AN5116-06B

Optical Line Terminal Equipment

Feature Description

Version: B

Code: MN000000522

FiberHome Telecommunication Technologies Co., Ltd.

February 2012

Thank you for choosing our products.

We appreciate your business. Your satisfaction is our goal. We will provide you with comprehensive technical support and after-sales service. Please contact your local sales representative, service representative or distributor for any help needed at the contact information shown below.

Fiberhome Telecommunication Technologies Co., Ltd.

Address: No.5 Dongxin Rd., Hongshan Dist., Wuhan, China
Zip code: 430073
Tel: +86 27 8769 1549
Fax: +86 27 8769 1755
Website: http://www.fiberhomegroup.com

Legal Notice

烽火通信® FiberHome®

GONST® FONST® e-Fim®

CiTRANS® E-jet® IBAS®

Freelink® FonsWeaver®

OTNPlanner™ SmartWeaver™

are trademarks of FiberHome Telecommunication Technologies Co., Ltd. (Hereinafer referred to as FiberHome)

All brand names and product names used in this document are used for identification purposes only and are trademarks or registered trademarks of their respective holders.

All rights reserved

No part of this document (including the electronic version) may be reproduced or transmitted in any form or by any means without prior written permission from FiberHome.

Information in this document is subject to change without notice.

Preface

Related Documentation

Document	Description
AN5116–06B Optical Line Terminal Equipment Documentation Guide	Introduces the retrieval method, contents, releasing, reading approach, and suggestion feedback method for the complete manual set for the AN5116-06B.
AN5116–06B Optical Line Terminal Equipment Product Description	Introduces the AN5116-06B's network location, functional features, hardware structure, FTTx application model, equipment configuration, network management system and technical specifications. It is the foundation of the complete manual set. Other manuals extend and enrich the concepts introduced in the Product Description.
AN5116–06B Optical Line Terminal Equipment Feature Description	Introduces the key features supported by the AN5116-06B, including GPON / EPON access, GPON / EPON terminal management, VLAN, multicast, voice and safety; and introduces these functions in details in terms of definition, features, specification, principle description, references and so on.
AN5116–06B Optical Line Terminal Equipment Hardware Description	Introduces the appearance, structure, functions, technical specifications, and operating method for the AN5116-06B's cabinet, PDP, subrack, cards, cables and wires, facilitating users' mastery of the hardware features of the equipment.
AN5116–06B Optical Line Terminal Equipment Installation Guide	Introduces the overall installation and acceptance inspection procedures from unpacking inspection to poweron examination after the equipment is delivered on site, and provides reference information (e.g. safety principles and wiring scheme of various interfaces) to guide users to install the equipment.
AN5116–06B Optical Line Terminal Equipment EPON Configuration Guide	Introduces the method for configuring the EPON services supported by the AN5116-06B via the ANM2000, such as basic configuration, voice service configuration, data service configuration, multicast service configuration, and software upgrading configuration, to guide users on startup for various services and software upgrading.

Document	Description
AN5116–06B Optical Line Terminal Equipment GPON Configuration Guide	Introduces the method for configuring the GPON services supported by the AN5116-06B via the ANM2000, such as basic configuration, voice service configuration, data service configuration, multicast service configuration, and software upgrading configuration, to guide users on startup for various services and software upgrading.
AN5116–06B Optical Line Terminal Equipment GUI Reference	Introduces the shortcut menu for every card of the AN5116-06B on the ANM2000, including the function, parameter explanation, precautions and configuration example of every command in the shortcut menu of each card, to help users master the operation of the AN5116-06B using the ANM2000.
AN5116–06B Optical Line Terminal Equipment Component Replacement	Introduces the operation procedures for replacing the AN5116-06B's components, including preparations, precautions, early operations, operation process and subsequent operations, so as to guide users with the component replacement on the hardware.
AN5116–06B Optical Line Terminal Equipment Routine Maintenance	Introduces the daily, weekly, monthly, quarterly and annual routine maintenance operations on the AN5116-06B. Users are able to eliminate silent failures in the equipment operation process as early as possible via implementing the routine maintenance.
AN5116–06B Optical Line Terminal Equipment Alarm Reference	Introduces the AN5116-06B's alarm / event information, including alarm / event names, alarm / event levels, possible reasons, effects on the system, and processing procedures, to guide users on effective alarm / event processing.
AN5116–06B Optical Line Terminal Equipment Troubleshooting Guide	Introduces the fault processing principles and methods of fault diagnosis and isolation for the AN5116-06B. Also discusses the typical fault cases of various EPON / GPON services. In case of complex issues, users can contact FiberHome for technical support according to the instructions in this document.

Version

Version	Description
A	Initial version. This manual corresponds to the AN5116-06B EPON V2.0 and GPON V1.0.
B	This manual corresponds to EPON V3.1 and GPON V3.1 of the AN5116-06B. Optimizes the content and the network diagrams.

Introduces the functions and features of the AN5116-06B GPON / EPON, helping users understand the technology, functions and features of the equipment.

Intended Reader

This manual is intended for the following readers:

- Commissioning engineers
- Equipment room maintenance engineers

To utilize this manual, these prerequisite skills are necessary:

- Access network technology
- EPON principle
- GPON principle
- Ethernet switch technology
- Computer network technology
- Basic operation methods on the ANM2000.

Conventions

Terminology Conventions

Terminology	Meaning
AN5116-06B	The AN5116-06B optical Line Terminal Equipment
EC4B	4×EPON-C Interface Card (type B)
EC8B	8×EPON-C Interface Card (type B)
GC4B	4×GPON-C Interface Card (type B)
GC8B	8×GPON-C Interface Card (type B)
XG2B	2×10G EPON-C Interface Card (type B)
C155A	4×GE + 1×10GE Optical Interface Uplink Card (CES Mode)
CE1B	32×E1 Optical Interface Card (CES mode) (type B)
PUBA	Public Card (type A)
HSWA	Core Switch Card (EPON) (card No.: 2.115.334)
	Core Switch Card (type A) (card No.: 2.115.331)
HU1A	4×GE + 1×10GE Optical Interface Uplink Card
HU2A	2×GE + +2×10GE Optical Interface Uplink Card
GU6F	6×GE Optical Interface Uplink Card

Symbol Conventions

Symbol	Refer to	Meaning
✎	Note	Important features or operation guide.
⚠	Caution	Possible injury to persons or systems, or cause traffic interruption or loss.
⚡	Warning	May cause severe bodily injuries.

Contents

Figures

Tables

1 Access to EPON

☑ Definition

☑ Features

☑ Specifications

☑ Basic Principles

☑ Reference Information

1.1 Definition

EPON means the Ethernet-based PON, which is defined and standardized by IEEE. The EPON system adopts the single-fiber bi-directional transmission mode, and its rate is 1.25 Gbit/s (for the digital signal). Its uplink direction uses the 1310 nm wavelength channel, and downlink direction uses the 1490 nm wavelength channel. An EPON system is composed of the OLT, the ODN, and the ONU.

1.2 Features

- Has a high transmission bandwidth and a good extensibility.
- The fiber has a low loss and a wide coverage.
- Its bandwidth can be allocated flexibly, and the QoS can be guaranteed.
- Uses the P2MP access, so as to conserve fiber consumption.
- The regeneration transmission node in the network is passive, and the operation and maintenance cost is low.

1.3 Specifications

- Supports two types of EPON interface cards: the EC4B card and the EC8B card. The EC4B card supports four EPON ports, and the EC8B card supports eight EPON ports.
- Supports the PON port protection.
- Each EPON port supports up to 64 ONUs; this means that its split ratio is 1:32, and can reach 1:64 via the expansion operation.
- An EPON port supports the maximum uplink / downlink rate of 1.25 Gbit/s.
- Supports the maximum transmission distance of 20 km.
- Supports the optical power detection function.
- Supports the CPU / memory utilization ratio query of an EPON interface card.
- Supports the query of current alarms, alarm history, instant performance, and performance history of an EPON interface card.

1.4 Basic Principles

System architecture

An EPON system is composed of the OLT, the ODN, and the ONU. The ODN is mainly composed of fibers and optical splitters. The EPON system architecture is shown in Figure 1-1.

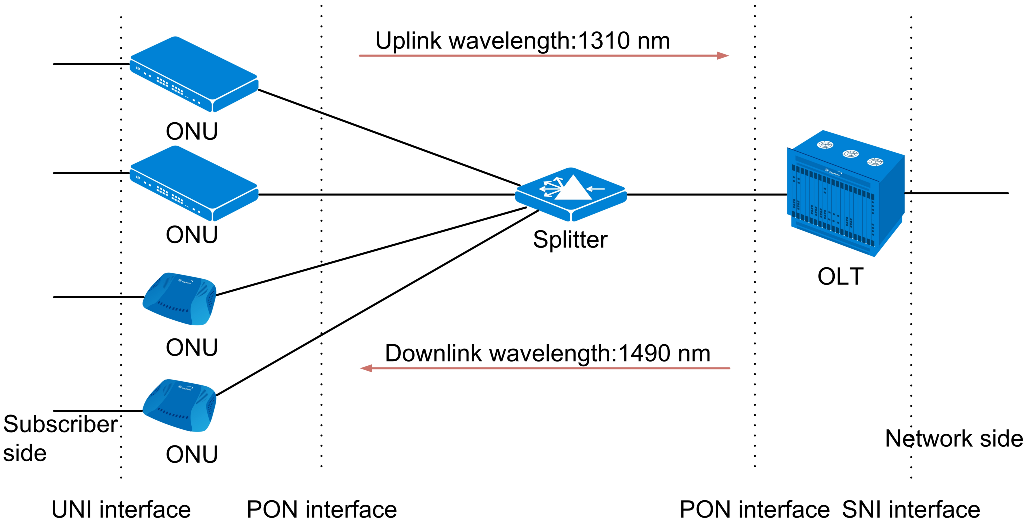


Figure 1-1 The EPON system architecture

As the OLT, the AN5116-06B is connected with the ONU equipment. Between the OLT and each ONU, one or multiple logical links (LLID) exist.

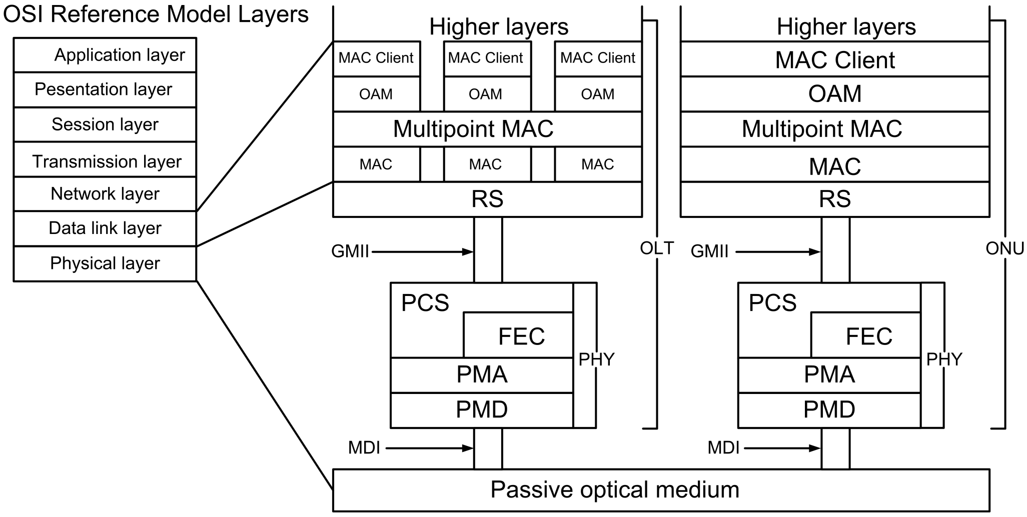
In the downlink direction from the OLT to the ONU, the Ethernet packets prefixed with the corresponding LLIDs are transmitted in the PON. The splitter in the ODN broadcasts the packets to each tributary; all ONUs in the tributaries can receive these packets, and select the needed packets depending on the LLIDs.

In the uplink direction from the ONU to the OLT, various ONUs use the TDM mechanism to share the uplink bandwidth. The OLT assigns uplink timeslots for each ONU via the MPCP message, and assigns the bandwidth dynamically according to the bandwidth request and the link conditions.

Protocol stack architecture

For the Ethernet technology, the PON is a new medium. So the IEEE 802.3 task force defines the new physical layer, and modifies the Ethernet MAC layer and above in the least degree, so as to support the new applications and media.

The EPON protocol stack is shown in Figure 1-2.



FEC Forward Error Correction
GMII Gigabit Medium Independent Interface
MDI Medium Dependent Interface
OAM Operation, Administration and Maintenance
OLT Optical Line Terminal
ONU Optical Network Unit

PCS Physical Coding Sub-layer
PHY Physical Layer
PMA Physical Medium Attachment (sub-layer)
PMD Physical Medium Dependent (sub-layer)
RS Reconciliation Sub-layer

Figure 1-2 The EPON protocol stack architecture

The EPON physical layer is divided into the physical coding sub-layer (the PCS sub-layer), the FEC sub-layer, the physical medium attachment sub-layer (PMA sub-layer), and the physical medium dependent sub-layer (the PMD sub-layer). Compared with the GE physical layer, the only difference is that the EPON physical layer has an additional FEC sub-layer, which enables users to select the laser, the split ratio of the splitter, and the maximum transmission distance as required. The EPON physical layer is connected with the RS sub-layer via the Gigabit medium independent interface (the GMII interface), and transports the reliable data for the MAC layer. The functions of each EPON physical sub-layer are described as follows:

- The PCS sub-layer: Is isolated at the top level of the physical layer, up linked with the GMII interface, and down connected with the PMA sub-layer. It mainly implements the coding conversion.
- The FEC sub-layer: Is isolated between the PCS sub-layer and the PMA sub-layer, and completes the FEC of the data.
- The PMA sub-layer: Compared with the GE PMA sub-layer technologies, it has few modifications. It mainly completes the functions such as the serial-parallel conversion.
- The PMD sub-layer: It mainly completes the O / E conversion.

Encapsulation mode

The frame structure of the data transmitted in the EPON system is shown in Figure 1-3.

Preamble 8 bytes	DA 6 bytes	SA 6 bytes	Length / type 2 bytes	Data 46 to 1500 bytes	Pad Variable length	FCS 4 bytes

Figure 1-3 The frame structure of the data transmitted in the EPON system

In the EPON system, the data are transmitted in the single-fiber bi-directional full-duplex mode. When the OLT broadcasts to various ONUs via the optical fiber, the IEEE 802.3ah standard uses the LLID to distinguish different ONUs and ensures that only the ONU sending the request can receive the data packets. The LLID is a two-byte field; the OLT assigns a unique LLID No. in the network for each ONU, and this LLID No. decides which ONU has the authorization to receive the broadcast data. The location of the LLID is shown in Figure 1-4.

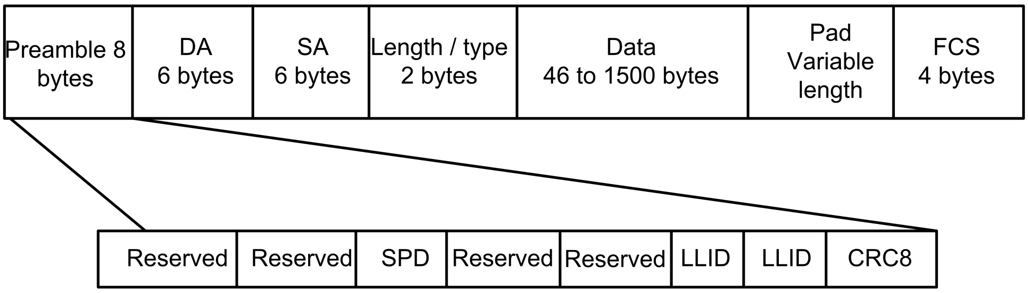


Figure 1-4 The location of the LLID in the EPON frame

When ONUs send the burst data to the OLT, the authorized ONU sends the data packets in the assigned timeslots, and the unauthorized ONU is under rest status. At the OLT side, the transmitting and receiving of the PCS sub-layer are both in the continuous working mode. At the ONU side, the PCS sub-layer receives the broadcast data from the OLT side continuously in the Rx direction, but works uncontinuously in the Tx direction. For this reason, the EPON PCS sub-layer not only needs to work normally with continuous data streams like the GE PCS sub-layer, but also needs to keep stable when the burst data are transmitted and received. The synchronization and receiving of the burst data at the OLT side is the key to implement the PCS sub-layer technologies of the EPON system.

EPON key technologies

- The dynamic bandwidth allocation
- The system synchronization
- Ranging and delay compensation
- The RTT compensation
- The burst receiving and transmitting
- The multiple access protocol of the uplink channel

OAM

The OAM functions of the EPON system mainly include the following aspects:

- Supports the uniform management by the network management system, and has the functions of the performance management, fault management, configuration management, and the security management.
- Supports the authentication and configuration of an ONU.
- Supports the loopback test.

