

2 GPON

Gigabit passive optical network (GPON) is a PON technology that is standardized by the ITU-T Recommendations G.984.x. A GPON device supports high-bandwidth transmission. GPON effectively solves the bandwidth bottleneck problem in the twisted-pair access and meets users demands on high-bandwidth services.

[2.1 Introduction to GPON](#)

[2.2 GPON Working Principle](#)

[2.3 GPON System Principle](#)

[2.4 Key GPON Techniques](#)

[2.5 GPON Terminal Authentication and Management](#)

[2.6 Continuous-Mode ONU Detection](#)

This function is used to detect the continuous-mode ONU of terminal devices such as the MDU and ONT.

[2.7 Remote Software Commissioning \(PON\)](#)

[2.8 GPON Configuration Guide \(Profile mode\)](#)

GPON configurations include the configurations on GPON profiles, ONTs, and ports. The following section describes configuration methods.

[2.9 GPON Configuration Guide \(Distributed mode\)](#)

GPON configurations include the configurations on GPON profiles, ONTs, and ports. The following section describes configuration methods.

[2.10 GPON Reference Standards and Protocols](#)

2.1 Introduction to GPON

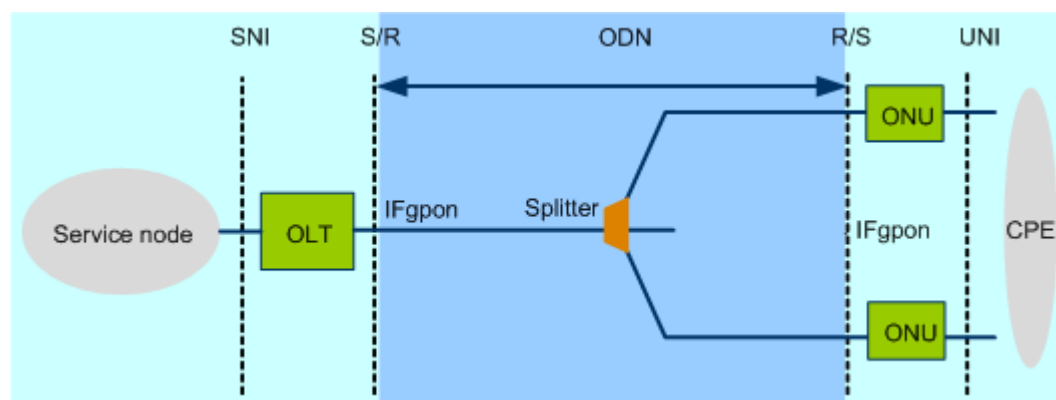
What Is GPON

Passive Optical Network (PON) is a point to multi-point (P2MP) passive optical network.

Gigabit passive optical network (GPON) is a PON technology that is standardized by the ITU-T Recommendations G.984.x.

Figure 2-1 shows a GPON network architecture.

Figure 2-1 GPON network architecture



IFgpon: GPON interface

SNI: Service Node Interface

UNI: User to Network Interface

CPE: Customer Premises Equipment

S/R: Optical line termination interface to optical trunk line

R/S: Optical network unit interface to optical distribution network

- The optical line terminal (OLT) is an aggregation device located at the central office (CO) for terminating the PON protocol.
- Optical network units (ONUs)/Optical network terminal (ONTs) are located on the user side, providing various ports for connecting to user terminals. The OLT and ONUs communicate with each other through the optical distribution network (ODN).
- The optical distribution network (ODN) is composed of passive optical components (POS), such as optical fibers, and one or more passive optical splitters. The ODN provides optical channels between the OLT and ONUs. It interconnects the OLT and ONUs and is highly reliable.

NOTE

The ODN network is passive, indicating that no optical amplifier or regenerator is deployed on the ODN network, thereby reducing maintenance costs of outdoor devices.

Why Is GPON Required

As the wide use of broadband services and fiber-in and copper-out development, carriers require a longer transmission reach, higher bandwidth, reliability, and lower operating expense (OPEX) on services. GPON supports the following functions to meet these requirements:

- Longer transmission distance: The transmission media of optical fibers covers up to 60 km coverage radius on the access layer, resolving transmission distance and bandwidth issues in twisted pair transmission.

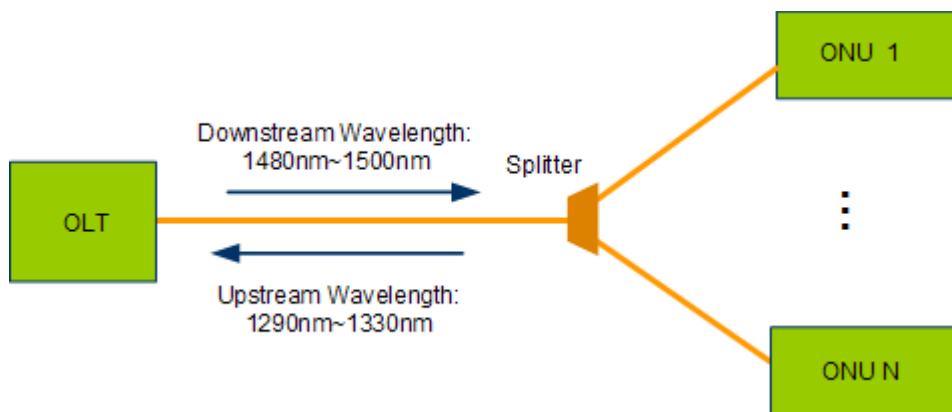
- Higher bandwidth: Each GPON port can support a maximum transmission rate of 2.5 Gbit/s in the downstream direction and 1.25 Gbit/s in the upstream direction, meeting the usage requirements of high-bandwidth services, such as high definition television (HDTV) and outside broadcast (OB).
- Flexible user experience on full services: Flexible QoS measures support traffic control based on users and user services, implementing differentiated service provisioning for different users.
- Optical splitting: A single optical fiber at the CO is split into multiple drop fibers, saving feeder optical fiber resources and reducing O&M costs.

2.2 GPON Working Principle

System Transmission Principle

Figure 2-2 shows the system transmission principle of the GPON network.

Figure 2-2 GPON System Transmission Principle

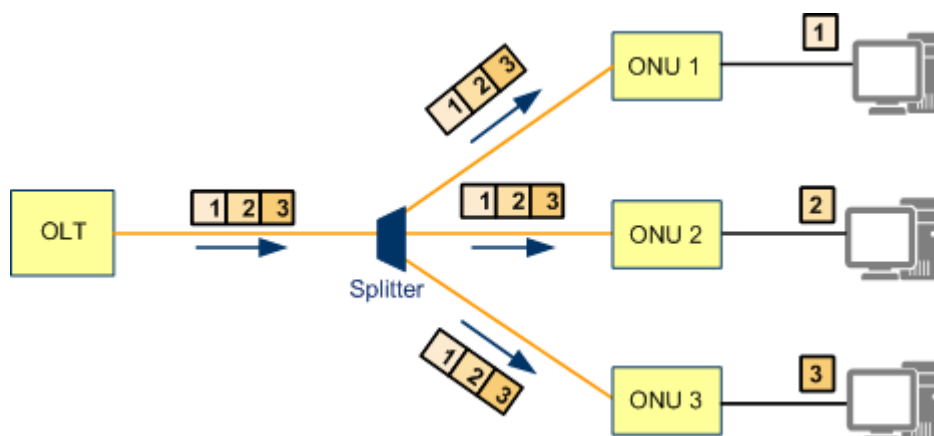


- In the GPON network, the OLT is connected to the optical splitter through a single optical fiber, and the optical splitter is then connected to ONUs. Different wavelengths are adopted in the upstream and downstream directions for transmitting data. Specifically, wavelengths range from 1290 nm to 1330 nm in the upstream direction and from 1480 nm to 1500 nm in the downstream direction.
- The GPON adopts WDM to transmit data of different upstream/downstream wavelengths over the same ODN. Data is broadcast in the downstream direction and transmitted in the TDMA mode (based on timeslots) in the upstream direction.

GPON Downstream Transmission Principle

All data is broadcast to all ONUs from the OLT. The ONUs then select and receive their respective data and discard the other data. **Figure 2-3** shows the details.

Figure 2-3 Downstream communication principle of GPON



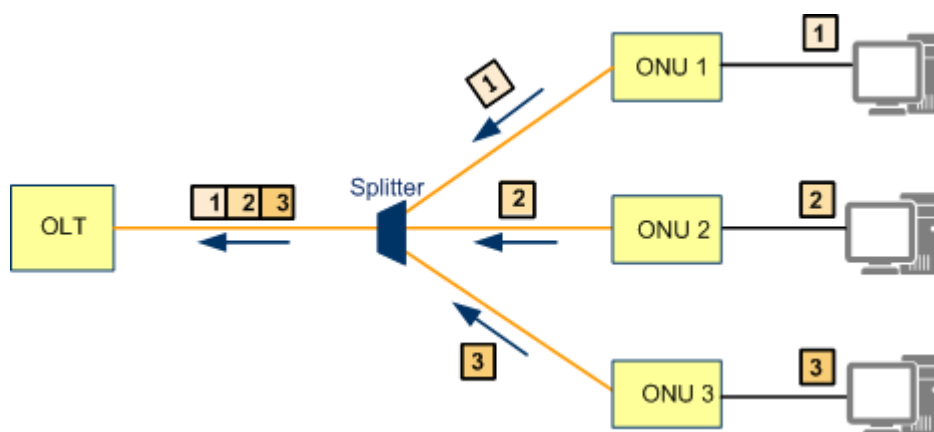
Main features:

- Supports point-to-multipoint (P2MP) multicast transmission.
- Broadcasts the same data to all ONUs and differentiates ONU data by GEM port ID.
- Allows an ONU to receive data packets intended for it and discards those not intended for it.

GPON Upstream Transmission Principle

In the upstream direction, each ONU can send data to the OLT only in the timeslot permitted and allocated by the OLT. This ensures that each ONU sends data in a given sequence, avoiding upstream data conflicts. [Figure 2-4](#) shows the details.

Figure 2-4 Upstream communication principle of GPON



Main features:

- Supports time division multiple access (TDMA).
- Transmits data on an exclusive timeslot.

- Couples optical signals on an optical splitter.
- Detects and prevents collisions through ranging.

2.3 GPON System Principle

2.3.1 GPON Basic Concepts

GEM Frame

In the gigabit-capable passive optical network (GPON) system, a GPON encapsulation mode (GEM) frame is the smallest service-carrying unit and the basic encapsulation structure. All services need to be encapsulated in GEM frames and transmitted on GPON lines, which are identified by GEM ports.

- Each GEM port is identified by a unique port ID. The port ID is globally allocated by the OLT. Therefore, the ONUs connected to the same OLT GPON port cannot use GEM ports that have the same port ID.
- A GEM port is used to identify the virtual service channel that carries the service stream between the OLT and the ONU. It is similar to the virtual path identifier (VPI)/virtual channel identifier (VCI) of the asynchronous transfer mode (ATM) virtual connection.

[Figure 2-5](#) shows the GEM frame structure.

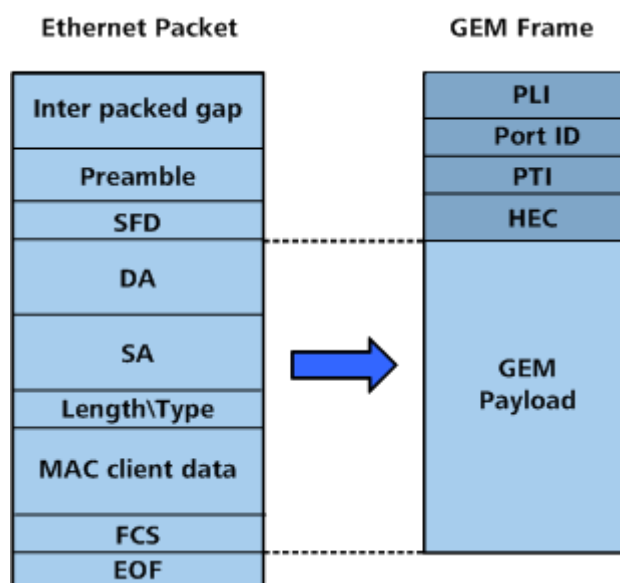
Figure 2-5 GEM frame structure

PLI 12-Bits	Port ID 12-Bits	PTI 3-Bits	HEC 13-Bits	Fragment Payload L Bytes
----------------	--------------------	---------------	----------------	-----------------------------

A GEM header consists of PLI, Port ID, PTI, and header error check (HEC) and is used for differentiating data of different GEM ports. The fields are described as follows:

- PLI: indicates the length of data payload.
- Port ID: uniquely identifies a GEM port.
- PTI: indicates the payload type. It is used for identifying the status and type of data that is being transmitted, for example, whether the operation, administration and maintenance (OAM) message is being transmitted and whether data transmission is complete.
- HEC: ensures the forward error correction (FEC) function and transmission quality.
- Fragment payload: indicates the data frame fragment.

The following section describes the GEM frame structure based on the mapping of the Ethernet service in GPON mode, as shown in [Figure 2-6](#).

Figure 2-6 GEM frame structure

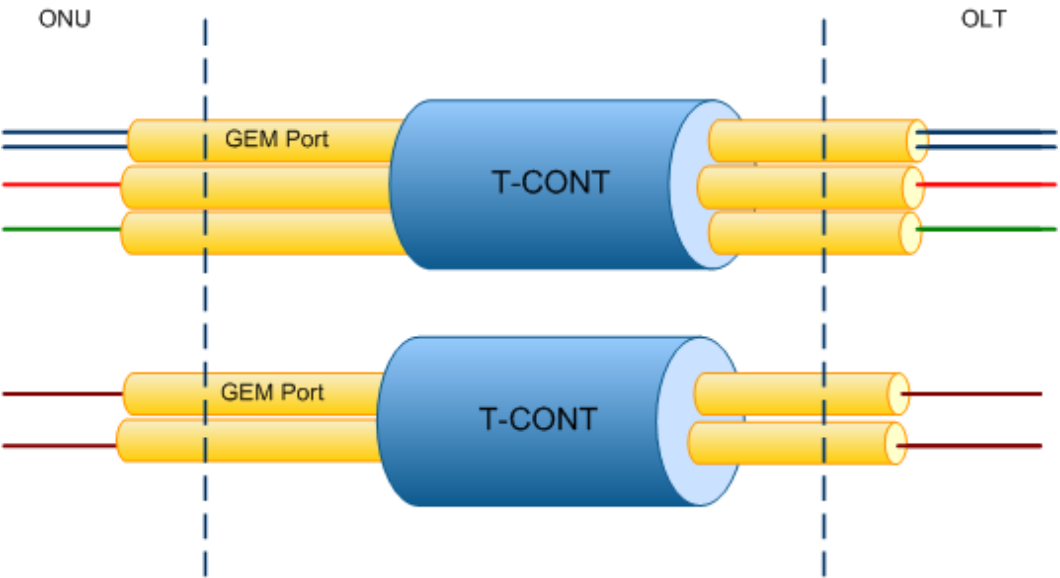
- The GPON system parses Ethernet frames and maps data into GEM payloads for transmission.
- Header information is automatically encapsulated into GEM frames.
- The mapping format is clear and has good compatibility.

T-CONT

Transmission container (T-CONT) is a service carrier in the upstream direction in the GPON system. All GEM ports are mapped to T-CONTs. Then service streams are transmitted upstream by means of OLT's dynamic bandwidth assignment (DBA) scheduling. T-CONT is the basis of DBA implementation. An ONU applies for bandwidth using T-CONTs, and the OLT grants bandwidth through T-CONTs, thereby realizing the upstream DBA in the entire GPON system.

T-CONT is the basic control unit of the upstream service stream in the GPON system. Each T-CONT is identified by Alloc-ID. The Alloc-ID is allocated by the GPON port of the OLT, and the T-CONTs used by ONUs connected to the same GPON port of OLT cannot have the same Alloc-IDs.

Figure 2-7 T-CONT structure



There are five types of T-CONT. T-CONT selection varies during the scheduling of different types of upstream service streams. Each T-CONT bandwidth type has its own quality of service (QoS) feature. QoS is mainly represented by the bandwidth guarantee, which can be classified into fixed, assured, non-assured, best-effort, and hybrid modes (corresponding to type 1 to type 5 listed in [Table 2-1](#)).

NOTE

In [Table 2-1](#), X indicates the fixed bandwidth value, Y indicates the assured bandwidth value, Z indicates the maximum bandwidth value, and No indicates not involved.

Table 2-1 T-CONT types

Bandwidth Type	T-CONT Type				
	Type1	Type2	Type3	Type4	Type5
Fixed Bandwidth	X	-	-	-	X
Assured Bandwidth	-	Y	Y	-	Y
Maximum Bandwidth	Z=X	Z=Y	Z>Y	Z	Z≥ X + Y

Bandwidth Type	T-CONT Type				
	Type1	Type2	Type3	Type4	Type5
Description	- The fixed bandwidth is reserved for specific ONUs or specific services on ONUs. It cannot be used by other ONUs even if no upstream service streams are carried on the specific ONUs. - It applies to services that are sensitive to service quality. The services can be TDM or VoIP services.	- The assured bandwidth is available at any time required by an ONU. When the bandwidth required by the service streams on the ONU is smaller than the assured bandwidth, the system can use the DBA mechanism to allocate the remaining bandwidth to services on other ONUs. - Because DBA is required, this type	Type3 is the combination of the assured bandwidth and maximum bandwidth. The system assures some bandwidth for subscribers and allows subscribers to preempt bandwidth. However, the total used bandwidth cannot exceed the maximum configured bandwidth. - It applies to VoIP services.	- This type is the maximum bandwidth that can be used by an ONU, fully providing the bandwidth required by the ONU. - It applies to IPTV and other high-speed Internet services.	Type5 is the combination of the fixed, assured, and maximum bandwidth. It supports the following functions: Reserves bandwidth for subscribers and the bandwidth cannot be preempted by other subscribers. Provides the bandwidth to an ONU at any time when required. Allows subscribers to preempt some bandwidth. (The total used bandwidth cannot exceed the maximum configured bandwidth.)

Bandwidth Type	T-CONT Type				
	Type1	Type2	Type3	Type4	Type5
		provide s a less real-time performance compared with the fixed bandwidth.			

2.3.2 GPON Service Multiplexing

GPON encapsulation mode (GEM) ports and transmission containers (T-CONTs) divide a PON network into virtual connections for service multiplexing.

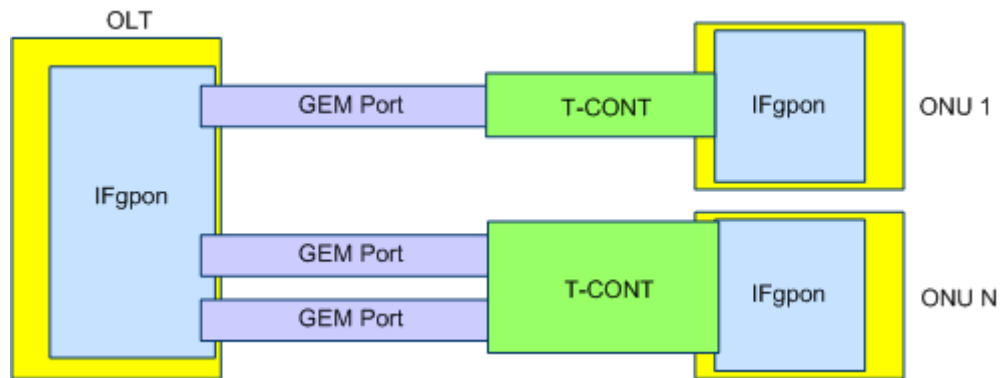
- Each GEM port can carry one or more types of service stream. After carrying service streams, a GEM port must be mapped to a T-CONT before upstream service scheduling. Each ONU supports multiple T-CONTs that can have different service types.
- A T-CONT can be bound to one or more GEM ports, depending on customers' data plan. On the OLT, GEM ports are demodulated from the T-CONT and then service streams are demodulated from the GEM port payload for further processing.

Service Mapping Relationships

- In the upstream direction,
 - An ONU sends Ethernet frames to GEM ports based on configured mapping rules between service ports and GEM ports. Then, the GEM ports encapsulate the Ethernet frames into GEM packet data units (PDUs) and add these GEM PDUs to T-CONT queues based on mapping rules between GEM ports and T-CONT queues. Then, the T-CONT queues use timeslots for upstream transmission to send GEM PDUs to the OLT.
 - The OLT receives the GEM PDUs and obtains Ethernet frames from them. Then, the OLT sends Ethernet frames from a specified uplink port based on mapping rules between service ports and uplink ports.

Figure 2-8 shows GPON service mapping relationships in the upstream direction.

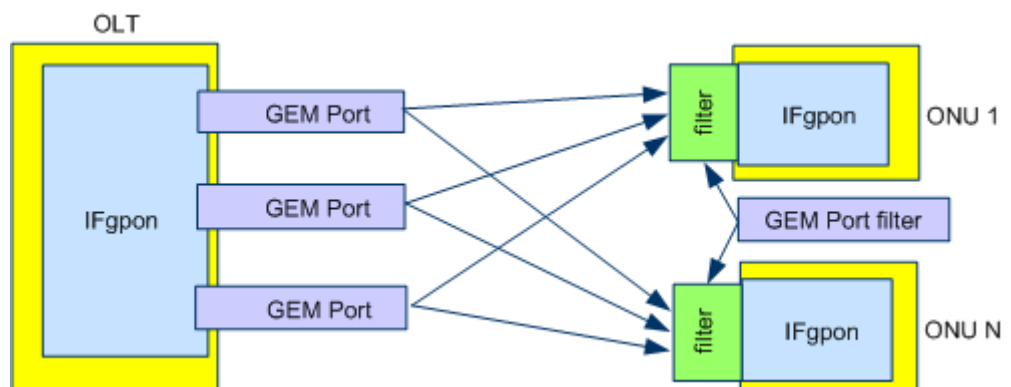
Figure 2-8 GPON service mapping relationships in the upstream direction



- In the downstream direction,
 - The OLT sends Ethernet frames to the GPON service processing module based on configured mapping rules between service ports and uplink ports. The GPON service processing module then encapsulates the Ethernet frames into GEM PDUs for downstream transmission using a GPON port.
 - GPON transmission convergence (GTC) frames containing GEM PDUs are broadcast to all ONUs connected to the GPON port.
 - The ONU filters the received data according to the GEM port ID contained in the GEM PDU header and retains the data only belonging to the GEM ports of this ONU. Then, the ONU decapsulates the data to Ethernet frames and sends them to end users using service ports.

Figure 2-9 shows GPON service mapping relationships in the downstream direction.

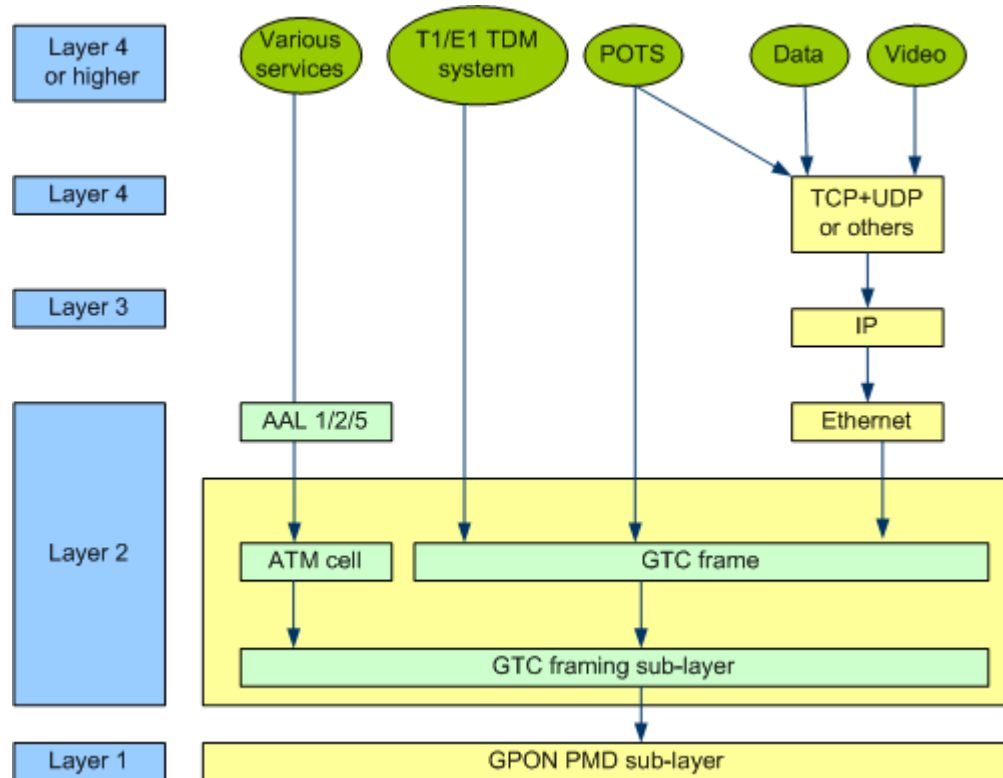
Figure 2-9 GPON service mapping relationships in the downstream direction



2.3.3 GPON Protocol Stacks

ITU-T Recommendation G.984.3 defines a new set of frame structures, which consider traditional voice, video, and Ethernet packets as payloads of GPON frames. **Figure 2-10** shows the structure of GPON protocol stacks.

Figure 2-10 Structure of GPON protocol stacks



GPON protocol stacks involve the physical medium dependent (PMD) layer and GPON transmission convergence (GTC) layer.

PMD Layer

The GPON PMD layer corresponds to the GPON interfaces between OLTs and ONUs. Parameter values of the GPON interfaces specify the maximum reach and split ratio for a GPON system.

GTC Layer

The GTC layer is used to encapsulate payloads using ATM cells or GEM frames, and GEM frames are commonly used in GPON systems. GEM frames can carry Ethernet, POTS, E1, and T1 cells.

GTC is the core GPON layer, where media access is controlled for upstream service flows and ONUs are registered. Ethernet frame payloads are encapsulated into GEM frames and then packetized as GTC frames. These GTC frames are converted to binary codes for transmission based on interface parameters configured at the physical layer. The process is reversed on the receive end. Specifically, the receive end decapsulates the data to obtain GTC frames, GEM frames, and then payloads for data transmission.

