations:

1. Perform a pre-upgrade check.
2. Save and back up the database file.
3. Load the combined package file.
4. Run the **upgrade issu** command to activate the package file.

NOTE

When MSTP is also configured on this board, ISSU does not take effect for this board. Services of this board are interrupted about 2-3 minutes and recover after the board resets.

5. Perform a post-upgrade check.

NOTE

For more details about the upgrade, see the Upgrade Guide released together with the product software. For its potential risks, it is recommended to perform an upgrade at night when the network carries a smaller volume of service traffic.

19.11 Anti-theft

Anti-theft for the MA5800 refers to using software to prevent the device from being misused by unauthorized users.

19.11.1 Anti-theft Feature Updates

Version	Description
V100R019C2X and later versions	First version to support this feature.

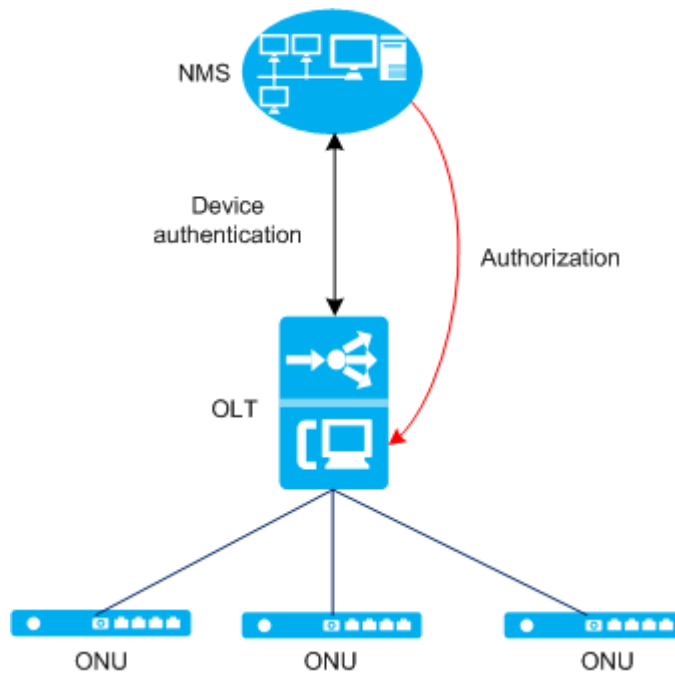
19.11.2 Anti-theft Introduction

Anti-theft for the MA5800 is a technology that allows users to lock and unlock the device using public and private keys. The public key is loaded onto the device for enabling anti-theft and the private key is used to generate an authentication file for unlocking the device. In this way, the device is locked and can be used only if it is unlocked using a matched private key. Anti-theft effectively prevents unauthorized users from using devices.

- Control boards and service boards are authorized separately.

- After a device is loaded with a public key (the anti-theft function is enabled) and powered on or restarted, it requests the NMS to perform private key authorization. After the authorization is successful, the device can be normally used.
- If a device to which the public key is loaded cannot obtain a private key from the NMS or the private key does not match, the device restriction policies are enabled.
- If a device is enabled with the anti-theft function but fails to be authorized, the device cannot be downgraded to a version that does not support the anti-theft function.

Figure 19-33 Anti-theft



19.11.3 Anti-theft Principles

After anti-theft is enabled on a hardware device, the functions of the device will be restricted upon unauthorized use of the device.

Anti-theft Modes

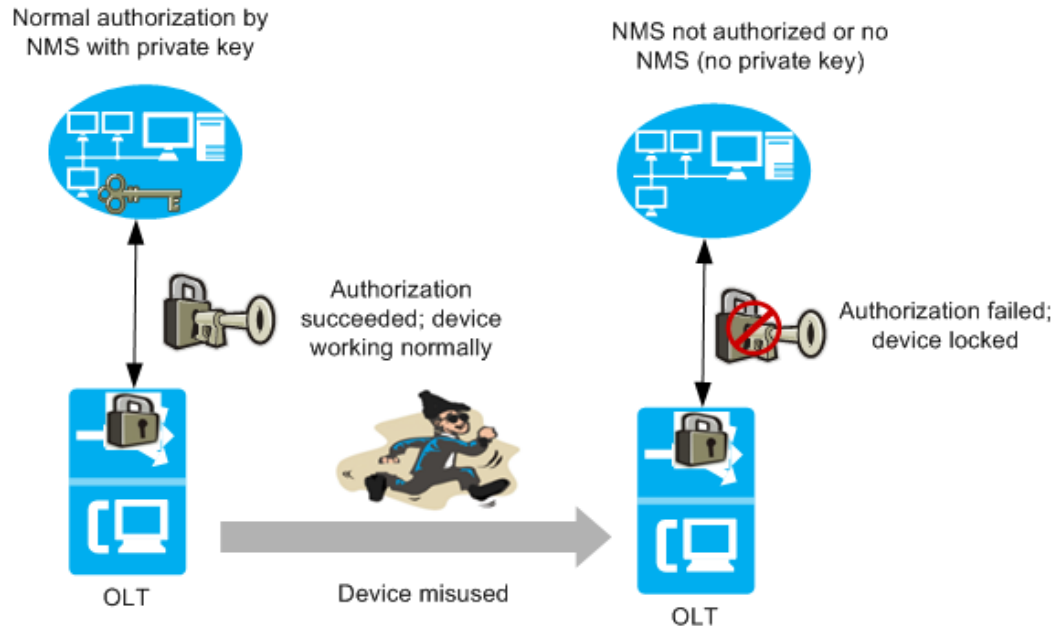
Anti-theft is based on an asymmetric encryption and decryption algorithm and the RSA public/private key algorithm. Users use the NMS or third-party software to generate two keys (public key and private key). The public key is like a lock and is loaded to the device that requires the anti-theft function. The private key is the key to the lock and is loaded to the NMS.

After a device is connected to the NMS and enabled with anti-theft, the NMS sends the public key to a device. After the main board is loaded, the anti-theft function is enabled. Any board that supports anti-theft automatically enables this function without additional configurations.

After a device to which the public key is loaded is powered on or restarted, the device instructs the NMS to perform private key authentication. After the

authentication succeeds, the device can be normally used. If a device to which the public key is loaded cannot obtain the private key from the NMS or the private key does not match, the device is locked to prevent misuse, as shown in [Figure 19-34](#).

Figure 19-34 Anti-theft principles



Anti-theft Mechanism

The anti-theft function restricts device usage using configuration and service control policies. If authorization fails after a device goes online or restarts, the configuration control policy takes effect immediately and the grace period countdown starts. The grace period can be customized and is set to 7 days by default. During the grace period, the service control policy does not take effect. After the grace period expires, the configuration and service control policies take effect at the same time.

Configuration Control Policy

If a device enabled with the anti-theft function cannot be authorized, the device is locked. If the device fails to obtain authorization, it enters the unauthorized state. After the grace period expires, the device enters the locked state.

- Device configurations can be viewed but cannot be modified. In addition, non-root users cannot log in to devices using commands.
- The upstream port works normally.

Service Control Policy

- If anti-theft is enabled on the control board, service boards follow the protection policy of the control board.
- If anti-theft is disabled on the control board or the authorization information of a service board is inconsistent with that of the control board, the service board enters the independent anti-theft control mode. After the grace period expires, the port bandwidth is limited.

19.11.4 Configuring Anti-theft

A device needs to work with the NMS to implement anti-theft. For details about how to configure anti-theft, see OLT management in the NMS operation guide.

NOTICE

- If a device is restarted due to a power failure or other reasons and cannot be connected to the NMS for authentication, the device enters the locked state and needs to be handled in time; otherwise, services will be affected due to anti-theft after the grace period expires.
- To facilitate management, it is recommended that an operator use the same key or root certificate on the entire network. If different certificates are used, different boards cannot be used together.

19.12 Environment Monitoring

This document describes the environment monitoring function of the MA5800 series products.

Purpose

This document provides:

- Basic knowledge about environment monitoring, including monitoring principles, hardware configuration, monitoring solutions, and sensors
- Guidance on configuring deployment data
- Guidance on troubleshooting maintenance faults

By reading this document, you can have a comprehensive understanding of environment monitoring.

19.12.1 EMUB Monitoring Solution

In the EMUB monitoring solution, the environment monitoring unit type B (EMUB) converts monitoring parameters and reports them to the control system.

19.12.1.1 DCDU-12E PDB

A direct current distribution unit-12E (DCDU-12E) provides –48 V DC power for all components in a cabinet. When working with the EMUB to provide environment monitoring for the MA5800, the DCDU-12E provides power input for the EMUB.

Function

The DCDU-12E provides ten –48 V DC outputs for communications equipment.

Appearance

[Figure 19-35](#) shows the exterior of a DCDU-12E.

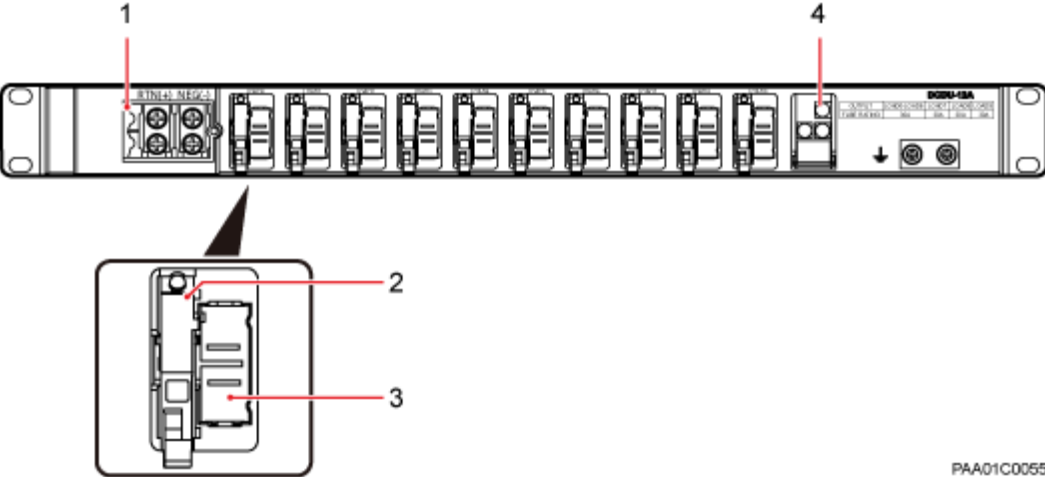
Figure 19-35 DCDU-12E power distribution box (PDB)



Ports

Figure 19-36 shows the ports on a DCDU-12E.

Figure 19-36 Ports on a DCDU-12E panel



PAA01C0055

Table 19-17 lists the ports on a DCDU-12E panel.

Table 19-17 Ports on a DCDU-12E panel

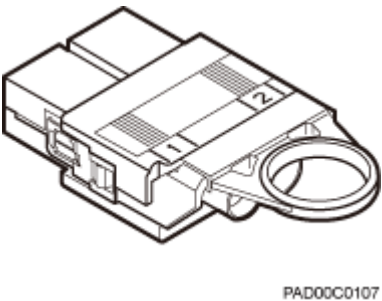
N o.	Port	Label	Connector and Cable	Description
(1)	DC input terminals	NEG(-)	Two one-hole OT terminals (M6). The default cross-sectional area of the cable is 16 mm ² .	Indicates the negative input terminal.
		RTN(+)		Indicates the positive input terminal.

N o.	Port	Label	Connector and Cable	Description
(2)	Fuse block	LOAD0–LOAD9	-	The fuse block controls ports LOAD0–LOAD9, and thereby controls the power supplies to the BBU, fan assemblies, and transmission equipment. The indicator on the fuse block indicates the status of a fuse. • If the indicator is on, the fuse is faulty and needs to be replaced. • If the indicator is off, the fuse is working properly.
(3)	DC output terminals	LOAD0–LOAD9	Figure 19-37 shows an EPC4 connector which applies to ports LOAD0–LOAD9. The cross-sectional area of the cable supported ranges from 1.5–4 mm ² .	-
(4)	Spare fuse box	-	-	It contains three 30 A spare fuses.

 NOTE

A fuse block and DC output terminals combined are called a fuse terminal block.

Figure 19-37 Exterior of an EPC4 connector



Specifications

Table 19-18 lists the technical specifications of a DCDU-12E.

Table 19-18 Technical specifications of a DCDU-12E

Parameter	Specifications
Dimensions (H x W x D)	A DCDU-12E is 1 U high and can be installed in a 19-inch cabinet or rack. Its dimensions are as follows: 42 mm x 442 mm x 65 mm (without mounting ears) 42 mm x 482.6 mm x 65 mm (with mounting ears)
Input voltage/ current	Input voltage: -48 V DC Input current: 160 A
Port surge protection	Surge protection for a -48 V DC power port: - Differential mode: 2 kV (1.2/50 μs) - Common mode: 4 kV (1.2/50 μs)
	Surge protection for a -48 V DC power port - Differential mode: 10 kA (8/20 μs) - Common mode: 20 kA (8/20 μs)

19.12.1.2 EMUB Monitoring Unit

This section describes the appearance, functions, ports, indicators, DIP switches, and technical specifications of the EMUB.

Appearance

The EMUB is a 19-inch wide and 1 U high case-shaped device. [Figure 19-38](#) shows the EMUB.

Figure 19-38 EMUB appearance



Function

The EMUB is an environment monitoring device. It monitors and detects various input signals. [Table 19-19](#) describes the functions of the EMUB.

Table 19-19 EMUB function description

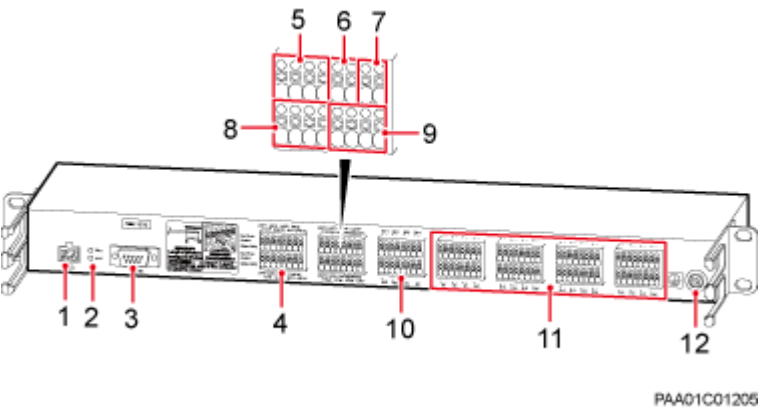
Function	Description
Power input	- Provides one power supply input port and supports –48 V DC power input (–36 V DC to –72 V DC). - Supports input voltage detection.
Environment detection	- Provides an independent port for the +12 V DC/+24 V DC current-type (4–20 mA) temperature/humidity (T/H) sensor. The temperature detection range is –20°C to +80°C. - Provides four ports for monitoring different analog signals. Voltage-type (0–5 V) and current-type (4–20 mA) sensors can be connected. - The input type is configured by the base transceiver station (BTS). You can set the DIP switch to match the BTS configuration type. - Provides monitoring ports for the +24 V DC smoke sensor, +24 V DC (or +12 V DC) water sensor, +24 V DC (or +12 V DC) infrared sensor, and dry contact-type door status sensor. These ports can meet most monitoring requirements of the system.
Boolean signal detection	Provides 32 ports for monitoring Boolean signals. The Boolean signals can be transmitted over dry contacts or open collectors (OCs).
Relay node control	Provides six ports of the relay node type for controlling the output of external Boolean signals.
Communication function	Provides two RS-485 communications ports.