1.5 Reference Information

Reference standard

- IEEE 802.3-2005：IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks–Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

Terminology

None

Abbreviations

Abbreviation	Meaning
EPON	Ethernet Passive Optical Network
FCS	Frame Check Sequence
GMII	Gigabit Media Independent Interface
LLID	Logical Link Identifier
MPCP	Multiple point control protocol
OAM	Operation, administration and maintenance
ODN	Optical Distribution Network
OLT	Optical Line Terminal
ONU	Optical Network Unit
PCS	Physical Code Sublayer
P2MP	Point to MultiPoint
PMA	Physical Medium Attachment
PMD	Physical Medium Dependent
RTT	Round Trip Time

2 Access to GPON

☑ Definition

☑ Features

☑ Specifications

☑ Basic Principles

☑ Reference Information

2.1 Definition

GPON means the Gigabit PON, which is defined by ITU-T G.984.x series standards. The GPON system adopts the single-fiber bi-directional transmission mode; its downlink rate can reach 1.25 Gbit/s or 2.5 Gbit/s, and its uplink rate can reach 1.25 Gbit/s. A GPON system is composed of the OLT, the ODN, and the ONU.

2.2 Features

- Has a high transmission bandwidth and a good extensibility.
- The fiber has a low loss and a wide coverage.
- Its bandwidth can be allocated flexibly, and the QoS can be guaranteed.
- Uses the GEM encapsulation mode, with high integrated transmission efficiency.
- Uses the P2MP access, so as to conserve fiber consumption.
- The regeneration transmission node in the network is passive, and the operation and maintenance cost is low.

2.3 Specifications

- Supports two types of GPON interface cards: the GC4B card and the GC8B card. The GC4B card supports four GPON ports, and the GC8B card supports eight GPON ports.
- Supports the PON port protection.
- Each GPON port supports up to 64 ONUs; this means that its split ratio is 1:64.
- A GPON port supports the maximum downlink rate of 2.5 Gbit/s and the maximum uplink rate of 1.25 Gbit/s.
- Supports the maximum transmission distance of 20 km.
- Supports the optical power detection function.
- Supports the CPU / memory utilization ratio query of a GPON interface card.
- Supports the query of current alarms, alarm history, instant performance, and performance history of a GPON interface card.

2.4 Basic Principles

System architecture

A GPON system is composed of the OLT, the ODN, and the ONU. The ODN is mainly composed of fibers and optical splitters. The EPON system architecture is shown in Figure 2-1.

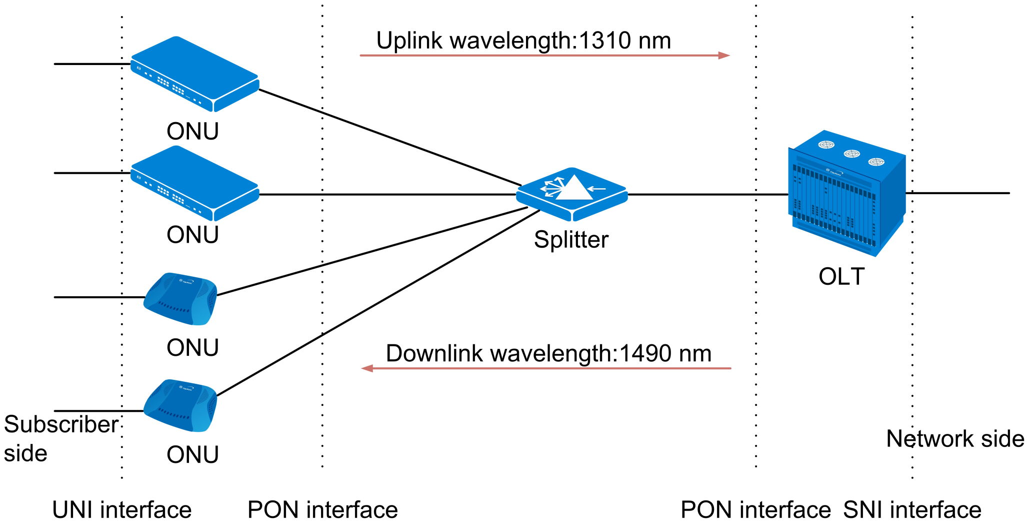


Figure 2-1 The GPON system architecture

As the OLT, the AN5116-06B is connected with the ONU equipment. The downlink packets from the OLT are broadcasted via the splitter in the ODN, and each ONU on the tributary only receives its dedicated packets.

In the uplink direction from the ONU to the OLT, various ONUs use the TDM mechanism to share the uplink bandwidth. The OLT assigns uplink timeslots for each ONU via the MPCP message, and assigns the bandwidth dynamically according to the bandwidth request and the link conditions.

T-CONT

GPON uses T-CONTs to implement service convergence. A T-CONT is the basic control unit for the uplink service streams in the GPON system. The GPON system defines four bandwidth priorities as follows: fixed, assured, not-assured, and best-effort.

Depending on the bandwidth combination used by the T-CONT, the T-CONT can be classified as five types. Table 2-1 lists the correspondence relationships between the T-CONT types and bandwidth types and their sensitivities to the delay.

Table 2-1 The T-CONT types

Band-width Type	Sensitivity to the Delay	T-CONT Type				
		Type 1	Type 2	Type 3	Type 4	Type 5
Fixed	True	True	False	False	False	True
Assured	False	False	True	True	False	True
Not-assured	False	False	False	True	False	True
Best-effort	False	False	False	False	True	True

In the GPON system, one ONU can be allocated with multiple T-CONTs; these T-CONTs are independent of each other, and each T-CONT is identified by an Alloc-ID. Each T-CONT is composed of one or multiple GEM ports, each GEM port carries one type of service stream, and a GEM port is identified by a unique Port-ID. A GEM port identifies the service channel between the OLT and the ONU, and this channel carries the service stream. The multiplex architecture of the GPON system is shown in Figure 2-2.

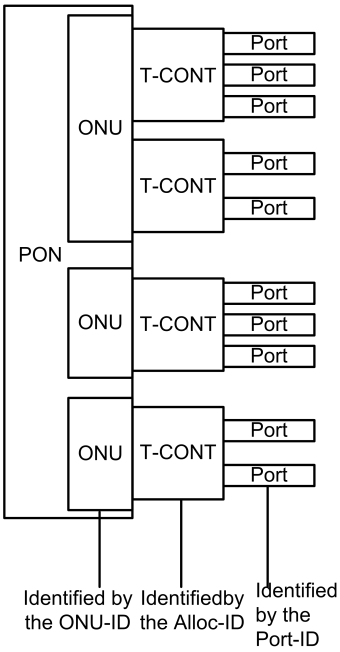


Figure 2-2 The multiplex architecture of the GPON system

Protocol stack architecture

The protocol stack model of the GPON system is shown in Figure 2-3, and is mainly composed of the PMD layer and the GTC layer. The GTC layer includes two sub-layers: the GTC framing sub-layer and the TC adaption sub-layer. The GPON equipment generally uses the GEM frame encapsulation mode, and the GTC layer in the GEM mode can provide three types of interfaces for the client layer: the ATM client interface, the GEM client interface, and the ONU management and control interface (OMCI).

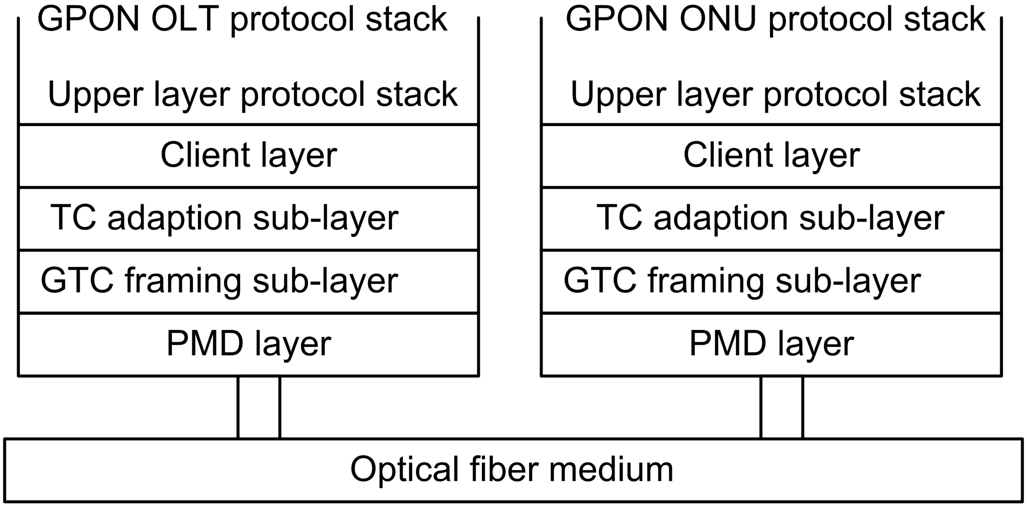


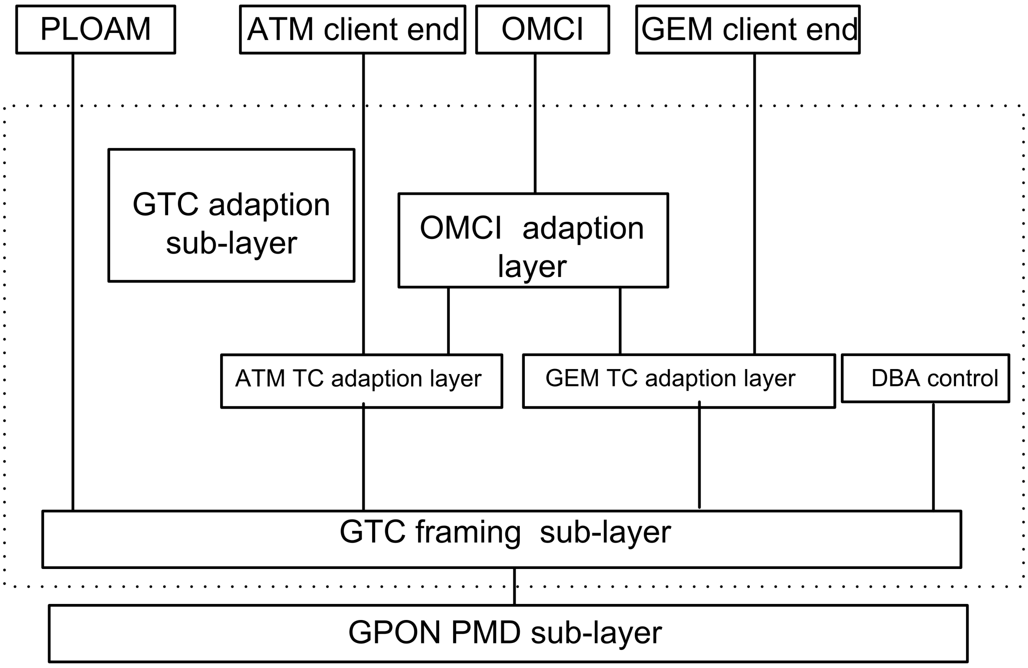
Figure 2-3 The GPON protocol stack architecture

◆ The PMD layer

The GPON PMD layer corresponds to the optical transmission interface between the OLT and the ONU (also called the PON interface); the maximum transmission distance and maximum split ratio of the GPON system depend on the parameter values in the PMD layer.

◆ The TC layer

The TC layer (also called the GTC layer) is the core layer of the GPON, and mainly performs the two key functions as follows: the MAC of the uplink service stream and the registration of an ONU. The protocol stack of the TC layer is shown in Figure 2-4, and the OLT controls the ONUs via the OMCI.



OMCI ONU management and control interface
GEM GPON Encapsulation mode
PLOAM Physical layer OAM

Figure 2-4 The TC layer architecture

The GTC layer includes two sub-layers: the GTC framing sub-layer and the GTC adaption sub-layer. The GTC framing sub-layer performs the following three functions: the multiplex / demultiplex function, the frame header generation and decoding function, and the internal routing function.

The GTC adaptive sub-layer provides three TC adapters: the ATM TC adapter, the GEM TC adapter, and the OMCI adapter. The ATM / GEM TC adapter generates the PDUs of various ATM / GEM blocks from the GTC framing sub-layer, and maps these PDUs into the corresponding blocks.

Encapsulation mode

In the GPON TC layer, the GEM frame structure is specially defined to encapsulate the services except for the ATM service, including the TDM and Ethernet data services. The GEM frame structure is shown in Figure 2-5.

PLI 12 bits	Port ID 12 bits	PTI 3 bits	HEC 13 bits	Payload Variable length

Figure 2-5 The GPON transmission frame structure

The data transmitted in the GPON system use the GEM encapsulation mode; the data type information of the valid payload in the GEM frame is displayed in the GEM frame header, so as to provide the GEM control frame for transferring the management and control information from the OLT.

GPON key technologies

- The generic framing protocol
- The dynamic bandwidth allocation
- The system synchronization
- Ranging and delay compensation
- The RTT compensation
- The burst receiving and transmitting
- The generic framing protocol
- The MPCP protocol
- The OMCI protocol

OAM

The OAM functions of the GPON system include the following aspects:

- Supports the uniform management by the network management system, and has the functions of the performance management, fault management, configuration management, and the security management.
- Supports the interconnection of the OMCI protocol.
- Supports the authentication and configuration of an ONU.
- Supports the loopback test.

2.5 Reference Information

Reference standard

- ITU-T G.984.1: General characteristics for Gigabit-capable Passive Optical Networks (GPON)
- ITU-T G.984.2: Gigabit-capable Passive Optical Networks (GPON):Physical Media Dependent (PMD) layer specification
- ITU-T G.984.3: Gigabit-capable Passive Optical Networks (GPON): Transmission convergence layer
- ITU-T G.984.4:Gigabit-capable Passive Optical Networks(GPON): ONT management and control interface specification

Terminology

None

Abbreviations

Abbreviation	Meaning
ATM	Asynchronous Transfer Mode
DBA	Dynamic Bandwidth Assignment
GEM	G-PON Encapsulation Method
GPON	Gigabit-capable Passive Optical Network
LLID	Logical Link Identifier
MPCP	Multiple point control protocol
OAM	Operation, administration and maintenance
ODN	Optical Distribution Network
OLT	Optical Line Terminal
OMCI	ONT Management Control Interface
ONU	Optical Network Unit
P2MP	Point to Multiple Point
PLOAM	Physical Layer Operations, Administration and Maintenance
PMD	Physical Medium Dependent
RTT	Round Trip Time
T-CONT	Transmission Container

3 EPON Terminal Management

☑ Definition

☑ Features

☑ Specifications

☑ Basic Principles

☑ Reference Information

3.1 Definition

The EPON terminal management function refers to the following operation: An EPON OLT performs the service configuration and management of the EPON ONU using the OAM extension protocol. Users can manage and configure the ONU via the GUI or CLI network management system at the OLT side.

3.2 Features

◆ Implements the automatic delivering of services

An EPON OLT supports the off-line configuration of an EPON ONU and the configuration recovery after the EPON ONU is on line. The EPON ONU does not need to save the configuration by itself.

◆ Implements the visual maintenance of the terminal equipment

The ONU acts as the remote equipment of the OLT; in the network management system, users can manage the OLT and the ONU as one network entity.

◆ Supports advanced management standards

The OAM extension protocols are used to manage the ONU, the ONU ports, and the port properties.

3.3 Specifications

◆ Supports multiple ONU types, such as the SFU and box-shape MDU (including the LAN type MDU and the xDSL type MDU), the plug-in MDU, and the HGU type ONU.

◆ Supports the access of up to 4096 (under the EC4B card) or 8192 (under the EC8B card) EPON ONUs.

◆ Supports the EPON ONU automatic discovery and detection function, and can report the SN and MAC address of an ONU to the network management system automatically.

- Supports the following authentication modes for the legality of an EPON ONU: the physical-address-based authentication, the logical-ID-based authentication, the logical-ID-and-password-based authentication, the mixed authentication 1 (the logical ID + the physical address), the mixed authentication 2 (the logical ID + the password + the physical address).
- Supports the pre-authorization, the pre-configuration, and the batch configuration of EPON ONUs.
- Supports the restriction on the number of MAC addresses accessed via the FE port of an EPON ONU.
- Supports the restriction on the number of multicast groups that an FE of an EPON ONU can join.
- Supports the port binding function of an EPON ONU, so as to prevent the access of illegal users.
- Supports the uplink / downlink port rate restriction function of an EPON ONU.
- Supports the classification, marking, queuing, and scheduling of the uplink service streams on an EPON ONU.
- Supports the management of the ports status and the auto-negotiation on an EPON ONU.
- Supports the flow control of the FE port on an EPON ONU.
- Supports the online query on the multicast information of an EPON ONU, and the multicast information includes the online multicast groups, the group members, the status, etc.
- Can control the forwarding of multicast packets by an EPON ONU.
- Supports the uploading, upgrade in a batch manner, and automatic upgrade of the EPON ONU software.
- Supports the automatic rollback function during the upgrade of the EPON ONU software.
- Supports the exporting of the configuration file of an ONU.
- Supports setting the MAC address aging time of an ONU.
- Supports the management on the FEC function of the PON port of an EPON ONU.