The GTC layer is classified as TC adaptation sub-layer and GTC framing sub-layer by structure.

- The TC adaptation sub-layer involves the ATM, GEM TC, and optical network terminal management and control interface (OMCI) adapters and dynamic bandwidth assignment (DBA) control module. ATM and GEM TC adapters

identify OMCI channels by virtual path identifier (VPI)/virtual channel identifier (VCI) or GEM port ID. OMCI adapters can exchange OMCI channel data with the ATM and GEM TC adapters and send the OMCI channel data to OMCI entities. The DBA control module is a common functional module, which generates ONU reports and controls DBA allocation.

- On the GTC framing sub-layer, GTC frames include GEM blocks, PLOAM blocks, and embedded OAM blocks. The GPON framing sub-layer provides the following functions:
 - Multiplexing and demultiplexing: The PLOAM part and the GEM part are multiplexed into the downlink TC frame according to the boundary information indicated by the frame header, and the PLOAM part and the GEM part can be extracted from the uplink TC frame according to the frame header indication.
 - Frame header generation and decoding: The TC frame header of the downstream frame is generated according to the format requirements, and the frame header of the upstream frame is decoded. At the same time, the embedded OAM information directly encapsulated in the GTC frame header is terminated, and is used to directly control the sub-layer.
 - Alloc-ID-based internal routing: The data from or to the GEM TC adapter is routed according to the internal representation of the Alloc-ID.

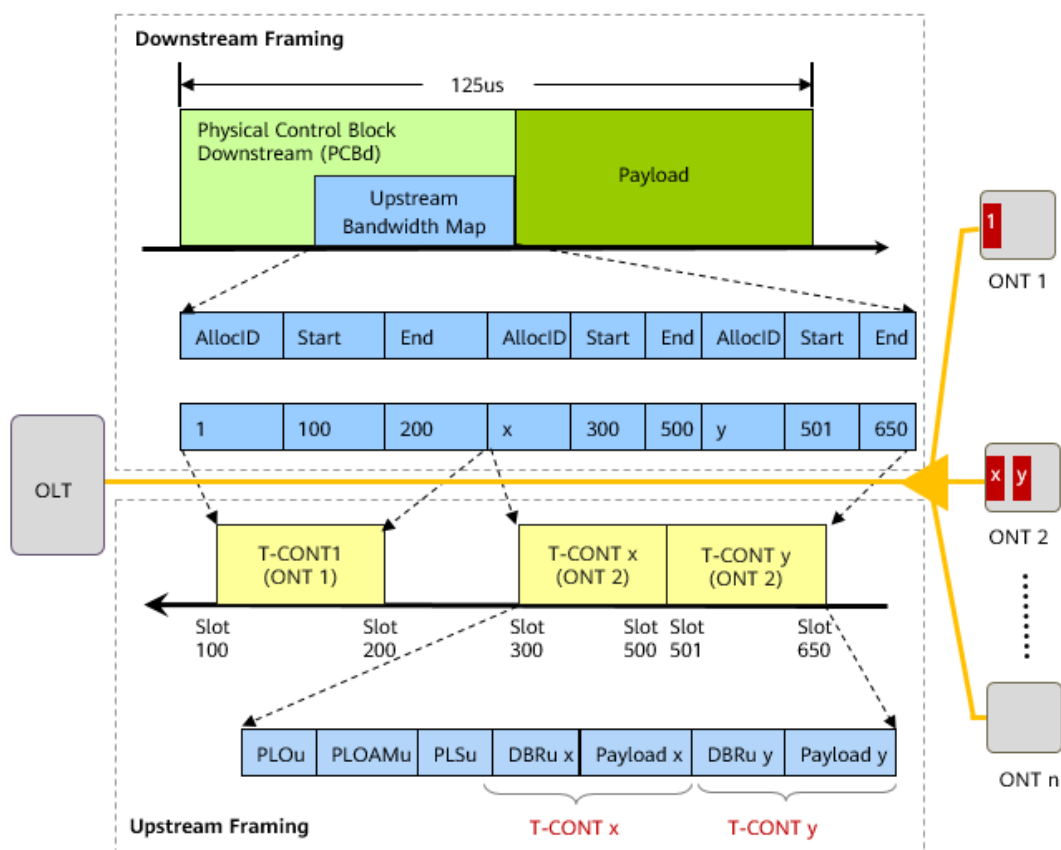
The GTC layer consists of plane C/M and plane U based on functions.

- The protocol stacks of plane C/M include embedded OAM, PLOAM, and OMCI. Embedded OAM and PLOAM channels are used for managing PMD and GTC sub-layer functions. OMCI provides a unified system for upper-layer sub-layer management.
 - Embedded OAM channels are defined in GTC frame headers for determining bandwidths, exchanging data, and dynamically allocating bandwidths.
 - Dedicated space is reserved in GTC frames for format-based PLOAM channels. The PLOAM channels carry the PMD and GTC management information that does not pass through the embedded OAM block.
 - OMCI channels are used for managing services.
- Service flows on plane U are identified based on service flow types (ATM or GEM) and port ID/VPI. Port IDs identify GEM service flows and VPIs identify ATM service flows. In T-CONTs, bandwidths are allocated and QoS is controlled using the timeslots that can be adjusted.

2.3.4 GPON Frame Structure

GPON Frame Structure

Figure 2-11 shows the GPON frame structure.

Figure 2-11 GPON frame structure

Upstream GPON Frame

An upstream GPON frame has a fixed length of 125 μ s. Each upstream frame contains the content carried by one or more T-CONTs. All ONUs connected to a GPON port share the upstream bandwidth.

- All ONUs connected to a GPON port send their data upstream at their own timeslots according to bandwidth map (BWmap) requirements.
- Each ONU reports the status of data to be sent to the OLT using upstream frames. Then, the OLT uses DBA to allocate upstream timeslots to ONUs and sends updates in each frame.

In [Figure 2-11](#), an upstream GPON frame consists of the physical layer overhead upstream (PLOu), PLOAM upstream (PLOAMu), power level sequence upstream (PLSu), dynamic bandwidth report upstream (DBRu), and payload fields, as described in [Table 2-2](#).

Table 2-2 Field description for an upstream GPON frame

Field	Description	Function
PLOu	Upstream physical layer overhead	Used for frame alignment, synchronization, and identification for an ONU.
PLOAMu	PLOAM messages of upstream data	Used for reporting ONU management messages, including maintenance and management status. This field may not be contained in a frame but must be negotiated.
PLSu	Upstream power level sequence	Used by ONUs for adjusting optical port power. This field may not be contained in a frame but must be negotiated.
DBRu	Upstream dynamic bandwidth report	Used for reporting the T-CONT status to apply for bandwidth next time and for allocating dynamic bandwidths. This field may not be contained in a frame but must be negotiated.
Payload	Payload user data	Can be a DBA status report or data frame. If this field is a data frame, this field consists of a GEM header and frames.

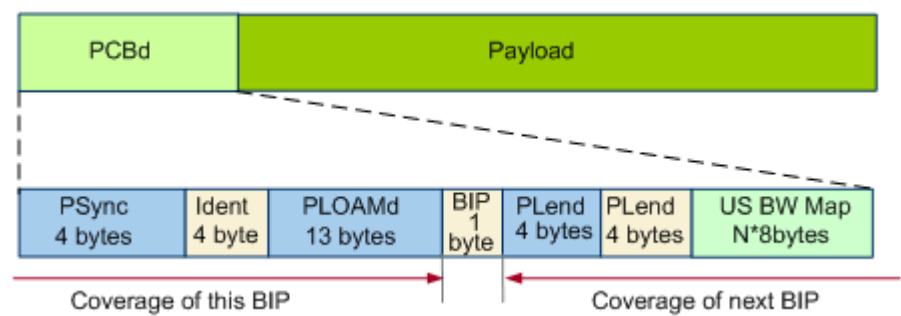
Downstream GPON Frame

A downstream GPON frame has a fixed length of 125 μ s and comprises physical control block downstream (PCBd) and payload. The OLT broadcasts PCBd to all ONUs. Then, the ONUs receive the PCBd and perform operations based on the information contained in PCBd. PCBd mainly consists of the GTC header and BWmap.

- The GTC header is used for frame delimitation, synchronization, and forward error correction (FEC).
- The BWMap field notifies every ONU of upstream bandwidth allocation. It specifies the start and end upstream timeslots for the T-CONTs of each ONU, ensuring that all ONUs send data using the timeslots specified by the OLT to prevent data conflict.

Figure 2-12 shows the structure of the PCBd shown in Figure 2-11.

Figure 2-12 PCBd structure



PCBd contains PSync, Ident, PLOAMd, BIP, PLeNd, and US BW Map fields, where US BW Map is the upstream bandwidth mapping sent by the OLT for each T-CONT. Table 2-3 describes each field.

Table 2-3 PCBd field description

Field	Description	Function
PSync	Physical synchronization domain, frame synchronization information	Used by ONUs to specify the start of each frame.
Ident	Identification domain	Used for sorting a frame in the frames of the same type in length sequence.
Downstream PLOAM (PLOAMd)	PLOAM messages of downstream data	It is used to transmit the OAM message of the physical layer to the ONU. This field may not be contained in a frame but must be negotiated.
BIP	Bit interleaved parity	Used for performing a parity check for all bytes between two BIP fields (excluding the preamble and delimit) to monitor error codes.
PLeNd	Length of downstream payloads	Used for specifying the length of the BWmap field.

Field	Description	Function
Upstream bandwidth map (US BW Map)	Upstream bandwidth mapping	Used by the OLT for sending the upstream bandwidth mapping to each T-CONT. The BWmap specifies the start and end times for each T-CONT in transmitting data. • The StartTime field contains the 16-bit number that indicates the starting time of the allocation. NOTE This time is measured in bytes, starting with zero at the beginning of the upstream GTC frame. This limits the size of the upstream GTC frame to 65536 bytes. • The StopTime field contains the 16-bit number that indicates the stopping time of the allocation. NOTE This time is measured in bytes, starting with zero at the beginning of the upstream GTC frame. The StopTime points to the last valid data byte associated with this allocation.

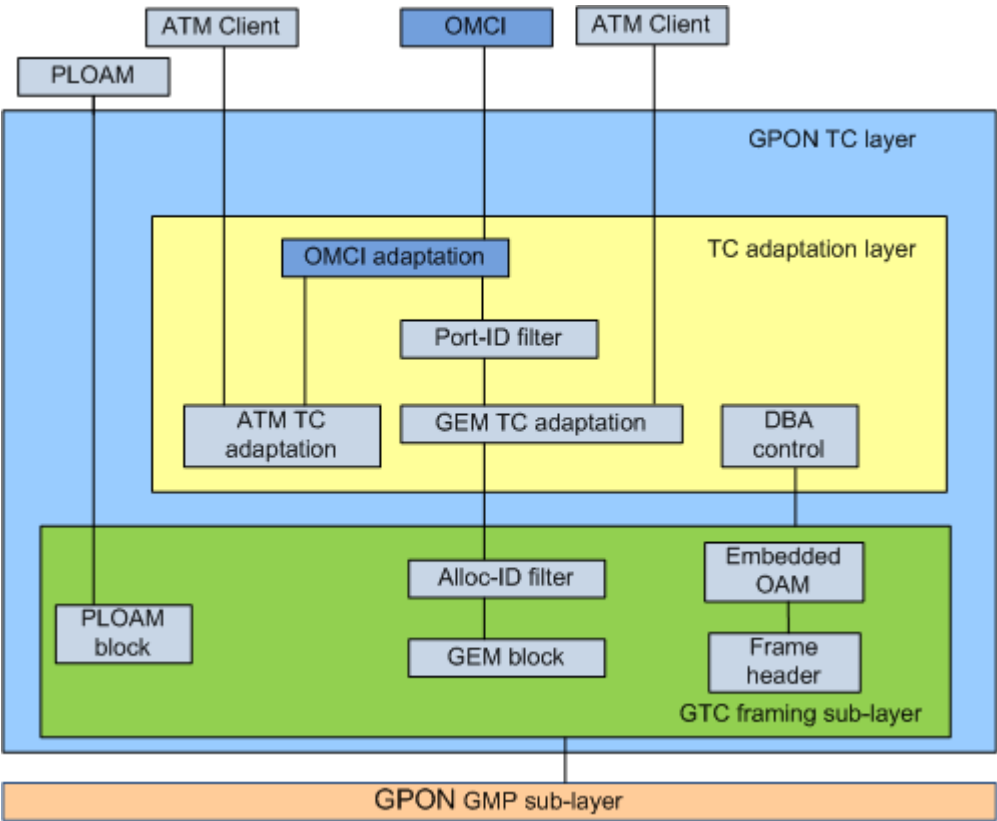
2.3.5 OMCI

Basic Concepts

OMCI is a type of ITU-T Recommendation G.984.4-compliant configuration and transmission channel, which is used to transmit OMCI messages over dedicated ATM PVCs or GEM ports established between an OLT and an ONT. The OMCI messages are used for discovering ONTs for management and control.

OMCI Position in GPON Protocol Stacks

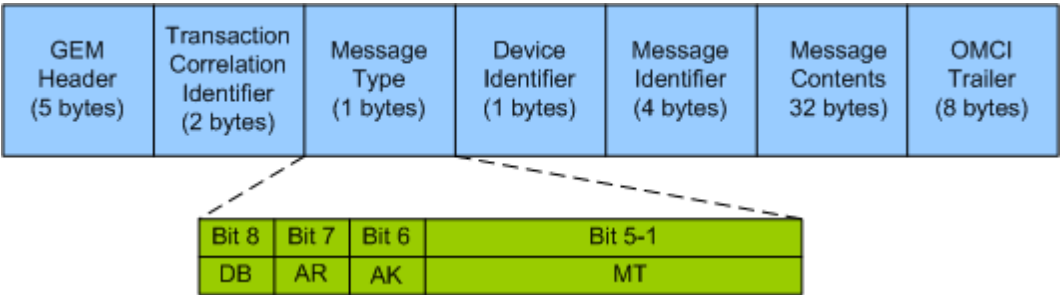
Figure 2-13 GPON Protocol Stacks



OMCI Message Format

OMCI messages are strictly limited in length and format. Specifically, the length is consistently 53 bytes and the length of the OMCI data unit is 48 bytes. For details, see [Figure 2-14](#).

Figure 2-14 OMCI message format



- GEM Header: includes GEM payload, GEM port ID, payload type indicator (PTI), and header error control (HEC).

- Transaction Correlation Identifier: The value of this field must be the same in a request and the response to this request. The highest order of this field indicates the priority of an OMCI message. Value 0 indicates a low priority and value 1 indicates a high priority.
- Message type:
 - DB: a destination bit, which is consistently 0.
 - AR: an acknowledge request, indicating whether an OMCI message requires the response from the peer end. Value 0 indicates that the response is not required and value 1 indicates that the response is required.
 - AK: acknowledgement, indicating whether an OMCI message is a response. Value 0 indicates not and value 1 indicates yes.
 - MT: message type, which supports up to 32 message types, including Create, Delete, Set, Get, and MIB upload. In the G.984.4 protocol, codes 4 to 28 are used, and other codes are reserved.
- Device identifier: The value of this field is consistently **0xA**.
- Message Identifier: a 2-byte entity or instance ID.
- Message Contents: packet payload.
- OMCI trailer: Two bytes are consistently 0, two bytes are packet length 0x28, and four bytes are CRCs.

OMCI Management

The OLT controls the ONU using the OMCI. The OMCI protocol allows the OLT to:

- Establish and release connections with the ONU.
- Manage the UNIs on the ONU.
- Request configuration information and performance statistics from the OSS.
- Autonomously inform the system administrator of events, such as link failures.

The OMCI protocol runs over a GEM connection between the OLT controller and the ONU controller. The GEM connection is established during ONU initialization. The OMCI protocol is asynchronous: the OLT controller is the master and the ONU controller is the slave. A single OLT controller using multiple protocol instances over separate control channels can control multiple ONUs.

The OLT manages an ONU using OMCI in the following aspects:

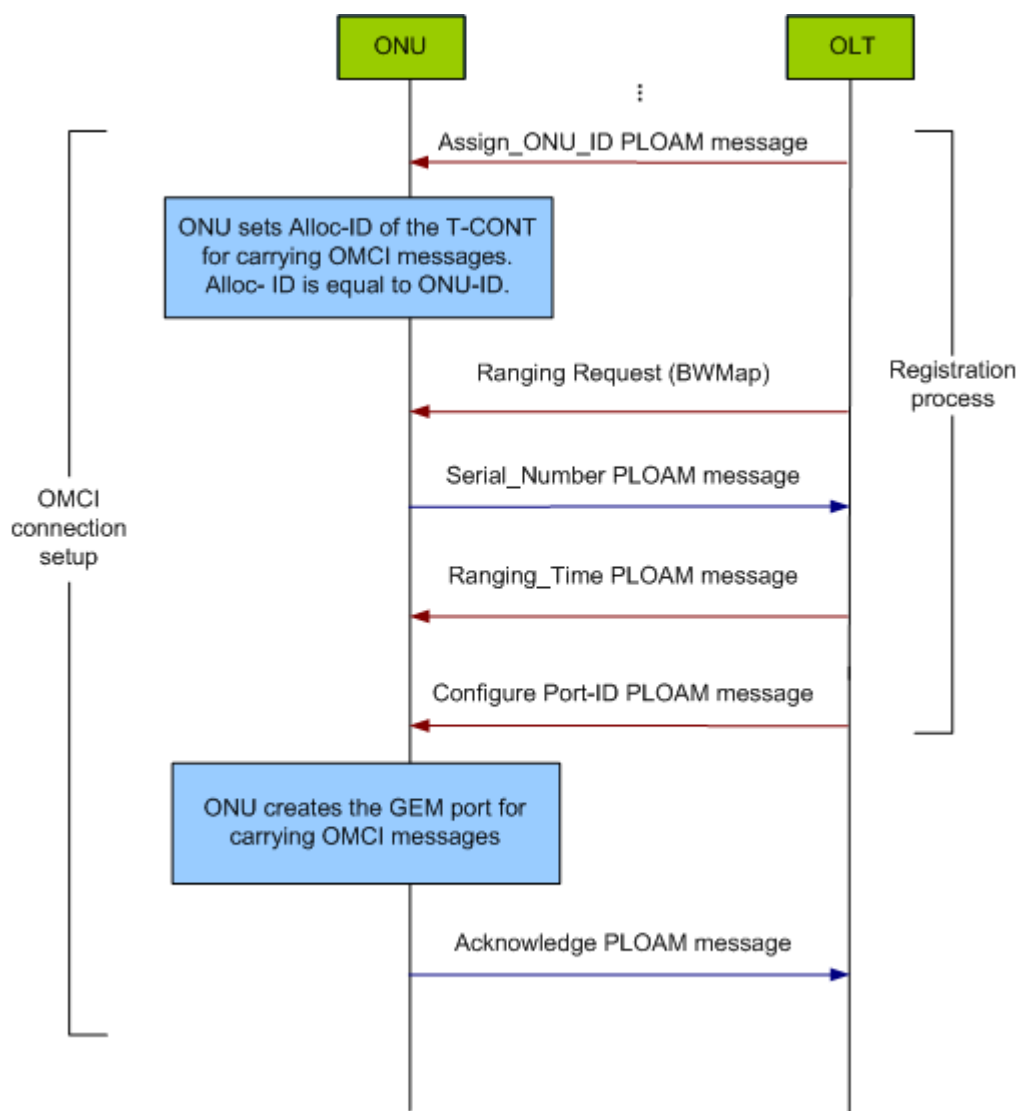
- Configuration management: Controls and identifies an ONU, and collects data from and provides data to the ONU.
- Fault management: Supports limited fault management. Most of the operations are limited to failure indication.
- Performance management: Collects and queries performance statistics.
- Security management: Enables/Disables downstream encryption.

Establishing the ONU Management and Control Channel (OMCC)

Upon initialization, the ONU creates a virtual OMCI T-CONT, an OMCC structure that contains an OMCI queue, a placeholder for an alloc-ID attribute, and – going beyond the definition of an ordinary T-CONT – a placeholder for an OMCI port-ID

attribute. The establishment of the OMCC follows the process shown in [Figure 2-15](#). During activation, the ONU receives a PLOAM message from the OLT indicating the assignment of the ONU-ID. The ONU populates the alloc-ID attribute of its virtual OMCI T-CONT with the ONU-ID. This makes the alloc-ID for OMCI the same as the assigned ONU-ID. It is therefore not necessary for the OLT to send an assign_alloc-ID message to establish the OMCC. If the OLT nevertheless chooses to send an assign_alloc-ID PLOAM with the default alloc-ID, the ONU should acknowledge this message without taking any specific further action. This is true regardless of the alloc-ID type value in the assign_alloc-ID message: it should not be possible to de-allocate the default alloc-ID with an assign_alloc-ID type 255 message.

Figure 2-15 OMCC establishment



Upon completion of ONU activation in G.984 systems, the OLT assigns a GEM port-ID to the ONU for OMCI messages. This is accomplished by a configure_port-ID PLOAM message. The ONU populates the OMCI port-ID attribute of the OMCC structure based on that message, and responds back to the OLT with an acknowledgment.

In G.987 systems, the GEM port for OMCI use is automatically assigned, and is equal to the ONU-ID.

At this point, the OMCC path has been successfully established.

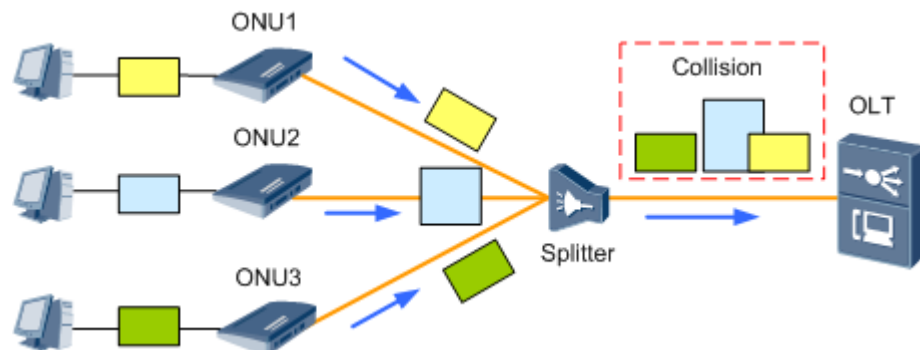
2.4 Key GPON Techniques

2.4.1 GPON Ranging

Why Is Ranging Required

The logic reaches from ONUs to an OLT vary. Therefore, the time required for transmitting optical signals over optical fibers is different and the times when the ONUs receive optical signals is different. In addition, the round trip delays (RTDs) between an OLT and ONUs also vary depending on time and environment. Therefore, collisions may occur when ONU sends data in TDMA mode (in this mode, only one of the ONUs connecting to a PON port sends data at a moment), as shown in [Figure 2-16](#). The OLT must precisely measure the distances between itself and each ONU to provide a proper timeslot for converged upstream data from all ONUs to prevent data conflict. In this way, the OLT controls the time for each ONU to send data upstream.

Figure 2-16 Cell transmission without ranging



Ranging Principles

Ranging process is as follows:

- The OLT starts ranging for an ONU when the ONU registers with the OLT for the first time and obtains the round trip delay (RTD) of the ONU. Based on the RTD, the OLT calculates the physical reach of this ONU.
- The OLT specifies a proper equalization delay (EqD) for the ONU based on the physical reach.

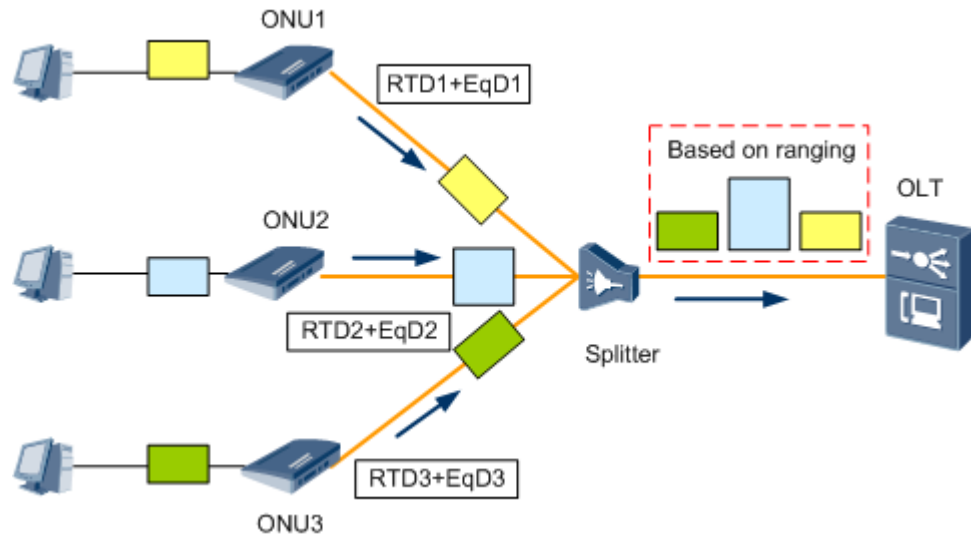
NOTE

The OLT requires a quiet zone during ranging to pause the upstream transmission channel of the ONUs connected to it. The quiet zone is implemented by emptying BWmap so that no timeslot is allocated for data transmission.

Ranging Results

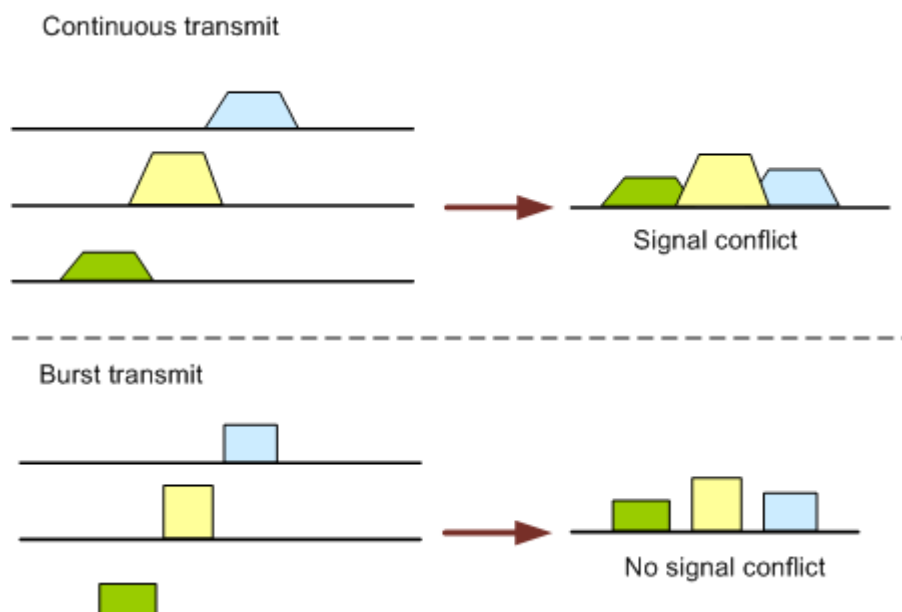
RTD and EqD synchronize data frames sent by all ONUs, preventing data conflict on optical splitters. In this way, all ONUs locate at the same logic reach and they send data at specified timeslots, thereby preventing upstream cell conflict.