Ports Definition

The EMUB provides a power port, RS485 communications ports, detection ports, and output control ports.

Figure 19-39 shows the ports on an EMUB.

Figure 19-39 Ports on an EMUB



(1) Power port	(2) Indicators	(3) RS485 port	(4) Analog signal port
(5) Infrared sensor port	(6) Smoke sensor port	(7) Door status sensor port	(8) T/H sensor port
(9) Water sensor port	(10) Relay node Boolean signal output control port	(11) Boolean signal port	(12) Ground terminal

Power port

Figure 19-40 shows the position of the power port on the EMUB.

Figure 19-40 Power port

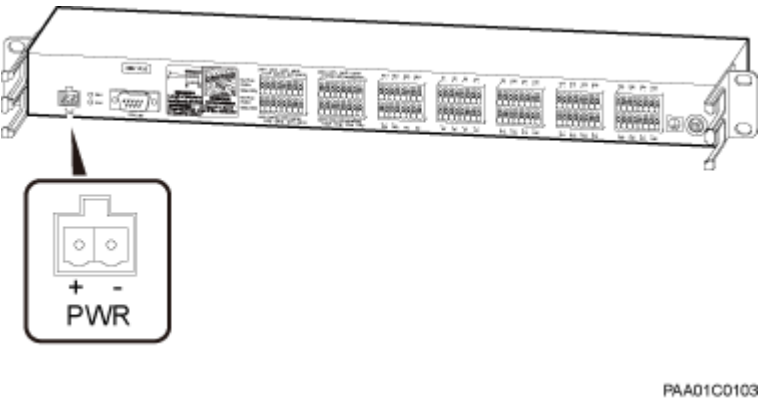


Table 19-20 describes the power port.

Table 19-20 Power port

Silk Screen	Connector Type	Description
PWR	2-pin connector	Power input port:

Communications port

Figure 19-41 shows the position and socket pins of the RS485 port on the EMUB.

Figure 19-41 RS485 port

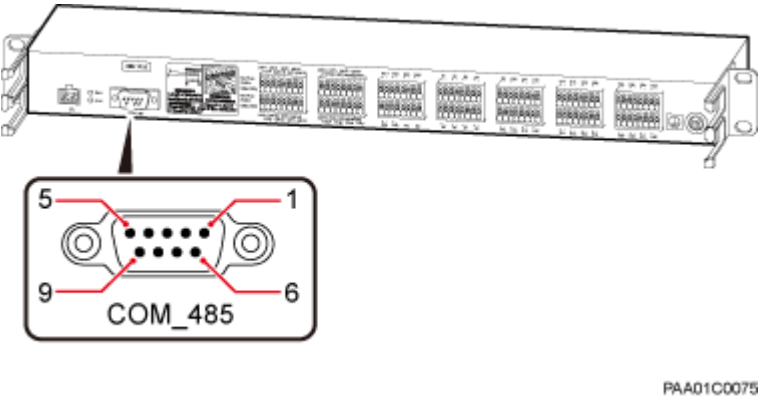


Table 19-21 RS485 port

Silk Screen	Connector Type	Description
COM_485	DB9 male connector	Communications port

Table 19-22 describes the pins of the RS485 port.

Table 19-22 RS485 port pins

PIN	Definition
1	NULL
2	RX1+: positive Rx end of port 1
3	TX1+: positive Tx end of port 1
4	RX2+: positive Rx end of port 2
5	TX2+: positive Tx end of port 2
6	RX1-: negative Rx end of port 1
7	TX1-: negative Tx end of port 1
8	RX2-: negative Rx end of port 2
9	TX2-: negative Tx end of port 2

 NOTE

- The Tx and Rx signals in the preceding table are defined in the direction from the EMUB.
- When the TXD+ is connected to the RXD+ and the TXD- is connected to the RXD-, the RS485 port can be used in two-wire mode.

Detection ports

The EMUB provides detection ports for the water sensor, smoke sensor, infrared sensor, door status sensor, and T/H sensor. It also provides input control detection ports for extended Boolean and analog signals.

Table 19-23 Detection ports on the EMUB

Signal Port	Silk Screen	Pin Function	Detected Signal Type
Water sensor port	24VW	+24 V DC power output	Voltage-type Boolean signal
	12VW	+12 V DC power output	
	WATER	Water sensor signal input	
	GND	Signal ground	
Smoke sensor port	24VS	+24 V DC power output	Current-type Boolean signal
	SMOKE	Smoke sensor signal input	
Infrared sensor port	24VO	24 V DC power output	Voltage-type Boolean signal
	12VO	12 V DC power output	
	OPTI	Infrared sensor signal input	

Signal Port	Silk Screen	Pin Function	Detected Signal Type
	GND	Signal ground	
Door status sensor port	GATE+	Positive input end of door status signals	Dry contact Boolean signal
	GATE-	Negative input end of door status signals	
T/H sensor port	24VT	24 V DC power output	Current-type analog parameter
	TEMP	Temperature signal input	
	24VH	24 V DC power output	
	HUMI	Humidity signal input	
Boolean signal port	Si+ (i = 1–32)	Positive input end of Boolean signals from route i	Boolean signals in dry contact and OC modes Ports S13–S16 and ports S29–S32 support input Boolean signals of the voltage type. Table 19-24 lists the valid Boolean signals of the voltage type.
	Si- (i = 1–32)	Negative input end of Boolean signals from route i	
Analog signal port	24Vi (i = 1–4)	24 V DC power output from route i	Current-type or voltage-type

Signal Port	Silk Screen	Pin Function	Detected Signal Type
	12Vi (i = 1-4)	12 V DC power output from route i	
	ANAi (i = 1-4)	Analog signal input from route i	
	GNDi (i = 1-4)	Signal ground of route i	
Relay node Boolean signal output control port	REi+(i=1-6)	Positive output from Relay node of route i	Boolean signal
	REi-(i=1-6)	Negative output from Relay node of route i	
	NC	Reserved	

Table 19-24 Definition of valid voltage-type Boolean signals

Amplitude of input voltage signals	Detection Result
$x \leq 3 \text{ V DC}$	Low level
$x \geq 5 \text{ V DC}$	High level
$3 \text{ V DC} < x < 5 \text{ V DC}$	Uncertain

Indicators

Table 19-25 describes the indicators on an EMUB.

Table 19-25 Indicators on the EMUB

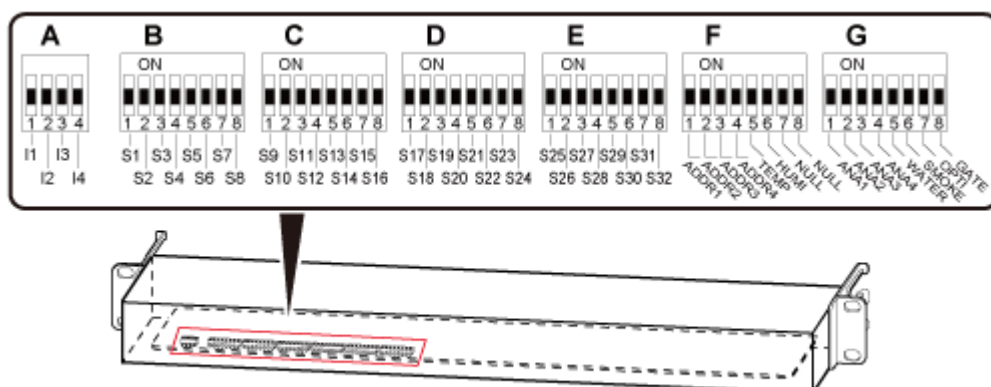
Label	Color	Status	Indication
RUN	Green	Steady off	No power is available.
		Blinking (on for 1s and off for 1s)	The board is registered and the communication is normal.
		Blinking (on for 0.125s and off for 0.125s)	The board is not registered or the communication is not set up.
ALM	Red	Steady off	The device is working properly.
		Steady on	An alarm is generated and the board needs to be replaced.
		Blinking (on for 1s and off for 1s)	An alarm is generated, and you need to locate the fault before determining whether to replace the board.

DIP Switches

This section describes the positions and functions of the DIP switches on the EMUB.

Figure 19-42 shows the positions of the DIP switches on the EMUB.

Figure 19-42 Positions of the DIP switches on the EMUB



PAAD1C0093

The ADDR DIP switch is used to select the communications protocol. It is located in position F in the preceding figure. The ADDR1-4 DIP switch is set to 0010 by default. 0 indicates that a toggle is set to ON, and 1 indicates that a toggle is set to OFF.

The DIP switches of sensors, Boolean signals, and analog signals are located in positions A, B, C, D, E, F, and G. [Table 19-26](#) describes functions of the DIP switches.

Table 19-26 DIP switches for sensors, Boolean signals, and analog signals

No.	DIP Switch	Function	Toggle State	Description
F(5)	TEMP	Bit 5: temperature sensor setting	ON	Used
			OFF	Not used
F(6)	HUMI	Bit 6: humidity sensor setting	ON	Used
			OFF	Not used
G(5)	WATER	Bit 5: water sensor setting	OFF regardless of whether it is used	
G(6)	SMOKE	Bit 6: smoke sensor setting	ON regardless of whether it is used	
G(7)	OPTI	Bit 7: infrared sensor setting	ON	Not used
			OFF	Used
G(8)	GATE	Bit 8: door status sensor setting	ON	Used
			OFF	Not used
G(1234)	ANA1 ANA2 ANA3 ANA4	Four analog sensor settings. Each bit corresponds to one analog sensor.	ON	Used
			OFF	Not used
A(1234)	I1 I2 I3 I4	Four analog sensor settings. Each bit corresponds to one analog sensor.	ON	Current type
			OFF	Voltage type

No.	DIP Switch	Function	Toggle State	Description
B, C, D, E	S1-S32	32 Boolean signal inputs S1-S32 corresponds to input signals 1 to 32.	ON	High level alarm
			OFF	Low level alarm or not used

Specifications

[Table 19-27](#) and [Table 19-28](#) and list the technical specifications of the EMUB.

Table 19-27 EMUB technical specifications

Item	Measurement Object	Specification
Input voltage detection	Measurement range	36–72 V DC
	Measurement precision	±1 V
Temperature measurement	Measurement range	–20°C to 80°C
	Measurement precision	±2°C
Humidity measurement	Measurement range	0%–100% RH
	Measurement precision	±5%
Boolean signal detection	Measurement content	Smoke, door status, water, and infrared sensors
	Alarm response time	< 10s
Analog signal detection	Measurement range	4–20 mA or 0–5 V
	Measurement precision	±1%
Relay output control	Control response time	<1s
	Dry-contact output capacity	Voltage: 110 V DC, 125 V AC, maximum load current: 1 A (30 V DC)
Communications rate	RS485	9600 bit/s

Table 19-28 Performance specifications of the EMUB

Parameter	Specifications
Storage temperature	-40°C to +70°C (non-condensing)
Operating temperature	-20°C to +55°C
Storage relative humidity	5%–95% RH
Working humidity	10–90% RH
Working voltage type	DC
Rated operating voltage	-48 V
Rated working current	0.1 A
Dimensions	442 mm x 110 mm x 41.6 mm
Weight	About 1.6 kg
RS485 protection	• 3 kA in differential mode • 5 kA in common mode
Power supply protection	• 3 kA in differential mode • 5 kA in common mode
Dry contact protection	• 3 kA in differential mode • 5 kA in common mode
Dust-proof	IP20

19.12.1.3 Checking the Environment Monitoring Cables of the EMUB

The EMUB monitors the environment monitoring parameters collected by sensors in real time, and reports the alarm information to the control system. You need to check whether the connections from the EMUB monitoring unit to the control system are correct.

Figure 19-43 shows the connections of the EMUB environment monitoring cables, and **Table 19-29** describes the cable connections. By referring to the cable connection diagram, check whether the connections from sensors to the EMUB monitoring unit and from the EMUB monitoring unit to the control system are correct.

Figure 19-43 Connection diagram for the environment monitoring cables of the EMUB

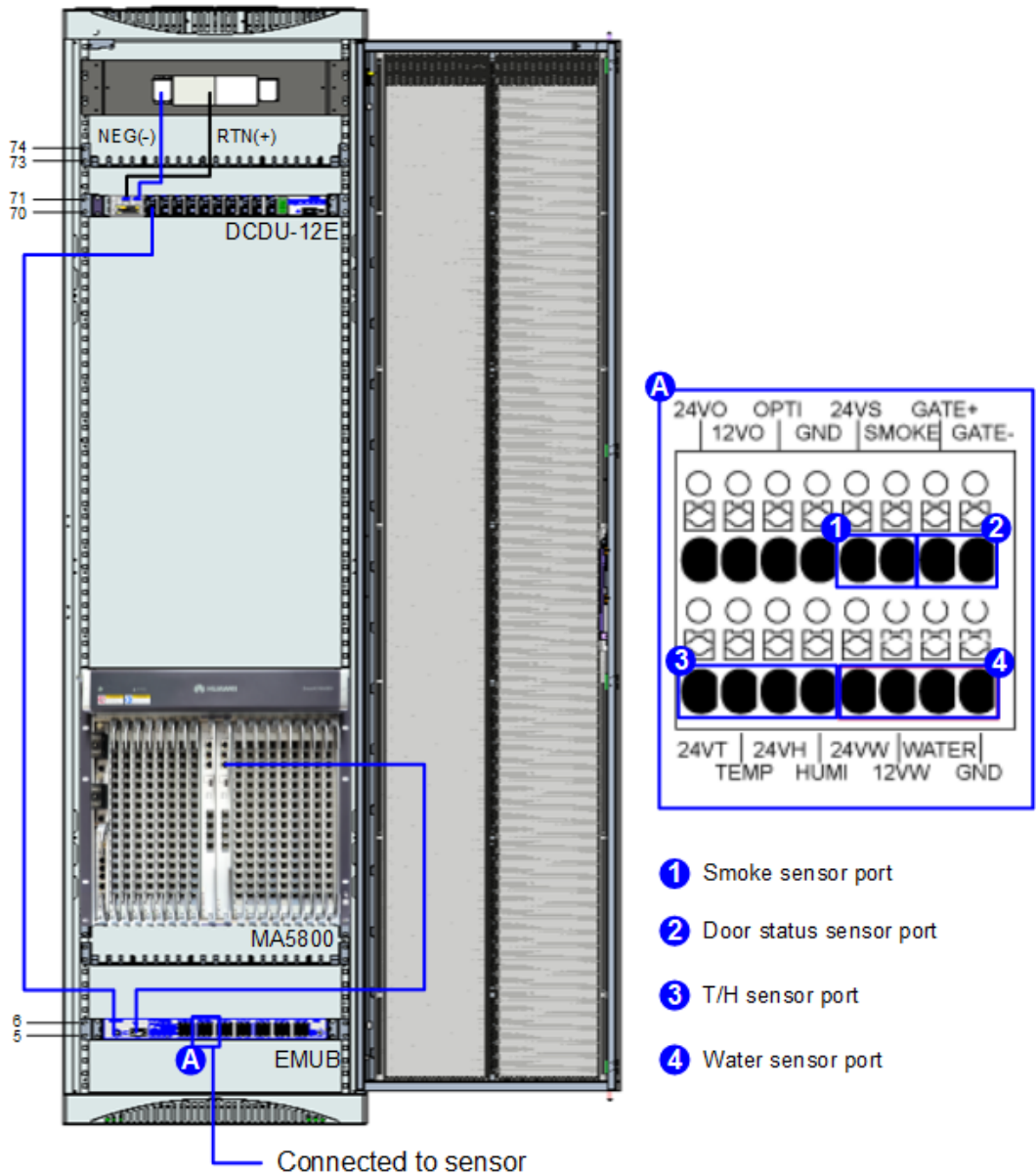


Table 19-29 Connection description for environment monitoring cables of the EMUB

Cable Name	From	To
Power cable from the cabinet PDB to the DCDU-12E	Output of the cabinet PDB	Input terminals on the DCDU-12E NOTE Only one power cable is required between the cabinet PDB and the DCDU PDB.