- ◆ Supports the collection of the user side interface performance parameters of an EPON ONU and the optical power monitor and detection of an ONU optical module.

3.4 Basic Principles

OAM protocol

The Ethernet OAM is a tool to monitor the faults in the network. It runs at the data link layer, and uses the regular interactivities of the OAM PDU between equipment sets to report the network status. It helps the network administrator to manage the network more efficiently and more validly.

The OAM protocol defines the message format of the interactivities between the OLT and the ONU, and provides a logical communication channel.

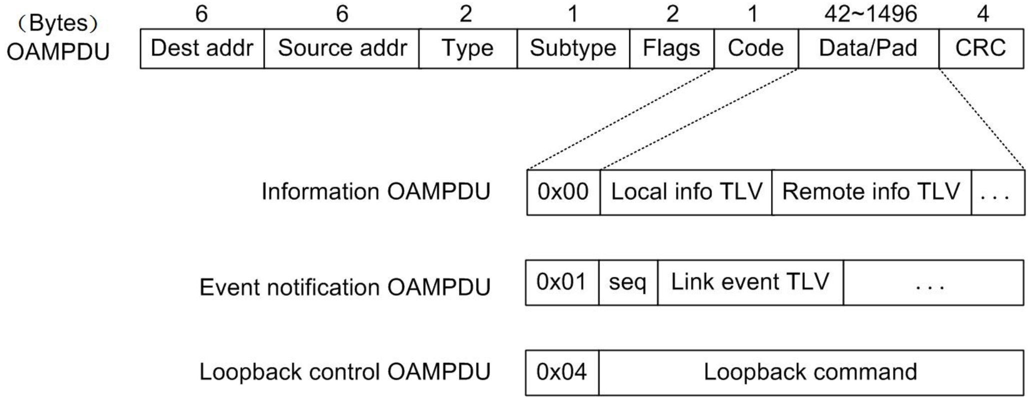


Figure 3-1 The OAM PDU message format and common OAM PDUs

Table 3-1 Meanings of key fields in the OAM PDU

Field	Meaning
Dest addr	The destination MAC address, and its value is the slow protocol multicast addresses: 0x0180-C200-0002. The feature of the slow protocol message is that it cannot be forwarded by the bridge; so the OAM message cannot be forwarded crossing multiple hops regardless of whether the system has the OAM function or the OAM function is enabled.
Source addr	The source MAC address, and its value is the MAC address of the Tx port (if this address does not exist, use the bridge MAC address of this equipment). It should be a unicast MAC address.

Table 3-1 Meanings of key fields in the OAM PDU (Continued)

Field	Meaning
Type	The protocol type, and its value is 0x8809.
Subtype	The protocol sub-type, and its value is 0x03.
Flags	The Flag field, and includes the status information of the OAM entity.
Code	The message code, and each value indicates a certain OAM PDU type.

Table 3-2 Common OAM PDUs

Code Value	Message Type	Purpose
0x00	Information OAM PDU	Exchanges the status information (including the local information TLV, the remote information TLV, and the user defined information TLV) between the OLT and the ONU.
0x01	Event Notification OAM PDU	Raises the alarms for the faults that occur in the OLT and ONU links.
0x04	Loopback Control OAM PDU	Is used to test the link quality and isolate the link faults. This message includes the enabling / disabling information, used to enable / disable the remote loopback function.

Hereinafter we introduce the operation mechanism of the OAM:

- The establishment process of an OAM connection is also called the discovery phase. In this phase, the OLT discovers the remote ONU, and establishes the stable session with it. After the OAM connection is established, the information OAM PDU will be sent periodically between the OLT and the ONU to test whether the connection is normal. If a certain party does not receive the information OAM PDU from the opposite end in the connection timeout interval, the system will regard that the OAM connection has failed.
- The event notification OAM PDU is exchanged between the ONU and the OLT to monitor the link. When the equipment at one end finds a common link event, it will send the event notification OAM PDU to the opposite end; then the administrator can understand the network status dynamically by observing the alarms reported in the network management system.

- When the fault or unavailability of the equipment causes the traffic interruption, the faulty end will deliver the fault information (the urgent link event type) to the opposite end via the flag field in the information OAM PDU; then the administrator can understand the link status dynamically by observing the alarms reported in the network management system and handle the corresponding faults in time.
- The remote loopback is described as follows: In the active mode, when the ONU (OLT) sends a packet except for the OAM PDU, the opposite end will loop back the packet to the local end directly after receiving it. This function can be used to identify the fault in the link and test the link quality. The network administrator can determine the link performance (including the packet loss rate, the delay, the jitter, etc.) by observing the returning condition of the non-OAM-PDU packet.

Extended OAM

The extended OAM extends the types of OAM PDUs based on the Ethernet OAM technology. Via the extended OAM PDUs, the request and response of the connection can be completed between the OLT and the ONU; in addition, the OLT can perform the remote management of the ONU.

The extended OAM defines a new kind of TLV field in the information OAM PDU: the organization specific information TLV; the information OAM PDU including this field is called the extended information OAM PDU.

The organization specific information field includes the following contents:

- The local OUI address: Identifies the manufacturer of the local equipment set.
- The supported OUI address: Identifies the equipment that can be connected with the local OLT or ONU and its manufacturer.
- The OAM version No.: Identifies the OAM protocol version used by the local OLT or ONU.

The organization specific OAM PDU is a newly-added OAM PDU. It uses 0xFE as the identifier type field; when users manage the ONU at the OLT end, the extended OAM can encapsulate various operation and confirmation information into the Data field of the organization specific OAM PDU for transmission.

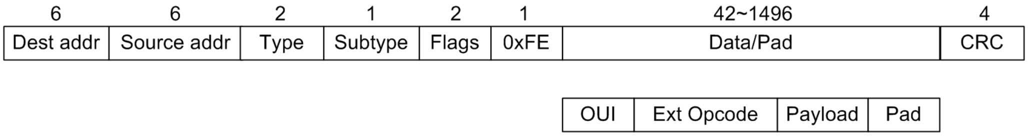


Figure 3-2 The packet format of the organization specific OAM PDU

The Data field is composed of the following parts:

- OUI: the OUI address of the Tx equipment.
- Ext.Opcode: the extension operation code. The extended OAM uses a dedicated code to identify the corresponding operation of the packet.
- Payload: Includes the code and contents to be configured corresponding to the function that needs to be configured or queried by the user.
- Pad: the padding field.

Table 3-3 The codes of the extension operations

Code	Operation Type	Description
0x01	Extended Variable Request	The OLT uses it to query the extension features of the ONU.
0x02	Extended Variable Response	The ONU uses it to return its extension features to the OLT.
0x03	Set Request	The OLT uses it to configure the extension features / operations of the ONU.
0x04	Set Response	The ONU uses it to return is acknowledgement for the extension features / operation configuration to the OLT.
0x05	ONU Authentication	Is used to perform the ONU authentication based on the logical ID.
0x06	Software Download	Is used for the ONU to download the software.
0x09	Churning	Is used to exchange the key related to Triple-Churning.
0x0A	DBA	It is used to query and configure the DBA function.
Other Value	Reserved for future use	Reserved.

Hereinafter we introduce the operation mechanism of the extended OAM:

- The discovery of the extended OAM

  Before performing the data transmission with the ONU equipment, the OLT needs to use the extended OAM discovery function to determine whether it can communicate with the opposite end equipment normally.

  First the OLT and the ONU need to complete the standard OAM discovery, and determine whether the link status is normal via the standard OAM. After determining that the link is normal, the OLT and the ONU will exchange the extended information OAM PDU to inform the other party on the OUI address, the OUI address that can be supported and the OAM version No. If the OUI addresses and OAM versions at the two ends are both in the range that is supported by the opposite end, the extended OAM discovery will end normally, and the data transmission will start; otherwise the communication cannot be performed normally.

- The management of the extended OAM

  After the discovery of the extended OAM is completed, the OLT can configure the ONU in the remote mode via the organization specific OAM PDU.

Message exchange mechanism

The terminal configuration management information of the AN116-06B is delivered to the EPON ONU through the OAM channel; the status and alarm information of the ONU is reported to the AN116-06B through the OAM channel.

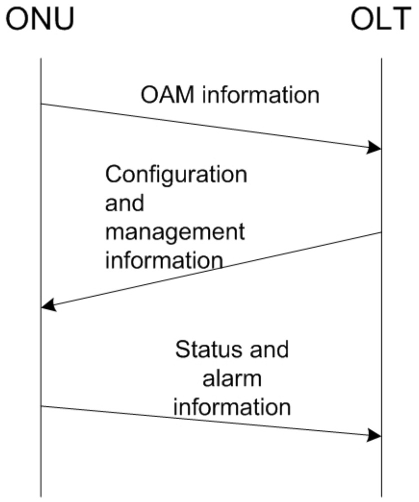

ONU
OLT
OAM information
Configuration and management information
Status and alarm information

Figure 3-3 The message exchange flow

The steps to establish the OAM channel between the AN516-06B and the EPON ONU are described as follows:

1. After the EPON ONU is powered on, it exchanges the OAM message with the AN5116-06B to complete the registration.
2. The AN5116-06B delivers the terminal configuration and management information to the ONU through the OAM channel.
3. The ONU reports the status and alarm information to the AN5116-06B through the OAM channel.

3.5 Reference Information

Reference standard

◆ IEEE 802.3-2005：IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks–Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

Terminology

None

Abbreviations

Abbreviation	Meaning
EPON	Ethernet Passive Optical Network
HGU	Home Gateway Unit
MDU	Multiple Dwelling Unit
OAM	Operations，Administration and Maintenance
OLT	Optical Line Termination
ONU	Optical Network Unit
OUI	Organizationally Unique Identifier
PDU	Protocol Data Units
SFU	Single Family Unit
TLV	Type Length Value

4 GPON Terminal Management

- ☑ Definition
- ☑ Features
- ☑ Specifications
- ☑ Basic Principles
- ☑ Reference Information

4.1 Definition

The GPON terminal management function refers to the following operation: A GPON OLT performs the service configuration and management of the GPON ONU using the OMCI extension protocol. Users can manage and configure the ONU via the GUI or CLI network management system at the OLT side.

4.2 Features

- ◆ Implements the automatic delivering of services

  A GPON OLT supports the off-line configuration of a GPON ONU and the configuration recovery after the GPON ONU is on line. The GPON ONU does not need to save the configuration by itself.

- ◆ Implements the visual maintenance of the terminal equipment

  The ONU acts as the remote equipment of the OLT; in the network management system, users can manage the OLT and the ONU as one network entity.

- ◆ Supports advanced management standards

  The OMCI protocols are used to manage the VLAN configuration and the port properties on the ONU.

4.3 Specifications

- ◆ Supports multiple ONU types, such as the SFU and box-shape MDU (including the LAN type MDU and the xDSL type MDU), the plug-in MDU, and the HGU type ONU.
- ◆ Supports the access of up to 4096 (under the GC4B card) or 8192 (under the GC8B card) GPON ONUs.
- ◆ Supports the GPON ONU automatic discovery and detection function, and can report the SN and MAC address of an ONU to the network management system automatically.

- Supports the following authentication modes for the legality of a GPON ONU: the physical-address-based authentication, the password-based authentication, the physical-address-and-password-based authentication, the logical SN (without password)-based authentication, the logical SN (without password)-based authentication, the logical SN (with password)-based authentication, physical SN / logical SN (without password)-based mixed authentication and physical SN / logical SN (with password)-based mixed authentication.
- Supports the pre-authorization, pre-configuration and configuration in a batch manner for the GPON ONU.
- Supports the configuration and management of the ONU T-CONT.
- Supports the configuration of the mapping from the ONU traffic to the GEM port.
- Supports the configuration of the mapping from the ONU GEM port to the T-CONT.
- Supports the restriction on the number of MAC addresses accessed via the FE port of a GPON ONU.
- Supports the restriction on the number of multicast groups that an FE of a GPON ONU can join.
- Supports the port binding function of a GPON ONU, so as to prevent the access of illegal users.
- Supports the uplink / downlink port rate restriction function of a GPON ONU.
- Supports the classification, marking, queuing, and scheduling of the uplink service streams on a GPON ONU.
- Supports the management of the ports status and the auto-negotiation on a GPON ONU.
- Supports the flow control of the Ethernet port on a GPON ONU.
- Supports the online query on the multicast information of a GPON ONU, and the multicast information includes the online multicast groups, the group members, the status, etc.
- Can control the forwarding of multicast packets by a GPON ONU.
- Supports the uploading and batch upgrade of the GPON ONU software.

- Supports the automatic rollback function during the upgrade of the GPON ONU software.
- Supports the exporting of the configuration file of an ONU.
- Supports copying the configuration of an ONU.
- Supports setting the MAC address aging time of an ONU.
- Supports the management on the FEC function of the PON port of a GPON ONU.
- Supports the collection of the user side interface performance parameters of a GPON ONU and the optical power monitor and detection of an ONU optical module.

4.4 Basic Principles

The OMCI protocol

The OMCI protocol is mainly defined by ITU-T G.984.4; in addition, it uses the definition architecture on the OMCI in BPON, such as ITU-T G.983.2. The OMCI protocol defines the format of the message interaction between the OLT and the ONU, and provides a logical communication channel.

In the GEM mode, the OMCI message is encapsulate in the GEM packet directly.

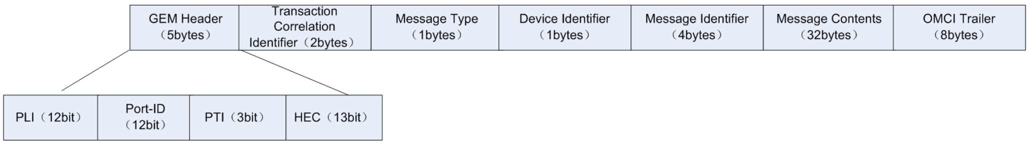

GEM Header（5bytes）
Transaction Correlation Identifier（2bytes）
Message Type（1bytes）
Device Identifier（1bytes）
Message Identifier（4bytes）
Message Contents（32bytes）
OMCI Trailer（8bytes）
PLI（12bit）
Port-ID（12bit）
PTI（3bit）
HEC（13bit）

Figure 4-1 The frame structure of the OMCI message

Table 4-1 Key fields of the OMCI message frame and their meanings

Field	Meaning
GEM Header	PLI identifies the length of payload following the header. Port-ID identifies the port ID. PTI identifies the content type and corresponding processing mode of the payload. HEC performs the error detection and correction function of the header.
Transaction Correlation Identifier	The transaction correlation identifier is used to correlate a request message and its response message. An OLT selects an transaction correlation identifier randomly for a request message, and the response message has the transaction correlation identifier of the message to which it responds.
Message Type	The message type mainly includes set, get, etc.
Device Identifier	For the GPON equipment, the equipment ID is 0x0A.
Message Identifier	The two most significant valid bytes of the message identifier are used to identify the destination managed entity of the designated operation in the message type field, and the two least significant valid bytes of the message identifier are used to identify the status of the destination managed entity.
Message Contents	The message contents. The OMCI frame is padded according to the message type of the managed entity.
OMCI Trailer	Is used to pad the check code.

The OLT controls the ONU using the OMCI protocol. The OMCI protocol allows the following operations of the OLT:

- Sets up and tears down the connection with the ONU;
- Manages the UNI on the ONU;
- Delivers the request of the configuration and performance statistics information.
- Reports events (such as the link fault) to the network administrator automatically.

Message exchange mechanism

The terminal configuration management information of the AN116-06B is delivered to the GPON ONU through the OMCI channel; the status and alarm information of the ONU is reported to the AN116-06B through the OMCI channel.

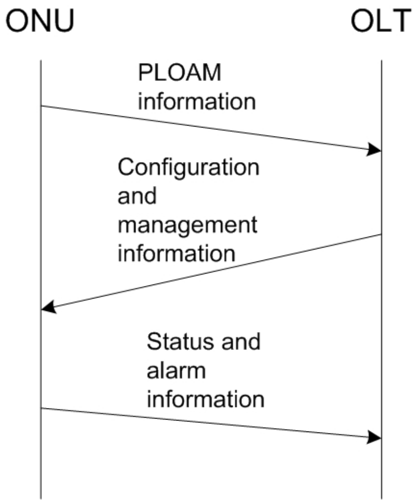

ONU
OLT
PLOAM information
Configuration and management information
Status and alarm information

Figure 4-2 The message exchange flow

The steps to establish the OMCI channel between the AN516-06B and the GPON ONU are described as follows:

1. After the GPON ONU is powered on, it exchanges the PLOAM (Physical Layer OAM) message with the AN5116-06B to complete the register operation.
2. The AN5116-06B obtains the OMCI capability of the ONU via the PLOAM message. When the ONU also supports the OMCI protocol, an OMCI channel can be established between the AN5116-06B and the ONU.
3. The AN5116-06B delivers the terminal configuration and management information to the ONU through the OMCI channel.
4. The ONU reports the status and alarm information to the AN5116-06B through the OMCI channel.