Figure 2-17 Cell transmission with ranging



2.4.2 GPON Burst Optical/Electrical Technology

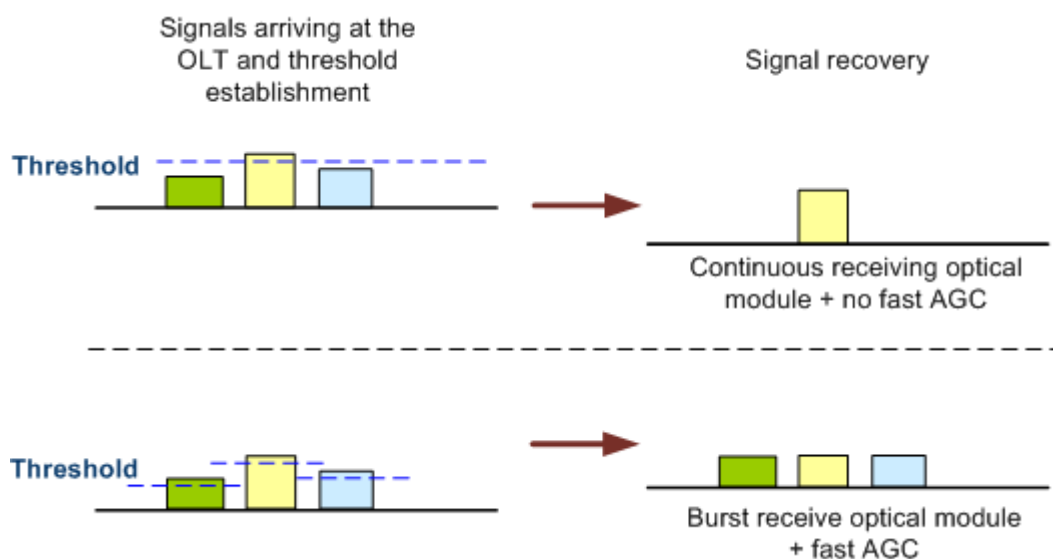
TDMA is used in GPON upstream direction. An ONU transmits data only within the allocated timeslots. In the timeslots that are not allocated to it, the ONU immediately disables the transmission of its optical transceiver to prevent other ONUs from being affected. The OLT then receives the upstream data from each ONU in a burst manner based on timeslots. Therefore, both OLT and ONU optical modules must support burst receive and transmit function to ensure normal running of the GPON system. [Figure 2-18](#) shows the burst transmit function supported by ONU optical modules, and [Figure 2-19](#) shows the burst receive function supported by OLT optical modules.

Figure 2-18 Burst transmit function supported by ONU optical modules

Ranging can be implemented to prevent cells transmitted by different ONUs from conflicting with each other on the OLT. However, the ranging accuracy is ± 1 bit and the cells transmitted by different ONUs have a protection time of several bits (not a multiple of 1 bit). If the ONU optical modules do not support the burst receive and transmit function, the transmitted signals overlap and distortion occurs.

NOTE

In the GPON system, all data is broadcast downstream to ONUs. The transmission requires OLT optical modules to transmit optical signals continuously and ONU optical modules to receive optical signals continuously. Therefore, in GPON downstream direction, the OLT optical modules are not required to support the burst transmit function, the ONU optical modules are not required to support the burst receive function.

Figure 2-19 Burst receive function supported by OLT optical modules

- The distance from each ONU to the OLT varies and therefore the optical signal attenuation varies for each ONU. As a result, the power and level of packets received by an OLT at different timeslots varies.
- If the OLT-side optical modules do not support the burst receive function, the OLT may restore incorrect signals because only the level greater than the threshold is considered valid and the signals with the level lower than the threshold cannot be restored. The automatic gain control (AGC) function dynamically adjusts the threshold of the receive optical power on the OLT based on the strength of the received optical signals to ensure that the signals of all ONUs can be restored.

2.4.3 GPON DBA

In the GPON system, the OLT controls an ONU's upstream data traffic by sending authorization signals to the ONU. PON requires an effective TDMA mechanism to control the upstream traffic so that data packets from multiple ONUs do not collide in upstream transmission. However, the collision-based mechanism needs to manage QoS in the passive ODN of the PON, which is physically impossible or causes severe efficiency deterioration.

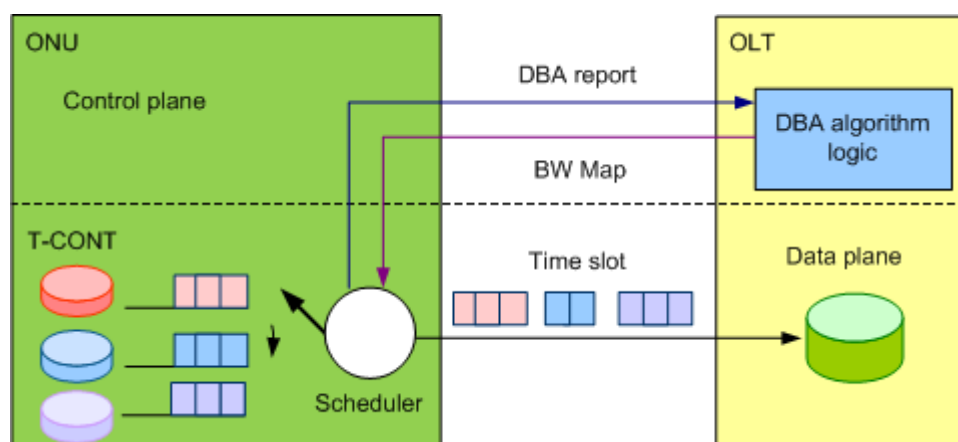
A mechanism for upstream GPON traffic management has been a primary focus in standardization of GPON traffic management. To resolve the problem, ITU-T Recommendation G.984.3 is developed, which defines the DBA protocol for managing upstream PON traffic.

DBA enables the OLT to monitor congestion on the PON network in real time. Then, the OLT can dynamically adjust bandwidths based on congestion, bandwidth usages, and configurations. DBA supports the following functions:

- Improves upstream bandwidth usages on a PON port.
- Supports more users on a PON port.
- Provides higher bandwidths for users, especially the services with significant bandwidth bursts.

Figure 2-20 shows DBA principles.

Figure 2-20 DBA principles



- The embedded DBA module of an OLT continuously collects DBA reports, performs calculation, and uses the BWMap field in the downstream frame to notify the ONU of the DBA calculation result.
- According to the BWMap information, the ONUs send data upstream in the timeslots allocated to them, and occupy the upstream bandwidth. Therefore, each ONU dynamically adjusts its upstream bandwidth according to its actually transmitted data traffic, improving upstream bandwidth usage.

Bandwidth can also be allocated in static mode, or fixed mode. In this mode, an OLT periodically allocates a fixed bandwidth to each ONU based on the ONU's service level agreement (SLA), bandwidth, and delay indicators.

- In fixed mode, an OLT uses a polling mechanism. The bandwidths allocated to ONUs may vary but the bandwidth allocated to each ONU is the same in each polling period. The bandwidth guarantee depends on an ONU's SLA but not on its upstream service traffic. An ONU is allocated a fixed bandwidth even carrying no upstream services.
- The static bandwidth allocation method is simple and easy to implement, and is suitable for carrying services with fixed traffic such as TDM. However, the upstream bandwidth cannot be adjusted in real time according to the traffic on the ONU, and the bandwidth utilization is low when the IP service with high burst traffic is carried.

2.4.4 GPON FEC

In actual applications, the transmission of digital signals introduces bit errors and jitter, which degrade signal transmission quality.

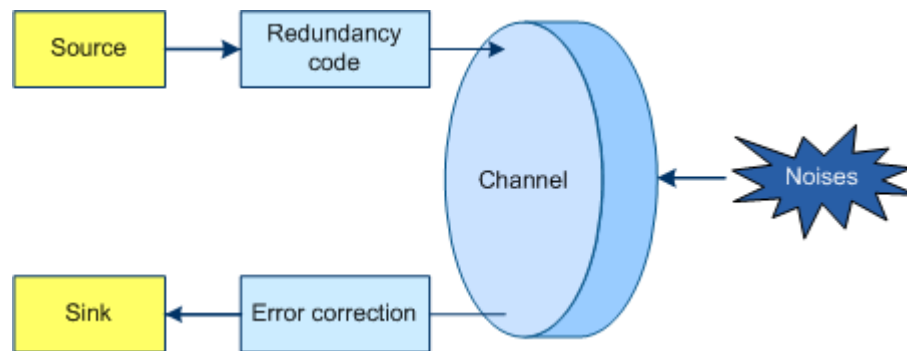
To resolve the preceding issue, an error correction technology is required. Among the error correction technologies, the effective ones achieve transmission reliability by reducing bandwidth usages, which also increases telecom device complexity. The error correction technologies are used for controlling errors. The codes involved in these technologies are classified as error detection codes and error correction codes based on usage scenarios.

- Error detection codes, such as parity check codes, are used for detecting error codes.
- Error correction codes, such as BCH codes, Reed-Solomon (RS) codes, and Hamming codes, are used for automatically correcting errors.

The only difference between the error detection codes and error correction codes lies in performance parameters applied in different usage scenarios. FEC uses error correction codes.

FEC is a data coding technology, which enables the RX end to check error bits in transmission based on the coding data. FEC is unidirectional, not supporting error information feedback.

Redundant codes are added to signals on the TX end. Then, the RX end checks the signals for errors based on error-correcting code (ECC) and corrects errors if there is any. Common FEC codes include Hamming codes, RS codes, and convolutional codes. [Figure 2-21](#) shows FEC principles.

Figure 2-21 FEC principles

In the GPON FEC algorithm, the most common RS code RS (255,239) is used, where the code word is 255 bytes long, consisting of 239 data bytes followed by 16 overhead redundant bytes. However, due to the overhead caused by multi-frame tail fragments, the bandwidth throughput of the GPON system with FEC enabled is about 90% of that with FEC disabled. RS code RS (255,239) complies with ITU-T Recommendation G.984.3. The FEC algorithm decreases the bit error rate (BER) from 10^{-3} to 10^{-12} on GPON lines.

FEC characteristics are as follows:

- Does not require data retransmission, thereby improving real-time efficiency.
- Enables lines to tolerate louder noises on a basis of a higher bandwidth overhead. (In this case, users must balance between the transmission quality and the bandwidth usage based on site requirements.)
- Based on the preceding characteristics, FEC applies to: The services requiring error detection and correction at the RX end without retransmission.
- Data transmission if the network is in a poor condition. For example, the transmission distance from the OLT to an ONT is long or the transmission line is of poor quality, which results in insufficient optical power budget or high BERs.
- The services requiring no delays (a retransmission prolongs the delay).
- FEC status can be configured in GPON systems based on GPON ports in the downstream direction (by running the **port fec** command) and based on ONUs in the upstream direction. To configure the FEC status in the upstream direction based on ONUs, run either of the following commands:
 - In profile mode, run the **fec-upstream** command.
 - In discrete mode, run the **ont fec-upstream** command.

2.4.5 GPON Line Encryption

In a GPON system, downstream data is broadcast to all ONUs. Then, unauthorized ONUs can receive the downstream data of authorized ONUs, causing system risks.

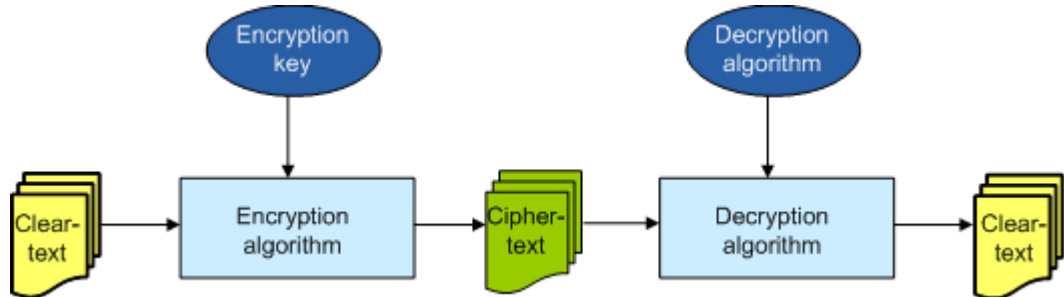
Line encryption is used to eliminate these security risks. The GPON system uses the Advanced Encryption Standard 128 (AES128) algorithm to encrypt the data packets transmitted in plaintext mode so that the packets are transmitted in ciphertext mode, improving system security. Enable line encryption if the usage scenarios promote high security requirements.

- The line encryption algorithms used in GPON systems neither increase overhead nor decrease bandwidth usages.

- The line encryption algorithms will not prolong transmission delays.

Figure 2-22 shows line encryption process.

Figure 2-22 Line encryption process



Key Exchange and Switchover

1. The OLT initiates a key exchange request to the ONU. The ONU responds to the request and sends a new key to the OLT.
2. After receiving the new key, the OLT switches the key to the new one and uses the new key to encrypt data.
3. The OLT sends the frame number that uses the new key to the ONU.
4. The ONU receives the frame number and switches the verification key on data frames.

NOTE

- Due to length limitation on PLOAM messages, the ONU sends the key to the OLT in two pieces and sends both parts of the key three times for extra redundancy. If the OLT is unsuccessful in receiving either part of the key all three times it is transmitted, the OLT initiates a key exchange request to the ONU again until the OLT receives the same key for three times.
- The OLT issues a command three times to the ONU to notify the ONU of using the frame number of the new key. The ONU switches the verification key on data frames after receiving the command only once.

Configuration Method

- In GPON systems, run either of the following commands to configure line encryption status based on GEM ports (excluding multicast and broadcast GEM ports).
 - In profile mode, run the **gem add** command.
 - In discrete mode, run the **gemport add** command.
- Run either of the following commands to encrypt a GEM port in ONT management and control channels (OMCCs):
 - In profile mode, run the **omcc encrypt** command.
 - In discrete mode, run the **ont omcc encrypt** command.

2.4.6 GPON Energy Conservation

Energy conversion enables the OLT to periodically shut down an ONU optical module when the ONU is idle, thereby conserving energy for GPON lines.

Overview

An ONU optical module is still working when the ONU is idle. Idle indicates that the traffic within the detection period is less than the specified threshold. In such a case, the OLT can periodically shut down the ONU optical module so that it does not transmit or receive data anymore. This configuration reduces ONU power consumption and conserves energy.

NOTE

Energy conservation is recommended for the FTTH scenario, which is more effective than in other scenarios.

Principles

The energy conservation feature supports the doze mode and cyclic sleep mode, which comply with the ITU-T G987.3 and G.984.3 recommendations.

- **Doze Implementation**

- After an ONU enters doze mode, the OLT shuts down the ONU optical module in the TX direction. In such a case, the ONU can only receive downstream data from the OLT.
- In doze mode, if there is traffic on the ONU waiting to be transmitted upstream, the ONU can end the shutdown state by using a local event, so that the transmit function of the ONU optical module is restored from the shutdown state to the normal state.
- In doze mode, if the OLT wants to make the ONU exit the shutdown state (for example, when the OLT needs to upgrade the ONU), the OLT can send an event to wake up the ONU, so that the transmit function of the ONU optical module is restored from the shutdown state to the normal state.

- **Cyclic Sleep Implementation**

- After an ONU enters the cyclic sleep mode, the OLT shuts down the receive and transmit channels of the ONU optical module. The ONU cannot receive downstream data from the OLT and cannot send upstream data to the OLT.
- In cyclic sleep mode, if there is traffic on the ONU waiting to be transmitted upstream, the ONU can end the shutdown state by using a local event, so that the transmit channel of the ONU optical module is restored from the shutdown state to the normal state.
- In cyclic sleep mode, if the OLT wants to make the ONU exit the shutdown state, the OLT needs to wait till the ONU sleep timer expires and the ONU enters the short wake-up state. The ONU responds to the wake-up event sent by the OLT only after entering this state, and the transmit and receive channel of the ONU optical module will be restored from the shutdown state to the normal state.

Key Techniques

After an energy conservation profile is bound to an ONU, the ONU automatically enters or exits the energy conservation mode if the in-mode or out-of-mode conditions are met.

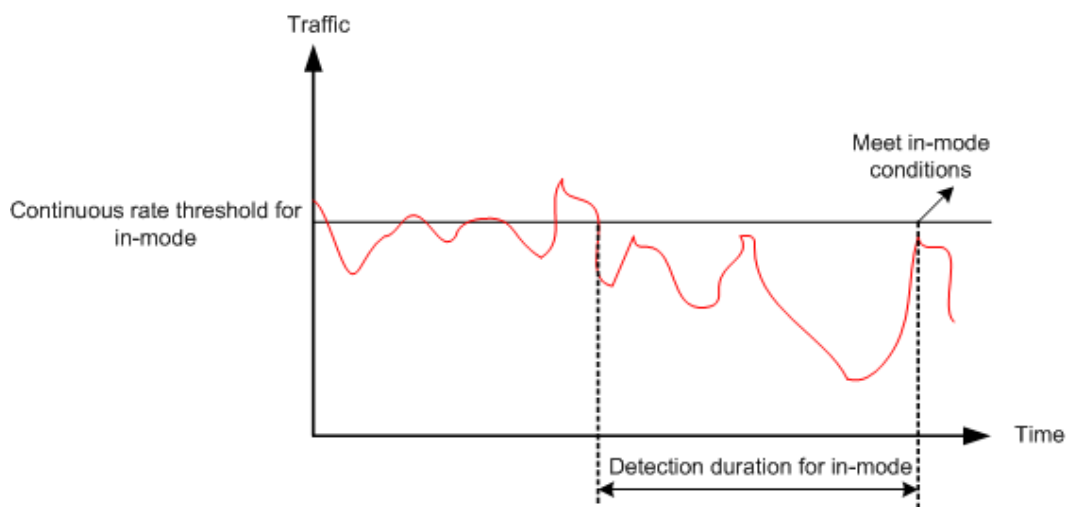
NOTE

In doze mode, the OLT shuts down only the data transmit channel of the ONU. Therefore, the ONU can enter or exit the energy conservation mode as long as its upstream traffic meets the in-mode or out-of-mode condition.

In-Mode Conditions

The energy conservation profile defines the upstream and downstream continuous rate thresholds for ONU in-mode. Within the detection duration, if the upstream and downstream traffic of an ONU is smaller than the configured continuous rate thresholds, the ONU enters the energy conservation mode, as shown in [Figure 2-23](#).

Figure 2-23 In-mode conditions

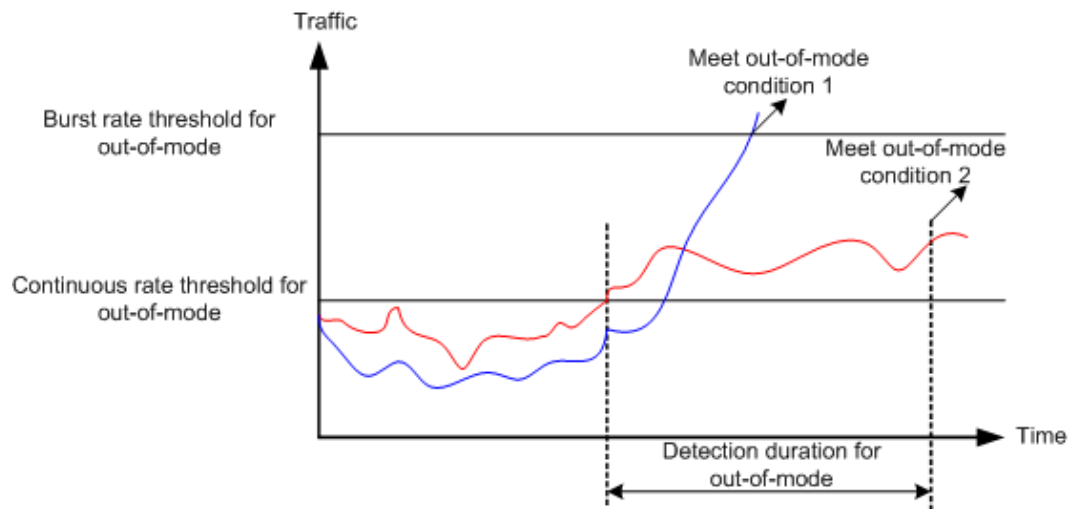
**Out-of-Mode Conditions**

The energy conservation profile defines the upstream and downstream continuous rate thresholds and burst rate thresholds for ONU out-of-mode. An ONU exits the energy conservation mode when its upstream and downstream traffic meets either of the following conditions:

- Out-of-mode condition 1: Within the detection duration, the ONU upstream or downstream burst traffic is larger than the configured burst rate threshold.
- Out-of-mode condition 2: Within the detection duration, the upstream traffic and downstream traffic are larger than the configured continuous rate thresholds.

[Figure 2-24](#) shows out-of-mode conditions.

Figure 2-24 Out-of-mode conditions



Configuring Energy Conservation

1. Create a GPON ONT energy conservation profile.

Run the **ont power-reduction-profile add** command to create a GPON ONT energy conservation profile.

NOTE

An OLT supports up to 32 ONT energy conservation profiles.

2. Query the information about an energy conservation profile.

Run the **display ont power-reduction-profile** command to query the information about the energy conservation profile.

3. Bind the energy conservation profile.

Run the **ont power-reduction-config** command to bind the energy conservation profile to the ONUs connected to a GPON port. After the binding, energy conservation configurations are automatically issued to the ONTs.

NOTE

- ONU energy conservation is incompatible with Type B single homing, Type B dual homing, Type C single homing, and Type C dual homing. When both ONU energy conservation and Type X homing are configured, ONU energy conservation fails to take effect.
- Energy conservation takes effect only between Huawei OLTs and ONUs but not with third-party ONUs.
- For a GPON port, the ONUs connected to it support the binding of up to 8 energy conservation profiles. For an XG-PON port, the number is 16.

2.4.7 ONU Automatic Registration and Service Flow Creation

Overview

The OLT supports the pre-configuration of the service flow creation policy on the PON port. When the ONU that meets conditions goes online, registration and service flow creation are automatically implemented based on the pre-configured policy. This function simplifies the configuration process and improves the installation and deployment efficiency.

NOTE

The ONU ID is configured during the pre-configuration of the service flow creation policy. When the ONU starts to register with the OLT, the ONU ID and vendor identity are verified. Only the ONU meeting conditions can implement automatic registration.

O&M for these automatically created service flows is the same as that for commonly created service flows.

NOTE

Automatic registration and service flow creation are supported in the PON profile mode only. They are not supported in the distributed mode.

Automatic Service Flow Creation

The automatic service flow creation process covers 2 scenarios: no ONU is manually added; the ONU is manually added.

Figure 2-25 Process of automatic service flow creation (no ONU is manually added)

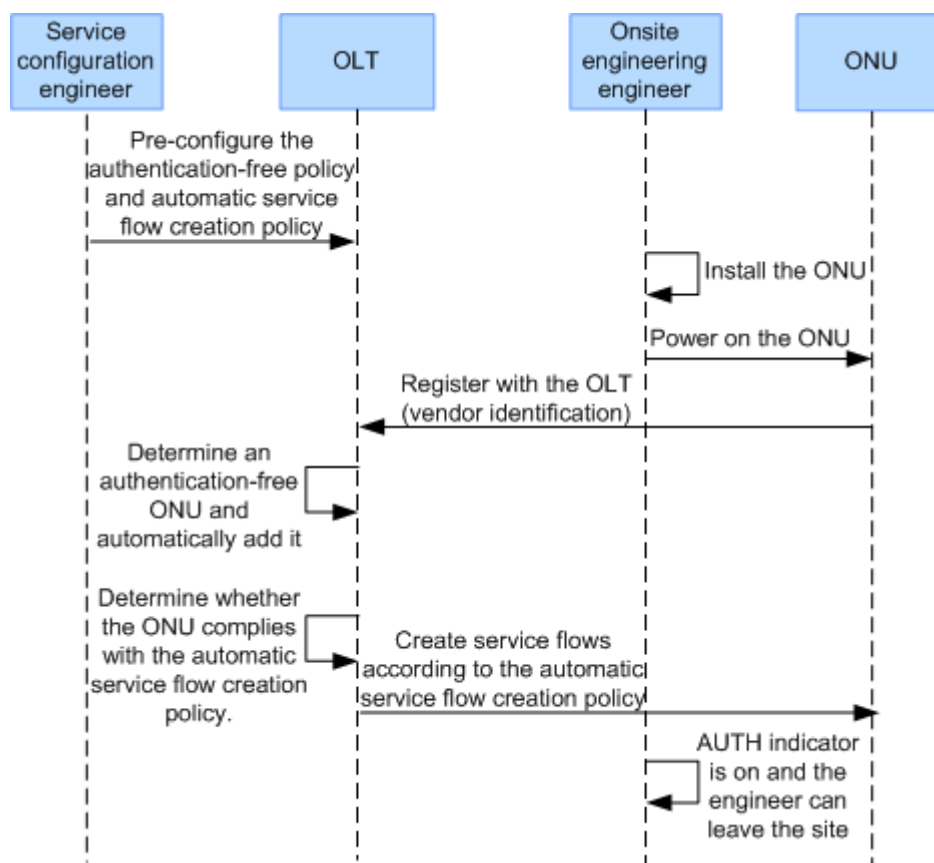
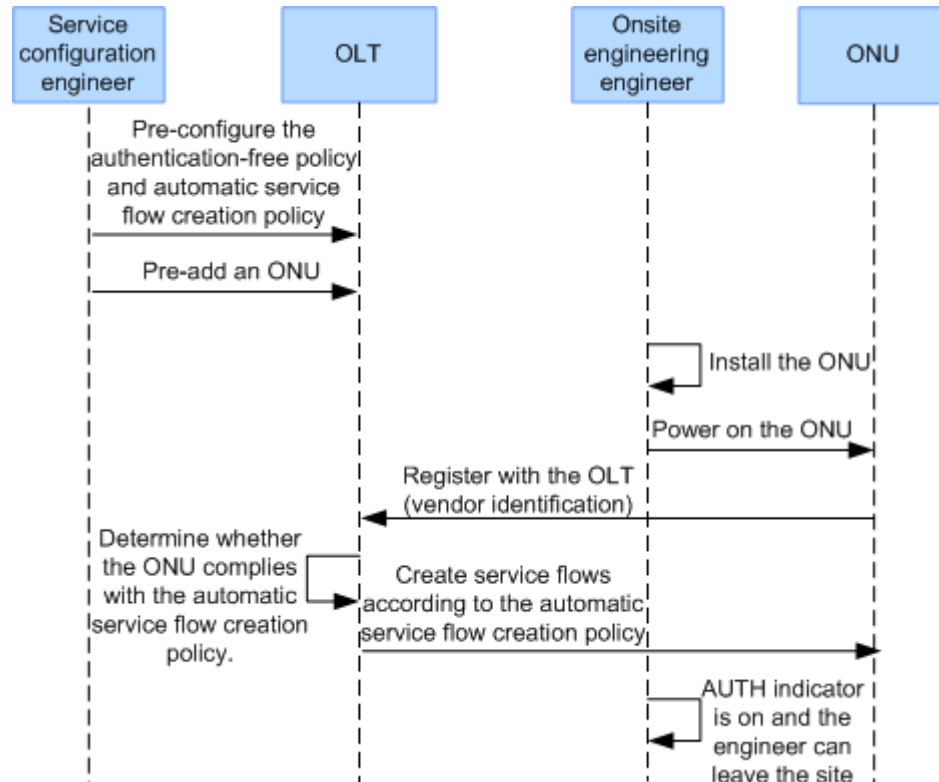


Figure 2-26 Process of automatic service flow creation (the ONU is manually added)



Configuring Automatic Service Flow Creation

1. Configure an automatic ONU addition policy.

Run the **ont auto-add-policy** command to configure an automatic ONU addition policy.