Cable Name	From	To
Power cable from the EMUB to the DCDU-12E	Power port on the EMUB	Output terminals of the DCDU-12E
Monitoring cable from the EMUB to the control board	RS485 port on the EMUB	ESC port on the control board
Monitoring cable of the smoke sensor	24 VS/SMOKE of EMUB	Smoke sensor
Monitoring cable of the door status sensor	GATE+/GATE- ports on the EMUB	Door status sensor
Monitoring cable of T/H sensor	24VT/TEMP/24VH/HUMI of the EMUB	T/H sensor
Monitoring cable of the water sensor	24VW/12VW/WATER/GND of the EMUB	Water sensor

19.12.1.4 Commissioning the EMUB

This section describes how to commission the environment monitoring unit (EMUB) to ensure that it can monitor the environment status of the device.

Context

The EMUB uses various sensors to monitor environment parameters such as the ambient temperature, humidity, smoke, water, and door status.

When commissioning the EMUB, pay attention to the following points:

- The value range of the EMU subnode is 0–31.
- When the system is configured with multiple EMUs simultaneously, make sure that all sub-nodes are unique.

The EMUB supports the following analog and digital parameters:

- Analog parameters 0–3: Fixedly allocated by the system to –48 V power supply, 24 V power supply, and temperature and humidity respectively. The analog parameter names cannot be changed. Analog parameter 1 is reserved internally and cannot be used. For other analog parameters, only the upper and lower alarm thresholds and the monitoring switch can be configured.
- Analog parameters 4–7: User-defined analog parameters to be allocated to other extended analog sensors.
- Digital parameters 0–3: Fixedly allocated by the system to the water sensor, smoke sensor, infrared sensor, and door status sensor respectively. The names

of these digital parameters cannot be changed. Digital parameter 2 is reserved internally and cannot be used.

- Digital parameters 4–35: user-defined digital parameters to be allocated to other extended digital sensors.

Procedure

- Step 1** Run the **emu add** command to add an EMUB.
- Step 2** Run the **interface emu** command to enter EMUB mode.
- Step 3** Run the **emub analog** command to configure the upper and lower alarm and measurement thresholds for analog parameters to be monitored by the device in real time.
- Step 4** Run the **emub digital** command to set the valid level, name, and alarm index of digital parameters of the EMU.
- Step 5** Run the **save** command to save the data.

----End

Example

To add an EMUB, configure the analog and digital parameters of the EMUB, and then save the data, do as follows:

[Table 19-30](#) shows the data planning.

Table 19-30 Data planning for configuring the EMUB

Item	Parameter	Remarks
EMU	Type: EMUB	The EMUB is displayed as EMUB in the command line.
	No.: 3	-
	Slave node ID: 2	-
Analog parameters	Analog parameter ID: 2	Fixedly allocated by the system to monitor the temperature. Only the upper and lower alarm thresholds and the monitoring switch can be configured. For the value and details of this parameter, refer to the emub analog command.
	Upper alarm threshold of analog parameter 2: 68°C	When the ambient temperature exceeds 68°C, the device reports an alarm.
	Lower alarm threshold of analog parameter 2: -5°C	When the ambient temperature is lower than -5°C, the device reports an alarm.

Item	Parameter	Remarks
	Analog parameter ID: 3	Fixedly allocated by the system to monitor the humidity. Only the upper and lower alarm thresholds and the monitoring switch can be configured. For the value and details of this parameter, refer to the emub analog command.
	Upper alarm threshold of analog parameter 3: 80% RH	When the ambient humidity exceeds 80% RH, the device reports an alarm.
	Lower alarm threshold of analog parameter 3: 5% RH	When the ambient humidity is lower than 5% RH, the device reports an alarm.
Digital parameters	Digital parameter ID: 0	Fixedly allocated by the system to monitor the water sensor. Users can only modify the valid level of the digital parameter. Other parameters cannot be modified.
	Valid level of digital parameter 1: low level	The low level is used to represent the valid level. When the actual level of the monitored digital parameter is inconsistent with the valid level configured in the system, the device reports an alarm.
	Digital parameter ID: 1	Fixedly allocated by the system to monitor the smoke sensor. Users can only modify the valid level of the digital parameter. Other parameters cannot be modified.
	Valid level of digital parameter 1: high level	The high level is used to represent the valid level. When the actual level of the monitored digital parameter is inconsistent with the valid level configured in the system, the device reports an alarm.
	Digital parameter ID: 3	Fixedly allocated by the system to monitor the door status sensor. Users can only modify the valid level of the digital parameter. Other parameters cannot be modified.
	Valid level of digital parameter 2: high level	The high level is used to represent the valid level. When the cabinet door is opened, the device reports an alarm.

```
huawei(config)#emu add 3 EMUB 0 2 EMUB
huawei(config)#interface emu 3
huawei(config-if-emub-3)#emub analog 2 alarm-upper-limit 68 alarm-lower-limit -5
huawei(config-if-emub-3)#emub analog 3 alarm-upper-limit 80 alarm-lower-limit 5
huawei(config-if-emub-3)#emub digital 0 available-level low-level
huawei(config-if-emub-3)#emub digital 1 available-level high-level
huawei(config-if-emub-3)#emub digital 3 available-level high-level
huawei(config-if-emub-3)#display emub system parameter
huawei(config-if-emub-3)#quit
huawei(config)#save
```

19.12.2 Power3000 Monitoring Solution

The Power3000 monitoring solution is implemented by the CPMU01 monitoring module in the Power3000 power system. In this solution, the CPMU01 monitoring module reports the monitored parameters to the control system.

19.12.2.1 Monitoring Module CPMU01 of the Power3000

The CPMU01 of the Power3000 implements functions such as environment monitoring, abnormality alarm reporting, battery management, rectifier module management and power distribution management by using the local device, NMS server or hand-held terminal.

The CPMU01 displays real-time information (including operation parameters, operation status, alarm status, configuration parameters and control parameters) about the DC, AC, module and battery in the power system on the (liquid crystal display) LCD. Connected to the upper device by using the RS-232 and RS-485 serial ports on the monitoring backplane, the CPMU01 remotely manages the Power3000 system.

Figure 19-44 shows the appearance of the CPMU01.

Figure 19-44 Appearance of the CPMU01



19.12.2.2 Checking the Environment Monitoring Cable of the Power3000

The CPMU01 is connected to the control system by using the RJ-45 serial port on the monitoring backplane. In the checking, ensure that the cable between the CPMU01 and the control system is connected properly.

Figure 19-45 shows the connection of the environment monitoring cable of the Power3000, and Table 19-31 describes the cable connection. You can check whether the cable between the CPMU01 and the control system is connected properly based on the connection diagram.

Figure 19-45 Connection diagram of the environment monitoring cable of the Power3000

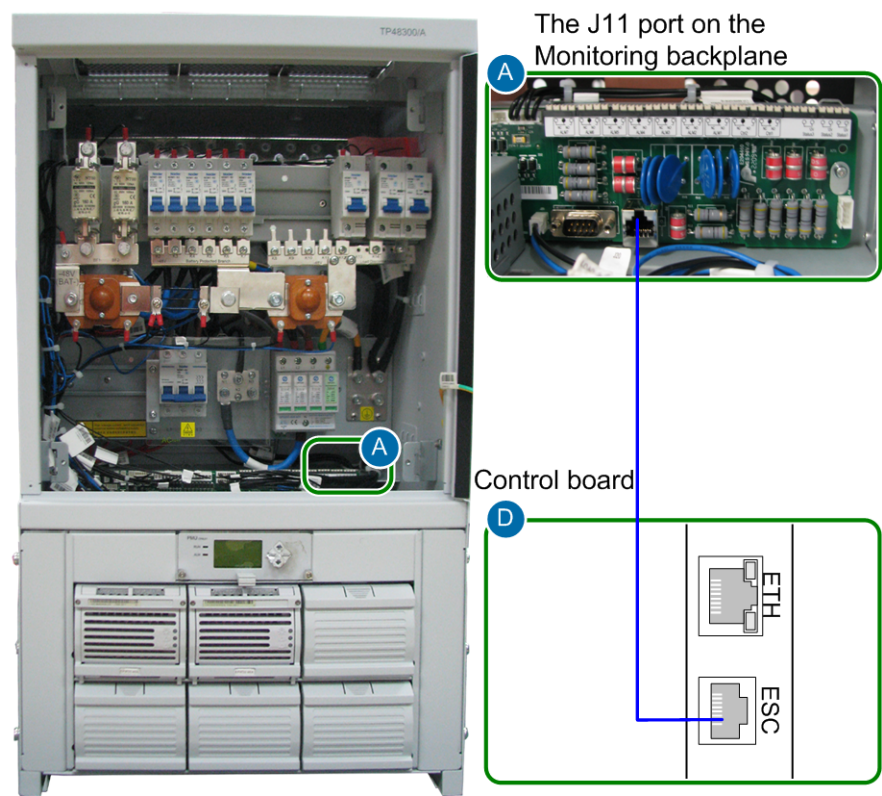


Table 19-31 Connection of the environment monitoring cable of the Power3000

Cable	Connection Position 1	Connection Position 2
Environment monitoring cable between the Power3000 and the control system	J11 port on the monitoring backplane of the Power3000	ESC port on the control board

19.12.2.3 Configuring the Power3000 Environment Monitoring Mode

This topic describes how to configure environment monitoring parameters by using the CLI.

Configuration Process

The monitoring parameters can be reported to the control system only when the data for the Power3000 is configured correctly in the system.

Table 19-32 lists the commands used during the configuration.

Table 19-32 Commands for configuring the Power3000

To...	Run the Command...
Add an EMU	emu add
Query the configuration parameters of the power system	display power system parameter
Query the power environment parameters	display power environment parameter
Configure the battery charging parameters	power charge
Configure the battery management parameters	power battery parameter
Configure the temperature compensation coefficient of the battery	power battery temperature
Configure the battery set power-off parameters	power off
Configure the power distribution parameters	power supply-parameter
Configure the battery discharging test parameters	power battery-test
Configure the parameters for the power rectifier module	power module-num
Configure the battery high-temperature power-off parameters	power temperature-off
Configure the environment monitoring parameters	power environment
Configure the external extended digital parameters	power outside-digital

1. Log in to the device through the maintenance terminal and add an EMU.
2. Query the status of the Power3000.
3. Enter the environment monitoring configuration mode and query the default configuration.
4. Configure the battery management parameters.
5. Configure the battery discharging test parameters.
6. Configure the battery high-temperature power-off parameters.
7. Configure the environment parameters.
8. Configure the extended digital parameters.
9. Query the information about the configured parameters and environment parameters of the power system.
10. Save the data.

Data Plan

Table 19-33 provides the data plan for configuring the monitoring parameters of the Power3000.

Table 19-33 Data plan for configuring the monitoring parameters of the Power3000

Item	Data Plan
EMU	Type: POWER3000 SN: 0 Subnode ID: 0 The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus.
Charging parameters of the battery	Charging mode of the battery: automatic Equalized charging voltage of the battery: 56.5 V Float charging voltage of the battery: 53.5 V
Battery management parameters	Current-limiting coefficient for battery charging: 0.15 Interval of battery equalized charging: 60 days Number of battery sets: 1 Capacity of the battery set: 65 AH The battery capacity is configured according to the actual value.
Temperature compensation parameter of the battery	Upper temperature threshold of the battery set: 80°C Lower temperature threshold of the battery set: -20°C Temperature compensation coefficient of the battery set: 80 mV

Item	Data Plan
Battery set power-off parameters	Battery set power-off permission status: permit Battery set power-off voltage: 43 V
Power distribution parameters	AC overvoltage alarm threshold of the power supply: 280 V AC undervoltage alarm threshold of the power supply: 180 V DC overvoltage alarm threshold of the power supply: 58 V DC undervoltage alarm threshold of the power supply: 45 V
Battery discharging test parameters	Battery auto-discharging test: auto-test Battery set auto-discharging test permission status: permit Battery auto-discharging test period: 60d
Power rectifier module parameters	The number of the power rectifier modules: 0 The number of the power rectifier modules is configured according to the actual value. POWER3000 supports up to 12 rectifier modules.
Battery high-temperature power-off parameters	Battery high-temperature power-off permission status: permit Temperature for battery high-temperature power-off: 53°C
Environment monitoring parameters	Upper alarm threshold of the temperature: 63°C Lower alarm threshold of the temperature: -5°C Upper test threshold of the humidity: 80°C Lower test threshold of the humidity: -20°C
External extended digital parameters	Digital parameter ID: 0-6 This digital parameter is set according to the actual requirements.

 NOTE

The preceding data is configured according to the actual requirements. When the actually planned value of a parameter is the same as the default value, it is not necessary to configure the parameter.

Configuration Example

The following considers the configuration plan of the Power3000 as an example to describe the process of configuring the environment monitoring parameters of the Power3000 after connected.

```
huawei(config)#display emu 0
huawei(config)#interface emu 0
huawei(config-if-power3000-0)#display power system parameter
huawei(config-if-power3000-0)#display power environment parameter
huawei(config-if-power3000-0)#power battery parameter 1 0.15 60 65
huawei(config-if-power3000-0)#power battery-test auto-test permit 60
huawei(config-if-power3000-0)#power temperature-off battery-off-state permit battery-off-
temperature 53
huawei(config-if-power3000-0)#power environment temperature 63 -5 80 -20
huawei(config-if-power3000-0)#power outside-digital 0 digital-alarm 9 available-level high-level
name door
huawei(config-if-power3000-0)#display power system parameter
huawei(config-if-power3000-0)#display power environment parameter
huawei(config-if-power3000-0)#quit
huawei(config)#save
```

19.12.3 ETP4890 Monitoring Solution (AC Power Supply)

The ETP4890 monitoring solution is implemented by the SMU01B monitoring module in the ETP4890 power system. In this solution, the SMU01B monitoring module reports the monitored parameters reported by the sensor transfer box to the control system.