4.5 Reference Information

Reference standard

- ITU-T G.983.2:ONT management and control interface specification for ATM PON
- ITU-T G.984.4:Gigabit-capable Passive Optical Networks (GPON): ONT management and control interface specification

Terminology

Terminology	Description
OMCI	The OMCI is an OAM service, and provides the standard methods for discovering the ONU capability and configuring / managing the ONU data. It is defined by ITU-TG.984.4.
T-CONT	The T-CONT manages the uplink bandwidth allocation of the PON in the transmission and convergence layer, and is mainly used to increase the uplink bandwidth usage efficiency of the PON.

Abbreviations

Abbreviations	Meaning
BPON	Broadband Passive Optical Network
GEM	GPON Encapsulation Method
GPON	Gigabit-capable Passive Optical Network
HGU	Home Gateway Unit
MDU	Multiple Dwelling Unit
OMCI	Optical Network Termination Management and Control Interface
OLT	Optical Line Termination
ONU	Optical Network Unit
SFU	Single Family Unit
T-CONT	Transmission Containers

5 Multicast Service Access

- ☑ Multicast
- ☑ IGMP Proxy
- ☑ IGMP Snooping
- ☑ Multicast VLAN Management
- ☑ User Management
- ☑ Program Management
- ☑ PIM-SM

5.1 Multicast

5.1.1 Definition

The multicast refers to the following operation: The multicast source sends the information to a certain subset of all the network nodes. The source host only sends one data packet, and multiple receivers can receive the same copy of this packet.

5.1.2 Features

- Adopts the single-point transmitting and multipoint receiving, so as to implement the point-to-multipoint data transport effectively.
- Saves the network bandwidth significantly and reduces the network load effectively.
- Enables some new value-added services, including live online radio, TV, remote medical care, remote education, and real-time video conferencing.

5.1.3 Specifications

- Supports the IGMP V2 / V3.
- Supports the IGMP Proxy.
- Supports the IGMP Snooping.
- Supports the tree and ring network.
- Supports the RPF.
- Supports the controllable multicast, including the multicast VLAN management, the user management, the program management, etc.

5.1.4 Basic Principles

Typical network

Uses the SCB + IGMP mode to deliver the multicast service, and the typical network of the multicast service is shown in Figure 5-1.

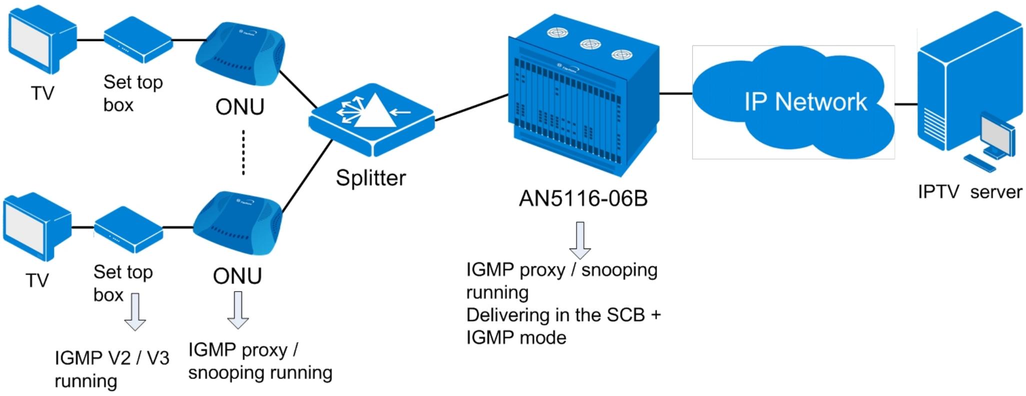
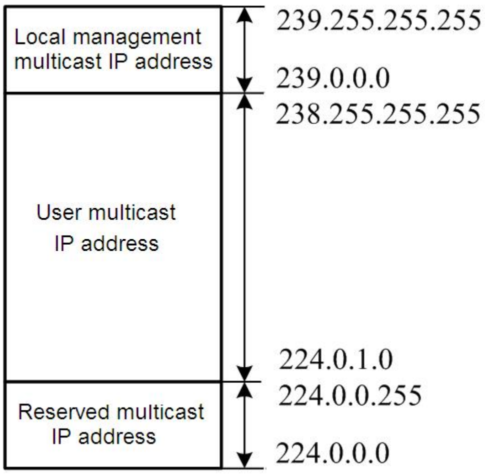

TV
Set top box
ONU
TV
Set top box
ONU
IGMP V2 / V3 running
IGMP proxy / snooping running
Splitter
AN5116-06B
IGMP proxy / snooping running
Delivering in the SCB + IGMP mode
IP Network
IPTV server

Figure 5-1 The typical network of the multicast service

Multicast IP address

The multicast IP address is used to identify an IP multicast group. The IANA allocates the D-type address space to the IP multicast service, and the value of an IP address ranges from 224.0.0.0 to 239.255.255.255.


Local management multicast IP address
239.255.255.255
239.0.0.0
238.255.255.255
User multicast IP address
224.0.1.0
224.0.0.255
Reserved multicast IP address
224.0.0.0

Multicast Protocols

- The protocol between the host and the route, namely the multicast membership management protocol, such as the IGMP. The IGMP establishes and maintains the group membership information of the directly-connected network segment on a certain router.

- The multicast routing protocol between various routers, including the intra-domain multicast routing protocol and the inter-domain multicast routing protocol.
  - The intra-domain multicast routing protocol includes the PIM-SM, the PIM-DM, the DVMRP, etc. The intra-domain multicast routing protocol forms the multicast distribution tree to forward the multicast packets using a certain multicast route algorithm, according to the multicast group member relationship information maintained by the IGMP.
  - The inter-domain multicast routing protocol includes the MBGP, the MSDP, etc. The inter-domain multicast routing protocol sends route information with multicast capability and multicast source information between various autonomous areas, so as to forward the multicast data between different domains.

IGMP protocol messages

- The IGMP report message: This message is sent to the multicast router by the multicast application terminal, and is used to request for joining a certain multicast group or responding to the IGMP query message.
- The IGMP general query message: This message is sent to multicast group members by the multicast router, and is used to query which multicast groups have members.
- The IGMP group-specific query message: This message is sent to multicast group members by the multicast router, and is used to query whether an designated multicast group has members. When the multicast router receives an IGMP group-specific query message, it only sends the query message to the IP multicast group to be queried.

- The IGMP leave message: This message is sent to the multicast router by a certain multicast group member router, and is used to notify the multicast router that the multicast application terminal has left a certain multicast group. When the multicast router receives the leave message of a certain multicast group, it will send an IGMP group-specific query message of this group to the port which receives the leave message for querying whether other members of this multicast group still exist under this port. At the same time, the system will start up a response query timer. If the system does not receive the report message of this multicast group in the timeout interval of this timer, this port will be deleted from the corresponding multicast group.

5.1.5 Reference Information

Reference standard

- IETF RFC 2236:Internet Group Management Protocol, Version 2
- IETF RFC 3376:Internet Group Management Protocol, Version 3
- IETF RFC 2117:Protocol Independent Multicast-Sparse Mode(PIM-SM): Protocol Specification
- IETF RFC 2362:Protocol Independent Multicast-Sparse Mode(PIM-SM): Protocol Specification
- IETF RFC 3973:Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)

Terminology

None.

Abbreviations

Abbreviations	Meaning
DVMRP	Distance Vector Multicast Routing Protocol
IANA	Internet Assigned Numbers Authority
IGMP	Internet Group Management Protocol
MBGP	Multiprotocol BGP
MSDP	Multicast Source Discovery Protocol
PIM-DM	Protocol Independent Multicast-Dense Mode

Abbreviations	Meaning
PIM-SM	Protocol Independent Multicast-Sparse Mode
RPF	Reverse Path Forwarding
SCB	Single Copy Broadcast
VLAN	Virtual Local Area Network

5.2 IGMP Proxy

5.2.1 Definition

The IGMP proxy refers to the following operation: The equipment acts as a multicast proxy between the multicast router and the multicast users. For the multicast router, the equipment can be regarded as a multicast user; for the multicast users, the equipment can be regarded as a multicast router.

5.2.2 Features

- The equipment manages the group member status actively.
- Can reduce the load of the uplink equipment effectively.

5.2.3 Specifications

- The HSWA card and PON interface card can implement the proxy of two levels.
- Supports the IGMP V2 / V3 Proxy.
- Implements the query function to support the general and group-specific query mechanism.
- Implements the report function to respond to the query from the upper-level router.
- Supports the IGMP host function, and sends the join and leave messages to the upper-level multicast router.
- Supports the tree and ring network.

5.2.4 Basic Principles

As an IGMP proxy, the AN5116-06B intercepts all IGMP requests sent by the multicast application terminal and processes them; then forwards them to the upper-level multicast router and establishes the correspondence relationships between the group members and the PON interfaces (this is called the multicast forwarding table). At the same time, the AN5116-06B forwards the multicast packets to various PON interfaces according to the multicast forwarding table. The AN5116-06B emulates the multicast application terminal on the uplink port, and emulates the multicast router on the PON interface.

When the equipment works in the IGMP proxy mode, the flow for a user to view the multicast program is described as follows:

1. The multicast application terminal sends an IGMP report message to subscribe to the object program.
2. After the AN5116-06B receives this report, the operations are described as follows: If the multicast service stream of the object channel has not been sent to the uplink port of the equipment (meaning that no users under the equipment are viewing this program), the equipment will subscribe to this channel to the multicast router and establish the corresponding multicast forwarding table; after the multicast service stream of the object channel is sent to the uplink port of the equipment, the equipment will forward it to the user PON interface and the corresponding ONU. If the multicast service stream of the object channel has been sent to the uplink port of the equipment but has not been sent to the user PON interface (meaning that a certain user under other PON interfaces of the equipment is viewing this program), the equipment will forward it to the user PON interface and the corresponding ONU. If the multicast service stream of the object channel has been sent to the user PON interface (meaning that a certain user under this PON interface is viewing this program), the equipment will map it to the user ONU directly.

3. The AN5116-06B sends the IGMP general query messages to all online users periodically. If the AN5116-06B does not receive the response messages of any multicast user in the set interval, it will delete this multicast group from the multicast forwarding table; at the same time, the AN5116-06B will send a leave message to the uplink multicast router for notifying the uplink multicast router to stop sending the service stream of this multicast program. If the AN5116-06B receives the response messages of a multicast user in the set interval, it will continue to send the service stream of this multicast program.

4. When the user is to leave a certain multicast channel to which the user has subscribed, the multicast application terminal will send an IGMP leave message to the AN5116-06B, and the AN5116-06B will send a designated number of IGMP group-specific query messages o this PON interface. The AN5116-06B determines whether to stop forwarding this multicast service stream depending on whether it has received the IGMP report message from the user PON interface in the set timeout interval. If another user is viewing this channel now, the AN5116-06B will maintain forwarding the multicast service stream of this channel in the downlink direction; if no other users exist under this PON interface after the object user leaves this channel, the AN5116-06B will stop forwarding the multicast service stream of this channel in the downlink direction.

5.2.5 Reference Information

Reference standard

- IETF RFC 2236:Internet Group Management Protocol, Version 2
- IETF RFC 3376:Internet Group Management Protocol, Version 3

5.3 IGMP Snooping

5.3.1 Definition

The IGMP snooping refers to the following operation: The equipment snoops the IGMP protocol packet between the multicast router and the multicast terminal user, establishes the multicast member relationship table, and forwards the multicast service according to the multicast member relationship. This is to ensure that a group member can receive the correct multicast service, and other hosts cannot.

5.3.2 Features

- The IGMP snooping influences the equipment load at least.
- The protocol processing load of the uplink equipment is relatively heavy.

5.3.3 Specifications

- The HSWA card and the PON interface card both work in the snooping mode.
- Supports the IGMP V2 / V3 snooping.
- Implements the query function to support the general and group-specific query mechanism.
- Supports the tree and ring network.

5.3.4 Basic Principles

Via snooping the IGMP member report message sent to the multicast router by the application terminal, the AN5116-06B forms the correspondence relationship between the group members and the switch interfaces (namely the multicast forwarding table). The AN5116-06B forwards the received downlink multicast packets to the corresponding interface of the group member according to the multicast forwarding table. The IGMP snooping can solve the problem of packets flooding of layer 2, but it requires that the AN5116-06B can extract the information of layer 3; in addition, the AN5116-06B needs to monitor and unscramble all multicast packets.

5.3.5 Reference Information

Reference standard

- IETF RFC 2236:Internet Group Management Protocol, Version 2
- IETF RFC 3376:Internet Group Management Protocol, Version 3

5.4 Multicast VLAN Management

5.4.1 Definition

For the multicast service, one or multiple dedicated multicast VLANs are used to isolate it from other services. One multicast VLAN corresponds to one multicast channel or one channel group (a channel group means the set of multicast channels under the management of a united entity). One multicast channel can belong to only one dedicated multicast VLAN.

5.4.2 Features

It increases the manageability of the multicast VLAN number and the multicast VLAN translation.

5.4.3 Specifications

- The equipment supports seven multicast VLANs.
- One multicast VLAN can include up to 1024 multicast programs.
- The equipment supports the translation function of the multicast VLAN.
- The equipment supports to manage and identify program sources and users based on the multicast VLAN.

5.4.4 Basic Principles

In the IGMP proxy or IGMP snooping working mode, the system uses the following flow to manage multicast VLANs:

- In the uplink direction: If an uplink IGMP Join packet or IGMP Leave packet is untagged, the system will tag it with a legal multicast VLAN ID; if an uplink IGMP Join packet or IGMP Leave packet is tagged, the system will translate its VLAN ID into a legal multicast VLAN ID that can be identified by the AN5116-06B.
- In the downlink direction: The system will translate the legal downlink multicast data stream and IGMP Query packet VLAN ID that can be identified by the AN5116-06B into a legal VLAN ID that can be identified by the ONU.

In the controllable working mode, the system uses the following flow to manage multicast VLANs:

- In the uplink direction: If an uplink IGMP Join packet or IGMP Leave packet is untagged, the system will tag it with a port No. to perform the port user identification; if an uplink IGMP Join packet or IGMP Leave packet is tagged, the system will translate its VLAN ID into a port No. to perform the port user identification.
- In the downlink direction: The system will translate the legal downlink multicast data stream and IGMP Query packet VLAN ID that can be identified by the AN5116-06B into a legal VLAN ID that can be identified by the ONU.

5.4.5 Reference Information

None.

5.5 User Management

5.5.1 Definition

The user management refers to the following operation: Authorizes multicast users and validates the legality of a user to prevent illegal users from viewing the controlled multicast program.

5.5.2 Features

It increases the manageability of the legality and authorization of a user.

5.5.3 Specifications

- A user can view up to 1024 multicast programs and preview up to 128 multicast programs.
- The equipment supports limiting the authorization for a user to view / preview programs. If the user is only allowed to preview a certain program, the equipment supports to limit the preview times, the preview time, the preview interval, etc.
- The equipment supports forcing an designated multicast user to leave.
- The equipment supports setting the leave mode of a multicast user. The leave mode includes the fast leave and the normal leave.
- The equipment supports the information statistics of multicast users, including the view times, the average view time, the maximum view time, and the total view time of each user.
- The equipment supports the hierarchical management of the online group information, including the uplink port online group information, the HSWA card online group information, the PON interface card online group information, and the ONU online group information.

5.5.4 Basic Principles

User authorization

When a multicast application terminal (such as a set top box) applies for a certain multicast channel, it will send the IGMP report message in the uplink direction. After receiving the uplink IGMP report message, the ONU tags it with a VLAN tag to identify the port, and then transmits this IGMP report message to the AN5116-06B transparently.

After receiving the uplink IGMP report message, the AN5116-06B queries the view authorization to this channel and relevant parameters of this port user, according to the port ID, the multicast IP address and source IP address of the report message (the source IP address is only applicable in IGMP V3, optional).