NOTE

When **auto-confirm** is set to **enable**, you do not need to run the **ont confirm** command on the GPON port to confirm the ONU. When **auto-confirm** is set to **disable**, you need to run the **ont confirm** command on the GPON port.

2. Configure the automatic service flow creation policy.

Run the **auto-service-port**

command to configure the automatic service flow creation policy.

For details about how to configure automatic service flow creation, see "[10.3.3.5 Configuring Automatic Service Flow Creation \(GPON\)](#)".

2.4.8 ONU Automatic Migration and Aging

Automatic Migration

When the ONU automatic migration function is enabled, if a PON port or fiber is faulty, the ONU connected to this faulty PON port is migrated to another PON port. If the ONU automatic adding policy is met, the ONU is automatically removed from the original PON port, and then added to the new PON port. In this

process, the OLT does not report the SN authentication conflict alarm. The ONU connected to the original PON port must meet the following conditions:

- The ONU is offline.
- The ONU supports OMCI management.
- The ONU is not a member of the type C protection group.
- The ONU supports SN authentication.

 NOTE

Automatic migration and aging are supported in the PON profile mode only. They are not supported in the disperse mode.

Automatic Aging

When an offline ONU is aged and meets automatic adding policy, the OLT automatically deletes the aged ONU to save resources. The ONU automatic aging period can be configured. The value range is 1–365. The default value is no-aging, which indicates no aging. For an aged ONU that meets the automatic adding policy, it will be automatically registered after being powered on.

Configuring Automatic Migration and Aging

1. Configure ONU automatic migration.
Run the **ont auto-migration** command to configure ONU automatic migration.
2. Configure ONU automatic aging.
Run the **ont auto-aging** command to configure ONU automatic aging.

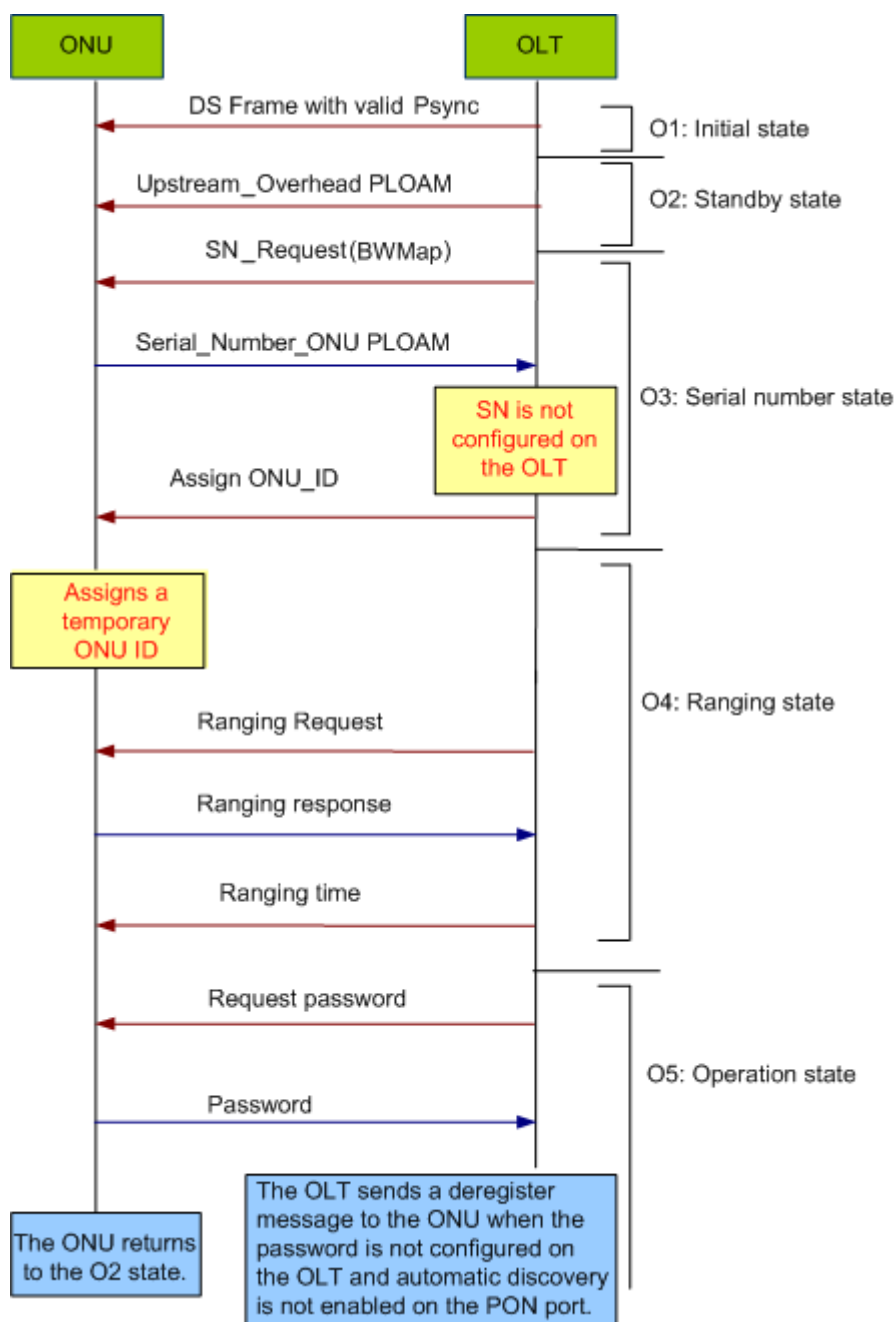
2.5 GPON Terminal Authentication and Management

GPON terminal authentication is a mechanism in which an OLT authenticates an ONU according to the authentication information reported by the ONU and in this way denies access to unauthorized ONUs. In the GPON system, only authenticated ONUs can access the system. After the ONU passes authentication and goes online, data can be transmitted between ONUs and the OLT.

2.5.1 GPON Terminal Authentication (ONU Is Not Preconfigured)

The authentication modes for ONUs pre-configured on the OLT include SN, SN +Password, and Password. [Figure 2-27](#) shows the registration flow for ONUs not pre-configured on the OLT.

Figure 2-27 Authentication process of an ONU that is not preconfigured



- The OLT sends a serial number (SN) request to the ONU.
- The ONU responds to the SN request message sent from the OLT.
- Upon receiving the SN response from the ONU, the OLT assigns a temporary ONU ID to the ONU.
- After the ONU enters the operation state, the OLT sends a password request message to the ONU. The ONU then responds with a password. The password is not configured on the OLT.
 - If the automatic discovery function is not enabled on the PON port to which the ONU is connected, the OLT sends a deregister message to the

ONU. Upon receiving this message, the ONU sends a register request message to the OLT.

- If the automatic discovery function is enabled on the PON port to which the ONU is connected, the port reports an alarm to the command line interface (CLI) or network management system (NMS), indicating that the ONU is automatically discovered. The ONU can go online only after being confirmed.

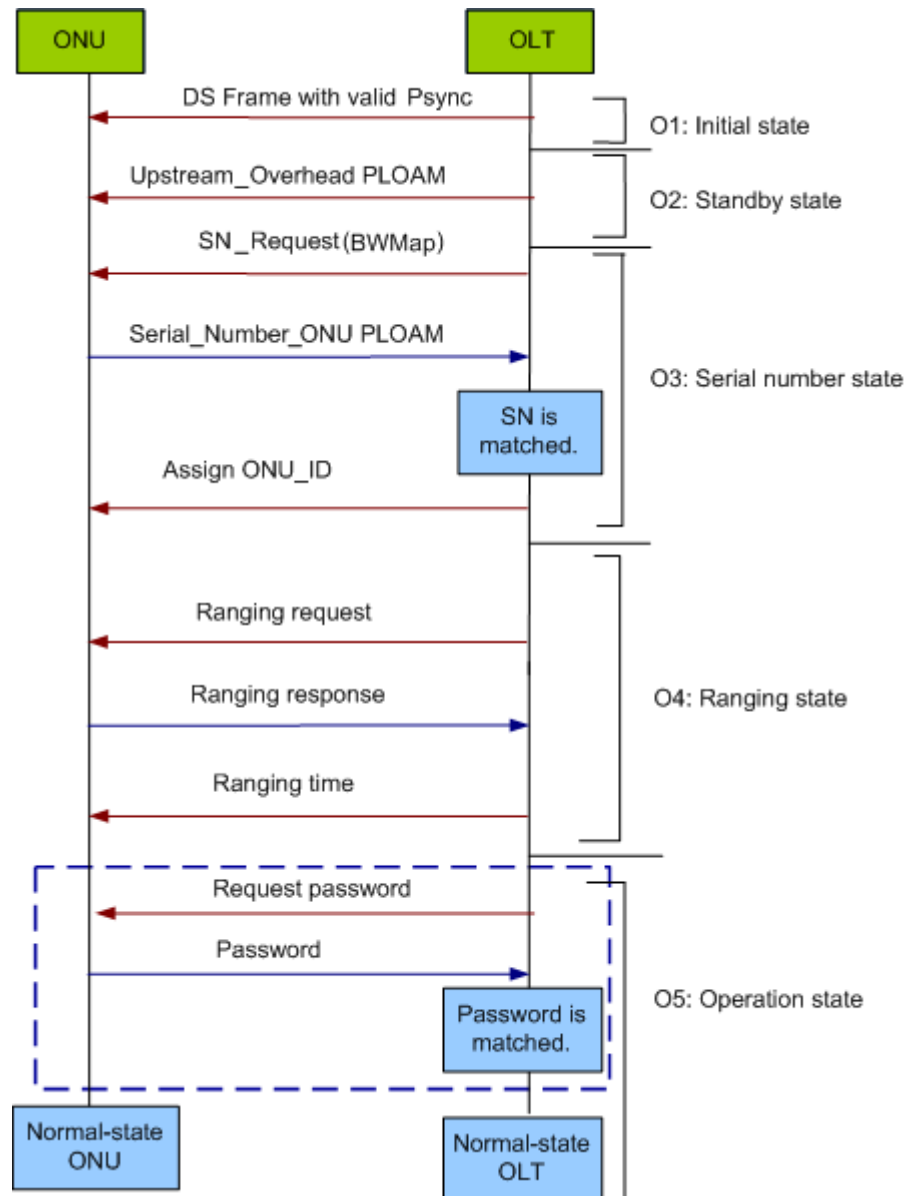
2.5.2 GPON Terminal Authentication (ONU Has Been Pre-configured)

A pre-configured ONU can be authenticated in three modes: SN, SN+password, and password.

SN/SN+Password Authentication

In SN authentication, the OLT matches only the ONU SN. In SN+password authentication, the OLT matches both the ONU SN and password. [Figure 2-28](#) shows the authentication flow.

Figure 2-28 SN/SN+password authentication flow



NOTE

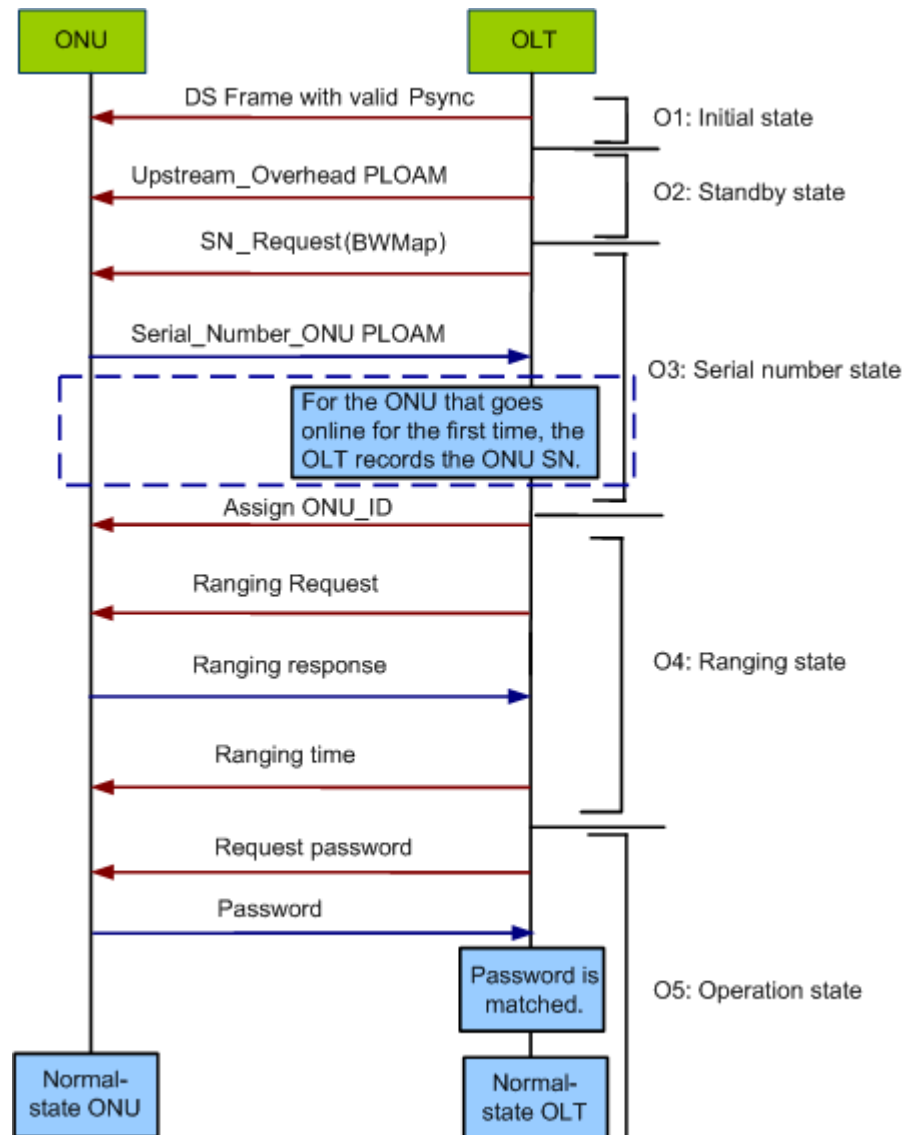
If an ONU is authenticated in SN mode, no password is required in the authentication process.

- After receiving an SN response message from an ONU, the OLT checks whether another ONU with the same SN is online. If yes, the OLT reports an SN conflict alarm to the CLI or NMS. If no, the OLT directly assigns a user-defined ONU ID to the ONU.
- After the ONU enters the operation state,
 - For the ONU that is authenticated in SN mode, the OLT does not send a password request message to this ONU. Instead, the OLT automatically configures a GEM port that has the same ID as the ONU ID for the ONU

- for carrying OMCI messages, and allows the ONU to go online. In addition, the OLT reports an ONU online alarm to the CLI or NMS.
- For the ONU that is authenticated in SN+password mode, the OLT sends a password request to the ONU, and compares the password reported by the ONU with the local password. If the two passwords are the same, the OLT directly configures a GEM port for the ONU to carry OMCI messages, and allows the ONU to go online. In addition, the OLT reports an ONU online alarm to the CLI or NMS. If the two passwords are not the same, the OLT reports a password error alarm to the CLI or NMS. The OLT does not report an ONU automatic discovery message even if the ONU automatic discovery function is enabled on the PON port. Instead, the OLT sends the Deactivate_ONU-ID PLOAM message to deregister the ONU.

Password Authentication

An ONU that uses password authentication is added to a PON port on an OLT in advance, and then this ONU is connected to the PON port. In password authentication, if finding that the SN or password of the ONU to be authenticated conflicts with that of an online ONU, the OLT deregisters the ONU to be authenticated. This does not affect the online ONU. Password authentication is available in two modes: once-on and always-on.

Figure 2-29 Initial ONU authentication in once-on mode

Once-on Application Scenarios

A carrier allocates a password to a user and requires the user to go online within a specified time. After going online, the user cannot change the ONU. To change the ONU, the user must notify the carrier. In once-on mode, the aging time is configurable. After the aging time is set, the ONU must register with the OLT and go online within the preset aging time. Otherwise, the ONU is not allowed to register with the OLT or go online. Once the ONU is authenticated, its SN cannot be changed.

In once-on mode,

- Only the initial authentication of an ONU is performed by password, as shown in [Figure 2-29](#).
- In subsequent authentications, the ONU can be authenticated by SN or SN +password according to the CLI configuration, as shown in [Figure 2-28](#).

 NOTE

In once-on mode, before the ONU registration times out or before the ONU successfully registers with the OLT for the first time, the ONU discovery status is ON. Only the ONU whose discovery status is ON is allowed to register with the OLT and go online. After the ONU registration times out or after the ONU successfully registers with the OLT for the first time, the OLT sets the ONU discovery status to OFF.

- The ONU whose registration times out is not allowed to register with the OLT or go online. The registration timeout flag of the ONU needs to be reset at the central office (CO), and then the ONU can go online.
- An ONU that successfully registers for the first time is allowed to register and go online again.

Always-on Application Scenarios

 NOTE

In the Always-on mode, the OLT does not need to record the SN when an ONU goes online for the first time.

The always-on mode applies to the following scenario: A carrier allocates a password to a user, and the user can use different ONUs with this password and different SNs. The user can change the ONU without informing the carrier. In always-on mode, there is no restriction on the time when the user goes online.

- An ONU is authenticated by password when it goes online for the first time. After the ONU passes the password authentication and goes online successfully, the OLT generates an SN+password entry according to the SN and password of the ONU. [Figure 2-29](#) shows the authentication process.
- The following scenarios are involved if it is not the first time that an ONU goes online:
 - If the SN and password of the ONU are the same as the SN and password of the ONU that successfully goes online for the first time, the ONU is authenticated by SN+password. [Figure 2-28](#) shows the authentication process.
 - If the user replaces the ONU with an ONU that has the same password but a different SN, the new ONU is authenticated by password. After this ONU passes authentication and goes online successfully, the original SN+password entry is updated. [Figure 2-29](#) shows the authentication process.

2.5.3 GPON Terminal Management

The ONUs (including MDUs and ONTs) in a GPON system are managed using physical layer OAM (PLOAM) messages and OMCI messages.

PLOAM, defined in ITU-T Recommendation G.984.3, is used for exchanging management and maintenance messages, such as DBA and DBRu messages, between the GPON physical layer and TC layer.

ONUs (including MDUs and ONTs) in a GPON system are managed using OMCI messages. The ONUs support offline deployment, plug-and-play, and automatic service provisioning. For details about OMCI management functions, see [OMCI](#).

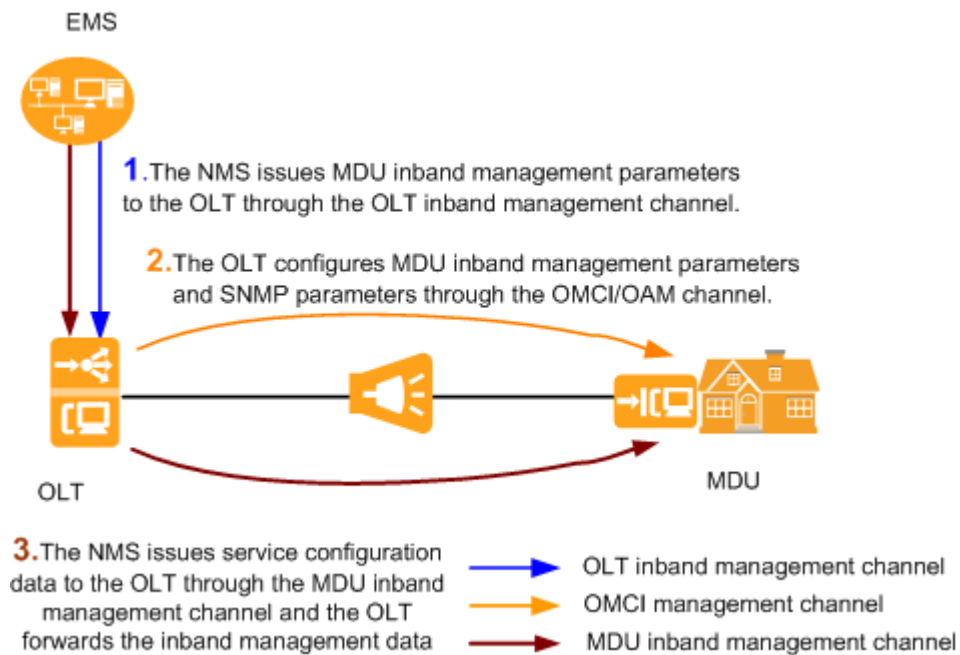
- OMCI messages are used for maintaining and managing service hierarchies, such as discovering device hardware capabilities and configuring alarm maintenance and service capabilities.

- OMCI enables ONUs to support offline configuration so that the ONUs do not need to store configuration data locally, facilitating service provisioning.

MDU Management

Figure 2-30 shows the process of configuring a management channel for an MDU.

Figure 2-30 Process of configuring a management channel for an MDU



1. The NMS issues MDU inband management parameters to the OLT through the OLT inband management channel.
2. The OLT configures the MDU inband management parameters and Simple Network Management Protocol (SNMP) parameters through the OMCI or OAM channel to set up the MDU inband management channel.
3. The NMS issues service configuration data through the MDU inband management channel. After the MDU inband management channel is set up, the NMS configures and manages the MDU through the SNMP channel. In such a manner, the OLT only needs to forward the MDU inband management data.

ONT Management

GPON terminals are managed using one of these protocols: optical network terminal management and control interface (OMCI), Extensible Markup Language (XML), or Technical Report 069 (TR069).

- The optical network terminal management and control interface (OMCI) protocol is defined by ITU-T G984.4, which applies to managing optical network terminals (ONTs) in a GPON system. Huawei ONTs comply with OMCI. OMCI messages are transmitted between an optical line terminal (OLT) and an ONT over a dedicated permanent virtual channel (PVC) in asynchronous transfer mode (ATM) or a GPON encapsulation mode (GEM) port. The OMCI protocol manages and provides O&M for the ONT.

- Extensible Markup Language (XML) is a text format used for message interaction between devices. The network management system (NMS) uses XML to manage ONTs in a Huawei FTTx system. XML is also a management mode extended from OAM because not all voice and Layer 3 gateway services are defined in the OAM.
- Technical Report 069 (TR069) is a network management protocol defined by the DSL Forum. The full name of TR069 is CPE WAN Management Protocol (CWMP). CPE is the acronym for customer premises equipment and WAN is the acronym for wide area network. It defines a new network management structure consisting of management models, interaction interfaces, and basic management parameters. In the network management structure, the management server functions as an Auto-Configuration Server (ACS) and is responsible for managing the CPE. The ACS and CPE use Hypertext Transfer Protocol (HTTP) to communicate with each other. The ACS serves as an HTTP server and the CPE serves as a client. Management operations are implemented using XML-based remote procedure call (RPC).

Optical network terminals (ONTs) are classified into three types: bridge type, bridge+voice type, and gateway type.

- A bridge-type ONT provides Layer 2 data and multicast services.
- A bridge+voice-type ONT provides Layer 2 data, Layer 2 multicast services, and voice over IP (VoIP) services.
- A gateway-type ONT provides Layer 3 data, Layer 3 multicast services, and VoIP services.

Each type of terminal management solution has a unique service management scope. Based on terminal types, different GPON terminal management solutions are available, including OMCI+NMS, OMCI+NMS+XML, OMCI+NMS+TR069.

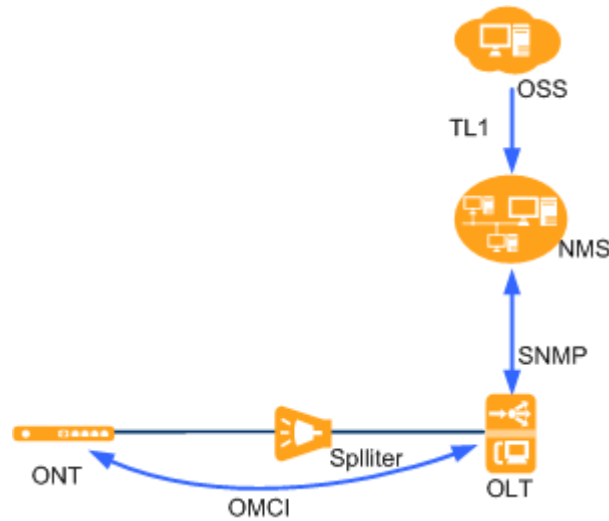
- The OMCI+NMS solution manages Layer 2 services, voice services and the PON link layer. This solution cannot manage Layer 3 services.
- The OMCI+NMS+XML solution manages Layer 2 services, Layer 3 services, and voice services.
- The OMCI+NMS+TR069 solution manages Layer 3 services and voice services, and remotely identifies faults. When this solution is used, OMCI is still required to manage Layer 2 services and the PON link layer.