19.12.3.1 ETP4890 Power System

An AC-powered cabinet uses the ETP4890 power system to convert the AC power to the DC power for power distribution. The small and modular ETP4890 power system supports easy installation and maintenance and effective LCD interface management. The power system supports a maximum of 90 A output current.

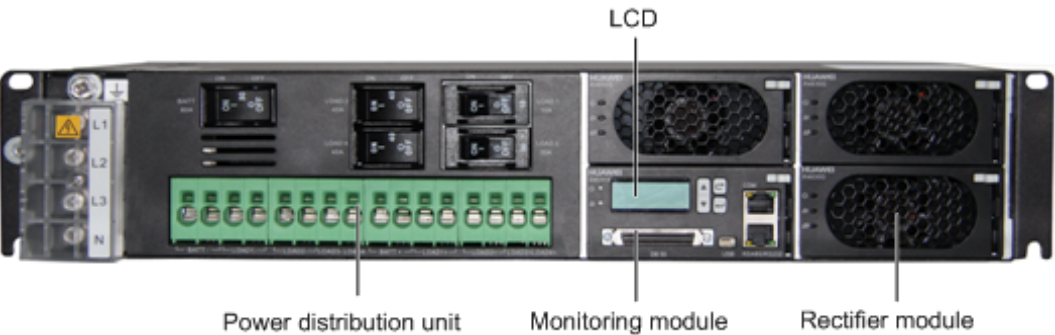
Function

- Converts AC power into stable DC power for communications equipment.
- Communicates with the upper device using a COM or an RS485/RS232 serial port; sends control signals based on the values of monitored parameters or the control command sent by the upper device; detects power distribution parameters, power supply module parameters, and auxiliary digital parameters in real time.
- Connects to one to two groups of lead acid batteries and uses a monitoring module to manage the batteries; provides complete management for battery charging and discharging, ensuring efficient battery usage.
- Connects to a sensor transfer box using a DB50 port, detecting analog parameters and digital parameters, and outputting control signals.
- Uses a monitoring module to monitor all running parameters for the ETP4890 power system in real time; determines the working status; reports alarms in a timely manner.
- Clearly displays the monitoring and alarm information on the liquid crystal display (LCD) of the monitoring module of the ETP4890; allows operations such as parameter setting on the LCD of the monitoring module.

Appearance

Figure 19-46 shows the appearance of the ETP4890 power system.

Figure 19-46 ETP4890 power system



Configuration

Table 19-34 lists the components of the ETP4890 power system.

Table 19-34 Component configuration of the ETP4890 power system

Component	Quantity
AC and DC power distribution subrack	1
Monitoring module	1
Power supply module R4830N1/ R4830G1	1 to 3 (optional; by default, the R4830N1 is configured)

The ETP4890 power system can be configured with three power supply modules, which are connected in parallel for output.

Table 19-35 shows the mapping between the quantity of power supply modules in the ETP4890 power system and the maximum output current.

Table 19-35 Mapping between the quantity of power supply modules of the ETP4890 power system and the maximum output current

Quantity of Power Supply Modules	Maximum Output Current
1	30 A (at 55°C) 25 A (at 60°C)
2	60 A (at 55°C) 50 A (at 60°C)
3	90 A (at 55°C) 75 A (at 60°C)

Communication Ports on the Monitoring Module

Table 19-36 lists the communication ports on the monitoring module. A user can set the baud rate of the device using the LCD interface of the monitoring module.

Table 19-36 Communication ports on the monitoring module

Communication Port	Communication Mode	Communication Parameter	Description
COM	RS485/RS232	Baud rate: 9600 bit/s or 19200 bit/s	Used as a serial port, communicating with the upper device
RS485/RS232	RS485/RS232	Baud rate: 9600 bit/s or 19200 bit/s	Used as a serial port, supporting the northbound/southbound communications

 NOTE

By default, the ETP4890 power system is equipped with a monitoring module, which is capable of the inband management (SMU01B). The COM port cannot be used as a network port.

Indicators

Table 19-37 lists the indicators on the power supply module of the ETP4890 power system.

Table 19-37 Indicators on the power supply module of the ETP4890 power system

Indicator	Color	Status	Description
Power indicator	Green	Steady on	Normal
		Blinking at a frequency of 0.5 Hz	There is AC input, and the power supply module is in the manual query state.
		Blinking at a frequency of 4 Hz	Data is being loaded online.
		Off	There is no AC input.

Indicator	Color	Status	Description
Alarm indicator	Yellow	Steady on	A protection mechanism is triggered. After the fault is rectified, the power supply module can be restored to the normal state.
		Blinking	Communication between the power supply module and the site monitoring module is interrupted.
		Off	Normal
Fault indicator	Red	Steady on	An unrecoverable fault occurs.
		Blinking	The power supply module equipped with the EMU does not match the actual power supply module.
		Off	Normal

Table 19-38 lists the indicators on the monitoring module.

Table 19-38 Indicators on the monitoring module

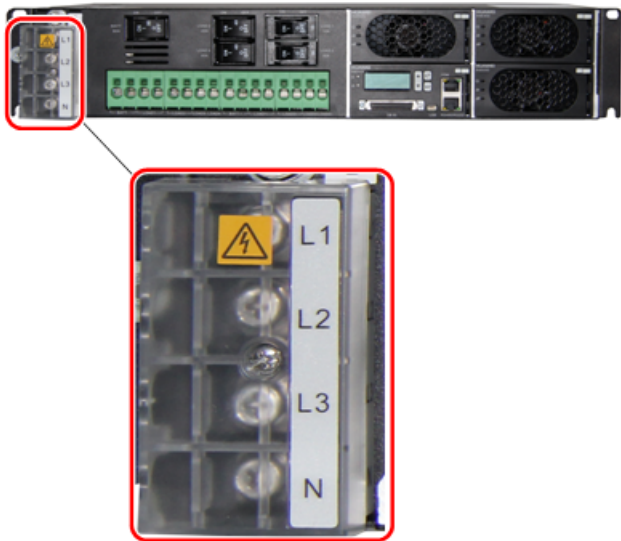
Indicator	Color	Status	Description
RUN	Green	Off	The monitoring module is faulty or there is no DC power input.
		Blinking at a frequency of 0.5 Hz	The monitoring module is working properly and communicating with the upper device properly.

Indicator	Color	Status	Description
		Blinking at a frequency of 4 Hz	The monitoring module works properly but does not communicate with the upper device properly.
ALM	Red	Off	The system does not generate any critical alarms.
		Steady on	The system generates critical alarms.

Input Terminal

The ETP4890 power system supports 220 V AC input. [Figure 19-47](#) shows the input terminals in the ETP4890 power system.

Figure 19-47 Input terminals in the ETP4890 power system



Output Terminal

The ETP4890 power system supports eight groups of output terminals. The left-side eight output terminals are negative and the right-side eight output terminals are positive.

[Figure 19-48](#) shows the output terminals in the ETP4890 power system.

Figure 19-48 Output terminals in the ETP4890 power system

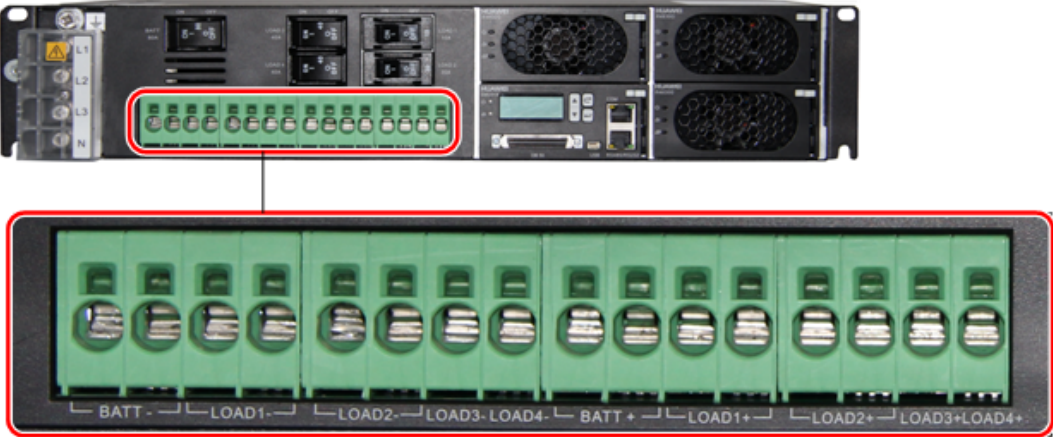


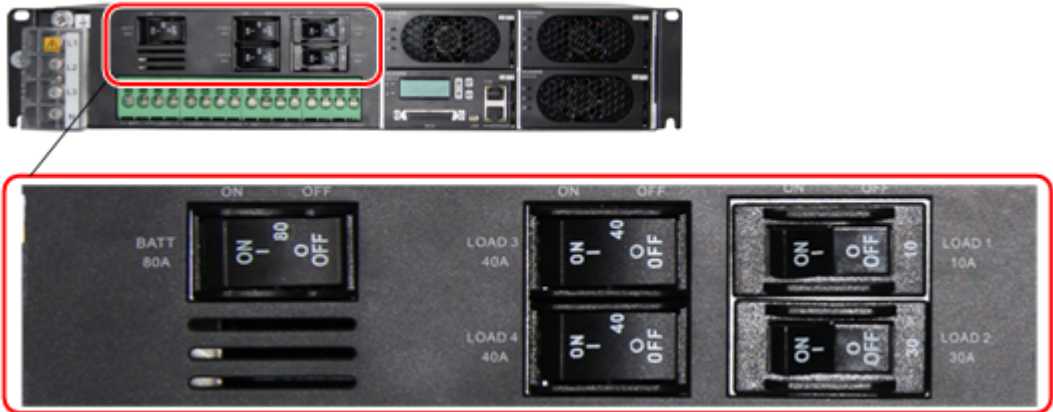
Table 19-39 lists the Specifications of the output terminals.

Table 19-39 Specifications of the output terminals

Port	Circuit Breaker
LOAD1	10 A
LOAD2	30 A
LOAD3	40 A
LOAD4	40 A
BATT	80 A

Figure 19-49 shows the output branch circuit breaker in the ETP4890 system.

Figure 19-49 Output branch circuit breaker in the ETP4890 system



Specifications

Table 19-40 lists the specifications of the ETP4890 power system.

Table 19-40 Specifications of the ETP4890 power system

Specification Class	Specification	Description
Environment conditions	Operating temperature	-40°C to +70°C NOTE The power system can work at a temperature of 70°C for 8 hours.
	Operating humidity	5% to 95% (no condensation)
	Altitude	0 m to 4000 m (Note that in the range of 2000 m to 4000 m, the operating temperature decreases by 1°C when the altitude increases by 200 m.)
AC input	Mode	mono-phase, dual-live wire
	Voltage	85 V AC to 290 V AC (rated value: 110 V/220 V)
	Frequency	45 Hz to 66 Hz (rated value: 50 Hz)
	Power factor	≥ 0.99 in the case of a rated load
	Power supply module peak efficiency	• R4830N1: 94% • R4830G1: 96%
DC output	Voltage	-42 V to -58 V
	Default voltage	-53.5 V
	Maximum power	• R4830N1: 4815 W (input voltage: 176 V AC to 290 V AC; if the temperature is higher than 55°C, power decreases linearly); 2407.5 W (input voltage: 85 V AC to 175 V AC; if the temperature is higher than 55°C, power decreases linearly) • R4830G1: 4800 W (input voltage: 176 V AC to 290 V AC; if the temperature is higher than 55°C, power decreases linearly); 2400 W (input voltage: 85 V AC to 175 V AC; if the temperature is higher than 55°C, power decreases linearly) NOTE Maximum output power of the system = Number of the configured power supply modules x Output power of each power supply module

Specification Class	Specification	Description
	Regulated voltage precision	≤ ±0.6%
	Peak noise voltage	≤ 200 mV (0 MHz to 20 MHz)
Structure	Dimensions (H x W x D) without brackets	86.1 mm x 442 mm x 255 mm
	Weight	≤ 10 kg (including three 30 A power supply modules and one SMU01B monitoring module)
	Protection class	IP20
	Installation mode	Installed in an IEC cabinet or an ETSI cabinet with brackets
	Maintenance mode	Front access
	Cooling method	Air cooling, with the built-in fan in the power supply module

19.12.3.2 PMIB02 Sensor Transfer Box

This topic describes the application and front panel of the sensor transfer box, and provides the specifications of the sensor transfer box.

Function

The sensor transfer box collects the signals of each sensor and forwards the signals to the monitoring module.

Overview

The sensor transfer box is an optional part. It provides diverse Sensor ports to connect the monitoring unit to the external sensors.

Front Panel

Figure 19-50 shows the PMIB02 sensor transfer box.

Figure 19-50 Front panel of the PMIB02 sensor transfer box



Sensor Port

Figure 19-51 shows the ports on the PMIB02 sensor transfer box, and Table 19-41 describes the functions.

Figure 19-51 Sensor ports of the PMIB02 sensor transfer box



Table 19-41 Pin functions of the sensor ports on the sensor transfer box PMIB02

Silk Screen	Signal Port	Pin Function	Remarks
BAT_W E	Sensor port of battery temperature 1	- Pin 1 is for grounding. - Pin 2 is for the signal cable. - Pin 3 is reserved. - Pin 4 is for the +12 V power supply. The external sensor outputs the 0-5 V voltage signal.	Used
VBTEM 2	Sensor port of battery temperature 2	- Pin 1 is for the +24 V power supply. - Pin 2 is for the temperature signal cable. The external sensor outputs the 4-20 mA current signal.	-
WATER	Water sensor port	- Pin 1 is for the +12 V power supply. - Pin 2 is for the signal cable. - Pin 3 is for grounding. - Pin 4 is reserved. When the impedance between pin 2 and pin 3 drops to a certain range, alarms are triggered.	-
TEM_H U	Sensor port of temperature and humidity 1	- Pin 1 and pin 3 are for the +24 V power supply. - Pin 2 is for the temperature signal cable. - Pin 4 is for the humidity signal cable.	Used

Silk Screen	Signal Port	Pin Function	Remarks
VTEM2	Sensor port of temperature and humidity 2	- Pin 1 is for the +24 V power supply. - Pin 2 is for the temperature or humidity signal cable. The external sensor outputs the 4-20 mA current signal.	-
JTP1	Sensor port of the MDF	- Pin 1 is for the signal cable. - Pin 2 is reserved.	Used
SMOKE	Smoke sensor port	- Pin 1 is for the signal cable. - Pin 2 is for the +24 V power supply.	-
JTM1	Door-status sensor port	- Pin 1 is for the signal cable. - Pin 2 is for the +24 V power supply. By default, when pin 1 and pin 2 are connected, the door is in the normal state; when they are disconnected, alarms are triggered. If no door-status sensor is used, connect pin 1 and pin 2 to disable door-status alarms.	Used
JK1, JK2	Alarm digital ports	The maximum voltage is 60 V DC and the maximum load current is 500 mA. - When minor alarms are generated, JK2 is short-circuited. - When critical alarms are generated, JK1 is short-circuited. - Users can define alarm levels through the BAM program.	Reserved
JKM1-JKM4	Digital ports	The maximum voltage is 5.6 V DC and the maximum current is 20 mA.	-
SIM1, SIM2	Battery unbalanced sensor ports	- Pin 1 is for the signal cable. - Pin 2 is reserved.	-
JAC1-JAC6	Output ports of the optical coupler	Pin 1 and pin 2 are connected to pole C and pole E of the optical coupler. The optical coupling parameter Vce max is 40 V DC and Ic max is 80 mA. Avoid setting the parameters to the maximum values.	Reserved
FU_ALM	Detecting port of the battery fuse	- Pin 1 is for the signal cable FU1+ and is connected to the negative pole of the battery. - Pin 2 is reserved for the FU1- signal.	-

Silk Screen	Signal Port	Pin Function	Remarks
JTD1-JTD7	Input ports of the standby Boolean value	- Pin 1 is for the +24 V power supply. - Pin 2 is for the +12 V power supply. - Pin 3 is for the signal cable. - Pin 4 is for grounding. According to the actual requirements, access related passive digital signals to pins 2 and pin 3.	Reserved
J1	DB50 port	A monitoring board and monitoring transfer board are connected through DB50 to input sensor signals and the output control signals.	-

 NOTE

"JTD1-JTD7" are the input ports of the standby Boolean value. By default, the sensors are not configured. You can determine the type of signal to be accessed. With related configuration, the monitor unit can monitor them.