- ◆ If the AN5116-06B finds that the view authorization to this channel of this port user is allowed, it will notify the ONU to add one entry in the multicast forwarding table via an extended multicast control OAM message. This entry indicates that the view authorization to this channel of this port user is allowed.
- ◆ If the AN5116-06B finds that the view authorization to this channel of this port user is forbidden, it performs no other operations, and the ONU performs no other operations either. If the multicast application terminal (such as a set top box) does not receive any IGMP message and multicast service stream in a certain interval, it will stop applying for this channel.
- ◆ If the AN5116-06B finds that the view authorization to this channel of this port user is preview, it will notify the ONU to add one temporary entry in the multicast forwarding table via an extended multicast control OAM message. At the same time, the AN5116-06B starts up a timer and a counter to control the preview time, preview counts, and preview interval of this user. The ONU forwards the multicast service stream from the AN5116-06B to the corresponding user port according to the temporary entry, and strips the tag. After the AN5116-06B preview timer or counter exceeds its threshold, the AN5116-06B will immediately notify the ONU to delete the temporary entry from the multicast forwarding table via an extended multicast control OAM message, and reset the timer and the counter. At the same time, the AN5116-06B will determine whether to stop forwarding the object multicast service stream to this PON interface according to whether other users in the same PON have ordered multicast service stream, and perform the relevant operations.

Fast leave

In the fast leave mode, the ONU will immediately stop forwarding the multicast service stream of the object group to the user port after receiving the IGMP Leave message (deletes the corresponding entry from the multicast authorization control table of this ONU); at the same time, the ONU will tag the IGMP Leave message with the VLAN tag identifying the Rx port of the Leave message, and then transmit it to the AN5116-06B. After receiving this IGMP Leave message, the AN5116-06B records the user port leaving multicast group event of this ONU, and determines whether other users in the same PON interface are applying for this multicast service according to the AN5116-06B local controllable multicast record information.

If other users in the same PON interface are applying for this multicast service, the equipment will keep forwarding this multicast service to the PON interface; If no other users in the same PON interface are applying for this multicast service, the equipment will stop forwarding this multicast service to the PON interface.

Normal leave

In the normal leave mode, the ONU will start the last member query mechanism after receiving the IGMP leave message; that is, send the group-specific query message to the UNI port having received the leave message and then start the response timer. If the ONU does not receive the IGMP report message from the multicast application terminal in group-specific query interval, the ONU will determine that no other members of this multicast exist under this port. So the ONU will delete this port from the multicast group and stop forwarding the corresponding multicast service stream to this port; then the ONU tags the IGMP leave message with the VLAN tag identifying the user identity, and transmit it to the AN5116-06B transparently. If the ONU receives the IGMP report message corresponding to this multicast group from this port in the group-specific query timeout interval, the ONU will keep the original multicast forwarding table and continue to forward this multicast service stream to this port; at the same time, the ONU will discard the IGMP leave message.

5.5.5 Reference Information

Reference standard

None.

Terminology

None.

Abbreviations

Abbreviations	Meaning
OAM	Operation, Administration and Maintenance

5.6 Program Management

5.6.1 Definition

The program management refers to the management on the multicast program properties, and the managed multicast program properties include the bandwidth, the preview parameters, the multicast VLAN, the leave delay, etc.

5.6.2 Features

It increases the manageability of the quantity, bandwidth, and preview parameters of the multicast programs.

5.6.3 Specifications

- The equipment supports 4096 multicast programs.
- Each PON interface supports 1024 multicast programs.
- Each FTTH ONU supports 32 multicast programs; each FTTB ONU supports 1024 multicast programs.
- The equipment supports the pre-joining of a multicast program.
- The equipment supports the bandwidth setting of a multicast program.
- The equipment supports the preview parameter setting of a multicast program.
- The equipment supports the information statistics of multicast programs, including the view times, the average view time, the maximum view time, and the total view time of each multicast program.
- The equipment supports the hierarchical management of the online group information, including the uplink port online group information, the HSWA card online group information, the PON interface card online group information, and the ONU online group information.

5.6.4 Basic Principles

Pre-joining of a multicast program

The pre-joining of a multicast program is described as follows: if no users view a multicast program, the AN5116-06B sends the IGMP report message to the multicast router and delivers this multicast program to the uplink port in advance; when needing to view this multicast program, a user can view it rapidly.

Multicast program bandwidth

By setting the port multicast service bandwidth and the multicast program bandwidth, the system controls the joining of a new multicast program. If the bandwidth occupied by the online programs exceeds the specified bandwidth, a new program cannot join.

Multicast program preview

The multicast program preview means that a user does not have the authorization to view a total multicast program, and the operator sets the preview times, the preview time, and the preview interval for the user to enable the user to have basic knowledge about this multicast program. According to the planning of the operator, the user needs to pay an additional fee for viewing the total multicast program.

5.6.5 Reference Information

Reference standard

None.

Terminology

None.

Abbreviations

Abbreviations	Meaning
FTTB	Fiber To The Building
FTTH	Fiber To The Home

5.7 PIM-SM

5.7.1 Definition

The protocol independent multicast routing protocol sets up multicast trees by transmitting information between routers. The multicast trees include dense mode and sparse mode.

5.7.2 Features

- The PIM-SM is a protocol independent multicast routing protocol in sparse mode, mainly applied to wide network whose members are located dispersedly.
- Supports multicast routing over large-scale network to meet the requirements of multicast services of large and medium scale network management.
- The PIM-SM protocol supports to perform route forwarding according to the unicast routing table and does not depend on any specified routing protocol, such as OSPF and RIP.

5.7.3 Specifications

Supports PIM-SM v2.

5.7.4 Basic Principles

The PIM-SM is used for the network in which the multicast users are located sparsely. A multicast routing equipment should first apply to join into the RST (Rendezvous Point Tree) before receiving the multicast data packets.

The group central point of the PIM-SM is called **public root node** RP (Rendezvous Point). RP can be responsible for the forwarding of several or all the multicast groups. One or multiple RPs can exist in the network.

The router can acquire the RP position using the following two methods.

- Statically configure the RP address manually on each router on which the PIM-SM is running.
- Start the BootStrap protocol and dynamically elect RP using the automatic election mechanism.

The working principle of the PIM-SM is as follows.

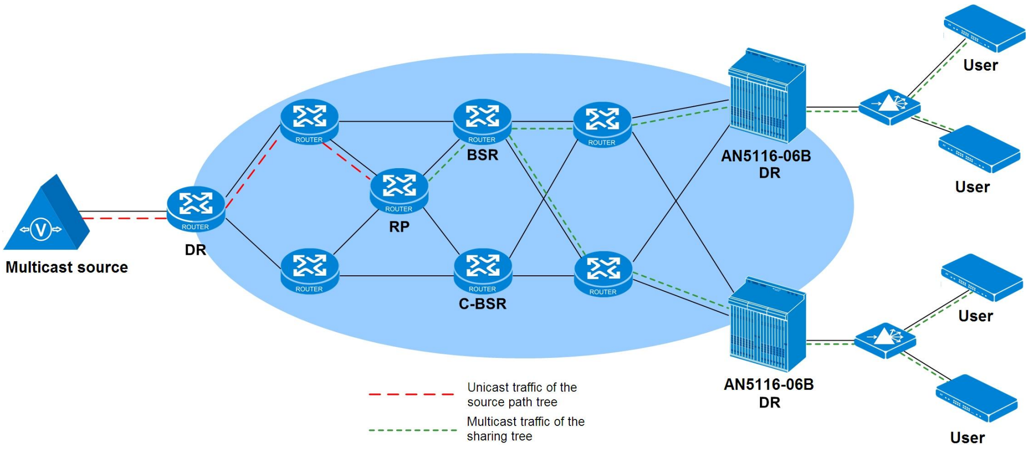

Multicast source
DR
ROUTER
RP
BSR
C-BSR
AN5116-06B
DR
AN5116-06B
DR
User
User
User
User
Unicast traffic of the source path tree
Multicast traffic of the sharing tree

Figure 5-2 PIM-SM network diagram

1. Elect the specified router DR (Designated Router).

   The PIM router discover and maintain the neighborhood by exchange the hello messages regularly. The hello messages include the router priority information. The PIM router with the highest priority in a network segment is elected as the specified router DR.

2. Elect the official BSR (BootStrap Router).

   The PIM-SM routers running on the manually configured part act as the C-BSRs (Candidate BootStrap Router), among which the C-BSR with the highest priority is elected as the BSR.

3. Elect the official RP.

   The BSR collects the announcement messages of the candidate RP, dynamically elect RP using the automatic election mechanism, and report the RP address to all the PIM routers in the domain unitedly.

4. Set up the RPT (Rendezvous Point Tree)

   The client side DR receives the IGMP messages from the multicast group users and transmit the joint messages one by one to the corresponding RP direction to form the branches of the RPT.

5. The multicast source sends the multicast data to the RP.

   The multicast source encapsulates the data package into the registrar information using the DR on the multicast source side and sends to the RP via the unicast router. After receiving the registrar information, the RP will decapsulate the data package and send the data to users along the RPT.

6. Set up the SPT (Shortest Path Tree)

   After acquiring the multicast source address, the client end DR sends the joint messages one by one to the DR on the multicast source side and sets up the SPT (Shortest Path Tree) branch.

7. Switch the RPT to the SPT

   When the data package sent by the RP received by the DR on the client end reaches a threshold value, the multicast flow will switch the RPT to the SPT. The DR on the client end sends the pruned messages to the RP one by one and the RP continues to send the pruned messages to the multicast source direction after receiving them, so as to switch the RPT to the SPT. The multicast flow can be sent to the DR on the client end directly by the SPT.

5.7.5 Reference Information

Reference standard

- IETF RFC 2117:Protocol Independent Multicast-Sparse Mode(PIM-SM): Protocol Specification
- IETF RFC 2362:Protocol Independent Multicast-Sparse Mode(PIM-SM): Protocol Specification

Terminology

Terminology	Description
Automatic election mechanism	The routers in the shared network send the Hello messages to each other (with the priority parameters of the campaign router). The router with the highest priority will be elected. If the routers has the same priority, or at least one router in the network does not support carrying the priority parameters, then the router with bigger IP address will be elected.
Pruning	The succeeding node with no receivers sends the prune messages to the previous node, so as to inform the previous node to delete the corresponding interface from the output interface list corresponding to the multicast forwarding list, and no longer forward the messages from the multicast group to this node.
Neighborhood	In the PIM domain, the router discover the PIM neighbors, maintain the PIM neighborhood between routers, and set up and maintain SPT by sending the PIM Hello messages to all the PIM routers in the multicast mode regularly.

Abbreviations

Abbreviations	Meaning
PIM-SM	Protocol Independent Multicast Sparse Mode
DR	Designated Router
BSR	BootStrap Router
RP	Rendezvous Point
RPT	Rendezvous Point Tree
SPT	Shortest Path Tree

6 VoIP Service Access

- ☑ VoIP
- ☑ H.248
- ☑ MGCP
- ☑ SIP

6.1 VoIP

6.1.1 Definition

The VoIP is a technology based on the IP telephone, and supports corresponding value-added services. The main advantage of the VoIP is that it can provide more and better services than the traditional ones by using Internet and the global IP interconnection widely. The VoIP can transport the voice, fax, video, and data services with a lower cost over the IP network, and the services supported by it include the unified messaging, the virtual telephone, the virtual voice / fax mailbox, the directory assistance service, the Internet call center, the Internet call management, the video conferencing, the E-Commerce, the fax store-and-forward, and the store-and-forward of other information types.

6.1.2 Features

- Supports the integration of multiple services, and can implement the high integration of services such as the voice, data, and fax services.
- Provides multiple network security functions (such as the access list, the record of illegal access operations, the authorization, and the accounting) and advanced QoS functions (such as the RSVP, the weighted fair queuing, the WRED, and the IP priority). Can perform powerful QoS guarantees that enable the IP telephone to provide the call quality almost like that of the PSTN telephone.
- Has an excellent configurability, and various modules can be configured as required to reduce the network construction cost greatly. The modular design of the modules allows excellent extensibility and upgradability. These features ensure profits of the enterprise investment.

6.1.3 Specifications

- Supports the access of up to 6k users at the same time.
- Supports the calling number identification presentation and restriction.
- Supports the call waiting.

- Supports the three party service.
- Supports the call forwarding (unconditional, busy and no answer).
- Supports the immediate hotline.
- Supports the blind transfer and attended transfer.
- Supports the outgoing call blocking.
- Supports the distinctive ring.
- Supports the fax service based on the T.30 / T.38 protocol.
- Supports the pulse accounting and polarity reversal accounting.
- Supports the IP CENTERX service.
- Supports the ITU-T H.248, MGCP and SIP protocol.
- Supports PSTN line quality and performance testing (for example, 112 testing made by China Telecom) which can locate phone line faults.
- The call processing capability is 25k BHCA.
- The call completing ratio is no less than 99.999%.
- Supports the voice coding modes defined by ITU-T G.711a / G.711u / G.723 / G.726 / G.729.
- Supports the silence compression and comfort noise generator functions.
- Supports the echo suppression function.
- Supports the multi-MGC list.
- Supports the 802.1Q VLAN and priority configuration of each voice channel.

6.1.4 Basic Principles

The VoIP uses the IP data network based on the router / packet switching for the transmission. Because a data packet is transferred using the store-forward mechanism in Internet and does not occupy an independent circuit, and the voice signals are compressed greatly, the IP telephone only needs to occupy a bandwidth of 8 kbit/s to 10 kbit/s. Internet uses the standard TCP / IP protocol to implement the communication and data exchange between various computers.

The TCP / IP protocol is in charge of sending the IP packets needing transmission to the network in packets and queues. Each packet includes the address and data reassembly information to assure that the data are secure and the data packets are switched correctly. The IP telephone uses Internet as the main medium of the voice transmission.

1. The voice signal is transmitted to the IP telephone gateway via the PSTN telephone network;
2. The IP telephone gateway converts and compresses the voice signal into the digital signal;
3. The digital signal is transmitted to opposite gateway via the IP network;
4. The opposite gateway converts the digital signal into the analog signal and transmits the analog signal to the local PSTN telephone network, and the local PSTN telephone network sends the voice signal to the called party.

The typical network diagram of the VoIP service is as follows:

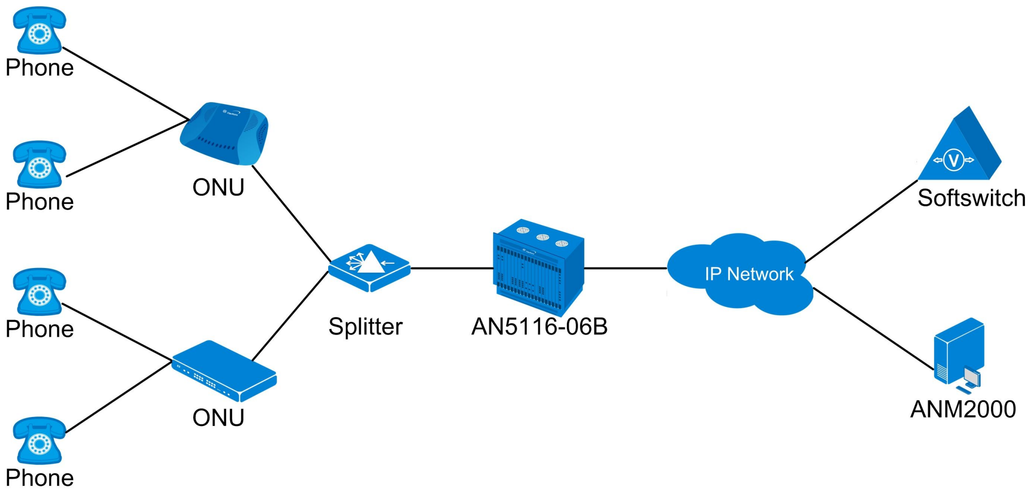


Figure 6-1 The typical network of the VoIP service

6.1.5 Reference Information

Reference standard

- ITU-T H.248.1：Gateway control protocol: Version 1
- IETF RFC 3435：Media Gateway Control Protocol (MGCP) Version 1.0
- IETF RFC 2543：SIP: Session Initiation Protocol

Terminology

Terminology	Description
PSTN	The PSTN (Public Switched Telephone Network) means the traditional switched telephone network, and is the most widely used telephone network in the world.
Gateway	The gateway is a type of network unit, and is used to implement the interconnection between the networks with different architectures. In the NGN architecture, the NGN is interconnected with other networks via some gateways.

Abbreviations

Abbreviations	Meaning
BHCA	Busy Hour Call Attempts
ISDN	Integrated Service Digital Network
IP	Internet Protocol
MGC	Media Gateway Controller
MOS	Mean Opinion Score
POTS	Plain Old Telephone Service
PSQM	Perceptual Speech Quality Measure
QoS	Quality of Service
RSVP	Resource ReSerVation Protocol
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
VoIP	Voice over IP
VPN	Virtual Private Network
WRED	Weighted Random Early Detection

6.2 H.248

6.2.1 Definition

The H.248 / Megaco protocol is a media gateway control protocol defined by IETF and ITU-T. It is a non-peer-to-peer protocol, and is used in the communication between the media gateway controller and the media gateway. Its main functions are described as follows: Establishes a good service bearing and connection model, and separates the call and the bearing connection; manages various service gateways, including the trunk gateway, the access gateway, and the register gateway, and implements the service interconnection between the packet based network and the PSTN.