OMCI+NMS

A standard optical network terminal management and control interface (OMCI) solution enables you to manage optical network terminals (ONTs) supplied by different vendors in diverse types of scenarios. An optical line terminal (OLT) and an ONT are closely coupled with each other. If a new service requirement is not defined in the OMCI, a new OMCI entity must be defined. An OMCI solution enables you to manage Layer 2 features and voice services. The OLT communicates with the ONT in OMCI mode.

Figure 2-31 shows the general principles of the OMCI+NMS solution for NMS+OLT+ONT deployment scenarios.

Figure 2-31 General principles of the OMCI+NMS solution

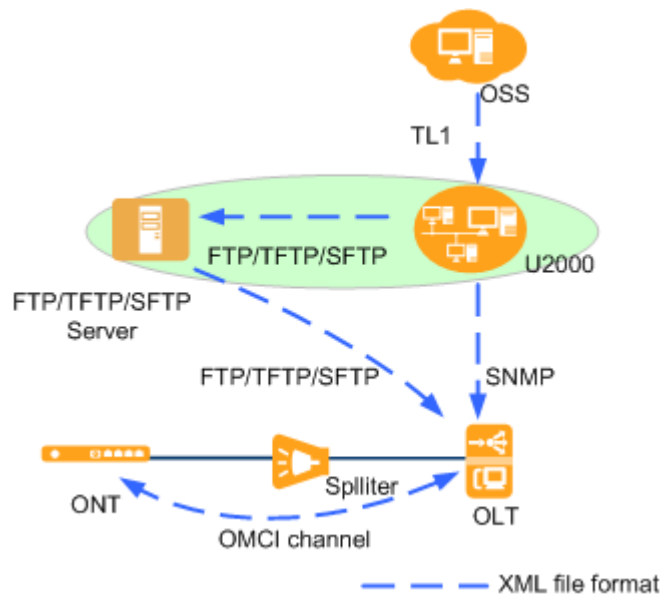


1. The Operations Support System (OSS) issues service configuration parameters to the NMS using the TL1 northbound interface (NBI).
2. The NMS uses the Simple Network Management Protocol (SNMP) to manage the OLT.
3. The OLT issues service configuration parameters to the ONT through an OMCI channel.

OMCI+NMS+XML

To overcome the limitations of the OMCI+NMS solution, Huawei provides the OMCI+NMS+XML solution. In this solution, the NMS uses XML files transmitted over an IP channel to communicate with the OLT, and the OLT uses XML files transmitted over an OMCI channel to communicate with ONTs. The OMCI protocol manages Layer 2 services and the XML protocol manages Layer 3 and voice services.

Figure 2-32 shows the general principles of the OMCI+NMS+XML solution for NMS+OLT+ONT deployment scenarios.

Figure 2-32 General principles of the OMCI+NMS+XML solution

The NMS uploads the XML file to the FTP/TFTP/SFTP server. The OLT obtains the XML file from the FTP/TFTP/SFTP server and transparently transmits the XML file to an ONT through the OMCI channel.

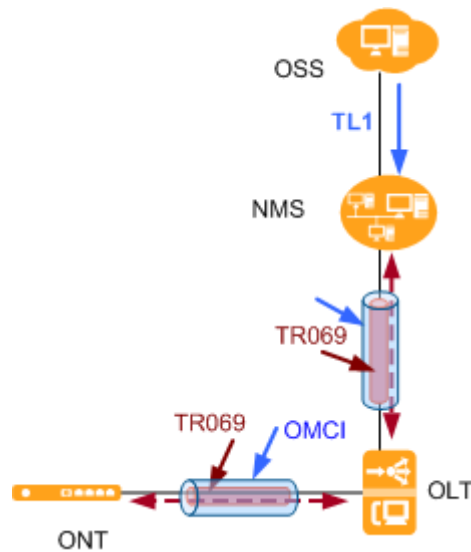
NOTE

TFTP/FTP has security risks due to protocol limitations. Therefore, the SFTP mode with high security is recommended for loading the XML file to the ONT.

1. The OSS issues service configuration parameters to the NMS using the TL1 NBI.
2. The NMS converts service information to XML files and uploads the files to the FTP/TFTP/SFTP server.
3. The NMS issues ONT configuration update commands to download the files.
4. The OLT obtains the XML files from the FTP/TFTP/SFTP server.
5. The OLT issues the XML files to the ONT through the OMCI channel.
6. The ONT returns execution results to the OLT using the OMCI entity.
7. The OLT reports the results to the NMS using traps.

The OMCI+NMS+XML solution meets all requirements for configuring ONTs but configuration files are transmitted in unidirectional mode. Due to this limitation, the configuration files only implement service configurations and status performance management, but cannot provide operation and maintenance (O&M) functions such as query of ONT status and configuration, and test and diagnose functions. To overcome OMCI+NMS+XML limitations, Huawei provides TR069 over OMCI. As a supplement to OMCI+NMS+XML, TR069 over OMCI is used for remote O&M and fault diagnosis. The NMS can use TR069 to remotely maintain ONTs without a dedicated TR069 server.

Figure 2-33 shows the general principles for NMS+OLT+ONT deployment scenarios.

Figure 2-33 General principles of the TR069 over OMCI solution

The solution manages configuration, performance, faults, and status of IP-based services by applying the associated methods described in the TR069 solution to the OMCI solution. The OLT and ONT transparently transmit data between each other.

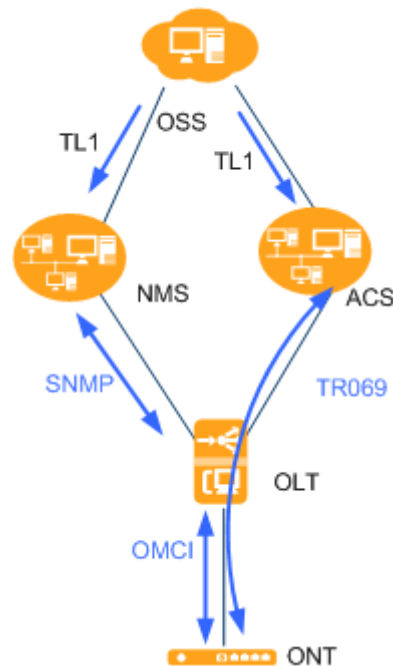
1. The NMS manages and maintains an ONT, and queries the ONT status. It encapsulates involved commands to character strings or binary code flows in a certain format, and issues the commands to the OLT through the MIB interface.
2. The OLT transparently transmits the character strings or binary code streams to the ONT using an extended OMCI entity.
3. The ONT returns execution results to the OLT using the OMCI entity.
4. The OLT reports the results to the NMS using traps.

OMCI+NMS+TR069

This solution allows an Auto-Configuration Server (ACS) to manage all the terminals on the network, locate faults, provide services, and collect performance statistics. Based on SNMP and TR069, this solution allows the ACS to manage home terminals in a unified manner, reducing O&M costs. TR069 automatically implements ONT configuration, dynamically provisions services, remotely locates faults, and rapidly collects terminal statistics.

Figure 2-34 shows the general principles of the solution.

Figure 2-34 General principles of the OMCI+NMS+TR069 solution



This solution allows the NMS to manage the OLT using SNMP, manage voice and Layer 3 services using TR069, and manage PON link layer using OMCI.

1. The OSS issues service configuration parameters to the NMS using the TL1 NBI.
2. The NMS manages the OLT using SNMP.
3. The OLT issues PON link layer configuration to the ONT using OMCI.
4. The ONT returns execution results to the OLT. Then the IP channel is set up.
5. The ONT registers with the ACS.
6. The ACS encapsulates user information in a TR069-compliant format and sends it to the ONT through the IP channel. The user information includes operations, maintenance items, and queries performed by a user. The IP channel is bidirectional.

Advantages and Disadvantages of the Terminal Management Solutions

Bridge type, bridge+voice type, and gateway type ONTs provide different types of services. Therefore, different solutions are used to manage these ONTs. [Table 2-4](#) lists the advantages and disadvantages of each solution. [Table 2-5](#) lists the recommended solution for each type of ONT.

Table 2-4 Advantages and disadvantages of each solution

Terminal Management Solution	Advantage	Disadvantage
OMCI+NMS	• A unified interface is used for ONT service management. • The OLT and ONT communicate with each other using OMCI-associated standards. • The ONT does not require a management IP address.	• The OLT and ONT are closely coupled with on each other. New services on the ONT require the OLT's support, adding to the difficulty in deploying new services. • The OMCI standard is not fully developed. If a new service requirement is not defined in the OMCI, a new OMCI entity must be defined.
OMCI+NMS+XML	• The ONT does not require a management IP address. • The OLT and ONT are not closely coupled with each other to certain extent. • A unified management server is used for swift service deployment.	• This is a Huawei's proprietary solution and cannot interact with devices from other vendors. • Voice and Layer 3 services cannot be configured using a command on the OLT.

Terminal Management Solution	Advantage	Disadvantage
OMCI+NMS+TR069	• An OLT version and an ONT version are not bound to each other. In other words, an OLT upgrade does not require an ONT upgrade; the opposite is also true. • TR069 provides an enhanced definition and deployment scenario for the IP-based customer premises equipment (CPE) service management model. Therefore, ONT vendors can easily deploy new gateway and voice services.	• TR069 is based on the IP protocol and requires an extra IP management network. • Different interfaces are used to manage the ONT. The EMS manages the link layer and the ACS manages IP-based services.

Table 2-5 Recommended solutions for each type of ONT

Terminal Type	Optional Solution	Recommended Solution
Bridge type	OMCI+NMS or OMCI+NMS+XML	OMCI+NMS
Bridge+voice type	OMCI+NMS or OMCI+NMS+XML	OMCI+NMS+XML (NMS provisions services) OMCI+NMS (OLT is connected to third-party ONTs)
Gateway type	OMCI+NMS+XML or OMCI+NMS+TR069	Only the NMS server is deployed: OMCI+NMS+XML The NMS and TR069 servers are deployed: OMCI+NMS+TR069

2.6 Continuous-Mode ONU Detection

This function is used to detect the continuous-mode ONU of terminal devices such as the MDU and ONT.

Overview

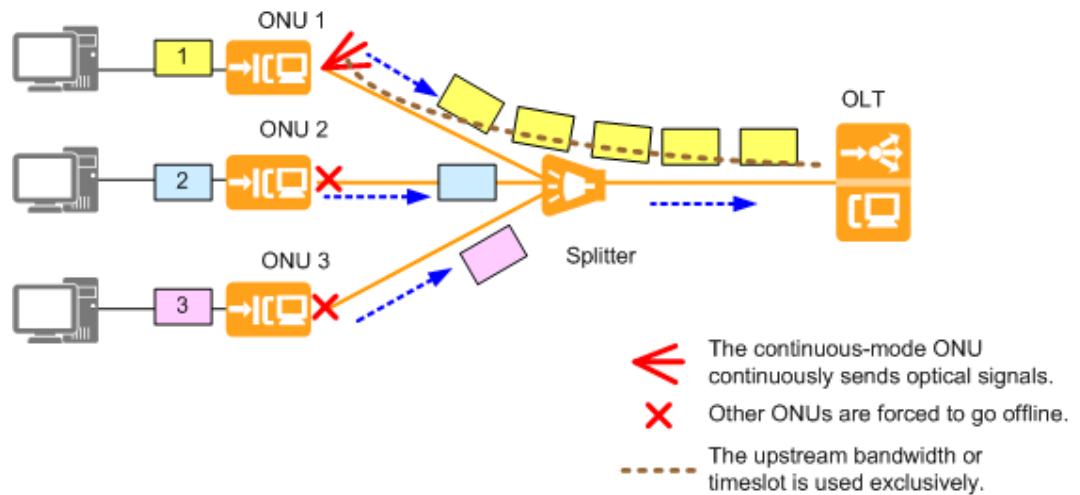
PON networks use the P2MP(point-to-multipoint) network architecture. They use time division multiple access (TDMA) in the upstream direction. ONUs must send optical signals upstream at the timeslots allocated by the OLT to prevent data conflict.

A continuous-mode ONU is also called a continuous-mode rogue ONU. It continuously sends optical signals to the upstream direction.

A continuous-mode ONU adversely affects the system as follows:

- If this ONU has been online, some or all ONUs connected to the same PON port go offline or frequently go offline and online.
- If this ONU has not been configured, other ONUs that have not been configured and connected to the same PON port will not be discovered by the OLT.

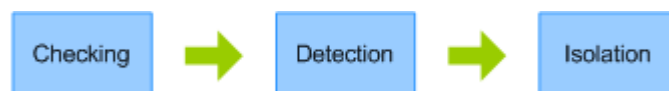
Figure 2-35 Rogue ONU



Continuous-Mode ONU Detection

Continuous-mode ONU detection, also called rogue ONU detection, is used for detecting continuous-mode ONUs in the system and isolating them, ensuring proper system running. A continuous-mode ONU detection process involves three stages, checking, detection, and isolation.

Figure 2-36 Continuous-Mode ONU detection process



- The three stages are as follows: Checking: The OLT periodically checks whether a continuous-mode ONU connects to a PON port. This checking cannot locate the continuous-mode ONU.

The OLT opens an empty window in the upstream direction of the PON to make all online ONUs stop sending upstream optical signals within a period of time, and detects ONU upstream optical signals. If the OLT receives optical signals, it then goes to the detection stage to locate the ONU.

- Detection: The OLT locates the continuous-mode ONU.

The OLT issues a command to ONUs to instruct the optical modules of the ONUs to send optical signals upstream and checks whether optical signals can be received in the upstream direction. If other ONUs go offline after an ONU sends optical signals, this ONU is a continuous-mode ONU. In a detection process, the OLT checks all ONUs connected to a PON port for detecting all continuous-mode ONUs.

- Isolation: The OLT issues a command to power off the continuous-mode ONU, preventing this ONU from adversely affecting other ONUs connected to the same PON port.

After an ONU is powered off by the OLT, the ONU cannot send optical signals upstream even after being reset or power recycled. This ONU can send optical signals upstream only after the OLT cancels the isolation.

NOTE

The OLT checks continuous-mode ONUs but does not detect or isolate them by default.

Handling a Continuous-Mode ONU

1. If an ONT goes online and other ONTs connected to the same PON port go offline or go online and offline frequently, or the **0x2e314021 There are illegal incursionary rogue ONTs under the port** alarm is reported to the OLT, a rogue ONT may exist in the system. In this case, locate the rogue ONT according to the following steps.

NOTE

You can also run the **display port state** command to query whether a rogue ONT exists under a PON port.

2. Run the **anti-rogueont manual-detect** command to detect, locate, and isolate a continuous-mode rogue ONT manually. Check whether the system generates alarm **0x2e314022 The ONT is rogue ONT** or **0x2e314021 There are illegal incursionary rogue ONTs under the port**.

NOTE

During rogue ONU detection, if the port of the ONU to be detected is configured with a type B protection group, you need to run the **force-switch** command to forcibly switch the protection group and then check for a rogue ONU to avoid protection switching. You can forcibly switch services to the work side for rogue ONU detection if you are not sure which feeder fiber functions properly. If the rogue ONU is not located on the working side, forcibly switch to the protection side to locate the rogue ONU. Then, run the **undo force-switch** command to cancel forced protection group switching.

- If the **The ONT is rogue ONT** or **There are illegal incursionary rogue ONTs under the port** alarm is generated, a continuous-mode rogue ONT may exist. In this case, go to [3](#).
- If the **The ONT is rogue ONT** or **There are illegal incursionary rogue ONTs under the port** alarm is not generated, an irregular-mode rogue ONT may exist. In this case, go to [4](#).

3. Handle the ONT according to the generated alarm.
 - If the **0x2e314022 The ONT is rogue ONT** alarm is generated, replace the ONU. Then, go to [7](#).
 - If the **0x2e314021 There are illegal incursionary rogue ONTs under the port** alarm is generated, go to [4](#).

NOTE

If the **0x2e314021 There are illegal incursionary rogue ONTs under the port** alarm is generated, a continuous-mode rogue ONU may exist and this rogue ONU does not support Huawei-defined extended PLOAM messages, or the optical signal transmission of the ONU optical module cannot be controlled.

4. Run the **ont reset** command or the **ont deactivate** command to reset or deactivate ONUs under the PON port one by one. Then, check whether other ONUs that encounter the fault (going offline or going online and offline repeatedly) can go online.
 - If yes, it indicates that the ONU is a rogue ONU. Replace the ONU. Go to [7](#).
 - If no, the ONT optical module may be damaged so that the rogue ONT fails to be reset or deactivated by running the command. In this case, go to [5](#).
5. Locate a rogue ONU manually: Remove the upstream optical fibers of ONUs one by one from the optical splitter, and check whether other faulty ONUs go online normally.
 - If yes, it indicates that the ONT is a rogue ONT. Replace the ONU. Then, go to [7](#).
 - If no, go to [6](#).
6. Obtain technical support from Huawei.
7. The fault is rectified.

Limitations and Restrictions

- The OLT checks and analyzes the abnormality in the sending of upstream optical signal over a PON line, and identifies and isolates rogue ONUs of only non-malicious users. This feature does not apply to the intentionally sabotaged ONU or sub-standard ONU.
- A continuous-mode ONU (rogue ONU) is required to parse and respond to downstream PLOAM messages.
- The OLT can quickly locate a continuous-mode ONU only when the ONU supports standard PLOAM messages and the ONU optical module is correctly controlled. When an unconfigured ONU connected to a PON port is in the continuous mode, all the other unconfigured ONUs connected to this PON port will fail to be automatically discovered.

2.7 Remote Software Commissioning (PON)

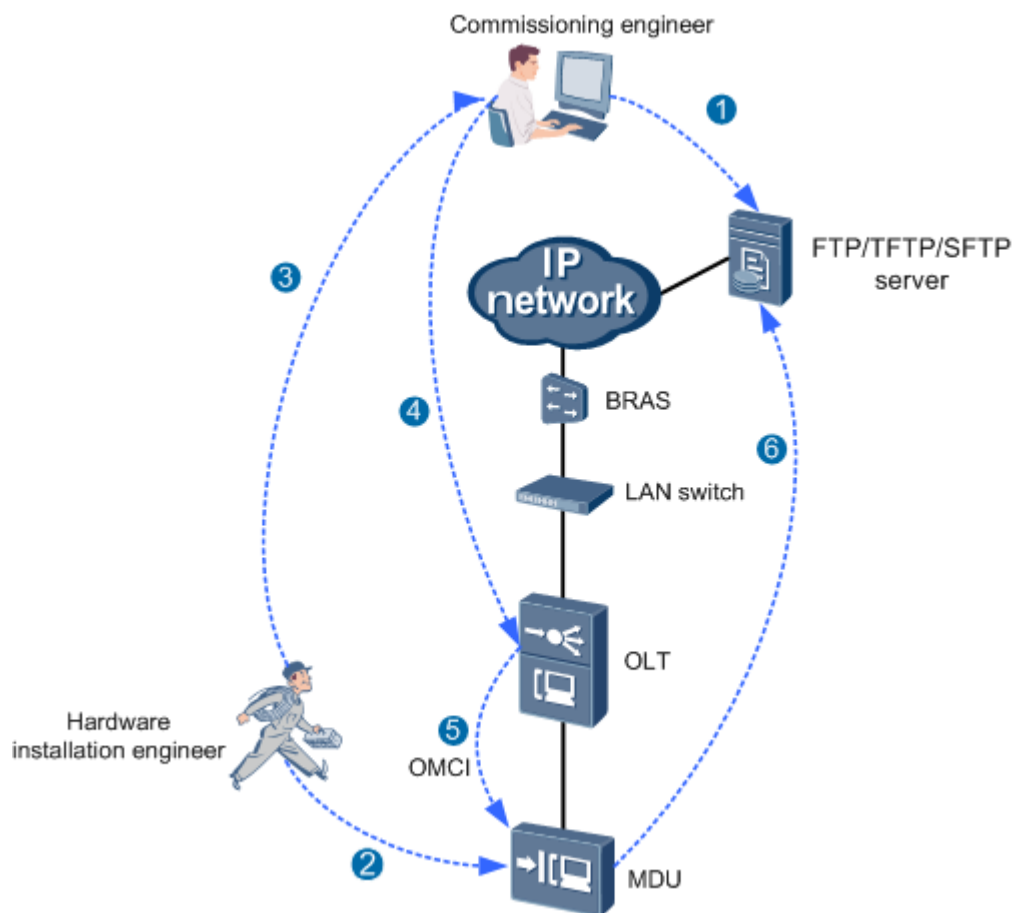
2.7.1 Introduction

During site deployment for a multi-dwelling unit (MDU) using PON upstream transmission, the MDU can be functional only after it is installed and manually commissioned by commissioning engineers onsite. To remove the need for onsite MDU commissioning, the MDU supports remote software commissioning. After the MDU is powered on, it automatically registers with the optical line terminal (OLT) and configures device data. This reduces site deployment costs.

2.7.2 Principles

Figure 2-37 shows the principles of remote software commissioning using PON upstream transmission.

Figure 2-37 Principles of remote software commissioning using PON upstream transmission



The process is as follows:

1. The commissioning engineer develops the automatic deployment policy file and configuration file, and uploads them to the FTP, TFTP or SFTP server.

 NOTE

The automatic deployment policy file must comply with the xxx.xml naming format. The file must contain the device type, control board, protocol for transferring the configuration file, IP address of the server, and configuration file name.

The configuration file name must be of string type.

One automatic deployment policy file applies to all MDUs in one site. An example automatic deployment policy file used in one site is as follows:

```
<config>
<deploy-version value="1"/>
<product name="MA5xxx">           // Device type
<mainboard name="H8xxxxxx">       // Control board
<mainboard name="H8xxxxxx">
<mainboard name="H8xxxxxx">
</load>
<transfer-protocol isSupport="1" protocol="ftp" username="user" password="user123" port=""
serveripaddr="10.10.10.10"/>
<init-load-script>
<common-script isSupport="1" value="script.txt"/>
</init-load-script>
</load>
</product>
</config>
```

- **protocol**: indicates the protocol for transferring the configuration file, which can be FTP, SFTP, or TFTP.

 NOTE

TFTP and FTP have security risks due to protocol limitations. You are advised to use SFTP.

- **username** and **password**: indicate the user name and password, respectively, when the configuration file is transferred using FTP or SFTP.
 - **port**: specifies a port. This parameter is required to configure only if the default port used by the transfer protocol must be changed.
 - **serveripaddr**: indicates the server IP address.
 - **value**: specifies a configuration file name. When the configuration file is transferred using FTP or SFTP, the configuration file name may contain the path where this file is stored.
2. The hardware installation engineer obtains the MDU from the warehouse and delivers it to the site. Then, the hardware installation engineer installs the MDU hardware, connects lines for the MDU, and powers on the MDU.
 3. The hardware installation engineer records and reports the SN of the MDU and site information to the commissioning engineer.
 4. A commissioning engineer adds an ONT offline, and configures the ONT IP address, service flows, and automatic deployment profile on the OLT.
 5. The OLT uses optical network terminal management and control interface (OMCI) to send the path where the automatic deployment policy file is stored to the MDU.
 6. After being powered on, the MDU receives the path where the automatic deployment policy file is stored and starts automatic device deployment.

 NOTE

The automatic device deployment takes effect on the MDU only if the MDU starts from an empty database. If the MDU database is not empty, run the **erase flash data** command to clear the database, or run the **load data** command to load an empty database to the MDU.

7. The MDU requests for the automatic deployment policy file from the FTP, TFTP or SFTP server and implements automatic device configuration based on the automatic deployment policy specified in the file.

2.7.3 Configuring Remote Software Commissioning (GPON)

The MDU supports remote software commissioning using GPON upstream transmission. After the MDU is powered on, it automatically registers with the OLT and configures device data.

Procedure

- Step 1** Run the **ont add** command add an ONT in offline mode.
- Step 2** Run the **rn ipconfig** command to set the IP address of this MDU.
- Step 3** Run the **service-port** command to create service flows.
- Step 4** Run the **rn deploy-profile add** command to configure an automatic deployment policy profile.

NOTE

In remote software commissioning, the **terminal user authentication-mode AAA domain-name** command needs to be set at the last of the configuration file. Otherwise, this command configuration fails to be issued.

- Step 5** Run the **rn deploy-config** command to bind the configured profile to the remote network (RN) equipment.
- Step 6** Run the **display rn deploy log** command to query automatic deployment results and failure causes if the deployment fails.

----End

Example

Example:

1. On port 0/14/0, set the IP address of the RN with ONT ID 0 to 192.168.1.33, subnet mask to 255.255.255.0, gateway IP address to 192.168.1.1, management VLAN ID to 1, and priority to 3.
2. Add an automatic deployment policy profile and bind the profile to port 0/14/0, where the profile ID is 1, file name is deploy-backup.xml, file server IP address is 10.10.10.10, file transfer protocol is SFTP, user name is user, and password is user123.

```
huawei(config)#interface gpon 0/14
huawei(config-if-gpon-0/14)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/14)#ont add 0 sn-auth 485754437B6F5130 snmp ont-lineprofile-id 1
huawei(config-if-gpon-0/14)#quit
huawei(config)#rn ipconfig 0/14/0 0 ip-address 192.168.1.33 mask 255.255.255.0 gateway 192.168.1.1
vlan 1 priority 3
huawei(config)#service-port vlan 1 gpon 0/14/0 ont 0 gempport 0 multi-service user-vlan 1
huawei(config)#rn deploy-profile add profile-id 1 filename deploy-backup.xml ip 10.10.10.10 sftp user
huawei(config)#rn deploy-config 0/14/0 0 profile-id 1
```

2.8 GPON Configuration Guide (Profile mode)

GPON configurations include the configurations on GPON profiles, ONTs, and ports. The following section describes configuration methods.