Specifications

Table 19-42 lists the specifications of the PMIB02 sensor transfer box.

Table 19-42 Specifications of the PMIB02 sensor transfer box

Sensor Transfer Box	Dimensions (W x D x H)
PMIB02	482.6 mm x 70 mm x 43.6 mm

19.12.3.3 Checking Environment Monitoring Cables

The SMU01B monitoring module monitors the environment parameters collected by the sensors in real time, and reports the alarm information to the control system. During the check, ensure that the cable connections from the sensors to the ports of the sensor transfer box, from the sensor transfer box to the monitoring module, and from the monitoring module to the control system are correct.

Checking Environment Monitoring Cables of the N66E-22 Cabinet

Figure 19-52 shows the connections of environment monitoring cables in the N66E-22 cabinet. Table 19-43 describes the cable connections. By referring to the connection diagram, check whether the connections from the sensors to the sensor transfer box (PMIB02), from the sensor transfer box to the monitoring module, and from the monitoring module to the control system are correct.

Figure 19-52 Connections of environment monitoring cables in the N66E-22 cabinet

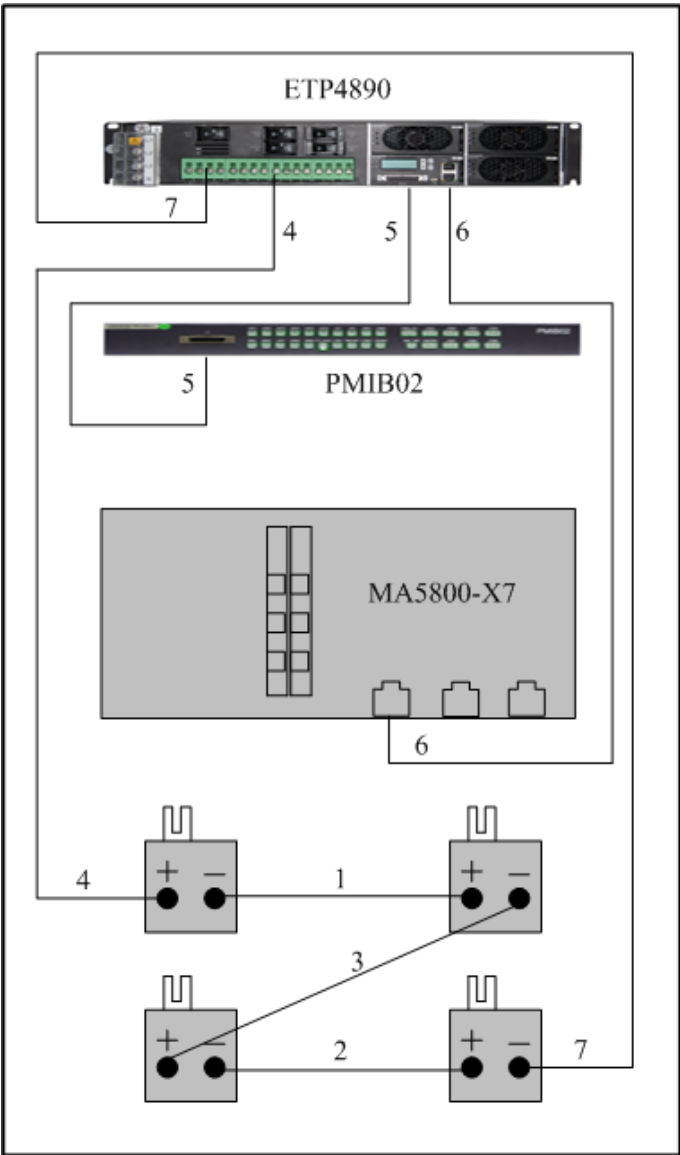


Table 19-43 Connections of environment monitoring cables in the N66E-22 cabinet

Cable	From	To
Monitoring cable of the ETP4890 to the control board	RS485/RS232 port or COM port on the ETP4890	ESC port on the control board

Cable	From	To
Monitoring cable of the PMIB02 to the ETP4890	J1 port on the PMIB02	DB50 port on the ETP4890
Monitoring cable of the battery temperature sensor	VBTEM2 terminal of the PMIB02	Battery temperature sensor

19.12.3.4 Configuring the Environment Monitoring Parameters of the ETP4890

This topic describes how to configure the environment monitoring parameters of the ETP4890 through the CLI.

Mapping Between Monitoring Parameters and Device Ports

The ETP4890 monitoring scheme can be used in the N66E-22 cabinet. [Table 19-44](#) describes the mapping between the monitoring parameters displayed

 NOTE

Before adding a user-defined analog or monitoring digital parameter, make sure that the port corresponding to this parameter is properly connected to an environment monitoring cable.

Table 19-44 Mapping between the monitoring parameters displayed on the host and the ports on the sensor transfer box

Monitoring Parameter Displayed on the Host	Device Port	Application in the N66E-22 Cabinet
Digital 0	JTD1	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 1	JTD2	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 2	JTD3	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 4	JTD5	Not connected by default, used to add a user-defined monitoring digital parameter
Battery Tem	VBTEM2	Battery temperature sensor

Procedure

- Step 1** Log in to the device through the maintenance terminal and add an ETP4890 (SMU).

Run the **display emu** command to query the ID of the ETP4890.

- Step 2** Check the default configurations of the power system according to the queried EMU ID.

Run the **interface emu** command to enter environment monitoring mode and then run the **display power system parameter** and **display power environment parameter** commands to query the default configurations.

- Step 3** Configure parameters required for lead-acid batteries.

Run the **power battery parameter** command to configure parameters required for batteries, including the management parameters, charging parameters, power-off parameters, and high-temperature power-off parameters. You can use default values of these parameters for configuration.

- Step 4** Run the **power battery temperature** command to configure the upper/lower temperature test limits, temperature compensation coefficient, and the upper/lower alarm temperature limits of the battery set.

- Step 5** (Optional) Configure discharging testing parameters.

- Run the **power battery-test** command to configure the discharging testing parameters, including the automatic power-off test, scheduled automatic test, test interval for automatic discharging, test time for delayed discharging, voltage at the stop of the test, number of batteries in a battery set, time limit for the discharging test, time limit for simplified discharging test, alarm thresholds for discharging efficiencies. You can use default values of these parameters for configuration.
- Run the **display power battery-test info** command to query the discharge testing information about the batteries.

- Step 6** Run the **power off** command to configure the battery set power-off voltage parameters

- Step 7** Run the **power temperature-off** command to configure the battery high-temperature power-off parameters.

- Step 8** Configure the environment monitoring parameters of the SMU system.

Run the **power environment** command to configure the upper alarm threshold and the upper and lower test thresholds for the temperatures and humidity. After these parameters are set, the system reports alarms if the working environment of the power system does not meet requirements.

- Step 9** Configure required parameters for the rectifier module.

Run the **power module-num** command to configure the required parameters for the rectifier module.

- Step 10** Configure the external extended digital variables of the power system.

Run the **power outside-digital** command to configure the external extended digital variables of the power system.

Step 11 Query the information about the configuration parameters and environment parameters of the power system.

Run the **display power system parameter** and **display power environment parameter** commands to query the configuration parameters and environment parameters of the power system.

Step 12 Run the **display power alarm** command to query the alarm information, and ensure that no alarm is generated for the monitored objects except the door status.

Step 13 Save the data.

Run the **quit** command to exit the SMU mode, and run the **save** command to save the data.

----End

Result

After the configuration, the ETP4890 power system works properly and monitors the configured parameters. If the status of a monitored parameter becomes abnormal, an alarm is generated on the device.

Data Plan

[Table 19-45](#) provides the data plan for configuring the monitoring parameters of the ETP4890.

Table 19-45 Data plan for configuring the power monitoring using the ETP4890

Item	Data Plan for the N66E-22 Cabinet
EMU	Type: SMU SN: 0 Subnode ID: 0 NOTE - The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus. - The EMU ID is the same as that queried by running the display emu command.
Charging parameters of the battery	Charging mode of the battery: automatic Equalized charging voltage of the battery (V): 56.5 Float charging voltage of the battery (V): 53.5

Item	Data Plan for the N66E-22 Cabinet
Battery management parameters	Current-limiting coefficient for battery charging: 0.15 Interval of battery equalized charging (day): 60 Number of battery sets: 1 Capacity of the battery set: - Two 75 Ah battery sets: 150 Ah - Two 100 Ah battery sets: 200 Ah
The upper/lower temperature test limits or temperature compensation coefficient of the battery set	Upper temperature threshold of the battery set (°C): 80 Lower temperature threshold of the battery set (°C): -20 Temperature compensation coefficient of the battery set (mV): 80
The upper/lower temperature alarm limits of the battery set	Upper temperature alarm limit of the battery set (°C): 50 Lower temperature alarm limit of the battery set (°C): -15
Battery discharging test parameters	Battery auto-discharging test: auto-test Battery set auto-discharging test permission status: permit Battery auto-discharging test period (day): 180
battery set power-off voltage parameters	Battery set power-off permission status: permit Battery set power-off voltage (V): 43
Battery high-temperature power-off parameters	Battery high-temperature power-off permission status: permit Temperature for battery high-temperature power-off (°C): 53
Environment temperature parameters	Upper alarm threshold of the temperature (°C): 68 Lower alarm threshold of the temperature (°C): -5 Upper test threshold of the temperature (°C): 80 Lower test threshold of the temperature (°C): -20
Environment humidity parameters	Upper alarm threshold of the humidity (% RH): 80 Lower alarm threshold of the humidity (% RH): 0 Upper test threshold of the humidity (% RH): 100 Lower test threshold of the humidity (% RH): 0
Power rectifier module parameters	The number of the power rectifier modules is configured according to the actual value. ETP4890 supports up to 3 rectifier modules.

 NOTE

The preceding data is configured according to the actual requirements. When the actually planned value of a parameter is the same as the default value, it is not necessary to configure the parameter.

Example

Assume that the N66E-22 cabinet is configured with two 75 AH battery sets, the ETP4890 is configured with 3 rectifier modules. To configure the environment monitoring parameters of the ETP4890 after connected, do as follows:

```
huawei(config)#display emu
huawei(config)#interface emu 1
huawei(config-if-smu-1)#display power system parameter
huawei(config-if-smu-1)#display power environment parameter
huawei(config-if-smu-1)#power battery parameter 1 0.15 60 200
huawei(config-if-smu-1)#power battery temperature 80 -20 80
huawei(config-if-smu-1)#power battery temperature alarm_upper-limit 50 alarm_lower-limit -15
huawei(config-if-smu-1)#power battery-test auto-test permit 180
huawei(config-if-smu-1)#display power battery-test info 1
huawei(config-if-smu-1)#power off battery-off-state permit battery-off-voltage 43
huawei(config-if-smu-1)#power temperature-off battery-off-state permit battery-off-temperature 53
huawei(config-if-smu-1)#power environment temperature 68 -5 80 -20
  This command is invalid unless in the contition of install the sensor, would
you continue? (y/n)[n]:y
huawei(config-if-smu-1)#power environment humidity 80 0 100 0
  This command is invalid unless in the contition of install the sensor, would
you continue? (y/n)[n]:y
huawei(config-if-smu-1)#power module-num 3 1 2 3

huawei(config-if-smu-1)#display power system parameter
huawei(config-if-smu-1)#display power environment parameter
huawei(config-if-smu-1)#display power alarm
huawei(config-if-smu-1)#quit
huawei(config)#save
```

19.12.4 ETP48200 Monitoring Solution

The ETP48200 monitoring solution is implemented by the SMU11C monitoring module in the ETP48200 power system. In this solution, the SMU11C monitoring module reports the monitored parameters reported by the sensor transfer box to the control system.

19.12.4.1 ETP48200-B2A1 Power System

The ETP48200-B2A1 (abbreviated as ETP48200) is an embedded power system that supplies power to -48 V DC telecom equipment. It has a maximum output current of 150 A.

Function

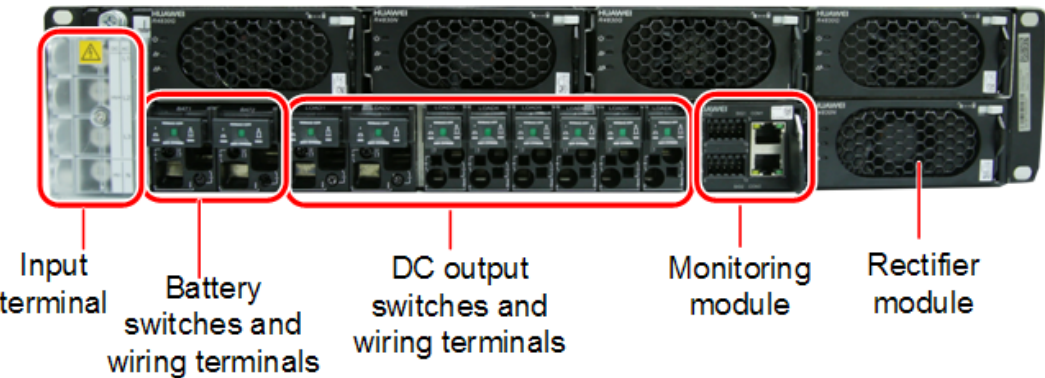
The ETP48200-B2A1 power system supports the following functions:

- Supports AC or HVDC input. AC input voltage range: 85–300 V AC; HVDC input voltage range: 85–420 V DC.
- Comprehensive battery management.
- Communication and alarm functions; remote management and online upgrade.

- One CAN port, RS485, or FE port for network connections.
- Hot-swappable rectifiers and monitoring module.

Appearance

Figure 19-53 Appearance of ETP48200-B2A1power system



Configuration

Table 19-46 Component configuration of the ETP48200-B2A1power system

Component	Configuration
Subrack	2 U power system
Power distribution unit (PDU)	• AC or DC input: M6 OT wiring terminal • DC output: supports a maximum of nine 63 A or lower circuit breakers or four 80 A and three 63 A circuit breakers. • Battery route: Two 100 A circuit breakers are supported.
Rectifier	A maximum of five R4830G1s, or R4815G1s can be configured.
Monitoring module	SMU11C

The ETP48200-B2A1 power system can be configured with 5 rectifiers, which are connected in parallel for output.