6.2.2 Features

- The H.248 protocol supports access technologies of multiple types, and supports a mobile terminal.
- The H.248 protocol supports the network application and protocol extension with a large scale, and has a powerful flexibility.

6.2.3 Specifications

- Supports the access of up to 6k users at the same time.
- Supports the calling number identification presentation and restriction.
- Supports the call waiting.
- Supports the three party service.
- Supports the call forwarding (unconditional, busy and no answer).
- Supports the immediate hotline.
- Supports the outgoing call blocking.
- Supports the distinctive ring.
- The fax service based on the T.30 / T.38 protocol
- Supports the pulse accounting and polarity reversal accounting.

- Supports the IP CENTERX service.
- Supports PSTN line quality and performance testing (for example, 112 testing made by China Telecom) which can locate phone line faults.
- Call processing capability is 25k BHCA.
- The call completing ratio is no less than 99.999%.
- Supports the voice coding modes defined by ITU-T G.711a / G.711u / G.723 / G.726 / G.729.
- Supports the silence compression and comfort noise generator functions.
- Supports the echo suppression function.
- Supports multi-MGC list.
- Supports the 802.1Q VLAN and priority configuration of each voice channel.

6.2.4 Basic Principles

The AN5116-06B system uses the H.248 protocol to perform the signaling interaction with the softswitch and complete the call control; the ONU uses the standard voice coding technology to convert the user voice signal into the IP packet, and then the OLT sends the IP packet to the IP network for transmission. The purpose is to deliver the VoIP service to users using the AN5116-06B system.

The H.248 protocol entity mainly includes the MG and the MGC.

- MG

  The MG processes the media stream, and sends the media stream to the IP network in packets. The ONU in the network diagram acts as the MG.

- MGC

  The MGC is in charge of the registration and management of the MG resources, and controls the call. The softswitch in the network diagram acts as the MGC.

6.2.5 Reference Information

Reference standard

ITU-T H.248.1：Gateway control protocol: Version 1

Terminology

Terminology	Description
SoftSwitch	The softswitch is the core equipment for the evolution from the circuit switched network to the packet network, and is also one of the key equipment types for the NGN. It is independent of the bottom bearing protocol, and mainly performs the following functions: call control, media gateway access control, resource allocation, protocol processing, routing, authentication, and accounting. In addition, it can provide all existing services that circuit switching can support and multiple third party services for users.
Gateway	The gateway is a type of network unit, and is used to implement the interconnection between the networks with different architectures. In the NGN architecture, the NGN is interconnected with other networks via some gateways.

Abbreviations

Abbreviations	Meaning
BHCA	Busy Hour Call Attempts
IP	Internet Protocol
MG	Media Gateway
MGC	Media Gateway Controller
MOS	Mean Opinion Score
POTS	Plain Old Telephone Service
PSQM	Perceptual Speech Quality Measure
RTP	Real-time Transport Protocol

6.3 MGCP

6.3.1 Definition

◆ The MGCP protocol defined by IETF decomposes the gateway into several functional sub-modules: the call control entity (MGC) and the media processing entity (MG), and appoints the standard protocols for the communication between these sub-modules. The MGCP protocol plays an important role in the VoIP solution.

- The main functions of the MGCP protocol are described as follows: Establishes a good service bearing and connection model, and separates the call and the bearing connection; manages various service gateways (currently mainly are access gateways), including the trunk gateway, the access gateway, and the register gateway, and implements the service interconnection between the packet based network, the packet user access network, and the PSTN.

6.3.2 Features

- The MGCP is coded in the text mode, and has a simple architecture. So it is easy to understand, develop, and maintain.
- The MGCP can be well integrated with the SS7 network, and provides more controls and turnover for the call processing.

6.3.3 Specifications

- Supports the access of up to 6k users at the same time.
- Supports the calling number identification presentation and restriction.
- Supports the call waiting.
- Supports the three party service.
- Supports the call forwarding (unconditional, busy and no answer).
- Supports the immediate hotline.
- Supports the outgoing call blocking.
- Supports the distinctive ring.
- Supports the fax service based on the T.30 / T.38 protocol.
- Supports the pulse accounting and polarity reversal accounting.
- Supports IP CENTERX service.
- Supports PSTN line quality and performance testing (for example, 112 testing made by China Telecom) which can locate phone line faults.
- Call processing capability is 25k BHCA.
- The call completing ratio is no less than 99.999%.

- Supports the voice coding modes defined by ITU-T G.711a / G.711u / G.723 / G.726 / G.729.
- Supports the silence compression and comfort noise generator functions.
- Supports the echo suppression function.
- Supports multi-MGC list.
- Supports the 802.1Q VLAN and priority configuration of each voice channel.

6.3.4 Basic Principles

The AN5116-06B system uses the MGCP protocol to perform the signaling interaction with the softswitch and complete the call control; the ONU uses the standard voice coding technology to convert the user voice signal into the IP packet, and then the OLT sends the IP packet to the IP network for transmission. The purpose is to deliver the VoIP service to users using the AN5116-06B system.

The MGCP protocol entity mainly includes the MG and the MGC.

- MG

  The MG translates the media format in a certain network into the media format complying with another network. For example, the MG can complete the translation between the bearer channel of the circuit switched network and the media stream of the packet network. The MG can process multiple types of media data, and can complete the signaling function under the control of the media gateway controller. The ONU in the network diagram acts as the MG.

- MGC

  The MGC controls the call status related to the media channel connection control The softswitch in the network diagram acts as the MGC.

6.3.5 Reference Information

Reference standard

- IETF RFC 3435：Media Gateway Control Protocol (MGCP) Version 1.0

Terminology

Terminology	Description
Softswitch	The softswitch is the core equipment for the evolution from the circuit switched network to the packet network, and is also one of the key equipment types for the NGN. It is independent of the bottom bearing protocol, and mainly performs the following functions: call control, media gateway access control, resource allocation, protocol processing, routing, authentication, and accounting. In addition, it can provide all existing services that circuit switching can support and multiple third party services for users.
Gateway	The gateway is a type of network unit, and is used to implement the interconnection between the networks with different architectures. In the NGN architecture, the NGN is interconnected with other networks via some gateways.

Abbreviations

Abbreviations	Meaning
BHCA	Busy Hour Call Attempts
IP	Internet Protocol
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MOS	Mean Opinion Score
POTS	Plain Old Telephone Service
PSQM	Perceptual Speech Quality Measure
RTP	Real-time Transport Protocol

6.4 SIP

6.4.1 Definition

The SIP is a text-coding-based IP telephone / multimedia conference protocol defined by IETF. It is used to establish, modify, and terminate a multimedia session.

The SIP protocol can be used to initiate a session, and also can be used to invite a member to join the session which has been established in other modes. The members joining a session can communicate with each other in one of the following modes: multicast, unicast interconnection, or the combination of multicast, unicast interconnection. The SIP protocol transparently support the name mapping and redirection services, and enables the ISDN, intelligent service, and personal mobile service.

6.4.2 Features

- Minimal state.
- Lower-layer-protocol neutral.
- Text-based.
- The robustness.
- The extensibility.
- Support the IN service easily.

6.4.3 Specifications

- Supports the access of up to 6k users at the same time.
- Supports the calling number identification presentation and restriction.
- Supports the call waiting.
- Supports the three party service.
- Supports the call forwarding (unconditional, busy and no answer).
- Supports the blind transfer and attended transfer.
- Supports the outgoing call blocking.
- Supports the distinctive ring.
- Supports the fax service based on the T.30 / T.38 protocol.
- Supports the pulse accounting and polarity reversal accounting.
- Supports IP CENTERX service.

- Supports PSTN line quality and performance testing (for example, 112 testing made by China Telecom) which can locate phone line faults.
- Call processing capability is 25k BHCA.
- Percent of call completed is larger than 99.999%.
- Supports the voice coding modes defined by ITU-T G.711a / G.711u / G.723 / G.726 / G.729.
- Supports the silence compression and comfort noise generator functions.
- Supports the echo suppression function.
- Supports the 802.1Q VLAN and priority configuration of each voice channel.

6.4.4 Basic Principles

The AN5116-06B system uses the SIP protocol to perform the signaling interaction with the softswitch and IMS and complete the call control; the ONU uses the standard voice coding technology to convert the user voice signal into the IP packet, and then the OLT sends the IP packet to the IP network for transmission. The purpose is to deliver the VoIP service to users using the AN5116-06B system.

The SIP protocol entity mainly includes the proxy server, the register server, and the user agent.

- Proxy server

  As a logical network entity, the proxy server forwards the request or response in behalf of the client. It has three conditions: stateless, stateful, and call stateful, and can attempt to forward the request to multiple addresses in the branch and circle modes. Its main functions include routing function, authentication, accounting monitor, call control, service providing, etc. The softswitch acts as the proxy server.

- Register server

  The register server receives the register request. It saves the address mapping relationship (in the register request) in the database so that the following relevant call processes can use the address mapping relationship; in addition, the register server can perform the location service. The softswitch acts as the register server.

- User agent

  A logical entity initiating or receiving the request is called the user agent. The user port of the ONU acts as the user agent.

6.4.5 Reference Information

Reference standard

IETF RFC 2543：SIP: Session Initiation Protocol

Terminology

Terminology	Description
SoftSwitch	The softswitch is the core equipment for the evolution from the circuit switched network to the packet network, and is also one of the key equipment types for the NGN. It is independent of the bottom bearing protocol, and mainly performs the following functions: call control, media gateway access control, resource allocation, protocol processing, routing, authentication, and accounting. In addition, it can provide all existing services that circuit switching can support and multiple third party services for users.
Gateway	The gateway is a type of network unit, and is used to implement the interconnection between the networks with different architectures. In the NGN architecture, the NGN is interconnected with other networks via some gateways.

Abbreviations

Abbreviations	Meaning
BHCA	Busy Hour Call Attempts
IP	Internet Protocol
ISDN	Integrated Service Digital Network
ISUP	ISDN User Part
MOS	Mean Opinion Score
POTS	Plain Old Telephone Service
PSQM	Perceptual Speech Quality Measure
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol

7 TDM Service Access

☑ Definition

☑ Features

☑ Specifications

☑ Basic Principles

☑ Reference Information

7.1 Definition

The TDM service in the GPON system is accessed as follows: the TDM frame resolved from the E1 line will be processed into the Ethernet frame using the CESoP over GEM method, and then encapsulated into the GEM frame of the GPON for transmission.

7.2 Features

The AN5116-06B can carry services effectively. It uses the CESoP over GEM mode to implement the TDM service, so the current switch & transmission system and client end TDM access equipment do not need replacement, and the traditional circuit switched service can be carried on the packet switched network.

7.3 Specifications

- Supports two types of TDM interface cards: The CE1B card and the C155A card. The CE1B card provide 32 E1 interfaces, and the C155A card provides two (1+1 backup) STM-1 interfaces.
- Supports two system timing modes: the asynchronous timing mode and the synchronous timing mode.
- Supports multiple clock types: local oscillator, external clock 1, external clock 2, clock extracted from E1 line, and clock extracted from STM-1 optical line.
- Supports multiple clock recovery mode: self adaptive clock, enhanced clock, differential clock and loopback clock.

7.4 Basic Principles

TDM service network

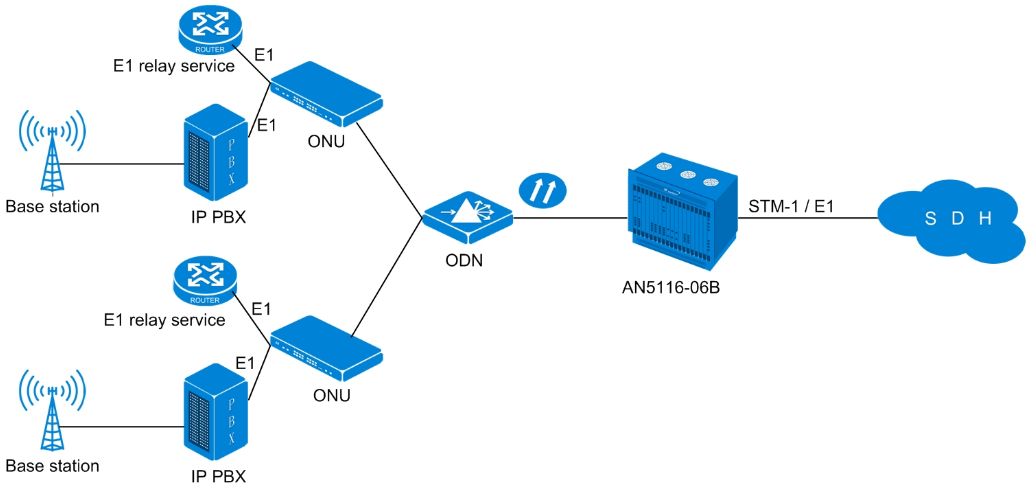


Figure 7-1 TDM service network diagram

The TDM service network in the CESoP over GEM mode is shown in the figure above.

The TDM services of E1 private line users and mobile users can be accessed via the ONU E1 interface; the ONU transmits the TDM services to the OLT side, and then the OLT identifies and forwards the TDM services, and transmits them to the upper level SDH network.

CESoP

At its most basic, the CESoP technology tunnels TDM services across a managed PSN (packet switched network). TDM traffic is packetized using an IP packet for each E1 frame, put into a packet payload and transported across the PON. The payload is then received at the OLT and converted to TDM, aggregated, and connected to the PSTN (public switched telephone network). For the TDM service, the CESoP supports the transparent transmission, so the CESoP is compatible with the traditional telecommunication network; this means that all traditional services, such as protocols, signaling, data services, voice services, and video services, can use the CESoP technology intactly. In addition, the relevant equipment needs no modification; so the telecommunication operator can utilize the current resources best by applying the traditional TDM service over the IP network.

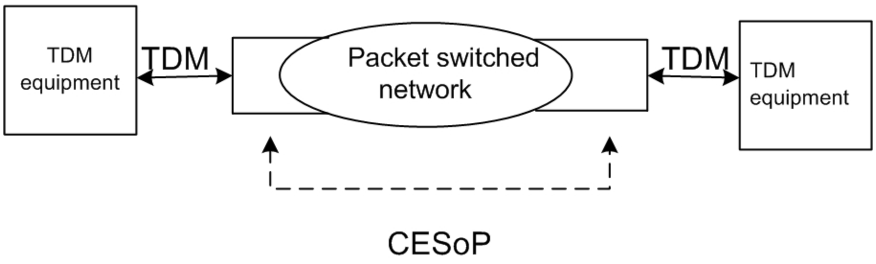


Figure 7-2 The basic thought of the CESoP technology

CESoP over GEM

The CESoP over GEM mode is described as follows: Uses the CESoP technology to map the TDM service into the packet frame (such as the Ethernet frame), and then encapsulates the packet frame that encapsulates the TDM service into the GEM frame. In general, it uses the Layer 2 encapsulation mode to carry the TDM service.

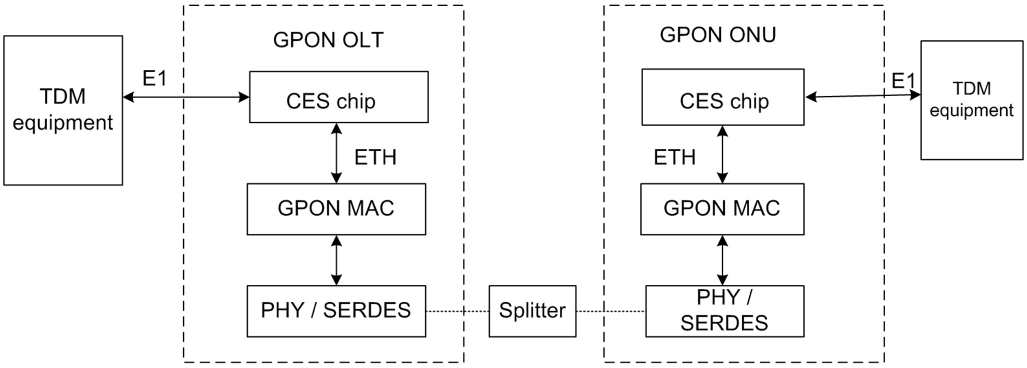


Figure 7-3 The TDM service carried by GPON

The TDM service is down linked to the OLT, and the TDM frame is received from the E1 line by the TDM service card; then the TDM service card adapts the TDM frame into the Ethernet frame via the CES chip, and sends the Ethernet frame to the core switch card of the system via the GE bus; then the core switch card forwards the Ethernet frame to the GPON service card, and the GPON MAC chip of the GPON service card encapsulates the Ethernet frame into the GEM frame, and sends the GEM frame to the remote end ONU supporting the CES function. The GPON MAC of this ONU receives the Ethernet frame from the GEM frame, and sends the Ethernet frame to the CES chip to convert the Ethernet frame to the TDM frame; then the TDM frame is transmitted to the downlink TDM equipment. The uplink direction follows a reverse process.