Context

The xPON mode includes two types: distributed (discrete) mode and profile mode. The differences between the two modes are as follows:

- In the distributing mode, ONTs cannot be added in batches. Instead, ONTs need to be configured one by one.
- In profile mode, you can pre-configure ONT line profiles and ONT service profiles and bind ONTs of the same configurations to the same profile to add them in batches, which significantly improves service provisioning efficiency.

The xPON mode is determined during site provisioning and will not be changed.

You can run the **display xpon mode** command to query the xPON mode of the current system.

2.8.1 Configuring a GPON ONT Profile (Profile mode)

In distributed mode, GPON ONT profiles include the GPON ONT capability profile and the GPON ONT alarm profile. In profile mode, GPON ONT profiles include DBA profiles, line profiles, service profiles, and alarm profiles. This topic describes how to configure these profiles.

Context

GPON ONT profiles contain the parameters required for configuring the GPON access service, of which,

- DBA profiles specify GPON traffic parameters. The DBA profile bound to an OLT enables the OLT to dynamically allocate bandwidths, improving upstream bandwidth utilization.
- In profile mode, the line profile is mainly used to configure the information related to DBA, T-CONT, and GEM port. The service profile is used to configure the actual ONT capability and the parameters related to services. The line profile is mandatory and the service profile is optional and dependent of service requirements. Set related attributes in line profile mode and service profile mode, and directly bind the ONT to the line profile and service profile.
- The GPON ONT alarm profile provides a series of alarm threshold parameters that are used for performance measurement and monitoring of activated ONU lines. After a GPON alarm profile is bound to an ONU, the ONU sends alarms to the log host and the NMS if the performance statistics of the line exceed the threshold that is specified in the profile.

NOTE

In this document, ONUs include MDUs and ONTs.

2.8.1.1 Configuring a DBA Profile

A DBA profile defines the traffic parameters of xPON and can be bound to a T-CONT to dynamically allocate the bandwidth and improve the usage of the upstream bandwidth.

Default Configuration

Table 2-6 lists the default settings of the DBA profiles.

Table 2-6 Default settings of the DBA profiles

Parameter	Default Setting	Remarks
Default DBA profile ID in the system	0-9	You can run the display dba-profile all command to query the parameter values of each default DBA profile.

Procedure

Step 1 Add a DBA profile.

Run the **dba-profile add** command to add a DBA profile. By default, the system provides DBA profiles 0–9 with typical traffic parameter values. The default profiles cannot be added or deleted.

 NOTE

- By default, a T-CONT is not bound to any DBA profile. You must bind a T-CONT to a DBA profile.
- When you add a DBA profile, the bandwidth value must be a multiple of 64. If you enter a bandwidth value not of a multiple of 64, the system adopts the closest multiple of 64 that is smaller than the value you enter.

Step 2 Query a DBA profile.

Run the **display dba-profile** command to query a DBA profile.

----End

Example

To add a DBA profile with the type of type3, set the profile name to DBA_100M and the required bandwidth to 100 Mbit/s, do as follows:

```
huawei(config)#dba-profile add profile-name DBA_100M type3 assure 102400 max 102400
huawei(config)#display dba-profile profile-name DBA_100M
```

2.8.1.2 Configuring a GPON ONT Line Profile (Profile Mode)

This topic describes how to configure a GPON ONT line profile and use it when adding an ONT. When an ONT is managed by OMCI or SNMP, the ONT must be bound to a GPON ONT line profile.

Default Configuration

Table 2-7 lists the default settings of a GPON ONT line profile.

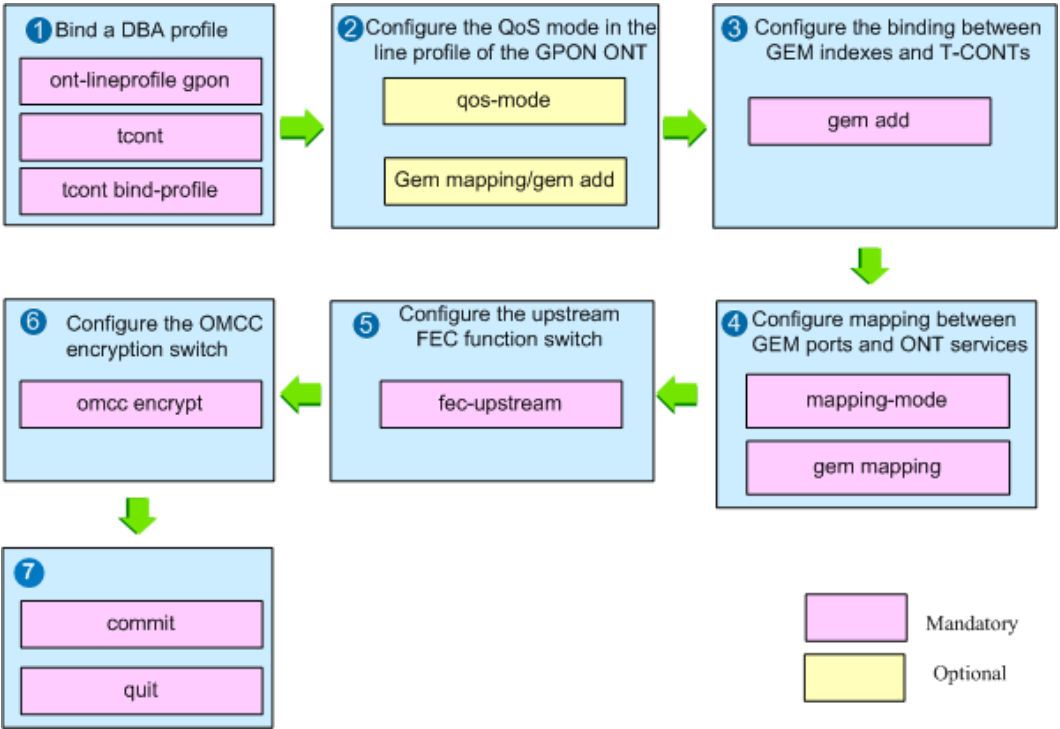
Table 2-7 Default settings of a GPON ONT line profile

Parameter	Default Setting
QoS mode	Priority-queue (PQ) scheduling mode
Mapping mode supported by the ONT	VLAN mapping mode
Upstream FEC switch	Disabled

Configuration Process

Figure 2-38 shows the process of configuring a GPON ONT line profile.

Figure 2-38 Process of configuring a GPON ONT line profile



Procedure

Step 1 Bind a T-CONT to a DBA profile.

- Run the **ont-lineprofile gpon** command to add a GPON ONT line profile and enter the GPON ONT line profile mode.

Regardless of whether the ONT is in the OMCI or SNMP management mode, the line profile must be configured for the ONT. After adding a GPON ONT

line profile, directly enter the GPON ONT line profile mode to configure the related attributes of the ONT line.

2. Use the following two methods to bind a DBA profile. Select either method as required. Both methods can coexist in the system.
 - In line profile mode:

This method is applicable to the scenario where the DBA profile is stable and the terminals are of a single type.

Run the **tcont** command to bind the T-CONT to a DBA profile. Ensure that [2.8.1.1 Configuring a DBA Profile](#) is completed before the configuration.
 - In GPON mode:

This method is applicable to the scenario where the DBA profile changes frequently and the terminals are of different types.

 - i. Run the **tcont** command to create a T-CONT, which is not bound to the DBA.
 - ii. After the configuration of a GPON ONT line profile is complete, enter the GPON mode. Run the **tcont bind-profile** command to bind the T-CONT to a DBA profile. Ensure that [2.8.1.1 Configuring a DBA Profile](#) is completed before the configuration.

NOTE

By default, T-CONT 0 of an ONT is used by OMCI and is bound to DBA profile 1. The configuration suggestions for the OMCI T-CONT are as follows:

- Do not modify the DBA profile bound to T-CONT 0. If you need to modify the profile, ensure that the fixed bandwidth of the modified profile is not lower than 1 Mbit/s.
- Do not bind a GEM port to the T-CONT. That is, ensure that the T-CONT does not carry any service.
- If the sum of the fixed bandwidth and assured bandwidth of the bound DBA profile is larger than the remaining bandwidth of the GPON port, the binding fails and the system displays a message "Failure: The bandwidth is not enough". In this case, you can run the **display port info** command to query the remaining bandwidth (Left guaranteed bandwidth (kbit/s)) of the GPON port, and then decrease the fixed bandwidth and assured bandwidth of the bound DBA profile accordingly.

Step 2 (Optional) Configure the QoS mode of the GPON ONT line profile.

Run the **qos-mode** command to configure the QoS mode of the GPON ONT line profile to be the same as the QoS mode of the GEM port. By default, the QoS mode of the ONT line profile is the PQ scheduling mode. The three QoS modes are as follows:

- flow-car: When this mode is selected, **flow-car** should be selected in the **gem mapping** command, and the maximum traffic depends on the traffic profile bound to the service port. Run the **traffic table ip** command to create a required traffic profile before the configuration.
- gem-car: When this mode is selected, **gem-car** should be selected in the **gem add** command, and the maximum traffic depends on the traffic profile bound to the GEM port.
- priority-queue: When this mode is selected, **priority-queue** should be selected in the **gem add** command. The system has eight default queues (0-7). Queue 7 has the highest priority and the traffic of this queue must be ensured first.

The maximum traffic depends on the DBA profile bound to the corresponding T-CONT.

Step 3 Configure the binding relationship between the GEM index and the T-CONT.

Run the **gem add** command to configure the binding relation between the GEM index and the T-CONT in the GPON ONT line profile.

The ONT can carry services only after the mapping between the GEM port and the T-CONT, and the mapping between the GEM port and the service port are configured for the ONT. A correct attribute should be selected for **service-type** based on the service type. Select **eth** when the Ethernet service is carried. Select **tdm** when the TDM service is carried.

Step 4 Configure the mapping between the GEM port and the ONT-side service.

Run the **gem mapping** command to set up the mapping between the GEM port and the ONT-side service.

Before the configuration, run the **mapping-mode** command to configure the mapping mode supported by the ONT to be the same as the configured mapping mode between the GEM port and the ONT-side service. By default, the ONT supports the VLAN mapping mode.

Mapping mode description

Parameter	Description	
	Mapping Mode	Mandatory Configuration Item for the gem mapping Command
vlan	Indicates the VLAN mapping. The VLAN mapping is the default mapping mode.	vlan
priority	Indicates the 802.1p priority mapping.	priority
vlan-priority	Indicates the VLAN + 802.1p priority mapping.	vlan and priority
port	Indicates the port ID mapping.	<i>ont-portid</i>
port-vlan	Indicates the port ID+VLAN mapping.	<i>ont-portid</i> and vlan
port-priority	Indicates the port ID+802.1p priority mapping.	<i>ont-portid</i> and priority
port-vlan-priority	Indicates the port ID+VLAN +802.1p priority mapping.	<i>ont-portid</i> , vlan , and priority

Parameter	Description	
	Mapping Mode	Mandatory Configuration Item for the gem mapping Command
iptos	Indicates the IP ToS field mapping. IP ToS is the ToS priority of the IP packet header. This mapping is based on the priority of the ToS domain and is considered as the extension of the 802.1p priority.	priority
vlan-iptos	Indicates the VLAN+IP ToS field mapping.	vlan and priority

- The mapping modes of the ETH port and the MOCA port are as follows:
 - If the port is specified and then the VLAN is further specified, the mapping mode should be configured to **port-vlan** in the **mapping-mode** command. That is, the port+VLAN mapping mode is used.
 - If the port is specified and then the priority is further specified, the mapping mode should be configured to **port-priority** in the **mapping-mode** command. That is, the port+priority mapping mode is used.
 - If the port and the VLAN are specified and then the priority is further specified, the mapping mode should be configured to **port-vlan-priority** in the **mapping-mode** command. That is, the port+VLAN+priority mapping mode is used.
- As a special port, the IPHOST or E1 port is not restricted by the ONT mapping mode.

When the mapping mode is **vlan-priority** or **port-vlan-priority**,

- If a GEM port is mapped to multiple VLANs, any of these VLANs cannot map to any other GEM port.
- If a VLAN is mapped to multiple GEM ports, any of these GEM ports cannot map to any other VLAN.

Step 5 Configure the upstream FEC switch.

Run the **fec-upstream** command to configure the upstream FEC switch of the GPON ONT line profile. By default, this switch is disabled.

In the FEC check, the system inserts redundancy data into normal packets. In this way, the line has certain error tolerant function, but certain bandwidth resources are wasted. Enabling the FEC function enhances the error tolerant capability of the line but occupies certain bandwidth. Therefore, determine whether to enable the FEC function based on the actual line planning.

Step 6 Configure the status of the ONT Management and Control Channel (OMCC) encryption switch.

Run the **omcc encrypt** command to configure the status of the OMCC encryption switch. When OMCC encryption is enabled, OMCC packets are encrypted; otherwise, OMCC packets are not encrypted. By default, this switch is disabled.

Step 7 Run the **commit** command to make the parameters of the profile take effect. The configuration of a line profile takes effect only after you perform this operation.

 NOTE

If this profile is not bound, all the parameters that are configured take effect when the profile is bound. If this profile is already bound, the configuration takes effect on all ONTs bound to this profile immediately.

Step 8 Run the **quit** command to return to the global configuration mode.

----End

Example

Example: Add GPON ONT line profile 5. Create a channel for carrying the ETH service. Set T-CONT to 1, bind DBA profile 12, set GEM index to 1, bind it to T-CONT 1, and map it to ETH port 1 of the ONT. Use the QoS policy of controlling the traffic based on GEM ports, and bind the GEM port to default traffic profile 6.

```
huawei(config)#ont-lineprofile gpon profile-id 5
huawei(config-gpon-lineprofile-5)#tcont 1 dba-profile-id 12
huawei(config-gpon-lineprofile-5)#qos-mode gem-car
huawei(config-gpon-lineprofile-5)#gem add 1 eth tcont 1 gem-car 6
huawei(config-gpon-lineprofile-5)#mapping-mode port
huawei(config-gpon-lineprofile-5)#gem mapping 1 0 eth 1
huawei(config-gpon-lineprofile-5)#commit
huawei(config-gpon-lineprofile-5)#quit
```

To modify GPON ONT line profile 5, and change the DBA profile bound to T-CONT 1 from DBA profile 12 to DBA profile 10, do as follows:

```
huawei(config)#ont-lineprofile gpon profile-id 5
huawei(config-gpon-lineprofile-5)#tcont 1 dba-profile-id 10
huawei(config-gpon-lineprofile-5)#commit
huawei(config-gpon-lineprofile-5)#quit
```

To modify GPON ONT line profile 5, bind GEM index 1 to T-CONT 2 (originally bound to T-CONT 3), and map GEM index 1 to ETH port 2 on the ONT, do as follows:

 NOTE

- To modify the binding between a GEM index and a T-CONT, you need to delete the existing binding entry and then bind the GEM index to the new T-CONT.
- If the GEM index is used by a service port, run the **undo service-port** command to delete the service port before deleting the GEM index.

```
huawei(config)#ont-lineprofile gpon profile-id 5
huawei(config-gpon-lineprofile-5)#undo gem mapping 1 0
huawei(config-gpon-lineprofile-5)#gem delete 1
huawei(config-gpon-lineprofile-5)#gem add 1 eth tcont 2
huawei(config-gpon-lineprofile-5)#gem mapping 1 0 eth 2
huawei(config-gpon-lineprofile-5)#commit
huawei(config-gpon-lineprofile-5)#quit
```

2.8.1.3 Configuring a GPON ONT Service Profile (Profile Mode)

The GPON ONT service profile provides a channel for configuring the service of the ONT managed in the OMCI mode. The ONT (such as the MDU) managed in

the SNMP mode does not support the configuration of the GPON ONT service profile. To configure the service of the ONT (such as the MDU) managed in the SNMP mode, you need to log in to the ONT.

Default Configuration

Table 2-8 lists the default settings of the GPON ONT service profile.

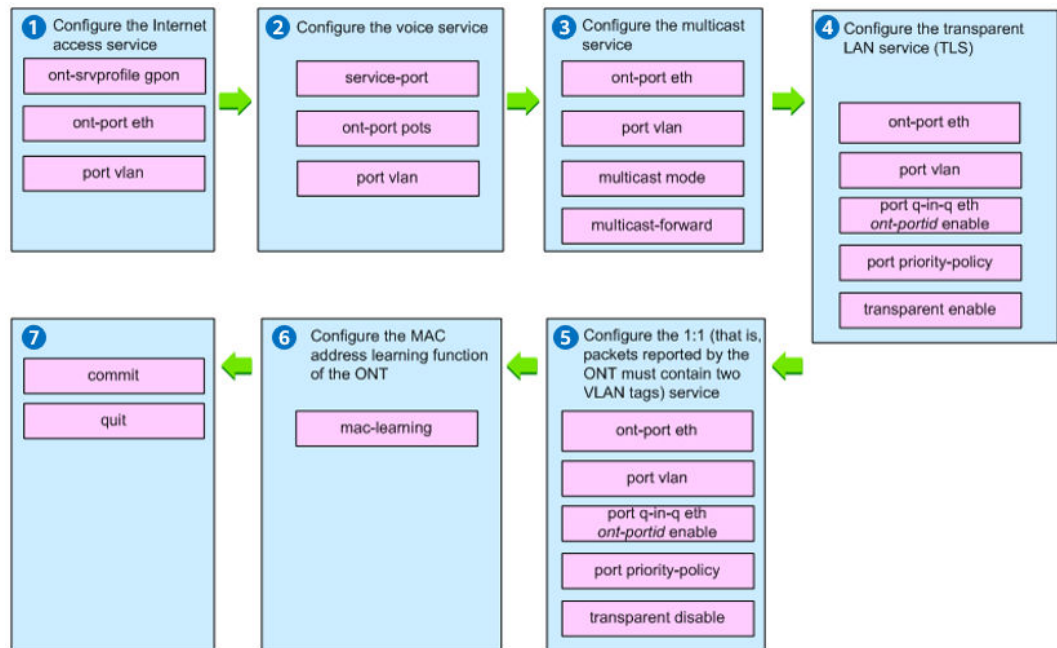
Table 2-8 Default settings of the GPON ONT service profile

Parameter	Default Setting
Multicast mode of the ONT	Unconcern (the OLT does not perform any processing)
Mode for the ONT to process the VLAN tag of the multicast data packets	Unconcern
Source of the priority copied for the upstream packets on the ONT port	Unconcern
QinQ attribute for the Ethernet port of the ONT	Unconcern
Transparent transmission function of the ONT	Disabled
MAC address learning function of the ONT	Enabled

Configuration Process

Figure 2-39 shows the process of configuring a GPON ONT service profile.

Figure 2-39 Process of configuring a GPON ONT service profile



Procedure

Step 1 Configure the Internet access service.

1. Run the **ont-srvprofile gpon** command to add a GPON ONT service profile, and then enter the GPON ONT service profile mode. If the ONT management mode is the SNMP mode, you do not need to configure the service profile. After adding a GPON ONT service profile, directly enter the GPON ONT service profile mode to configure the related items. Select the configuration items according to the service requirements.
2. Run the **ont-port eth** command to configure the port capability set of the ONT. The capability set plans the number of various ports supported by the ONT. The port capability set of the ONT must be the same as the actual capability set of the ONT.

If the port capability set of an ONT is set to **adaptive**, the system automatically adapts to the actual capabilities of the online ONT. By default, 8 ETH ports and 1 IPHOST port are displayed.

3. Run the **port vlan(gpon profile)** command to configure the port VLAN of the ONT.

VLAN Configuration Description

Table 2-9 Packet Processing Policy

Transparent transmission based on the port	Transparently transmit the tagged packet directly.	Add a native VLAN tag to the untagged packet.	Transparently transmit the untagged packet directly.
QinQ based on the port	Add a native VLAN tag to the tagged packet. NOTE The native VLAN item must be set to concern by running the native vlan(gpon) command. You can run the display ont-srvprofile gpon command to query the status of the native VLAN item.	Add a native VLAN tag to the untagged packet.	Add a native VLAN tag to the untagged packet.
Translation based on the VLAN	- When only parameter <i>SVLAN</i> is configured, it indicates that CVLAN is the same as SVLAN. - If the VLAN of the packet is <i>user-vlanid</i>, the VLAN of the packet will be translated. - Otherwise, the packet will be discarded.	The VLAN translation pair for untagged packets cannot be configured when the native VLAN is enabled. A native VLAN tag is added to the untagged packet and the VLAN translation pair will not be checked. That is, regardless of whether the native VLAN is in the VLAN translation pair or not, packets are allowed to pass through the VLAN.	- The native VLAN cannot be enabled for the whole ONT when the VLAN translation pair for untagged packets is configured. - Otherwise, the packet will be discarded.

- The transparent transmission mode of a port conflicts with the transparent transmission mode of the VLAN of the port. That is, after

setting the transparent transmission mode of a port, you need not set the transparent transmission mode of the VLAN of the port.

- In single-bridge mode, the transparent transmission mode of the VLAN of multiple ports must be set to be the same as the transparent transmission mode of these ports. In multiple-bridge mode, the transparent transmission modes of the VLAN and the ports can be different.
- When you configure the transparent transmission mode of the untagged packets by using QinQ, this command cannot be directly used to configure the transparent transmission mode of the untagged packets.
- The Ethernet port and VDSL port of an ONT can be configured to add a VLAN QinQ tag to untagged packets on the user side based on the packet encapsulation type. In this case, the Native VLAN item in the **ont native-vlan(distributing-mode)** command must be set to unconcern.
- Configure whether the ONT concerns the Native VLAN in the ONT service profile. By default, the ONT concerns the Native VLAN item.
 - You can run the **ont port native-vlan(gpon)** command to configure the native VLAN of an ONT port only when the native VLAN is set to concern. If the native VLAN of an ONT port is set to a non-default value, the native VLAN cannot be set to unconcern. To query the VLAN configuration of an ONT port, run the **display ont port vlan(distributing-mode)** command.
 - You can run the **port q-in-q** command to configure the QinQ attribute of the Ethernet port on an ONT only when the Native VLAN is set to concern. You cannot change the Native VLAN item to unconcern when the QinQ attribute of the Ethernet port on the ONT is enabled. You can run the **display ont-srvprofile gpon** command to query the QinQ attribute of an ONT port.
 - You can run the **ont port vlan(distributing-mode)** command to configure the policy of processing untagged packets on an ONT port only when the Native VLAN is set to unconcern. When the policy of processing untagged packets on an ONT port is configured, the Native VLAN item cannot be set to concern. You can run the **display ont port vlan(distributing-mode)** command to query the policy for processing untagged packets on an ONT port.

Step 2 Configure the voice service.

NOTE

The voice service of the ONT is configured by issuing an XML file to the NMS and the OLT performs only transparent transmission. You only need to run the **service-port** command to create a service port carrying the voice service.

1. Run the **ont-port pots** command to configure the port capability set of the ONT. The port capability set in the ONT service profile must be the same as the actual ONT capability set.

If the port capability set of an ONT is set to **adaptive**, the system automatically adapts to the actual capabilities of the online ONT. By default, 8 ETH ports and 1 IPHOST port are displayed.

2. Run the **port vlan(gpon profile)** command to configure the port VLAN of the ONT.

VLAN Configuration Description

Step 3 Configure the multicast service.

1. Run the **ont-port eth** command to configure the port capability set of the ONT. The port capability set in the ONT service profile must be the same as the actual ONT capability set.

If the port capability set of an ONT is set to **adaptive**, the system automatically adapts to the actual capabilities of the online ONT. By default, 8 ETH ports and 1 IPHOST port are displayed.

2. Run the **port vlan(gpon profile)** command to configure the port VLAN of the ONT.

VLAN Configuration Description

3. Run the **multicast mode** command to configure the multicast mode of the ONT. By default, the multicast mode of the ONT is **unconcern**.
 - Unconcern: indicates the unconcern mode. After this mode is selected, the OLT does not limit the multicast mode, and the multicast mode on the OLT automatically matches the multicast mode on the ONT.
 - Icmp-snooping: IGMP snooping obtains the related information and maintains the multicast forwarding entries by listening to the IGMP packets in the communication between the user and the multicast router.
 - Olt-control: indicates the dynamic controllable multicast mode. A multicast forwarding entry can be created for the multicast join packet of the user only after the packet passes the authentication. This mode is supported by the MDU, but is not supported by the ONT.
4. Run the **multicast-forward** command to configure the processing mode on the VLAN tag of the multicast data packets for the ONT. By default, the multicast forwarding mode of the ONT is **unconcern**.
 - Unconcern: indicates the unconcern forwarding mode. After this mode is selected, the OLT does not process the VLAN tag of the multicast data packets.
 - tag: Sets the multicast forwarding mode to with VLAN tag. To transparently transmit the VLAN tag of the multicast packets, select **transparent**. To translate the VLAN tag of multicast packets, select **translation** and configure the translated VLAN tag.
 - Untag: Set the multicast forwarding mode not to contain the VLAN tag.

Step 4 Configure the transparent LAN service (TLS).

1. Run the **ont-port eth** command to configure the port capability set of the ONT. The port capability set in the ONT service profile must be the same as the actual ONT capability set.

If the port capability set of an ONT is set to **adaptive**, the system automatically adapts to the actual capabilities of the online ONT. By default, 8 ETH ports and 1 IPHOST port are displayed.

2. Run the **port vlan(gpon profile)** command to configure the port VLAN of the ONT.

VLAN Configuration Description

3. Run the **port q-in-q eth ont-portid enable** command to enable the QinQ function of the Ethernet port on the ONT. By default, the QinQ function of the Ethernet port on the ONT is unconcerned.
4. Run the **port priority-policy** command to configure the source of the priority copied for the upstream packets on the ONT port. By default, the source of the priority copied for the upstream packets on the ONT Ethernet port is unconcerned.
 - unconcern: The upstream priority copy source of the ONT Ethernet port is not concerned.
 - assigned: Specifies the priority. Run the **ont port native-vlan** command to specify the **priority** of the port.
 - copy-cos: Copy the priority. Copy the priority from C-TAG.
5. Run the **transparent enable** command to enable the transparent transmission function of the ONT. By default, the transparent transmission function of the ONT is disabled. After the transparent transmission function of the ONT is enabled, all packets (including service packets and protocol packets) are transparently transmitted by the ONT.

NOTE

The service port for the TLS service must also be of the TLS type. Run the **service-port** command to create a service port of the TLS type. Select **other-all** for the multi-service type.