[Table 19-47](#) shows the mapping between the quantity of power supply modules in the ETP48200-B2A1 power system and the maximum output current.

Table 19-47 Mapping between the quantity of power supply modules of the ETP48200-B2A1 power system and the maximum output current

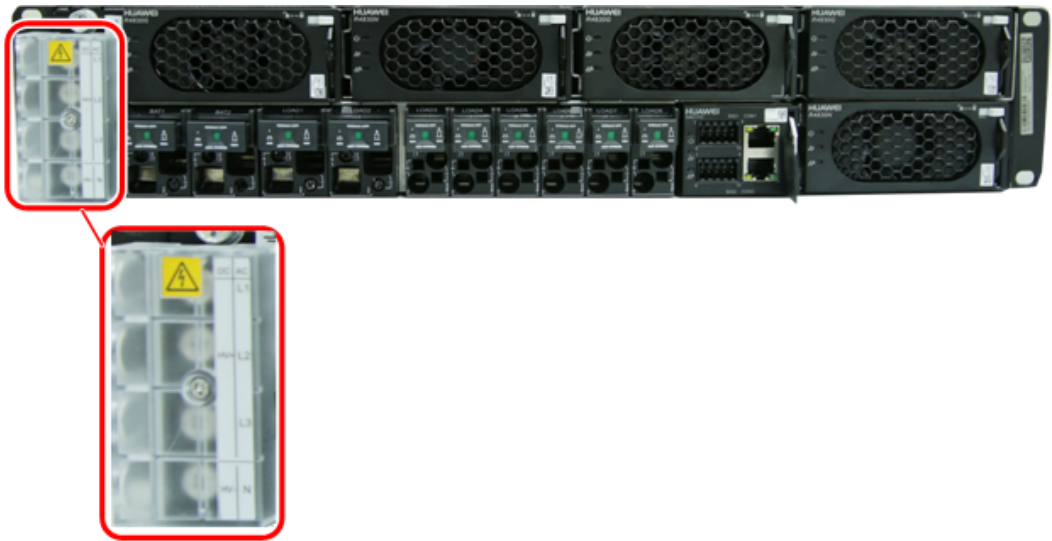
Quantity of Power Supply Modules	Maximum Output Current
1	30 A
2	60 A
3	90 A
4	120 A
5	150 A

Input Terminal

The ETP48200-B2A1 power system supports single-phase, three-phase, four-wire, dual-live-wire, or HVDC input.

Figure 19-54 shows the input terminals in the ETP48200-B2A1 power system.

Figure 19-54 Input terminals in the ETP48200-B2A1 power system

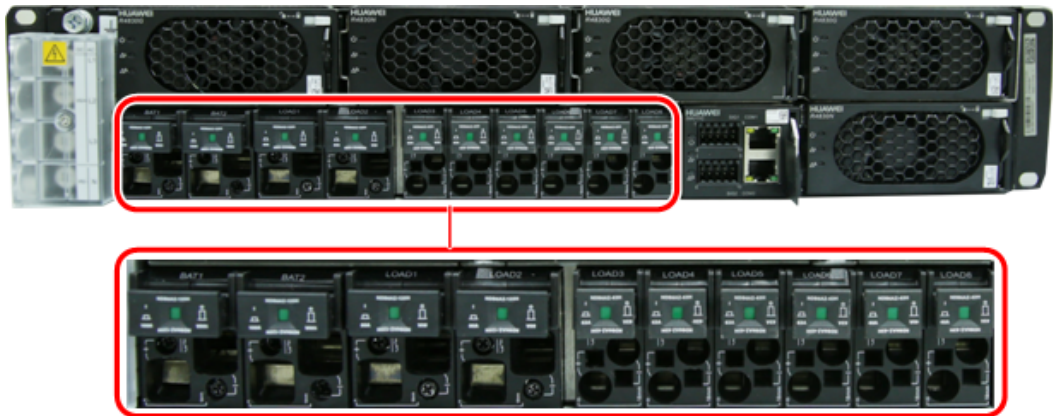


Output Terminal

The ETP48200-B2A1 power system supports flexible configuration and supports 63A or lower current. 20 mm width; 80A, 100A, and 125A: 30 mm width; The 20 mm and 30 mm cover can be flexibly interchanged. Two 30 mm circuit breakers can be replaced with three 20mm shells.

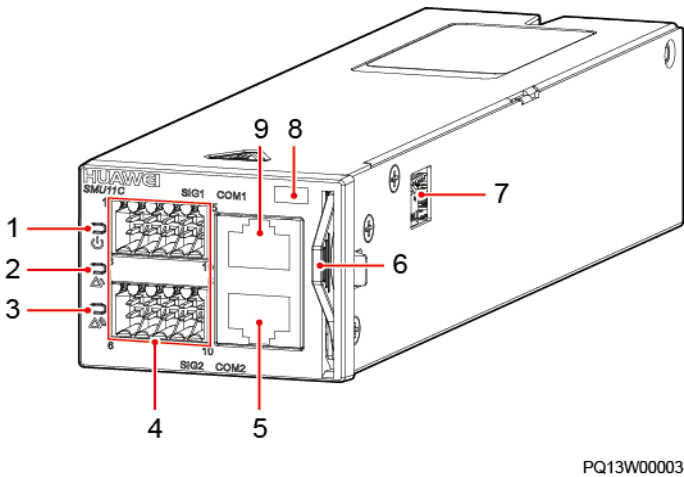
Figure 19-55 shows the output terminals in the ETP48200-B2A1 power system.

Figure 19-55 Output terminals in the ETP48200-B2A1 power system



Monitoring Module SMU11C

Figure 19-56 SMU11C appearance (without terminals)



(1) Running indicator	(2) Minor alarm indicator	(3) Major alarm indicator
(4) Wiring terminals	(5) Communications port COM2	(6) Handle
(7) Dual-in-line package (DIP) switch	(8) Position of the SN code	(9) Communications port COM1

Table 19-48 Description of the indicators on the SMU11C panel

Name	Color	Status	Description
Running indicator	Green	Off	The SMU is faulty or has no power input.

Name	Color	Status	Description
		Blinking slowly (0.5 Hz)	The SMU is running and communicating with the host properly.
		Blinking fast (4 Hz)	The SMU is running properly but fails to communicate with the host properly.
Minor alarm indicator	Yellow	Off	No minor alarm or warning is generated.
		Steady on	A minor alarm or warning is generated.
Major alarm indicator	Red	Off	No critical or major alarm is generated.
		Steady on	A critical or major alarm is generated.

Figure 19-57 Wiring terminals of monitoring module SMU11C

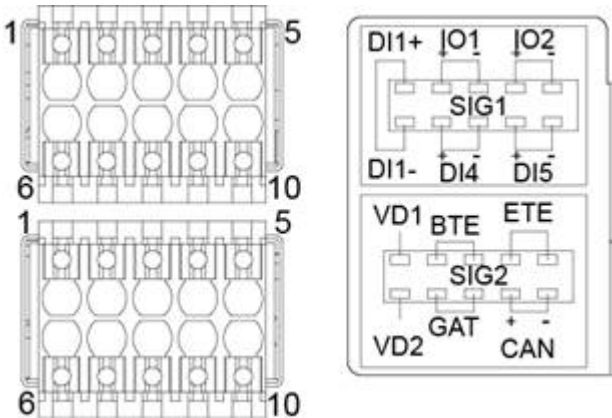


Table 19-49 Pin definitions for SIG1 wiring terminals of monitoring module SMU11C

Pin	Signal	Description
1	DI1+	Dry contact input
6	DI1-	
7	DI4+	
8	DI4-	
9	DI5+	
10	DI5-	

Pin	Signal	Description
2	IO1+	Dry contact input/Dry contact output (When used as a dry contact input, the alarm condition is as follows: normal when open, alarm when closed. When used as a dry contact output, the alarm action is as follows: open when normal, closed when alarm.)
3	IO1-	
4	IO2+	
5	IO2-	

Table 19-50 Pin definitions for SIG2 wiring terminals of monitoring module SMU11C

Pin	Signal	Description
1	VD1	Midpoint voltage detection port 1
6	VD2	Midpoint voltage detection port 2
2	BTE	Battery temperature sensor port
3		
4	ETE	Ambient temperature sensor port
5		
7	GAT	Door status sensor port
8		
9	CAN+	CAN communications port
10	CAN-	

Table 19-51 Communications port description of monitoring module SMU11C

Communications Port	Communication s Parameter	Communications Protocol	Function
COM1	Baud rate: 9600 bit/s, 19200 bit/s, or 115200 bit/s	Master/slave protocols	Connects to an upper-level network management system (NMS).

Communications Port	Communication s Parameter	Communications Protocol	Function
COM2	Baud rate: 9600 bit/s, 19200 bit/s, or 115200 bit/s	Master/slave and Modbus protocols	Connects to an upper-level NMS or intelligent equipment.
NOTE All these ports are protected by a security mechanism.			

Figure 19-58 COM port pins on the SMU11C panel

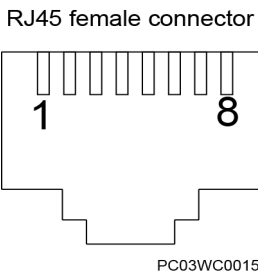


Table 19-52 Pin definitions for the COM1 port of monitoring module SMU11C

Pin	Signal	Description
1	TX+	Transmits data over RS485.
2	TX-	
3	RX232	Receives data over RS232.
4	RX+	Receives data over RS485.
5	RX-	
6	PGND	Grounds the port (PE).
7	TX232	Transmits data over RS232.
8	Reserved	-

Table 19-53 Pin definitions for the COM2 port of monitoring module SMU11C

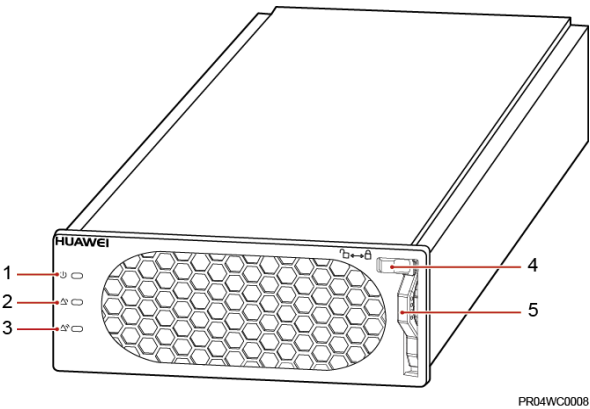
Pin	Signal	Description
1	TX+	Transmits data over RS485.
2	TX-	
3	12 V	12 V output (rated current: 500 mA)

Pin	Signal	Description
4	RX+	Receives data over RS485.
5	RX-	
6	I ² C_SCL	I ² C clock signal
7	I ² C_SDA	I ² C data signal
8	PGND	Grounds the port (PE).

Rectifier Module

A rectifier module converts AC or DC input power into stable DC power.

Figure 19-59 Rectifier module appearance



(1) Run indicator	(2) Alarm indicator	(3) Fault indicator
(4) Locking latch	(5) Handle	

Table 19-54 Rectifier module indicator description

Indicator	Color	Status	Description
Run indicator	Green	Steady on	The rectifier has an AC power input.
		Off	The rectifier has no AC power input.
			The rectifier is faulty.
		Blinking at 0.5 Hz	The rectifier is being queried.
		Blinking at 4 Hz	The rectifier is loading an application program.

Indicator	Color	Status	Description
Alarm indicator	Yellow	Off	No alarm has been generated.
		Steady on	- The rectifier has generated an alarm due to ambient overtemperature. - The rectifier has generated an alarm for shutdown due to ambient overtemperature or undertemperature.
			The rectifier is protecting itself against AC input overvoltage or undervoltage.
			The rectifier is hibernating.
		Blinking at 0.5 Hz	The communication between the rectifier and the SMU has been interrupted.
Fault indicator	Red	Off	The rectifier is running properly.
		Steady on	The rectifier has been locked out due to output overvoltage.
			The rectifier has no output due to an internal fault.

Technical Specifications

The following table shows the technical specifications of the ETP48200-B2A1power system.

Table 19-55 Technical specifications

Category	Item	Specifications
Environmental condition	Operating temperature	−40°C to +65°C; when the operating temperature ranges from 55°C to 65°C, rectifier power is derated automatically.
	Transportation/Storage temperature	−40°C to +70°C
	Operating humidity	5%–90% RH (non-condensing)
	Storage humidity	5%–95% RH (non-condensing)

Category	Item	Specifications
	Altitude	0–4000 m When the altitude ranges from 2000 m to 4000 m, high temperature derating applies and the operating temperature decreases by 1°C for each additional 200 m.
AC input	Input system	220/380 V AC three-phase four-wire (compatible with 220 V AC single-phase and 110 V AC dual-live wire)
	Rated voltage	200/346–240/415V AC
	Voltage range	85/148–300/520V AC
	Input frequency	45–65 Hz (rated frequency: 50 Hz/60 Hz)
DC input	Input system	HVDC (HV+, HV–) input
	Rated voltage	380 V DC
	Voltage range	85–420 V DC
DC output	Output voltage range	–42 V DC to –58 V DC
	Maximum output power	10000 W
	Regulated voltage precision	≤ ±1%
	Peak-to-peak noise voltage	≤ 200 mV
AC input protection	AC input over-voltage protection threshold	> 300 V AC
	AC input overvoltage recovery threshold	When the voltage is restored to 290 V AC, the output resumes.
	AC input under-voltage protection threshold	< 80 V AC
	AC input under-voltage recovery threshold	When the voltage is restored to 85 V AC, the output resumes.
DC input protection	DC input overvoltage protection threshold	> 420 V DC

Category	Item	Specifications
	DC input overvoltage recovery threshold	When the voltage is restored to 414 V DC, the output resumes.
DC output protection	DC output overvoltage protection threshold	Range: 56–60 V DC
Structure	Dimensions (H x W x D)	86.1 mm x 442 mm x 255 mm (without mounting ears)
	Weight	≤ 16 kg (including five rectifiers and one monitoring module)
	Protection level	IP20
	Installation mode	Installed horizontally or vertically in a cabinet
	Maintenance mode	Maintained from the front
	Cooling	Free cooling

19.12.4.2 Checking the Environment Monitoring Cable

The SMU11C monitoring module monitors environment monitoring parameters collected by sensors in real time, and reports alarms to the control system. During the check, ensure that the cable connections from the sensors to the ports of the sensor transfer box, from the sensor transfer box to the monitoring module, and from the monitoring module to the control system are correct.

Checking Environment Monitoring Cables of the N66E-22 Cabinet

[Figure 19-60](#) shows the connections of the N66E-22 environment monitoring cables, and [Table 19-56](#) describes the cable connections. By referring to the connection diagram, check whether the connections from the sensors to the sensor transfer box (PMIB02), from the sensor transfer box to the monitoring module, and from the monitoring module to the control system are correct.