7.5 Reference Information

Reference standard

- IETF RFC4197: Requirements for Edge-to-Edge Emulation of Time Division Multiplexed (TDM) Circuits over Packet Switching Networks
- ITU-T G.812: Timing requirements of slave clocks suitable for use as node clocks in synchronization networks
- ITU-T G.813: Timing characteristics of SDH equipment slave clocks (SEC)
- ITU-T G.823: The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy
- ITU-T G.824: The control of jitter and wander within digital networks which are based on the 1544 kbit/s hierarchy
- ITU-T G.8261/Y.1361: Timing and synchronization aspects of packet networks

Terminology

Terminology	Description
SDH	The SDH is a series of hierarchical digital transmission architecture, and is used to standardize the transmission of the payload in the physical transmission network.
Circuit switch	The circuit switch is described as follows: An actual electronic circuit (physical line) is maintained the communication process; after this electronic circuit is established, the user occupies the fixed transmission bandwidth from the Tx end to the Rx end until this connection terminates.
Packet switch	The packet switch is described as follows: Divides the user data into multiple equal-length segments, and each segment is called a data segment. Each data segment and the header ahead of the data segment (the header is composed of the additional control information) form a packet. The header is used to identify the destination address of the corresponding packet; the switch forwards each packet to the destination address depending on its address ID. This process is called the packet switch.
Frame	The frame is a kind of data transmission unit defined by IEEE 802, and is used to transmit the protocol data unit between MAC service users. The frame has the following three types: the untagged frame, the VLAN-tagged frame, and the priority-tagged frame.

Abbreviations

Abbreviations	Meaning
GEM	GPON Encapsulation Mode
GPON	Gigabit-capable Passive Optical Network
OLT	Optical Line Terminal
ONU	Optical Network Unit
PSTN	Public Switched Telephone Network
SDH	Synchronous Digital Hierarchy
TDM	Time Division Multiplexing
CESoP	Circuit Emulation Services over Packet

8 Layer 2 Features

☑ MAC Address Management

☑ 802.1Q VLAN

☑ QinQ VLAN

☑ VLAN Translation

☑ RSTP

☑ Ethernet Link Aggregation

☑ Ethernet Port Mirroring

8.1 MAC Address Management

8.1.1 Definition

The MAC address management is a basic function of the broadband layer 2, including the MAC address aging time and maximum MAC address quantity limit.

8.1.2 Features

- After the AN5116-06B MAC address aging time, users can delete the idle addresses in the MAC address forwarding table, so as to improve the MAC address forwarding efficiency.
- The maximum MAC address quantity limit function can restrict the MAC address quantity that access the network, so as to reduce the burden on the OLT equipment.

8.1.3 Specifications

- Supports the automatic MAC address learning.
- Supports up to 32K MAC address.
- Supports setting the MAC address aging time of an ONU.

8.1.4 Basic Principles

MAC address aging time

The system check the aging dynamic MAC address regularly. If no message with a MAC address is not sent or received during the aging time, the system will delete this MAC address from the MAC address table. The regular aging of the dynamic MAC address can release the MAC address resource to prevent the failure of learning the new MAC address.

Follow the rules below to set the MAC address aging time:

- If the MAC address aging time is set over short, the system will delete the dynamic MAC address too soon. When re-receiving the message of modifying the MAC address, the system will broadcast the message to all the ports in the same VLAN, which influences the system performance.
- If the MAC address aging time is set over long, the system may not be able to learn the new MAC address. When the system fails to find the destination address of new messages in the MAC address forwarding table, it will broadcast the message.

MAC address quantity limit

Configuring the MAC address quantity limit can limit the connected user quantity. When the learned address quantity reaches the maximum value, the port will no longer learn the new messages of MAC address.

The processing methods for the messages not learned by the port:

- The downlink messages that cannot find forwarding port floods.
- The messages with unknown MAC addresses will be discarded.

8.1.5 Reference Information

Abbreviations

Abbreviations	Meaning
VLAN	Virtual Local Area Network

8.2 802.1Q VLAN

8.2.1 Definition

The virtual local area network (VLAN) is a technology used to form virtual workgroups by grouping the devices of a LAN logically. The IEEE issued draft IEEE 802.1Q in 1999, aiming at standardizing VLAN implementations. The 802.1Q standard optimizes the architecture of the VLAN, and unifies the tag format of different manufacturers for frame tagging.

8.2.2 Features

- Controls the broadcast storm

  A VLAN is a logical broadcast domain. The data packets from a certain VLAN member are only forwarded to the other members of the same VLAN. Through the establishment of a VLAN, the system isolates the broadcast and reduces the broadcast range, so as to control the generation of the broadcast storm.

- Increases the security of the entire network

  Supports multiple VLAN setting modes, and can control the user access authorization and the size of a logical network segment, so as to set various user groups to different VLANs and increase the overall performance and security of the interactive network.

- Implements the simple and visual network management

  A VLAN can set network users at different physical locations in the same logical network segment according to the functional divisions, the object groups, or the applications. Without modifying the physical connection of the network, users can move a workstation as required from workgroup to workgroup, or from subnet to subnet. This can reduce the burden of the network management and maintenance greatly, and save the network maintenance cost.

8.2.3 Specifications

- The AN5116-06B supports up to 4k VLANs.
- Supports the VLAN setting based on the IEEE 802.1Q standard.

8.2.4 Basic Principles

VLAN frame structure

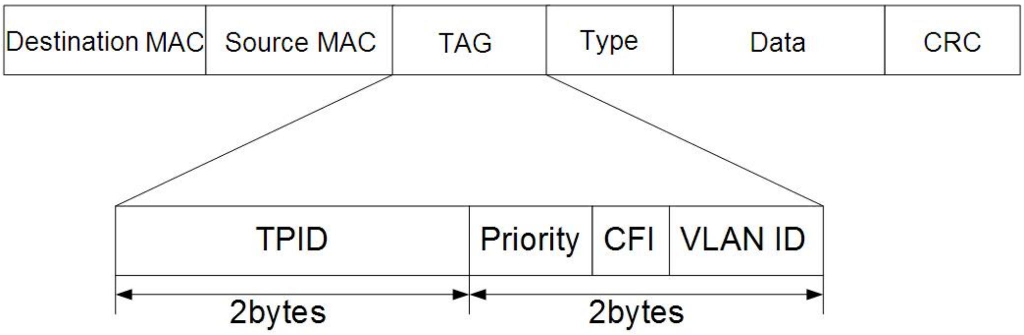


Figure 8-1 The VLAN frame structure

An 802.1Q tag header includes the TPID (two bytes) and the TCI (two bytes):

- TPID: The TPID domain can be modified. In Ethernet, the TPID value of a VLAN tag is usually set to 0x8100; the TPID values may vary with the network or the equipment provider.
- TCI
    - Priority: Is 3-bit. Its values range from 0 to 7, meaning the priority from low to high.
    - CFI: Is 1-bit (0 or 1). 0 indicates the canonical format, and 1 indicates the non-canonical format.
    - VLAN ID: Is 12-bit. It means the ID of a VLAN, with the value ranging from 0 to 4095.

VLAN setting

The AN5116-06B uses the VLAN setting mode based on the IEEE 802.1Q standard. In this mode, the system adds the 802.1Q tag to the Ethernet frame, and identifies VLANs using the VID. When a certain data frame passes through the equipment, the equipment will identify the VLAN which it belongs to according to the VID information of the tag in the Ethernet frame; if no tags exist in the frame, the equipment will identify the VLAN which it belongs to according to the default VID information of the port that the frame passes through.

8.2.5 Reference Information

Reference standard

IEEE 802.1Q：IEEE Standards for Local and metropolitan area networks—Virtual Bridged Local Area Networks

Terminology

None.

Abbreviations

Abbreviations	Meaning
CFI	Canonical Format Indicator
TCI	Tag Control Information
TPID	Tag Protocol Identifier
VID	VLAN Identified
VLAN	Virtual Local Area Network

8.3 QinQ VLAN

8.3.1 Definition

802.1Q in 802.1Q (QinQ) is a visualized name for the tunnel protocol encapsulated based on IEEE 802.1Q. A packet in a VLAN that has the QinQ attribute contains two VLAN tags: inner VLAN tag from the private network and outer VLAN tag from the device. Through the outer VLAN tag, a layer 2 VPN tunnel can be set up to transparently transmit service data from private networks to public networks. To be specific, the VLAN tag of the private network is encapsulated to the VLAN tag of the public network. The packet thus carries two IEEE 802.1Q VLAN tags to traverse the service provider's backbone network. In this way, the QinQ VLAN provides users with a simple layer 2 VPN private line service.

8.3.2 Features

- Increases the number of VLANs inside the network

The IEEE 802.1ad (QinQ) was defined for increasing the number of VLANs early; the function is implemented by adding a 802.1Q tag to the 802.1Q packet, and the number of VLANs can reach 4k×4k.

- Provides an easier layer 2 VPN tunnel

  In the public network, a packet is transmitted according to the outer VLAN tag (public VLAN tag), and the user private network VLAN tag is filtered. For this reason, a user can plan the private network VLAN IDs as required, and the private network VLAN IDs do not conflict with the public VLAN ID.

8.3.3 Specifications

- Supports increasing the number of VLANs: By adding QinQ VLANs, the system can increase the number of VLANs to 4k×4k on the basis of the initial VLAN.
- Supports the flexible QinQ functions: Supports adding the inner and outer VLANs according to the conditions such as the source MAC address, the destination MAC address, the source IP address, the destination IP address, the L4 source port No., the L4 destination port No., the Ethernet type, the inner VLAN, the outer VLAN, the service type, the TTL (time to live), the protocol, the layer 1 CoS, and the layer 2 CoS.
- Supports distinguishing users and services via the VLAN as follows: The two tags of the QinQ can indicate different information; for example, the inner tag indicates the user, and the outer tag indicates the service.
- Supports setting the SVLAN based on the card / PON / ONU / ONU port.
- Supports the selective QinQ at the same port; this means that some services use the VLAN stacking, and some services use the single-layer VLAN.

8.3.4 Basic Principles

QinQ VLAN frame structure

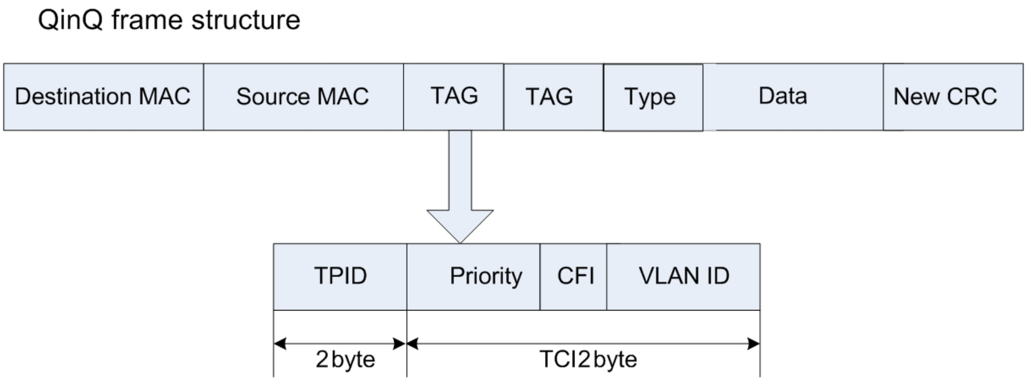


Figure 8-2 The QinQ VLAN frame structure

For the meanings of various parameters in the tag header, please see 802.1Q VLAN.

Service processing flow

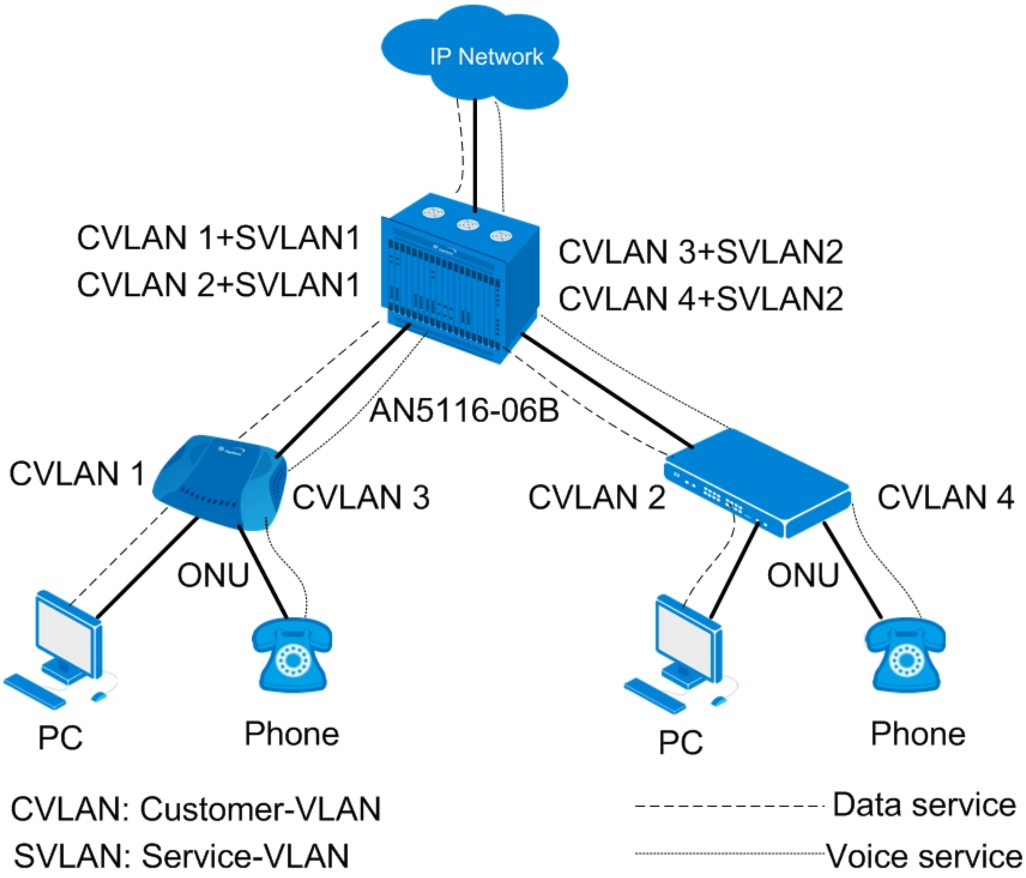


Figure 8-3 The service processing of the QinQ VLAN

◆ The uplink direction: At the AN5116-06B user side, the data and voice services of two users are tagged with the CVLAN tags respectively after passing through the two ONUs. ONU1 accesses the data and voice services with the CVLAN ID being 1 and 3 respectively; ONU2 accesses the data and voice services with the CVLAN ID being 2 and 4 respectively. When the services of the two users are transmitted to the AN5116-06B, the AN5116-06B adds corresponding SVLAN tags for the data and voice services respectively; the SVLAN IDs of the data and voice services are 1 and 2 respectively. After the QinQ VLAN is added, the user service with double VLAN encapsulation is transmitted to the upper level network.

- The downlink direction: When the successfully-configured user service with double VLAN encapsulation mentioned previously is transmitted to the AN5116-06B from the upper level network, the system processes it as follows: If the VID of the SVLAN tag packet brought by the service is not the same as the VID configured by the AN5116-06B, this packet will be discarded; if the VID of the SVLAN tag packet brought by the service is the same as the VID configured by the AN5116-06B, the equipment will stripe the SVLAN tag directly, and then forward the service to the downlink ONU. In the same mode, the ONU determines whether the VID of the CVLAN tag packet brought by the service is the same as the configured VID; if so, the ONU directly strips CVLAN tag and sends the untagged packet to the user, and if not, the ONU discards the packet.

Flexible QinQ

The AN5116-06B uses the following flexible QinQ modes:

- The port-based flexible QinQ

  The basic principle is described as follows: When the equipment port receives a packet, no matter whether the packet has a VLAN tag, the equipment tags it with the VLAN tag (PVID) of the default VLAN for this port. In this mode, if a packet with the VLAN tag is received, this packet will become a QinQ packet; if an untagged packet is received, this packet will become a packet with the default VLAN tag of the port.

- The traffic-based flexible QinQ

  - The QinQ encapsulation according to the VLAN ID in the Ethernet frame

    The basic principle is described as follows: When various services of the same user use different CVLAN tags, the system can distinguish the services according to their VLAN IDs. For example, the VLAN ID of the PC Internet access service ranges from 301 to 400, the VLAN ID of the IPTV service ranges from 201 to 300, and the VLAN ID of the VoIP service ranges from 101 to 200; so after receiving the packets, the AN5116-06B will tag each type of service with the SVLAN tag according to the VLAN ID value (the corresponding SVLAN IDs are 3, 2, 1 respectively).