Step 5 Configure the 1:1 (that is, packets reported by the ONT must contain two VLAN tags) service.

1. Run the **ont-port eth** command to configure the port capability set of the ONT. The port capability set in the ONT service profile must be the same as the actual ONT capability set.

If the port capability set of an ONT is set to **adaptive**, the system automatically adapts to the actual capabilities of the online ONT. By default, 8 ETH ports and 1 IPHOST port are displayed.
2. Run the **port vlan(gpon profile)** command to configure the port VLAN of the ONT.

VLAN Configuration Description

3. Run the **port q-in-q eth ont-portid enable** command to enable the QinQ function of the Ethernet port on the ONT. By default, the QinQ function of the Ethernet port on the ONT is unconcerned.
4. Run the **port priority-policy** command to configure the source of the priority copied for the upstream packets on the ONT port. By default, the source of the priority copied for the upstream packets on the ONT Ethernet port is unconcerned.
 - Unconcern: The source of the priority copied for the upstream packets on the Ethernet port of the ONT is not concerned.
 - assigned: Specifies the priority. Run the **ont port native-vlan** command to specify the **priority** of the port.
 - Copy-cos: Copy the priority. Copy the priority from C-TAG.
5. Run the **transparent disable** command to disable the transparent transmission function of the ONT.

Step 6 Run the **mac-learning** command to configure the MAC address learning function of the ONT. This function is enabled by default.

Step 7 Run the **commit** command to make the parameters of the profile take effect. The configuration of a service profile takes effect only after you perform this operation.

 NOTE

If this profile is not bound, all the parameters that are configured take effect when the profile is bound. If this profile is already bound, the configuration takes effect on all ONTs bound to this profile immediately.

Step 8 Run the **quit** command to return to the global config mode.

----End

Example

Add GPON ONT service profile 5 for the Internet access service. The ONT supports 4 ETH ports. The VLAN ID of the ETH port is 10. Do as follows:

```
huawei(config)#ont-srvprofile gpon profile-id 5
huawei(config-gpon-srvprofile-5)#ont-port eth adaptive
huawei(config-gpon-srvprofile-5)#port vlan eth 1-4 10
huawei(config-gpon-srvprofile-5)#commit
huawei(config-gpon-srvprofile-5)#quit
```

Add GPON ONT service profile 6 for the multicast service. The ONT supports 4 ETH ports. The VLAN ID of the ETH port is 100. The multicast mode of the ONT is the controllable multicast mode. The STB supports only VLAN tag 841, and multicast VLAN tag needs to be translated. Do as follows:

```
huawei(config)#ont-srvprofile gpon profile-id 6
huawei(config-gpon-srvprofile-6)#ont-port eth adaptive
huawei(config-gpon-srvprofile-6)#port vlan eth 1-4 100
huawei(config-gpon-srvprofile-6)#multicast mode olt-control
huawei(config-gpon-srvprofile-6)#multicast-forward tag translation 841
huawei(config-gpon-srvprofile-6)#commit
huawei(config-gpon-srvprofile-6)#quit
```

2.8.1.4 Configuring a GPON ONT Alarm Profile

This topic describes how to add an alarm profile, and configure most of the performance parameters for various ONT lines as a profile. After the alarm profile is configured and bound successfully, the ONT can directly use the profile when it is activated.

Context

An ONT alarm profile defines a series of alarm thresholds that are used to monitor the performance of an activated ONT line. When the statistics result of a parameter reaches the alarm threshold, the NE is notified and an alarm is sent to the log server and the NMS.

The system has a default alarm threshold profile with ID 1. This profile cannot be deleted but can be modified.

Procedure

Step 1 Run the **gpon alarm-profile add** command to add a GPON ONT alarm profile.

If default alarm thresholds are used in a new alarm profile, the system does not report any alarm.

Step 2 Run the **display gpon alarm-profile** command to query the alarm profile.

----End

Example

To add GPON ONT alarm profile 5, set the alarm threshold for the packet loss of the GEM port to 10, set the alarm threshold for the number of mis-transmitted packets to 30, and use the default value 0 for all other thresholds, do as follows:

```
huawei(config)#gpon alarm-profile add profile-id 5
{ <cr>|profile-name<K> }:
```

Command:

```
gpon alarm-profile add profile-id 5
Press 'Q' or 'q' to quit input
> GEM port loss of packets threshold (0~100)[0]:10
> GEM port misinserted packets threshold (0~100)[0]:30
> GEM port impaired blocks threshold (0~100)[0]:0
> Ethernet FCS errors threshold (0~100)[0]:
> Ethernet excessive collision count threshold (0~100)[0]:
> Ethernet late collision count threshold (0~100)[0]:
> Too long Ethernet frames threshold (0~100)[0]:
> Ethernet buffer (Rx) overflows threshold (0~100)[0]:
> Ethernet buffer (Tx) overflows threshold (0~100)[0]:
> Ethernet single collision frame count threshold (0~100)[0]:
> Ethernet multiple collisions frame count threshold (0~100)[0]:
> Ethernet SQE count threshold (0~100)[0]:
> Ethernet deferred transmission count threshold (0~100)[0]:
> Ethernet internal MAC Tx errors threshold (0~100)[0]:
> Ethernet carrier sense errors threshold (0~100)[0]:
> Ethernet alignment errors threshold (0~100)[0]:
> Ethernet internal MAC Rx errors threshold (0~100)[0]:
> PPPOE filtered frames threshold (0~100)[0]:
> MAC bridge port discarded frames due to delay threshold (0~100)[0]:
> MAC bridge port MTU exceeded discard frames threshold (0~100)[0]:
> MAC bridge port received incorrect frames threshold (0~100)[0]:
> CES general error time threshold(0~100)[0]:
> CES severely time threshold(0~100)[0]:
> CES bursty time threshold(0~100)[0]:
> CES controlled slip threshold(0~100)[0]:
> CES unavailable time threshold(0~100)[0]:
> Drop events threshold(0~100)[0]:
> Undersize packets threshold(0~100)[0]:
> Fragments threshold(0~100)[0]:
> Jabbers threshold(0~100)[0]:
> Failed signal of ONT threshold(Format:1e-x, x: 3~8)[3]:
> Degraded signal of ONT threshold(Format:1e-x, x: 4~9)[4]:
> FEC uncorrectable code words threshold(0~1101600000)[0]:
> FEC correctable code words threshold(0~1101600000)[0]:
> Upstream PQ discarded byte alarm threshold(0~65535)[0]:
> Downstream PQ discarded byte alarm threshold(0~65535)[0]:
> Encryption key errors threshold(0~100)[0]:
> XGEM key errors threshold(0~100)[0]:
> XGEM HEC error count threshold(0~100)[0]:
```

Adding an alarm profile succeeded
Profile ID : 5
Profile name: alarm-profile_5

2.8.2 Configuring a GPON ONT (Profile Mode)

The OLT provides end users with services through the ONT. The OLT can manage the ONT and the ONT can work in the normal state only after the channel between the OLT and the ONT is available.

Prerequisites

The GPON ONT profile is already created.

- For an ONT, [2.8.1.2 Configuring a GPON ONT Line Profile \(Profile Mode\)](#), [2.8.1.3 Configuring a GPON ONT Service Profile \(Profile Mode\)](#), and [2.8.1.4 Configuring a GPON ONT Alarm Profile](#) are already completed.
- For an MDU or ONU, [2.8.1.2 Configuring a GPON ONT Line Profile \(Profile Mode\)](#) and [2.8.1.4 Configuring a GPON ONT Alarm Profile](#) are already completed.

Context

The OLT uses the ONT Management and Control Interface (OMCI) protocol to manage and configure the GPON ONT, and supports the offline configuration of the ONT.

In the profile mode, the related configuration of the GPON ONT is already integrated in the service profile and the line profile. When adding an ONT, you only need to bind the ONT with the corresponding service profile and line profile.

[Table 2-10](#) lists the default settings of the GPON ONT.

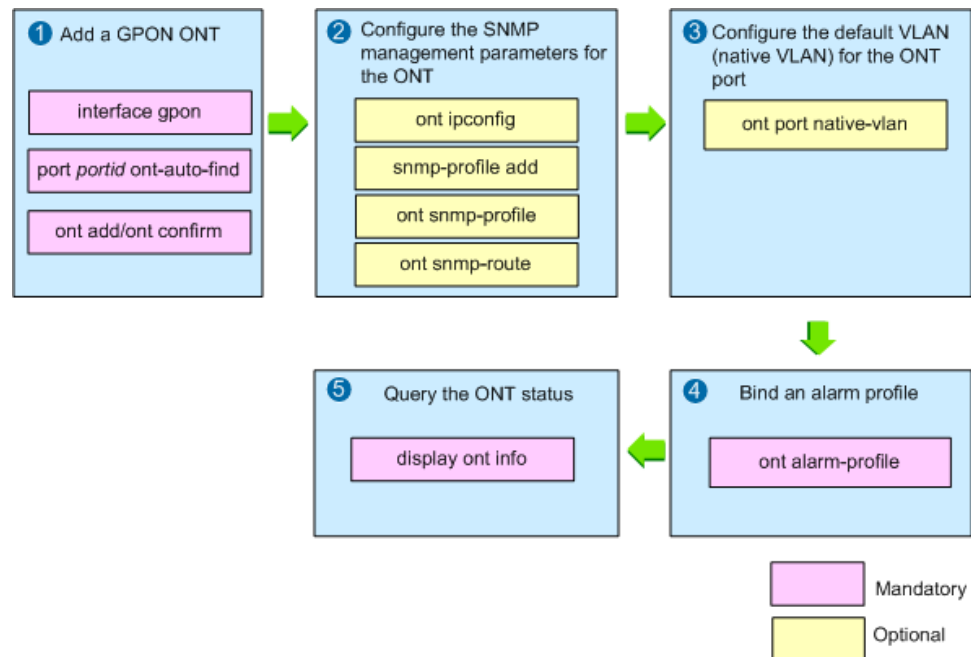
Table 2-10 Default settings of the GPON ONT

Parameter	Default Setting
ONT auto-find function of a GPON port	Disabled
ONT status after an ONT is added	Activated
Default VLAN of the ONT port	1

Configuration Process

[Figure 2-40](#) shows the process of configuring a GPON ONT.

Figure 2-40 Process of configuring a GPON ONT



Procedure

Step 1 Add a GPON ONT.

1. Run the **interface gpon** command to enter the GPON mode.
2. Run the **port portid ont-auto-find** command to enable the auto discovery function of the ONT. After the function is enabled, you can add an ONT according to the information reported by the system. By default, the ONT auto discovery function of a GPON port is disabled.

NOTE

An auto discovery ONT is in the auto discovery state. The auto discovery ONT can work in the normal state only after it is confirmed or added.

3. Run the **ont add** command to add an ONT offline, or run the **ont confirm** command to confirm the auto discovery ONT.

When ONTs are added or confirmed, the system provides four authentication modes: SN, password, SN+password, LOID+CHECKCODE.

- SN authentication: The OLT detects the serial number (SN) reported by an ONT. If the SN is consistent with the OLT configuration, authentication is passed and the ONT goes online. This mode requires recording all ONT SNs. Hence, it is used to confirm auto discovery ONTs and is not applicable to adding ONTs in batches.
- Password authentication: The OLT detects the password reported by an ONT. If the password is consistent with the OLT configuration, the ONT goes online normally. This mode requires planning ONT passwords and does not require manually recording ONT SNs. Hence, it is applicable to adding ONTs in batches. The password authentication provides two discovery modes: always-on and once-on.

- always-on: After first password authentication is passed, no SN is allocated and password authentication is always used in subsequent authentications. This discovery mode is easy for future maintenance. In the always-on discovery mode, configurations do not need to be modified when an ONT is replaced and only the password is required. The always-on discovery mode has lower security. If other users know the password, the users will illegally have service permissions.
- once-on: Password authentication is used for the first authentication. After the authentication is successful, the SN is automatically matched. The SN+password authentication mode is used for subsequent authentications. The ONT can go online only when both the password and SN are correct. The once-on authentication mode has high security. After an ONT is replaced or the password is mistakenly changed, the ONT needs to run the **ont re-discovery** command to be re-discovered, which requires more maintenance effort.
- SN+password authentication: The OLT detects the password and SN reported by an ONT. If the password and SN are consistent with the OLT configuration, the ONT goes online normally. This authentication mode has the highest security but it requires manually recording ONT SNs.
- LOID+CHECKCODE authentication: defined by a telecom operator. In this authentication mode, LOID has 24 bytes, and CHECKCODE has 12 bytes and is optional. Whether 24 bytes or 36 bytes are used for authentication depends on data planning, which is unified over the entire network. The OLT determines whether LOID+CHECKCODE reported by the ONT is the same as the configured one. If they are the same, the ONT authentication is passed. If they are different, the OLT obtains the ONT password and compares it with the last 10 bytes of the LOID. If they are the same, the ONT authentication is also passed. This operation is for compatibility with the ONTs using password authentication.

Adding ONTs in offline mode is applicable to the batch deployment scenario. All ONTs are added to the OLT to complete service provisioning beforehand. When a user subscribes to the service, an installation engineer takes an ONT to the user's house and completes configurations. After the ONT goes online and passes authentication, the service is provisioned. Generally, the password authentication mode or LOID authentication mode is used to confirm an ONT.

Adding ONTs in auto discovery mode is applicable to the scenario where a small number of ONTs are added. When users subscribe to the service, installation engineers take ONTs to the users' houses. After the ONTs go online, the OLT confirms the ONTs one by one. Generally, the MAC address authentication mode is used to confirm the ONTs.

 NOTE

- If the ONU is an independent NE and is directly managed by the NMS through the SNMP management mode, select the SNMP management mode. For this mode, you only need to configure the parameters for the GPON line and the parameters for the management channel on the OLT. You only need to bind the ONU with a line profile.
- If the ONU is not an independent NE and all its configuration data is issued by the OLT through OMCI, select the OMCI management mode. For this mode, you need to configure all parameters (including line parameters, UNI port parameters, and service parameters) that are required for the ONU on the OLT. Configuring management channel parameters is not supported. You need to bind the ONT with a line profile and a service profile.
- Generally, the ONT management mode is set to the OMCI mode. You need to bind the ONT with a line profile and a service profile.

Step 2 (Optional) Configure the SNMP management parameters for the ONT. When the ONT management mode is the SNMP mode, you need to configure the SNMP management parameters for the ONT. The procedure is as follows:

1. Run the **ont ipconfig** command to configure the management IP address of the ONT. The IP address should not be in the same subnet for the IP address of the VLAN port.
2. Run the **ont snmp-profile** command to bind an SNMP profile to the ONT. Before running this command, ensure that an SNMP profile has been added by running the **snmp-profile add** command.
3. Run the **ont snmp-route** command to configure the static route of the NMS server. That is, configure the IP address of the next hop.

Step 3 Configure the default VLAN (native VLAN) for the ONT port.

Run the **ont port native-vlan** command to configure the default VLAN for the ONT port. By default, the default VLAN ID of the ONT port is 1.

- If the packets reported from a user (such a PC) to the ONT are untagged, the packets are tagged with the default VLAN of the port on the ONT and then reported to the OLT.
- If the packets reported from a user to the ONT are tagged, you need to configure the port VLAN of the ONT to be the same as the VLAN in the user tag. The packets are not tagged with the default VLAN of the port on the ONT but are reported to the OLT with the user tag.

Step 4 Bind an alarm profile.

Run the **ont alarm-profile** command to bind an alarm profile. Ensure that [2.8.1.4 Configuring a GPON ONT Alarm Profile](#) is completed before the configuration.

Step 5 Query the ONT status.

Run the **display ont info** command to query the ONT running status, configuration status, and matching status.

----End

Example

To add five ONTs in offline mode with password authentication mode (ONT passwords are 0100000001-0100000005), set the discovery mode of password

authentication to always-on, and bind line profile 10 and service profile 10, do as follows:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 password-auth 0100000001 always-on omci ont-lineprofile-id 10
ont-srvprofile-id 10
huawei(config-if-gpon-0/1)#ont add 1 password-auth 0100000002 always-on omci ont-lineprofile-id 10
ont-srvprofile-id 10
huawei(config-if-gpon-0/1)#ont add 2 password-auth 0100000003 always-on omci ont-lineprofile-id 10
ont-srvprofile-id 10
huawei(config-if-gpon-0/1)#ont add 3 password-auth 0100000004 always-on omci ont-lineprofile-id 10
ont-srvprofile-id 10
huawei(config-if-gpon-0/1)#ont add 4 password-auth 0100000005 always-on omci ont-lineprofile-id 10
ont-srvprofile-id 10
```

To add an ONT that is managed by the OLT through the OMCI protocol, confirm this ONT according to the SN 3230313185885B41 automatically reported by the system, and bind the ONT with line profile 3 and service profile 3 that match the ONT, do as follows:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/1)#ont confirm 0 sn-auth 3230313185885B41 omci ont-lineprofile-id 3 ont-
srvprofile-id 3
```

To add an ONU that is managed as an independent NE and whose SN is known as 3230313185885641, bind the ONU with line profile 4 that matches the ONU, configure the NMS parameters for the ONU, and set the management VLAN to 100, do as follows:

```
huawei(config)#snmp-profile add profile-id 1 v3 public private 10.10.10.53 161 bodyname
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 2 sn-auth 3230313185885641 snmp ont-lineprofile-id 4
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 static ip-address 10.20.20.20 mask 255.255.255.0 gateway
10.10.20.1 vlan 100
huawei(config-if-gpon-0/1)#ont snmp-profile 0 2 profile-id 1
huawei(config-if-gpon-0/1)#ont snmp-route 0 2 ip-address 10.20.20.19 mask 255.255.255.0 next-hop
10.20.20.100
```

2.8.3 Configuring a GPON Port

To work normally and carry the service, a GPON port must be enabled first. This topic describes how to enable a GPON port and configure related attributes of the port.

Default Configuration

Table 2-11 lists the default settings of the GPON port.

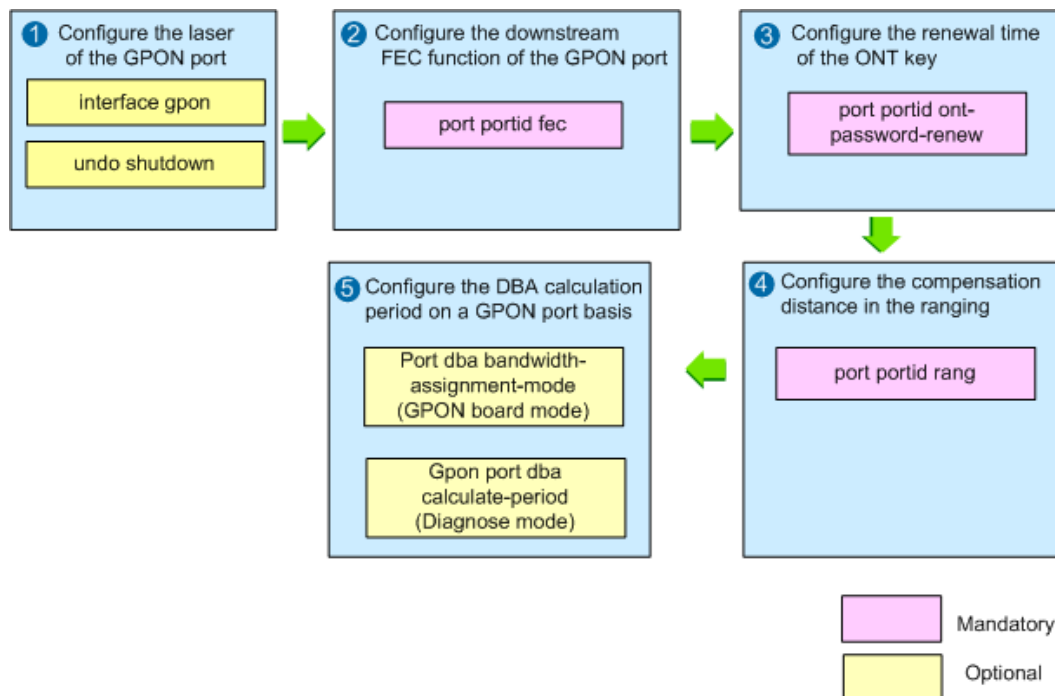
Table 2-11 Default settings of the GPON port

Parameter	Default Setting
GPON port	Enabled
Downstream FEC function of the GPON port	Disabled
Compensation distance range of the GPON port ranging	Minimum logical distance: 0 km; maximum logical distance: 20 km

Configuration Process

Figure 2-41 shows the process of configuring a GPON Port.

Figure 2-41 Process of configuring a GPON Port



Procedure

Step 1 (Optional) Configure the optical port switch.

1. Run the **interface gpon** command to enter GPON mode.
2. Run the **undo shutdown** command to enable the laser of the GPON port. By default, the laser of the GPON port is enabled and the GPON port is available. In this case, skip this step.

NOTICE

- If an optical port is not required, run the **shutdown** command to disable the optical port.
- Disabling a PON port that carries services will cause the interruption of such services.

Step 2 Enables or disables the downstream FEC function of a port.

Run the **port portid fec** command to configure the FEC function of the GPON port. By default, the function is disabled.

 NOTE

- FEC is to insert redundant data into normal packets so that the line has certain error tolerance. Some bandwidth, however, must be consumed. Enabling FEC enhances the error correction capability of the line but at the same time occupies certain bandwidth. Determine whether to enable FEC according to the actual line planning.
- If a large number of ONTs are online, enabling the FEC function of the optical port may cause some ONTs to go offline. Therefore, it is recommended that you do not configure the FEC function of the optical port when there are online ONTs.

Step 3 Configure the renewal time of the ONT key.

Run the **port portid ont-password-renew** command to configure the interval for renewing the ONT key. To ensure the system security, the key renewal must be configured.

Step 4 Configure the compensation distance in the ranging.

Run the **port portid range** command to configure the compensation distance range of the GPON port ranging.

Step 5 (Optional) Configure the DBA calculation period on a GPON port basis.

When different GPON ports provide different access services, the bandwidth delays on these ports are different. In this case, the DBA calculation period needs to be configured on a GPON port basis.

1. In GPON board mode, run the **port dba bandwidth-assignment-mode** command to configure the DBA mode on a GPON port.
2. In diagnose mode, run the **gpon port dba calculate-period** command to configure the DBA calculation period on the GPON port.

 NOTE

- The DBA calculation period on a GPON port can be configured only when the DBA mode is set to **manual** on this GPON port.
- By default, the DBA mode on a GPON port is **default**, which means the global DBA mode is used as the bandwidth assignment mode for the GPON port. In this case, if the global DBA mode is modified by running the **gpon dba bandwidth-assignment-mode** command, the bandwidth assignment mode on the GPON port is also modified. If the DBA mode on a GPON port is not **default**, the bandwidth assignment mode on the GPON port is not affected by the global DBA mode.
- If ONTs are configured on a GPON port, modifying the DBA mode is not allowed on this GPON port.
- For the TDM service, the DBA mode must be set to **min-loop-delay**.