Figure 19-60 Connections of environment monitoring cables in the N66E-22 cabinet

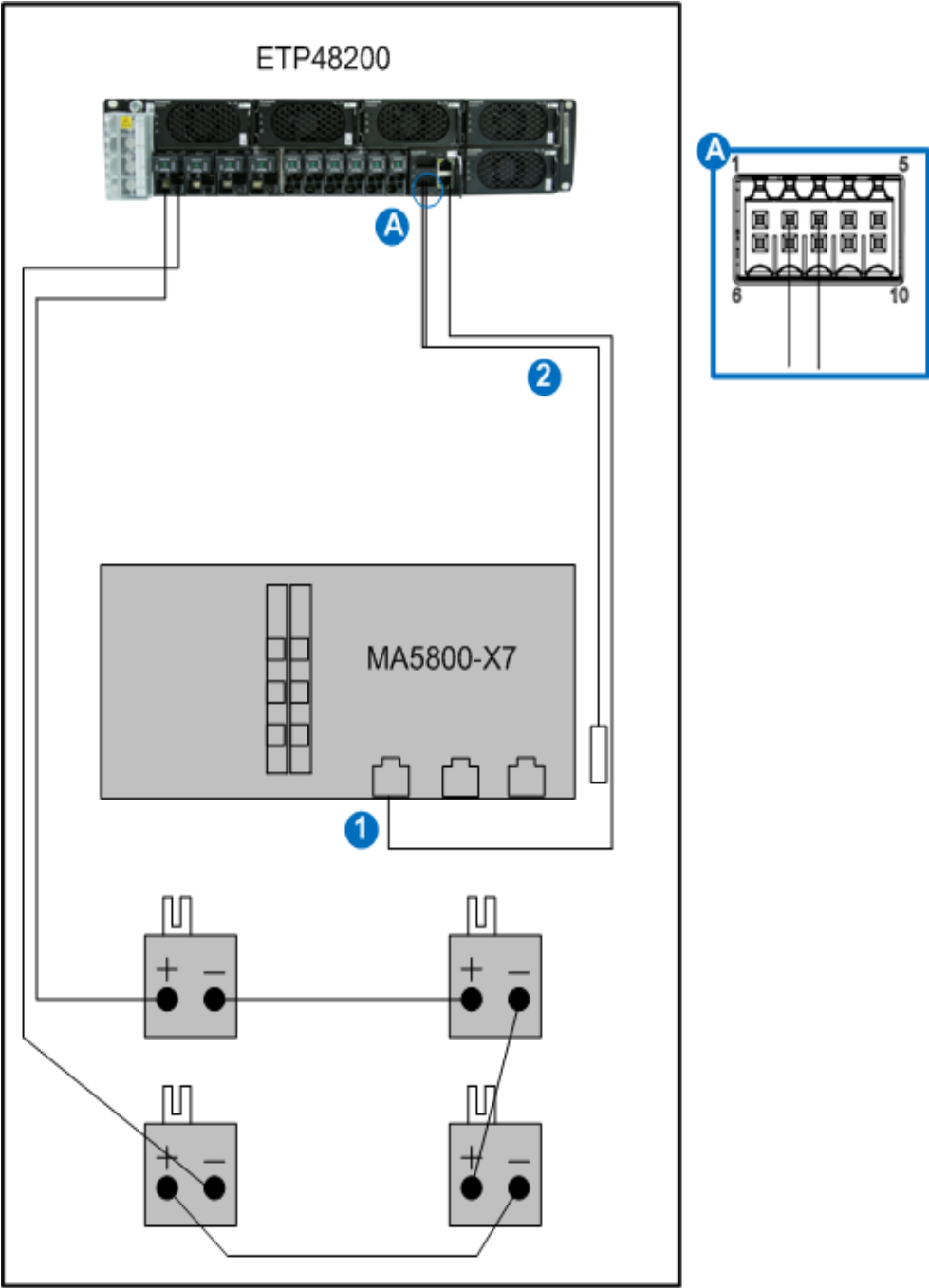


Table 19-56 Connections of environment monitoring cables in the N66E-22 cabinet

Cable Name	From	To
Monitoring cable between the ETP48200 and the control board	COM2 port on the ETP48200 monitoring module	ESC port on the control board
Monitoring cable of the battery temperature sensor	ETE port on the ETP48200 monitoring module	Battery temperature sensor

19.12.4.3 Configuring the Environment Monitoring Parameters of the ETP48200

This topic describes how to configure the environment monitoring parameters of the ETP4890 through the CLI.

Mapping Between Monitoring Parameters and Device Ports

The ETP4890 monitoring scheme can be used in the N66E-22 cabinet. [Table 19-57](#) describes the mapping between the monitoring parameters displayed

 NOTE

Before adding a user-defined analog or monitoring digital parameter, make sure that the port corresponding to this parameter is properly connected to an environment monitoring cable.

Table 19-57 Mapping between the monitoring parameters displayed on the host and the ports on the sensor transfer box

Monitoring Parameter Displayed on the Host	Device Port	Application in the N66E-22 Cabinet
Digital 0	JTD1	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 1	JTD2	Not connected by default, used to add a user-defined monitoring digital parameter
Digital 2	JTD3	Not connected by default, used to add a user-defined monitoring digital parameter

Monitoring Parameter Displayed on the Host	Device Port	Application in the N66E-22 Cabinet
Digital 4	JTD5	Not connected by default, used to add a user-defined monitoring digital parameter
Battery Tem	VBTEM2	Battery temperature sensor

Procedure

- Step 1** Log in to the device through the maintenance terminal and add an ETP4890 (SMU).
- Run the **display emu** command to query the ID of the ETP4890.
- Step 2** Check the default configurations of the power system according to the queried EMU ID.
- Run the **interface emu** command to enter environment monitoring mode and then run the **display power system parameter** and **display power environment parameter** commands to query the default configurations.
- Step 3** Configure parameters required for lead-acid batteries.
- Run the **power battery parameter** command to configure parameters required for batteries, including the management parameters, charging parameters, power-off parameters, and high-temperature power-off parameters. You can use default values of these parameters for configuration.
- Step 4** Run the **power battery temperature** command to configure the upper/lower temperature test limits, temperature compensation coefficient, and the upper/lower alarm temperature limits of the battery set.
- Step 5** (Optional) Configure discharging testing parameters.
- Run the **power battery-test** command to configure the discharging testing parameters, including the automatic power-off test, scheduled automatic test, test interval for automatic discharging, test time for delayed discharging, voltage at the stop of the test, number of batteries in a battery set, time limit for the discharging test, time limit for simplified discharging test, alarm thresholds for discharging efficiencies. You can use default values of these parameters for configuration.
 - Run the **display power battery-test info** command to query the discharge testing information about the batteries.
- Step 6** Run the **power off** command to configure the battery set power-off voltage parameters
- Step 7** Run the **power temperature-off** command to configure the battery high-temperature power-off parameters.
- Step 8** Configure the environment monitoring parameters of the SMU system.
- Run the **power environment** command to configure the upper alarm threshold and the upper and lower test thresholds for the temperatures and humidity. After

these parameters are set, the system reports alarms if the working environment of the power system does not meet requirements.

Step 9 Configure required parameters for the rectifier module.

Run the **power module-num** command to configure the required parameters for the rectifier module.

Step 10 Configure the external extended digital variables of the power system.

Run the **power outside-digital** command to configure the external extended digital variables of the power system.

Step 11 Query the information about the configuration parameters and environment parameters of the power system.

Run the **display power system parameter** and **display power environment parameter** commands to query the configuration parameters and environment parameters of the power system.

Step 12 Run the **display power alarm** command to query the alarm information, and ensure that no alarm is generated for the monitored objects except the door status.

Step 13 Save the data.

Run the **quit** command to exit the SMU mode, and run the **save** command to save the data.

----End

Result

After the configuration, the ETP4890 power system works properly and monitors the configured parameters. If the status of a monitored parameter becomes abnormal, an alarm is generated on the device.

Data Plan

Table 19-58 provides the data plan for configuring the monitoring parameters of the ETP4890.

Table 19-58 Data plan for configuring the power monitoring using the ETP4890

Item	Data Plan for the N66E-22 Cabinet
EMU	Type: SMU SN: 0 Subnode ID: 0 NOTE - The subnode ID must be the same as the subnode setting of the corresponding DIP switches on the EMU, but the subnode ID must be different from IDs of the other subnodes on the same bus. - The EMU ID is the same as that queried by running the display emu command.

Item	Data Plan for the N66E-22 Cabinet
Charging parameters of the battery	Charging mode of the battery: automatic Equalized charging voltage of the battery (V): 56.5 Float charging voltage of the battery (V): 53.5
Battery management parameters	Current-limiting coefficient for battery charging: 0.15 Interval of battery equalized charging (day): 60 Number of battery sets: 1 Capacity of the battery set: - Two 75 Ah battery sets: 150 Ah - Two 100 Ah battery sets: 200 Ah
The upper/lower temperature test limits or temperature compensation coefficient of the battery set	Upper temperature threshold of the battery set (°C): 80 Lower temperature threshold of the battery set (°C): -20 Temperature compensation coefficient of the battery set (mV): 80
The upper/lower temperature alarm limits of the battery set	Upper temperature alarm limit of the battery set (°C): 50 Lower temperature alarm limit of the battery set (°C): -15
Battery discharging test parameters	Battery auto-discharging test: auto-test Battery set auto-discharging test permission status: permit Battery auto-discharging test period (day): 180
battery set power-off voltage parameters	Battery set power-off permission status: permit Battery set power-off voltage (V): 43
Battery high-temperature power-off parameters	Battery high-temperature power-off permission status: permit Temperature for battery high-temperature power-off (°C): 53
Environment temperature parameters	Upper alarm threshold of the temperature (°C): 68 Lower alarm threshold of the temperature (°C): -5 Upper test threshold of the temperature (°C): 80 Lower test threshold of the temperature (°C): -20
Environment humidity parameters	Upper alarm threshold of the humidity (% RH): 80 Lower alarm threshold of the humidity (% RH): 0 Upper test threshold of the humidity (% RH): 100 Lower test threshold of the humidity (% RH): 0

Item	Data Plan for the N66E-22 Cabinet
Power rectifier module parameters	The number of the power rectifier modules is configured according to the actual value. ETP4890 supports up to 3 rectifier modules.

 NOTE

The preceding data is configured according to the actual requirements. When the actually planned value of a parameter is the same as the default value, it is not necessary to configure the parameter.

Example

Assume that the N66E-22 cabinet is configured with two 75 AH battery sets, the ETP4890 is configured with 3 rectifier modules. To configure the environment monitoring parameters of the ETP4890 after connected, do as follows:

```
huawei(config)#display emu
huawei(config)#interface emu 1
huawei(config-if-smu-1)#display power system parameter
huawei(config-if-smu-1)#display power environment parameter
huawei(config-if-smu-1)#power battery parameter 1 0.15 60 200
huawei(config-if-smu-1)#power battery temperature 80 -20 80
huawei(config-if-smu-1)#power battery temperature alarm_upper-limit 50 alarm_lower-limit -15
huawei(config-if-smu-1)#power battery-test auto-test permit 180
huawei(config-if-smu-1)#display power battery-test info 1
huawei(config-if-smu-1)#power off battery-off-state permit battery-off-voltage 43
huawei(config-if-smu-1)#power temperature-off battery-off-state permit battery-off-temperature 53
huawei(config-if-smu-1)#power environment temperature 68 -5 80 -20
  This command is invalid unless in the contition of install the sensor, would
you continue? (y/n)[n]:y
huawei(config-if-smu-1)#power environment humidity 80 0 100 0
  This command is invalid unless in the contition of install the sensor, would
you continue? (y/n)[n]:y
huawei(config-if-smu-1)#power module-num 3 1 2 3

huawei(config-if-smu-1)#display power system parameter
huawei(config-if-smu-1)#display power environment parameter
huawei(config-if-smu-1)#display power alarm
huawei(config-if-smu-1)#quit
huawei(config)#save
```

19.12.5 Fan Tray Monitoring Solution

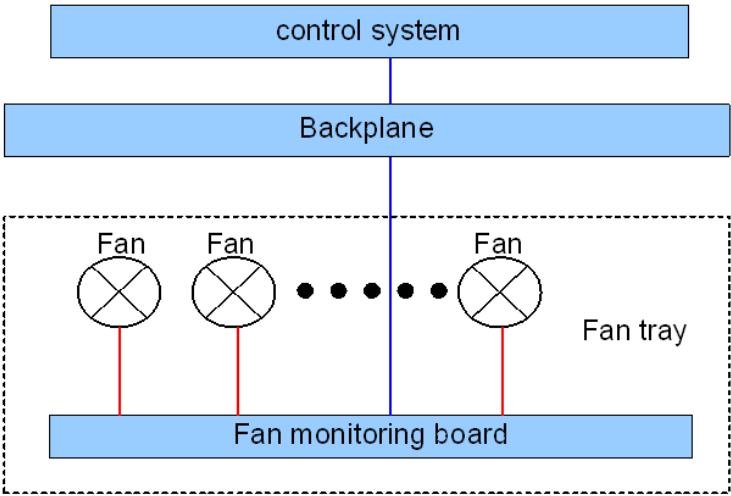
Fans are monitored through the fan monitoring board that reports the fan status to the control system.

19.12.5.1 Fan Tray Monitoring Principles

This topic describes the principles of monitoring the fan tray through the fan monitoring board.

Figure 19-61 shows the fan tray monitoring principles.

Figure 19-61 Fan tray monitoring principles



NOTE

- The fans connect to the fan monitoring board through the signal cable. The fan monitoring board monitors the working status of the fans.
- The fan tray is connected to the backplane of the shelf through cables directly or indirectly.
- The fan monitoring board reports the collected status to the control system through the backplane.

19.12.5.2 MA5800-X17 Fan Tray

The fan tray of the MA5800-X17 service subrack has eight fans and fan monitoring board FMLA, and functions heat dissipation, monitoring, and fan speed adjustment, which ensures that the device works at a stable temperature.



Specification

Item	Specification
BOM number	02122392
Dimensions (W x D x H)	503 mm x 284 mm x 76 mm
Weight	4.40 kg (Fan tray)

Item	Specification
Power consumption NOTE The power consumption of the fan board is measured under the following conditions: • Static power consumption: power consumption when the fan speed is 0. • Maximum power consumption: power consumption of the fan board and fan assembly when the fan speed is 100%.	• Static: 20 W • Maximum: 139 W

Function

The functions of the fan tray are as follows:

- **Heat dissipation**
The fan tray is at the top of the service subrack and exhausts hot air for heat dissipation. The cool air flows to the subrack from the bottom of the subrack and then is exhausted from the top of the subrack after passing the boards.
- **Monitoring**
The fan tray is configured with the fan monitoring board to detect whether the fans are working in the normal state. The fan monitoring board also provides the port for communication with the control board. The detected information is transmitted to the control board through the fan monitoring board periodically.
- **Speed adjustment**
The rotating speed of the fans can be adjusted according to the detected temperature automatically or be adjusted by setting the related data manually.