----End

Example

To enable the FEC function of GPON port 0/1/0, set the key renewal interval for the ONT connected to this port to 10 h, the minimum ranging compensation distance to 10 km, and the maximum ranging compensation distance to 15 km, do as follows:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 0 fec enable
huawei(config-if-gpon-0/1)#port 0 ont-password-renew 10
huawei(config-if-gpon-0/1)#port 0 range min-distance 10 max-distance 15
```

This command will result in the ONT's re-register in the port.
Are you sure to execute this command? (y/n)[n]: y

To set the global DBA mode to **min-loop-delay**, DBA mode on GPON port 0/1/0 to **manual**, and DBA calculation period to **4**, do as follows:

```
huawei(config)#gpon dba bandwidth-assignment-mode min-loop-delay
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port dba bandwidth-assignment-mode 0 manual
huawei(config-if-gpon-0/1)#quit
huawei(config)#diagnose
huawei(diagnose)%%gpon port dba calculate-period 0/1/0 4
```

2.9 GPON Configuration Guide (Distributed mode)

GPON configurations include the configurations on GPON profiles, ONTs, and ports. The following section describes configuration methods.

Context

The xPON mode includes two types: distributed (discrete) mode and profile mode. The differences between the two modes are as follows:

- In the distributing mode, ONTs cannot be added in batches. Instead, ONTs need to be configured one by one.
- In profile mode, you can pre-configure ONT line profiles and ONT service profiles and bind ONTs of the same configurations to the same profile to add them in batches, which significantly improves service provisioning efficiency.

The xPON mode is determined during site provisioning and will not be changed.

You can run the **display xpon mode** command to query the xPON mode of the current system.

2.9.1 Configuring a GPON ONT Profile (Distributed Mode)

In distributed mode, GPON ONT profiles include the GPON ONT capability profile and the GPON ONT alarm profile. This topic describes how to configure these profiles.

Context

GPON ONT profiles contain the parameters required for configuring the GPON access service, of which,

- DBA profiles specify GPON traffic parameters. The DBA profile bound to an OLT enables the OLT to dynamically allocate bandwidths, improving upstream bandwidth utilization.
- In distributed mode, the GPON ONT capability profile contains the physical port type and quantity of the ONU, mapping mode from service port to GEM port, and traffic control type.
- The GPON ONT alarm profile provides a series of alarm threshold parameters that are used for performance measurement and monitoring of activated ONU lines. After a GPON alarm profile is bound to an ONU, the ONU sends alarms to the log host and the NMS if the performance statistics of the line exceed the threshold that is specified in the profile.

 NOTE

In this document, ONUs include MDUs and ONTs.

2.9.1.1 Configuring a DBA Profile

A DBA profile defines the traffic parameters of xPON and can be bound to a T-CONT to dynamically allocate the bandwidth and improve the usage of the upstream bandwidth.

Default Configuration

Table 2-12 lists the default settings of the DBA profiles.

Table 2-12 Default settings of the DBA profiles

Parameter	Default Setting	Remarks
Default DBA profile ID in the system	0-9	You can run the display dba-profile all command to query the parameter values of each default DBA profile.

Procedure

Step 1 Add a DBA profile.

Run the **dba-profile add** command to add a DBA profile. By default, the system provides DBA profiles 0–9 with typical traffic parameter values. The default profiles cannot be added or deleted.

 NOTE

- By default, a T-CONT is not bound to any DBA profile. You must bind a T-CONT to a DBA profile.
- When you add a DBA profile, the bandwidth value must be a multiple of 64. If you enter a bandwidth value not of a multiple of 64, the system adopts the closest multiple of 64 that is smaller than the value you enter.

Step 2 Query a DBA profile.

Run the **display dba-profile** command to query a DBA profile.

----End

Example

To add a DBA profile with the type of type3, set the profile name to DBA_100M and the required bandwidth to 100 Mbit/s, do as follows:

```
huawei(config)#dba-profile add profile-name DBA_100M type3 assure 102400 max 102400
huawei(config)#display dba-profile profile-name DBA_100M
```

2.9.1.2 Configuring a GPON ONT Capacity Profile (Distributed Mode)

A GPON ONT capability profile identifies the actual capability of a GPON ONU. After an ONT is added and bound to a GPON ONT capability profile, the ONU carries the corresponding services according to parameters configured in the capability profile.

Context

- All GPON ONUs must be bound to the GPON ONT capability profile. Specify the ONT capability profile when running the **ont add** command to add an ONU offline or running the **ont confirm** command to confirm an automatically discovered ONU.
- Currently, the system provides seven default ONT capability profiles that are solidified in the system. The default profiles cannot be modified. The default profile IDs range from 1-7. The reserved ONT capability profile IDs are 8-16.
- The contents of the capability profile restrict the port number that is used in commands for GEM port mapping, T-CONT/PQ mapping, and the ONT VLAN management.
- The ONT capability profile must be configured according to the actual capability of the ONU. Different the capability profile parameters vary according to different ONUs.

Procedure

Step 1 Run the **ont-profile add** command to configure an ONT capability profile.

- When you add an ONT capability profile, if the profile ID is not specified, the system automatically allocates the least idle profile ID; if the profile name is not specified, the system adopts the default name **ont-profile_x**, where, x is the corresponding ONT capability profile ID.
- The system supports up to 128 ONT capability profiles.
- The system default profiles include the MDU profile and several common ONT (such as OT925, HG850, and HG810) profiles, which can be directly used. It is recommended to manually configure an ONT capability profile only when the default ONT capability profile fails to meet actual requirements.
- When you add an MDU profile manually, the number of the ports must be set to zero.

Step 2 Run the **display ont-profile** command to query the ONT capability profile.

----End

Example

To add an ONT capability profile for ONT HG850a with the profile index of 30, 2 POTS ports, 4 Ethernet ports, mapping mode of VLANID, and flow control type of PQ, and query the capability profile after the configuration is complete, do as follows:

```
huawei(config)#ont-profile add profile-id 30  
{ <cr>|profile-name<K> }:
```

Command:

```
ont-profile add profile-id 30
Press 'Q' or 'q' to quit input
> Are you sure you want to set the number of POTS ports to auto-adaptive? (y/n)
[n]:
> Number of POTS ports<0-8> [0]:2
> Are you sure you want to set the number of ETH ports to auto-adaptive? (y/n)
[n]:
> Number of ETH ports<0-8> [0]:4
> Are you sure you want to set the number of VDSL ports to auto-adaptive? (y/n)
[n]: y
> TDM port type<1-E1,2-T1> [1]:
> TDM service type<1-TDMoGEM> [1]:
> Number of TDM ports<0-8> [0]:
> Number of MOCA ports<0-8> [0]:
> Are you sure you want to set the number of CATV UNI ports to auto-adaptive? (
y/n) [n]:
> Number of CATV UNI ports<0-8> [0]:
> Mapping mode<1-VLANID, 2-802_1pPRI, 3-VLANID_802_1pPRI, 4-PORTID,
5-PORTID_VLANID, 6-PORTID_802_1pPRI, 7-PORTID_VLANID_802_1pPRI,
9-IPTOS, 10-VLANID_IPTOS> [1]:
> The type of flow control<1-PQ, 2-GEMPORT-CAR, 3-FLOW-CAR> [1]:
Adding an ONT profile succeeded
Profile ID : 30
Profile name: ont-profile_30
huawei(config)#display ont-profile profile-id 30
-----
Profile ID : 30
Profile name: ont-profile_30
-----
Number of POTS ports:          2
Number of ETH ports:          4
Number of VDSL ports:         0
TDM port type:                E1
TDM service type:             TDMoGem
Number of TDM ports:          0
Number of MOCA ports:         0
Number of CATV UNI ports:     0
Mapping mode:                  VLAN ID
The type of flow control:      PQ
-----
Binding times:                 0
-----
```

2.9.1.3 Configuring a GPON ONT Alarm Profile

This topic describes how to add an alarm profile, and configure most of the performance parameters for various ONT lines as a profile. After the alarm profile is configured and bound successfully, the ONT can directly use the profile when it is activated.

Context

An ONT alarm profile defines a series of alarm thresholds that are used to monitor the performance of an activated ONT line. When the statistics result of a parameter reaches the alarm threshold, the NE is notified and an alarm is sent to the log server and the NMS.

The system has a default alarm threshold profile with ID 1. This profile cannot be deleted but can be modified.

Procedure

Step 1 Run the **gpon alarm-profile add** command to add a GPON ONT alarm profile.

If default alarm thresholds are used in a new alarm profile, the system does not report any alarm.

Step 2 Run the **display gpon alarm-profile** command to query the alarm profile.

----End

Example

To add GPON ONT alarm profile 5, set the alarm threshold for the packet loss of the GEM port to 10, set the alarm threshold for the number of mis-transmitted packets to 30, and use the default value 0 for all other thresholds, do as follows:

```
huawei(config)#gpon alarm-profile add profile-id 5
{ <cr>|profile-name<K> }:
```

Command:

```
gpon alarm-profile add profile-id 5
```

Press 'Q' or 'q' to quit input

```
> GEM port loss of packets threshold (0~100)[0]:10
> GEM port misinserted packets threshold (0~100)[0]:30
> GEM port impaired blocks threshold (0~100)[0]:0
> Ethernet FCS errors threshold (0~100)[0]:0
> Ethernet excessive collision count threshold (0~100)[0]:0
> Ethernet late collision count threshold (0~100)[0]:0
> Too long Ethernet frames threshold (0~100)[0]:0
> Ethernet buffer (Rx) overflows threshold (0~100)[0]:0
> Ethernet buffer (Tx) overflows threshold (0~100)[0]:0
> Ethernet single collision frame count threshold (0~100)[0]:0
> Ethernet multiple collisions frame count threshold (0~100)[0]:0
> Ethernet SQE count threshold (0~100)[0]:0
> Ethernet deferred transmission count threshold (0~100)[0]:0
> Ethernet internal MAC Tx errors threshold (0~100)[0]:0
> Ethernet carrier sense errors threshold (0~100)[0]:0
> Ethernet alignment errors threshold (0~100)[0]:0
> Ethernet internal MAC Rx errors threshold (0~100)[0]:0
> PPPOE filtered frames threshold (0~100)[0]:0
> MAC bridge port discarded frames due to delay threshold (0~100)[0]:0
> MAC bridge port MTU exceeded discard frames threshold (0~100)[0]:0
> MAC bridge port received incorrect frames threshold (0~100)[0]:0
> CES general error time threshold(0~100)[0]:0
> CES severely time threshold(0~100)[0]:0
> CES bursty time threshold(0~100)[0]:0
> CES controlled slip threshold(0~100)[0]:0
> CES unavailable time threshold(0~100)[0]:0
> Drop events threshold(0~100)[0]:0
> Undersize packets threshold(0~100)[0]:0
> Fragments threshold(0~100)[0]:0
> Jabbers threshold(0~100)[0]:0
> Failed signal of ONT threshold(Format:1e-x, x: 3~8)[3]:
> Degraded signal of ONT threshold(Format:1e-x, x: 4~9)[4]:
> FEC uncorrectable code words threshold(0~1101600000)[0]:0
> FEC correctable code words threshold(0~1101600000)[0]:0
> Upstream PQ discarded byte alarm threshold(0~65535)[0]:0
> Downstream PQ discarded byte alarm threshold(0~65535)[0]:0
> Encryption key errors threshold(0~100)[0]:0
> XGEM key errors threshold(0~100)[0]:0
> XGEM HEC error count threshold(0~100)[0]:0
```

Adding an alarm profile succeeded

Profile ID : 5

Profile name: alarm-profile_5

2.9.2 Configuring a GPON ONT (Distributed Mode)

The OLT provides end users with services through the ONT. The OLT can manage the ONT and the ONT can work in the normal state only after the channel between the OLT and the ONT is available.

Prerequisites

The GPON ONT profile is already created. [Configuring a GPON ONT Capability Profile](#) and [Configuring a GPON ONT Alarm Profile](#) are already completed.

Context

The OLT uses the ONT Management and Control Interface (OMCI) protocol to manage and configure the GPON ONT, and supports the offline configuration of the ONT. The ONT does not need to save the configuration information locally. This helps to provision services.

[Table 2-13](#) lists the default settings of the GPON ONT.

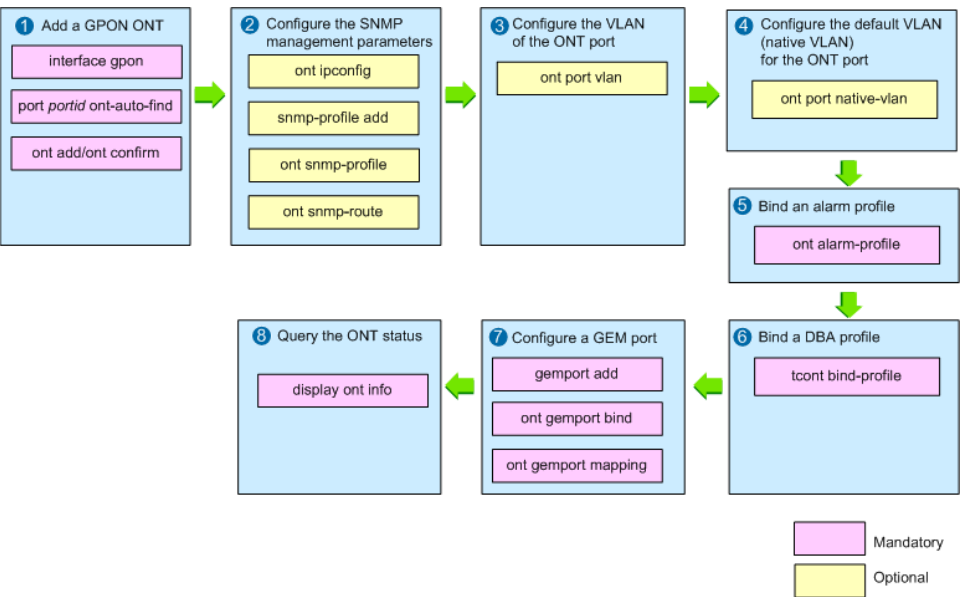
Table 2-13 Default settings of the GPON ONT

Parameter	Default Setting
ONT auto-find function of a GPON port	Disabled
ONT status after an ONT is added	Activated
Default VLAN of the ONT port	1

Configuration Process

[Figure 2-42](#) shows the process of configuring a GPON ONT.

Figure 2-42 Process of configuring a GPON ONT



Procedure

Step 1 Add a GPON ONT.

1. Run the **interface gpon** command to enter the GPON mode.
2. Run the **port portid ont-auto-find** command to enable the auto-find function of the ONT. After the function is enabled, you can add an ONT according to the information reported by the system. By default, the ONT auto-find function of a GPON port is disabled.

NOTE

An auto-find ONT is in the auto-find state. The auto-find ONT can work in the normal state only after it is confirmed or added.

3. Run the **ont add** command to add an ONT offline, or run the **ont confirm** command to confirm the auto-find ONT.

When ONTs are added or confirmed, the system provides four authentication modes: SN, password, SN+password, LOID+CHECKCODE.

- SN authentication: The OLT detects the serial number (SN) reported by an ONT. If the SN is consistent with the OLT configuration, authentication is passed and the ONT goes online. This mode requires recording all ONT SNs. Hence, it is used to confirm auto discovery ONTs and is not applicable to adding ONTs in batches.
- Password authentication: The OLT detects the password reported by an ONT. If the password is consistent with the OLT configuration, the ONT goes online normally. This mode requires planning ONT passwords and does not require manually recording ONT SNs. Hence, it is applicable to adding ONTs in batches. The password authentication provides two discovery modes: always-on and once-on.
 - always-on: After first password authentication is passed, no SN is allocated and password authentication is always used in subsequent authentications. This discovery mode is easy for future maintenance. In the always-on discovery mode, configurations do not need to be modified when an ONT is replaced and only the password is required. The always-on discovery mode has lower security. If other users know the password, the users will illegally have service permissions.
 - once-on: Password authentication is used for the first authentication. After the authentication is successful, the SN is automatically matched. The SN+password authentication mode is used for subsequent authentications. The ONT can go online only when both the password and SN are correct. The once-on authentication mode has high security. After an ONT is replaced or the password is mistakenly changed, the ONT needs to run the **ont re-discovery** command to be re-discovered, which requires more maintenance effort.
- SN+password authentication: The OLT detects the password and SN reported by an ONT. If the password and SN are consistent with the OLT configuration, the ONT goes online normally. This authentication mode has the highest security but it requires manually recording ONT SNs.

- LOID+CHECKCODE authentication: defined by a telecom operator. In this authentication mode, LOID has 24 bytes, and CHECKCODE has 12 bytes and is optional. Whether 24 bytes or 36 bytes are used for authentication depends on data planning, which is unified over the entire network. The OLT determines whether LOID+CHECKCODE reported by the ONT is the same as the configured one. If they are the same, the ONT authentication is passed. If they are different, the OLT obtains the ONT password and compares it with the last 10 bytes of the LOID. If they are the same, the ONT authentication is also passed. This operation is for compatibility with the ONTs using password authentication.

Adding ONTs in offline mode is applicable to the batch deployment scenario. All ONTs are added to the OLT to complete service provisioning beforehand. When a user subscribes to the service, an installation engineer takes an ONT to the user's house and completes configurations. After the ONT goes online and passes authentication, the service is provisioned. Generally, the password authentication mode or LOID authentication mode is used to confirm an ONT.

Adding ONTs in auto discovery mode is applicable to the scenario where a small number of ONTs are added. When users subscribe to the service, installation engineers take ONTs to the users' houses. After the ONTs go online, the OLT confirms the ONTs one by one. Generally, the MAC address authentication mode is used to confirm the ONTs.

NOTE

- If the ONU is an independent NE and is directly managed by the NMS through the SNMP management mode, select the SNMP management mode. For this mode, you only need to configure the parameters for the GPON line and the parameters for the management channel on the OLT.
- If the ONU is not an independent NE and all its configuration data is issued by the OLT through OMCI, select the OMCI management mode. For this mode, you need to configure all parameters (including line parameters, UNI port parameters, and service parameters) that are required for the ONU on the OLT.
- Generally, the ONT management mode is set to the OMCI mode.

Step 2 (Optional) Configure the SNMP management parameters. When the ONT management mode is the SNMP mode, you need to configure the SNMP management parameters for the ONT. The procedure is as follows:

1. Run the **ont ipconfig** command to configure the management IP address of the ONT. The IP address should not be in the same subnet for the IP address of the VLAN port.
2. If an ONU is not managed as an independent NE, all configurations of the ONU are managed by the OLT through the OMCI protocol, and the OMCI management mode is selected. In this mode, you need to configure all the parameters (including line parameters, UNI port parameters, and service parameters) required by the ONU on the OLT.
3. Run the **ont snmp-route** command to configure a static route for the NMS server, that is, configure the IP address of the next hop.

Step 3 (Optional) Configure the VLAN of the ONT port.

Run the **ont port vlan** command to configure the VLAN of the ONT port.

Step 4 (Optional) Configure the default VLAN (native VLAN) for the ONT port.

Run the **ont port native-vlan** command to configure the default VLAN for the ONT port.

- If the packets reported from a user (such a PC) to the ONT are untagged, the packets are tagged with the default VLAN of the port on the ONT and then reported to the OLT.
- If the packets reported from a user to the ONT are tagged, you need to configure the port VLAN of the ONT to be the same as the VLAN in the user tag. The packets are not tagged with the default VLAN of the port on the ONT but are reported to the OLT with the user tag.

Step 5 Bind an alarm profile.

Run the **ont alarm-profile** command to bind an alarm profile. Ensure that [2.8.1.4 Configuring a GPON ONT Alarm Profile](#) is completed before the configuration.

Step 6 Bind a DBA profile.

Run the **tcont bind-profile** command to bind a DBA profile to a T-CONT.

A DBA profile can be bound to a T-CONT after an ONT is added.

Step 7 Configure a GEM port.

1. Run the **gemport add** command to add a GEM port. When adding a GEM port, select the correct attribute according to the service type.
2. Run the **ont gemport bind** command to bind the GEM port to an ONT T-CONT, that is, allocating the T-CONT resources to the GEM port.

 NOTE

If traffic streams are configured on a GEM port and an ONT is the working ONT in a single-homing protection group, the GEM port cannot be bound to or unbound from the ONT.

3. Run the **ont gemport mapping** command to create the mapping between the GEM port and the ONT-side service.

Step 8 Query the ONT status.

Run the **display ont info** command to query the ONT running status, configuration status, and matching status.

----End

Example

To add five ONTs in offline mode with password authentication mode (ONT passwords are 0100000001-0100000005), set the discovery mode of password authentication to always-on, and bind ONT capability profile 30, do as follows:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 password-auth 0100000001 always-on profile-id 30 manage-mode omci
huawei(config-if-gpon-0/1)#ont add 0 password-auth 0100000002 always-on profile-id 30 manage-mode omci
huawei(config-if-gpon-0/1)#ont add 0 password-auth 0100000003 always-on profile-id 30 manage-mode omci
huawei(config-if-gpon-0/1)#ont add 0 password-auth 0100000004 always-on profile-id 30 manage-mode omci
huawei(config-if-gpon-0/1)#ont add 0 password-auth 0100000005 always-on profile-id 30 manage-mode omci
```

To add an ONT that is managed by the OLT through the OMCI protocol, confirm this ONT according to the SN 3230313185885B41 automatically reported by the system, and bind the ONT with capability profile 3 that match the ONT, do as follows:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/1)#ont confirm 0 sn-auth 3230313185885B41 profile-id 3
manage-mode omci
```

To add an ONU that is managed as an independent NE and whose SN is known as 3230313185885641, bind the ONU with capability profile 4 that matches the ONU, configure the NMS parameters for the ONU, and set the management VLAN to 100, do as follows:

```
huawei(config)#snmp-profile add profile-id 1 v3 public private 10.10.5.53 161 bodyname
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 2 sn-auth 3230313185885641 profile-id 4 manage-mode snmp
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 static ip-address 10.20.20.20 mask 255.255.255.0 gateway 10.10.20.1 vlan 100
huawei(config-if-gpon-0/1)#ont snmp-profile 0 2 profile-id 1
huawei(config-if-gpon-0/1)#ont snmp-route 0 2 ip-address 10.10.20.190 mask 255.255.255.0 next-hop 10.10.20.100
```

2.9.3 Configuring a GPON Port

To work normally and carry the service, a GPON port must be enabled first. This topic describes how to enable a GPON port and configure related attributes of the port.

Default Configuration

[Table 2-14](#) lists the default settings of the GPON port.

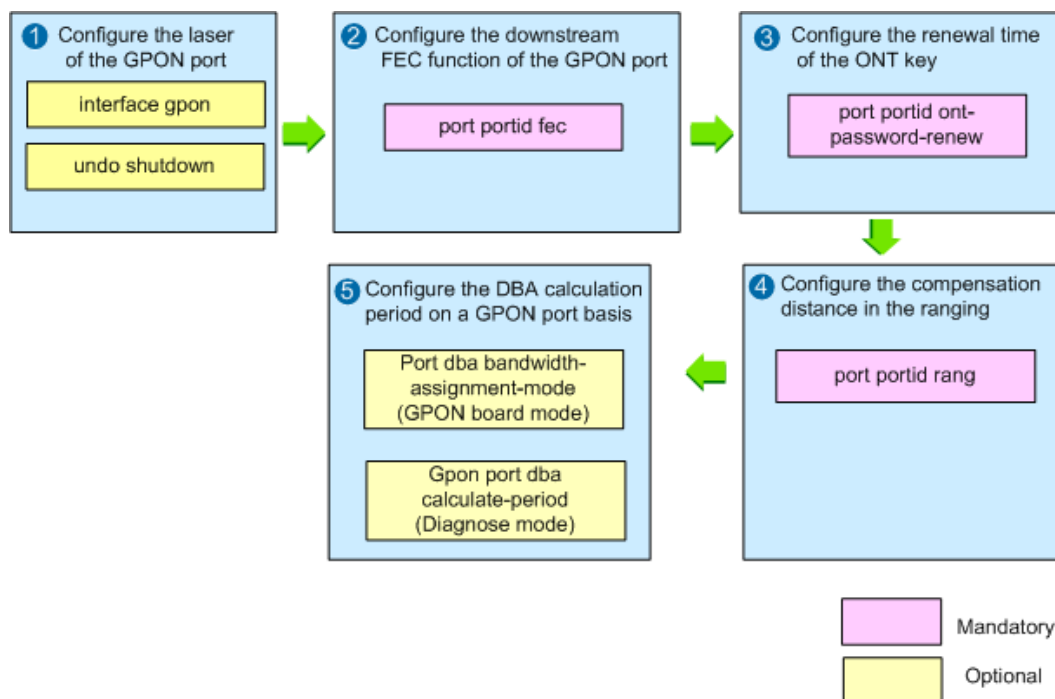
Table 2-14 Default settings of the GPON port

Parameter	Default Setting
GPON port	Enabled
Downstream FEC function of the GPON port	Disabled
Compensation distance range of the GPON port ranging	Minimum logical distance: 0 km; maximum logical distance: 20 km

Configuration Process

[Figure 2-43](#) shows the process of configuring a GPON Port.

Figure 2-43 Process of configuring a GPON Port



Procedure

Step 1 (Optional) Configure the optical port switch.

1. Run the **interface gpon** command to enter GPON mode.
2. Run the **undo shutdown** command to enable the laser of the GPON port. By default, the laser of the GPON port is enabled and the GPON port is available. In this case, skip this step.

NOTICE

- If an optical port is not required, run the **shutdown** command to disable the optical port.
- Disabling a PON port that carries services will cause the interruption of such services.

Step 2 Enables or disables the downstream FEC function of a port.

Run the **port portid fec** command to configure the FEC function of the GPON port. By default, the function is disabled.

NOTE

- FEC is to insert redundant data into normal packets so that the line has certain error tolerance. Some bandwidth, however, must be consumed. Enabling FEC enhances the error correction capability of the line but at the same time occupies certain bandwidth. Determine whether to enable FEC according to the actual line planning.
- If a large number of ONTs are online, enabling the FEC function of the optical port may cause some ONTs to go offline. Therefore, it is recommended that you do not configure the FEC function of the optical port when there are online ONTs.

Step 3 Configure the renewal time of the ONT key.

Run the **port portid ont-password-renew** command to configure the interval for renewing the ONT key. To ensure the system security, the key renewal must be configured.

Step 4 Configure the compensation distance in the ranging.

Run the **port portid range** command to configure the compensation distance range of the GPON port ranging.

Step 5 (Optional) Configure the DBA calculation period on a GPON port basis.

When different GPON ports provide different access services, the bandwidth delays on these ports are different. In this case, the DBA calculation period needs to be configured on a GPON port basis.

1. In GPON board mode, run the **port dba bandwidth-assignment-mode** command to configure the DBA mode on a GPON port.
2. In diagnose mode, run the **gpon port dba calculate-period** command to configure the DBA calculation period on the GPON port.

 NOTE

- The DBA calculation period on a GPON port can be configured only when the DBA mode is set to **manual** on this GPON port.
- By default, the DBA mode on a GPON port is **default**, which means the global DBA mode is used as the bandwidth assignment mode for the GPON port. In this case, if the global DBA mode is modified by running the **gpon dba bandwidth-assignment-mode** command, the bandwidth assignment mode on the GPON port is also modified. If the DBA mode on a GPON port is not **default**, the bandwidth assignment mode on the GPON port is not affected by the global DBA mode.
- If ONTs are configured on a GPON port, modifying the DBA mode is not allowed on this GPON port.
- For the TDM service, the DBA mode must be set to **min-loop-delay**.

----End

Example

To enable the FEC function of GPON port 0/1/0, set the key renewal interval for the ONT connected to this port to 10 h, the minimum ranging compensation distance to 10 km, and the maximum ranging compensation distance to 15 km, do as follows:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 0 fec enable
huawei(config-if-gpon-0/1)#port 0 ont-password-renew 10
huawei(config-if-gpon-0/1)#port 0 range min-distance 10 max-distance 15
This command will result in the ONT's re-register in the port.
Are you sure to execute this command? (y/n)[n]: y
```

To set the global DBA mode to **min-loop-delay**, DBA mode on GPON port 0/1/0 to **manual**, and DBA calculation period to **4**, do as follows:

```
huawei(config)#gpon dba bandwidth-assignment-mode min-loop-delay
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port dba bandwidth-assignment-mode 0 manual
huawei(config-if-gpon-0/1)#quit
huawei(config)#diagnose
huawei(diagnose)%%gpon port dba calculate-period 0/1/0 4
```

2.10 GPON Reference Standards and Protocols

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

Standard No.	Description
ITU-T G.984.1	General Characteristics. This protocol mainly describes the basic features and major protection modes of GPON.
ITU-T G.984.2	Physical Media Dependent (PMD) Layer Specification. This protocol mainly describes the PMD layer parameters, including physical parameters (such as the transmit optical power, receiver sensitivity, and overload optical power) of optical transceivers, and also defines optical budget of different levels, for example, the most common Class B+.
ITU-T G.984.3	Transmission Convergence Layer Specification. This protocol mainly describes the TC layer specifications, including the upstream and downstream frame structures and GPON principle.
ITU-T G.984.4	ONT Management And Control Interface Specification. This protocol mainly describes the GPON management and maintenance protocols, such as OAM, PLOAM, and OMCI.
ITU-T G.984.5	Enhancement Band. This protocol mainly describes the GPON wavelength planning, including reserving bands for next-generation PON.
ITU-T G.984.7	Long Reach. This protocol mainly describes several long reach PON schemes for extending GPON transmission distance.
ITU-T G.988	ONU management and control interface (OMCI) specification.
TR-156	Using GPON Access in the context of TR-101.