Indicator

Indicator	Color	Status	Meaning	Operation Description
STATUS	Yellow	Blinking quickly (on for 0.125 s and off for 0.125 s repeatedly)	The fan tray is not registered , is being loaded, or fails to communicate with the control board.	• If the fan tray is not registered or is being loaded, no action is required. • If the fan tray fails to communicate with the control board, check the communication connection between the fan tray and the control board.
	Green	Blinking	The fan tray works in the normal state.	No action is required.
	Yellow	Blinking slowly (on for 1 s and off for 1 s repeatedly)	The fan tray generates alarms that do not affect services.	Handle it based on the corresponding alarm.
	Red	Blinking	The fan tray is faulty or the fan tray generates an over-temperature alarm.	• Replace the faulty fan tray. • Increase the fan speed to lower the temperature.

Fan Speed Adjustment

Set the fan speed adjustment mode to "automatic" or "manual" in the command line interface (CLI). After the fans are installed, they work in automatic mode by default.

- Automatic mode
 - Control-system-triggering: The control system automatically adjusts the fan speed according to the board temperatures for energy conservation.

- Monitoring-board-triggering: The control system adjusts the fan speed according to the temperature information collected by the monitoring board.

 NOTE

The automatic mode has two variants (automatically selected by the system): control-system-triggering and monitoring-board-triggering.

- Manual mode
Commands are executed to adjust the fan speed. The levels range from 0 to 6, level 0 being the lowest speed and level 6 being the highest speed.
Alternatively, the fan speed can be set from 20% to 100%.

19.12.5.3 MA5800-X15 Fan Tray

The fan tray of the MA5800-X15 service subrack has six fans or eight fans and fan monitoring board FMLA, and functions heat dissipation, monitoring, and fan speed adjustment, which ensures that the device works at a stable temperature.

Figure 19-62 Appearance



Specification

Item	Specification
BOM number	02122393 (Configured with 6 fans) 02122797 (Configured with 8 fans)
Dimensions (W x D x H)	448 mm x 284 mm x 76 mm
Weight	About 4.85kg (Configured with 6 fans) About 4.84kg (Configured with 8 fans)

Item	Specification
Power consumption NOTE The power consumption of the fan board is measured under the following conditions: • Static power consumption: power consumption when the fan speed is 0. • Maximum power consumption: power consumption of the fan board and fan assembly when the fan speed is 100%.	Configured with 6 fans: • Static: 18W • Maximum: 225W Configured with 8 fans: • Static: 28W • Maximum: 354W

Function

The functions of the fan tray are as follows:

- **Heat dissipation**
The fan tray is at the top of the service subrack and exhausts hot air for heat dissipation. The cool air flows to the subrack from the bottom of the subrack and then is exhausted from the top of the subrack after passing the boards.
- **Monitoring**
The fan tray is configured with the fan monitoring board to detect whether the fans are working in the normal state. The fan monitoring board also provides the port for communication with the control board. The detected information is transmitted to the control board through the fan monitoring board periodically.
- **Speed adjustment**
The rotating speed of the fans can be adjusted according to the detected temperature automatically or be adjusted by setting the related data manually.

Indicator

Indicator	Color	Status	Meaning	Operation Description
STATUS	Yellow	Blinking quickly (on for 0.125 s and off for 0.125 s repeatedly)	The fan tray is not registered , is being loaded, or fails to communicate with the control board.	• If the fan tray is not registered or is being loaded, no action is required. • If the fan tray fails to communicate with the control board, check the communication connection between the fan tray and the control board.
	Green	Blinking	The fan tray works in the normal state.	No action is required.
	Yellow	Blinking slowly (on for 1 s and off for 1 s repeatedly)	The fan tray generates alarms that do not affect services.	Handle it based on the corresponding alarm.
	Red	Blinking	The fan tray is faulty or the fan tray generates an over-temperature alarm.	• Replace the faulty fan tray. • Increase the fan speed to lower the temperature.

Fan Speed Adjustment

Set the fan speed adjustment mode to "automatic" or "manual" in the command line interface (CLI). After the fans are installed, they work in automatic mode by default.

- Automatic mode
 - Control-system-triggering: The control system automatically adjusts the fan speed according to the board temperatures for energy conservation.

- Monitoring-board-triggering: The control system adjusts the fan speed according to the temperature information collected by the monitoring board.

 NOTE

The automatic mode has two variants (automatically selected by the system): control-system-triggering and monitoring-board-triggering.

- Manual mode
Commands are executed to adjust the fan speed. The levels range from 0 to 6, level 0 being the lowest speed and level 6 being the highest speed.
Alternatively, the fan speed can be set from 30% to 100%.

19.12.5.4 MA5800-X7 Fan Tray

The fan tray of the MA5800-X7 service subrack has 6 fans and a fan monitoring board FMMA and supports heat dissipation, monitoring, and fan speed adjustment to ensure that the device works at a proper temperature.



Specification

Item	Specification
BOM number	02122461
Dimensions (H x W x D)	43.6 mm x 257.5 mm x 260.4 mm
Weight	2.00 kg (Fan tray)

Item	Specification
Power consumption NOTE The power consumption of the fan board is measured under the following conditions: • Static power consumption: power consumption when the fan speed is 0. • Maximum power consumption: power consumption of the fan board and fan assembly when the fan speed is 100%.	• Static: 14 W • Maximum: 189 W

Function

The functions of the fan tray are as follows:

- **Heat dissipation**
The fan tray is on the right side of the service subrack to exhaust hot air. The air flow is from left to right.
- **Monitoring**
The fan monitoring board detects whether the fans are working in a normal state and sends the results to the control board periodically.
- **Speed adjustment**
The rotating speed of the fans can be adjusted manually or automatically based on the detected temperature.

Indicator

Indicator	Color	Status	Meaning	Operation Description
STATUS	Yellow	Blinking quickly (on for 0.125 s and off for 0.125 s repeatedly)	The fan tray is not registered , is being loaded, or fails to communicate with the control board.	• If the fan tray is not registered or is being loaded, no action is required. • If the fan tray fails to communicate with the control board, check the communication connection between the fan tray and the control board.

Indicator	Color	Status	Meaning	Operation Description
	Green	Blinking	The fan tray works in the normal state.	No action is required.
	Yellow	Blinking slowly (on for 1 s and off for 1 s repeatedly)	The fan tray generates alarms that do not affect services.	Handle it based on the corresponding alarm.
	Red	Blinking	The fan tray is faulty or the fan tray generates an over-temperature alarm.	• Replace the faulty fan tray. • Increase the fan speed to lower the temperature.

Fan Speed Adjustment

The fan speed adjustment mode can be set to "automatic" or "manual" in the command line interface (CLI). The default mode is "automatic".

 NOTE

The fan tray is used for heat dissipation of the system so that the device can work at a normal temperature. When the ambient temperature exceeds the upper limit, the system automatically reports a high temperature alarm.

- Automatic mode
 - Based on the control system: The control system automatically adjusts the fan speed according to the board temperatures for energy conservation.
 - Based on the monitoring board: The control system adjusts the fan speed based on the temperature information collected by the monitoring board.

 NOTE

When the automatic speed adjustment mode is used, the device automatically switches between adjustment based on the control system and the adjustment based on the monitoring board.

- Manual mode

You can also manually adjust the fan speed to a level between level 0 (the lowest speed) and level 6 (the highest speed) or a percentage between 20% and 100% using commands.

19.12.5.5 MA5800-X2 Fan Tray

The fan tray of the MA5800-X2 service subrack has 2 fans and a fan monitoring board (FMSA) and supports heat dissipation, monitoring, and fan speed adjustment to ensure that the device works at a proper temperature.



Specification

Item	Specification
Dimensions (H x W x D)	43.6 mm x 286.7 mm x 88.1 mm
Weight	0.70 kg (Fan tray)
Power consumption NOTE The power consumption of the fan board is measured under the following conditions: • Static power consumption: power consumption when the fan speed is 0. • Maximum power consumption: power consumption of the fan board and fan assembly when the fan speed is 100%.	• Static: 6 W • Maximum: 63 W

Function

The functions of the fan tray are as follows:

- **Heat dissipation**
The fan tray is on the right side of the service subrack to exhaust hot air. The air flow is from left to right.
- **Monitoring**
The fan monitoring board detects whether the fans are working in a normal state and sends the results to the control board periodically.
- **Speed adjustment**

The rotating speed of the fans can be adjusted manually or automatically based on the detected temperature.

Indicator

Indicator	Color	Status	Meaning	Operation Description
STATUS	Yellow	Blinking quickly (on for 0.125 s and off for 0.125 s repeatedly)	The fan tray is not registered , is being loaded, or fails to communicate with the control board.	• If the fan tray is not registered or is being loaded, no action is required. • If the fan tray fails to communicate with the control board, check the communication connection between the fan tray and the control board.
	Green	Blinking	The fan tray works in the normal state.	No action is required.
	Yellow	Blinking slowly (on for 1 s and off for 1 s repeatedly)	The fan tray generates alarms that do not affect services.	Handle it based on the corresponding alarm.
	Red	Blinking	The fan tray is faulty or the fan tray generates an over-temperature alarm.	• Replace the faulty fan tray. • Increase the fan speed to lower the temperature.

Fan Speed Adjustment

The fan speed adjustment mode can be set to "automatic" or "manual" in the command line interface (CLI). The default mode is "automatic".

- Automatic mode

- Based on the control system: The control system automatically adjusts the fan speed according to the board temperatures for energy conservation.
- Based on the monitoring board: The control system adjusts the fan speed based on the temperature information collected by the monitoring board.
- Manual mode
You can also manually adjust the fan speed to a level between level 0 (the lowest speed) and level 6 (the highest speed) or a percentage between 20% and 100% using commands.

19.12.5.6 Commissioning the Fan EMU

This topic describes how to commission the fan EMU to ensure that it monitors the environmental conditions of the fans of the device according to the actual conditions.

Context

NOTE

When the device is delivered, the fan EMU is correctly connected to the shelf. The connection need not be changed for the device commissioning. In certain cases, if the EMU needs to be configured in other shelves, reconnect the EMU. For details, see this topic.

The fan EMU is used to monitor the running status of the fans and to set the fan rotation speed according to actual conditions to ensure the normal heat dissipation of the device.

When commissioning the fan EMU, pay attention to the following points:

- The EMU sub-nodes are numbered from 0 to 31.
- When the system is configured with multiple EMUs simultaneously, make sure that the sub-nodes do not conflict with each other.
- It is recommended that you use the **auto** mode as the fan speed adjustment mode.

Table 19-59 lists the default configuration of the fan EMU.

Table 19-59 Default configuration of the fan EMU

Parameter	Default Value
Sub-node	1
Fan speed adjustment mode	Automatic
Whether to report the fan alarm	Permit

Procedure

- Step 1** Set the DIP switches of the sub-nodes for the fan EMU. By default, the sub-node ID is 1.

 NOTE

The fan EMU communicates with the MA5800 in the master node and sub-node mode. Therefore, the DIP switches of the sub-nodes for the fan EMU must be consistent with those for the MA5800.

- Step 2** Insert the fan tray into the corresponding slot of the service shelf.

- Step 3** Run the **emu add** command to add a fan EMU. By default, the sub-node ID is 1.

- Step 4** Run the **interface emu** command to enter the FAN mode.

- Step 5** Run the **fan speed mode auto** or **fan speed mode manual** command to set the fan speed adjustment mode. By default, the fan speed adjustment mode is automatic.

 NOTE

When the fan speed adjustment mode is the manual mode, you can run the **fan speed mode manual** command to set the fan speed. The speed level can be 0, 1, 2, 3, 4, 5 or 6. Here, 6 stands for the highest speed, and 0 stands for the lowest speed.

- Step 6** Run the **fan alarmset** command to configure the fan alarm reporting function. The fan alarms are read temperature failure alarm, fan block alarm, over temperature alarm, and power fault alarm. By default, the fan alarm reporting is permitted.

- Step 7** Run the **save** command to save the data.

----End

Result

- In the FAN mode, run the **display fan system parameter** command to query the parameter configuration of the fan tray and ensure that the configuration is the same as the data plan.
- In the FAN mode, run the **display fan environment info** command to query the running status of the fan tray and ensure that it is the same as the data plan.
- In the FAN mode, run the **display fan alarm** command to query the alarm information reported by the fan tray. The status of all the fan alarms is normal.

Example

To add a fan EMU, and adopt the default settings for the speed adjustment mode and alarm function, do as follows:

```
huawei(config)#emu add 0 FAN 0 1 FAN
huawei(config)#interface emu 0
huawei(config-if-fan-0)#display fan system parameter
```

```
EMU ID: 0
FAN configuration parameter:
-----
FAN timing mode: Auto timing by temperature
-----
Alarm_name          Permit/Forbid
Read temperature fault      Permit
Fan block             Permit
Temperature high         Permit
Power fault            Permit
-----
```

19.13 RTU

Definition

Right to Use (RTU) is a part of hardware and is used to authorize the use of hardware capabilities in phases, such as ports, bandwidth and optical power. RTU is a license for the use of hardware resources and has the same lifecycle as hardware.

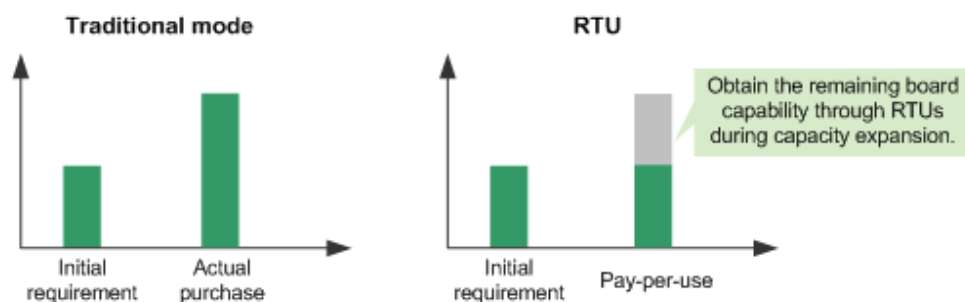
Carrier

To provision services using RTUs, the following requirements must be met:

1. Hardware: service subracks, boards , and optical modules that support RTUs.
2. Software: software version that supports the RTU, including the host version and NMS version.
3. RTU authorization certificate: type and number of RTUs that have been applied for.

Benefits

- Reduced initial investment: The RTU provides customers with a method of purchasing hardware capabilities in installments, which can significantly reduce initial investment and quickly achieve balance between income and expenditure.



- Reduced OPEX: Services can be provisioned by remotely loading RTUs. Therefore, customers do not need to install boards onsite to achieve capacity expansion.

Traditional mode



Install boards onsite for capacity expansion.

RTU



Remotely load RTUs for capacity expansion.

RTU Type

Table 19-60 RTU types supported by access products

RTU Type	Function
Port RTU	Controls the number of available ports based on port access modes, including GPON, 10G PON, and so on.
Optical power RTU	Controls the number of ports whose working mode is enhanced based on the optical module type, such as GPON Class C+ Pro and 10G PON Class C+ Pro optical modules.
Bandwidth capability RTU	Controls the number of ports with specific access bandwidth capabilities, such as 10G PON initial bandwidth, 2.5G upstream bandwidth, and 2.5G downstream bandwidth capability, based on XGS PON/XGS combo PON physical ports.

For more information, see the following:

- Carrier users: [Access Network Product RTU](#).
- Enterprise users: [Access Network Product RTU](#).