  - The QinQ encapsulation according to the VLAN ID + priority in the packet

The basic principle is described as follows: Each service has its dedicated priority; when various services of the same user use the same CVLAN ID, the system can distinguish the services according to their priorities and then tag the corresponding SVLAN tag for each type of service.

- The QinQ encapsulation according to the source and destination IP addresses

  The basic principle is described as follows: When the services of different users include both the Internet service and the voice service, each service has its dedicated source and destination IP addresses; under this condition, the system can distinguish the IP addresses according to their ACLs and then tag the corresponding SVLAN tag for each type of service.

- The QinQ encapsulation according to the source and destination MAC addresses

  The basic principle is described as follows: When the service access is performed between different users, the source and destination MAC addresses in the Ethernet frame are different with each other; under this condition, the system can distinguish the source and destination MAC addresses and then tag the corresponding SVLAN tag for each type of service.

- The QinQ encapsulation according to the Ethernet type

  The basic principle is described as follows: When the services of the same user include both the Internet service (PPPoE) and the IPTV service (IPoE), the protocol No. of IPoE is 0x0800, and the protocol No. of PPPoE is 0x8863 / 8864; under this condition, the system can distinguish the services according to their Ethernet types and then tag the corresponding SVLAN tag for each type of service.

8.3.5 Reference Information

Reference standard

- IEEE 802.1Q：IEEE Standards for Local and metropolitan area networks—Virtual Bridged Local Area Networks
- IEEE 802.1ad：Local and metropolitan area networks - Virtual bridged local area networks - Amendment 4: Provider bridges

Terminology

None.

Abbreviations

Abbreviations	Meaning
CFI	Canonical Format Indicator
CoS	Class of Service
IP	Internet Protocol
IPoE	IP over Ethernet
ONU	Optical Network Unit
PON	Passive Optical Network
PPPoE	Point to Point Protocol over Ethernet
TCI	Tag Control Information
TPID	Tag Protocol Identifier
VID	VLAN Identified
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

8.4 VLAN Translation

8.4.1 Definition

The VLAN translation is described as follows: When multiple uplink services from the user side pass through the terminal equipment supporting the 802.1Q protocol, if the terminal equipment tags a fixed tag to the user service, the newly-tagged tag may exceed the valid range of the operator; so when the service is up linked to the ONU, the ONU will translate the default tag tagged by the terminal equipment into the unique valid tag at the network side. Now the VLAN translation is completed.

8.4.2 Features

The VLAN translation reduces maintenance workload of the operator. Via the VLAN translation function, the VLAN trunking can be implemented at the user access side, and one system only needs to use one SVLAN. The use of VLAN translation can reduce maintenance workload and conserve limited VID resources because only one SVLAN is needed for a system.

8.4.3 Specifications

- Supports three VLAN translation modes: the 1:1 translation, the N: 1 translation, and the hybrid translation.
- Supports flexible VLAN translation functions: Can set and translate the CVLAN and CoS based on the source MAC address, the destination MAC address, the Ethernet type, the VLAN ID, the CoS, the source IP address, the destination IP address, the ToS, the protocol type, the source port No., the destination port No., etc.

8.4.4 Basic Principles

VLAN translation modes

Here we take the home gateway as an example to describe the terminal equipment supporting the 802.1Q protocol.

- The 1:1 VLAN translation mode:

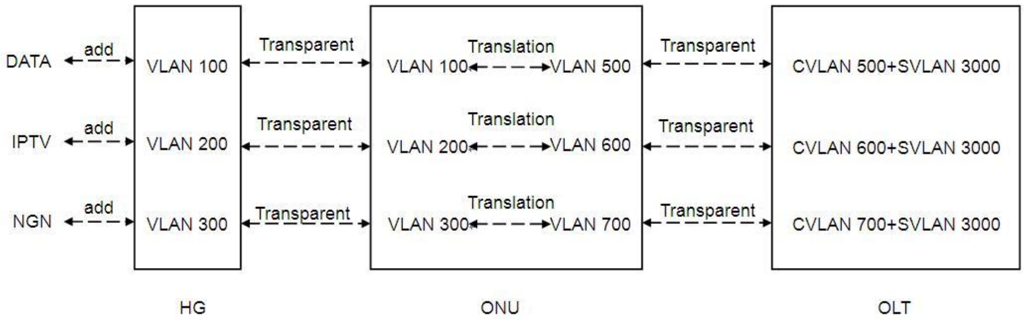


Figure 8-4 The 1:1 VLAN translation mode

At the user side of the AN5116-06B the users' data, voice, and multicast services go through gateways and are labeled with fixed default VLAN tags (for example 100, 200, 300 respectively). When the users' services are received at the ONU configured for 1:1 VLAN translation, the ONU will substitute the configured Customer-VLAN tags for data, voice and multicast services (for example 500, 600, and 700 respectively). When the services are sent to the AN5116-06B, they are labeled with the Service-VLAN tags (for example 3000) on the AN5116-06B. After the QinQ VLAN is added, the user service with double VLAN encapsulation is transmitted to the upper level network. In the downlink direction, the reverse process is used.

◆ The N:1 VLAN translation mode:

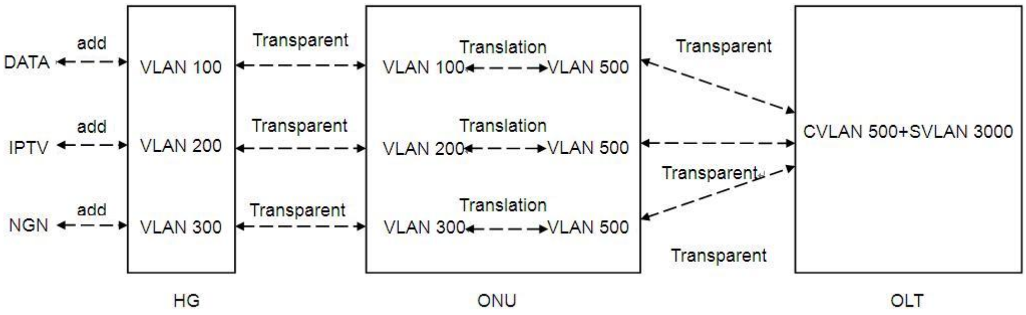


Figure 8-5 N:1 VLAN translation

At the user side of the AN5116-06B the users' data, voice, and multicast services go through gateways and are labeled with fixed default VLAN tags (for example 100, 200, 300 respectively). When the users' services are received at the ONU configured for N:1 VLAN translation, the ONU will substitute a single configured Customer-VLAN tag for all services (for example 500). When the services are sent to the AN5116-06B, they are labeled with the Service-VLAN tags (for example 3000) on the AN5116-06B. After the QinQ VLAN is added, the user service with double VLAN encapsulation is transmitted to the upper level network. In the downlink direction, the reverse process is used.

◆ The mixed VLAN translation mode:

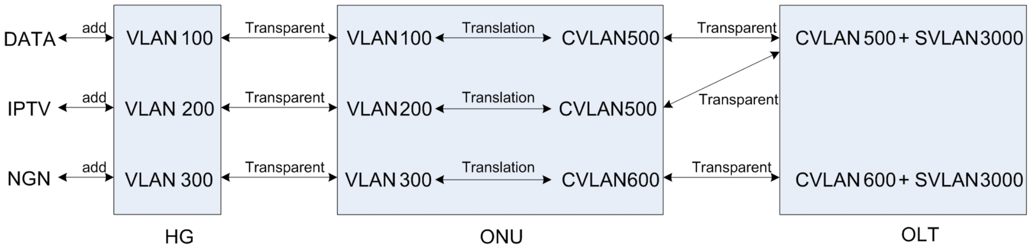


Figure 8-6 The mixed VLAN translation mode

The mixed mode means using the 1:1 and N:1 translation modes at the same time.

At the user side of the AN5116-06B the users' data, voice, and multicast services go through gateways and are labeled with fixed default VLAN tags (for example 100, 200, 300 respectively). When the users' services are received at the ONU configured for hybrid mode VLAN translation, the ONU will substitute a unique Customer-VLAN tag for some services (for example voice services are labeled 600) and a single configured Customer-VLAN tag for some groups of services (for example 500 for date and multicast services). When the services are sent to the AN5116-06B, they are labeled with the Service-VLAN tags (for example 3000) on the AN5116-06B. After the QinQ VLAN is added, the user service with double VLAN encapsulation is transmitted to the upper level network. In the downlink direction, the reverse process is used.

8.4.5 Reference Information

Reference standard

- IEEE 802.1Q：IEEE Standards for Local and metropolitan area networks—Virtual Bridged Local Area Networks
- IEEE 802.1ad：Local and metropolitan area networks - Virtual bridged local area networks - Amendment 4: Provider bridges

Terminology

None.

Abbreviations

Abbreviations	Meaning
CoS	Class of Service
HG	Home Gateway
IP	Internet Protocol
ONU	Optical Network Unit
ToS	Type of Service
VID	VLAN Identified
VLAN	Virtual Local Area Network

8.5 RSTP

8.5.1 Definition

The RSTP means the rapid spanning tree protocol, and is one of the layer 2 management protocols. The RSTP is an improvement of STP (Spanning Tree Protocol) in terms of being newer and faster. It implements path redundancy through certain algorithms. RSTP also prunes a loop network into a loop-free tree network. This helps to avoid proliferation and infinite loop of packets in the loop network. RSTP features fast convergence in the event of network topology changes.

8.5.2 Features

◆ By blocking the redundant links in the network selectively, the RSTP can eliminate the layer 2 loops in the network, so as to solve the broadcast storm problem of the looped Ethernet network and eliminate the circle connections caused by mistakes or accidents.

◆ The RSTP enables a bridge connection / switch, bridge connection port, or LAN to resume its connectivity instantly after a fault occurs. The root port and designated port can be switched to the forwarding status rapidly. The RSTP can reduce the re-configuration and service resuming time after a connection fault occurs to less than one second.

8.5.3 Specifications

All AN5116-06B uplink cards (the HU1A card, the HU2A card, and the GU6F card) and their uplink ports support the RSTP function. The RSTP parameters and their value ranges are described as follows:

- Port priority: 0 to 240;
- Port path: 0 to 200000000.

8.5.4 Basic Principles

Basic thought

The RSTP uses the rapid spanning tree algorithm to block some redundant paths in the switching network and establish a loop-free tree network. The RSTP runs at all bridges (or switches) in a bridge, and it works out the tree active topology of the simple interconnection for the bridge network. When performing the calculation operation, the RSTP first selects a bridge to act as the root (namely root bridge), and it assigns a role for each port of each bridge at the same time.

The RSTP increases the convergence speed greatly.

- Sends BPDUs intermittently: a bridge of the RSTP sends its own BPDU configuration information in each hello time interval (the default is two seconds), no matter whether it receives the BPDUs from the root bridge.
- Rapidly ages information: The RSTP uses the heartbeat mechanism as follows: When a certain bridge does not receive the BPDU three consecutive times, the bridge will determine that the root of the neighbor and the designated roots have been lost, so it will age its BPDU configuration information at once.

Basic concepts

In the RSTP, a bridge has two roles: the root bridge and the designated bridge. The topology information is exchanged between various bridges. The root has the highest priority ID in all bridges. Before the spanning tree is formed, each bridge regards itself as the root bridge by default. After the spanning tree is formed stably, one root bridge and several designated bridges will be generated. When the topology architecture changes, the root bridge will notify other bridges to calculate the topology again.

Depending on the action of a port in the active topology, the RSTP defines five types of port roles (the STP only has three types of port roles): disabled port, root port, designated port, alternate port, and backup port. They are detailed as follows:

- Root port: When the switch forwards a packet to the root bridge, the **root port** can provide a minimum path cost for this packet.
- Designated port: This port is connected to the designated switch; when the designated switch forwards the packets from the LAN to the **root bridge**, this port can provide a minimum path cost. The port connected with the LAN via the designated switch is called the designated switch.
- Alternate port: This is a dedicated port role of the RSTP. It provides an alternate path for the connection from the current **root port** to the **root bridge**.
- Backup port: This is a dedicated port role of the RSTP. It provides a backup path for the **designated port** reaching the spanning tree leaf. The **backup port** can exist only under the following conditions: Two ports are connected with each other via a loop composed of a point-to-point link, or the switch has two or more connections to reach the shared LAN network segment.
- Disabled port: This is a port role already existing in the STP. It does not act as any role in the spanning tree operation, and does not join the RSTP calculation.

Protocol working flow

The main working flow of the RSTP protocol is to determine the bridge role and the port role and status.

1. Determines the root bridge. When the equipment is started for the first time, it always regards itself as the root bridge and sends a BPDU message for notification. Each equipment set will analyze the corresponding information after receiving the BPDU message and compares the IDs of various bridges (first compares the bridge priorities; if they are the same, then it compares the MAC address), and the bridge whose ID is the least is selected as the root bridge. If a certain equipment set whose bridge ID is less than that of the current root bridge joins the network, it will declare that it is the root bridge first. After other equipment sets receive the BPDU message from this equipment set, they will determine that it is the new bridge and record it after the comparison.

2. Determines the root port. The port whose connection path with the root bridge has the minimum cost is the root port.

3. After the root bridge and the root port are determined, the system starts to prune the redundant loops. This is implemented by blocking the corresponding ports on the non-root bridges. Finally one root bridge and several designated bridges will appear in the entire network.

Network diagram

The RSTP network diagram of the AN5116-06B is shown in Figure 8-7.

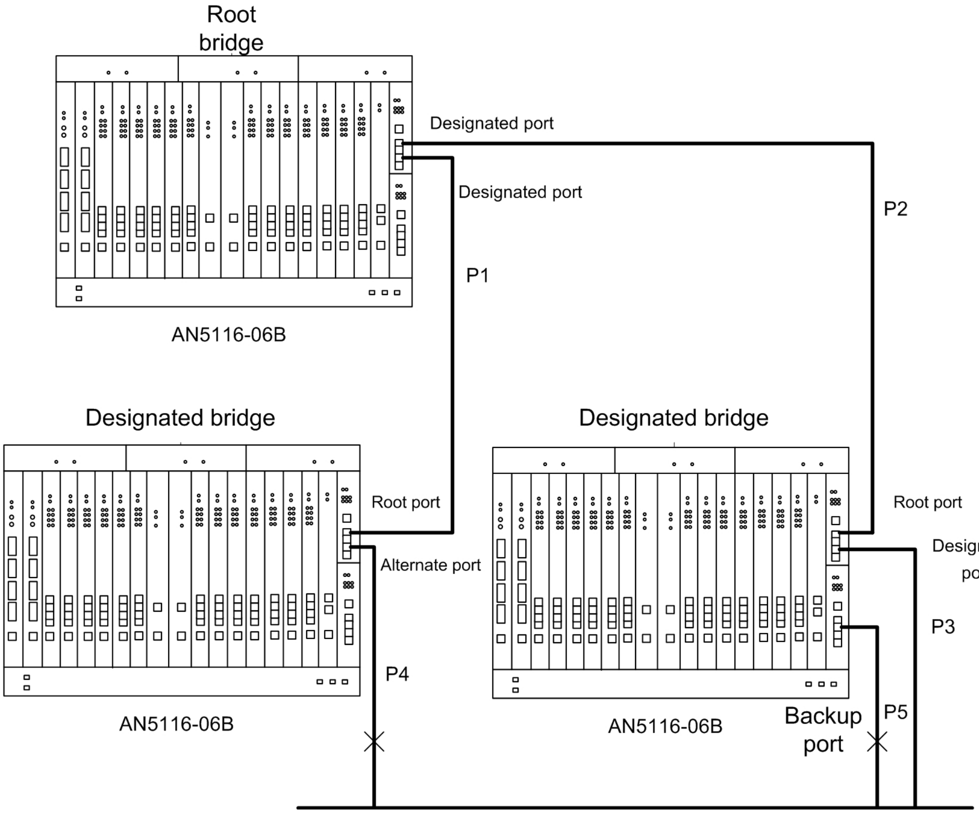


Figure 8-7 The RSTP network

As Figure 8-7 shows, three AN5116-06Bs performs the RSTP calculation operation to avoid forming loops. Via the comparison, the system determines the root bridge and the designated bridges, and then determines the status of each port. P1 has a higher priority than P4, so the alternate port of the P4 connection is blocked. P3 has a smaller ID than P5, so the backup port of the P5 connection is blocked. When P1 or P2 has faults, the RSTP will perform the calculation operation again, and the alternate port or the backup port will enter the forwarding status; so the network communication will not be influenced.

8.5.5 Reference Information

Reference standard

- IEEE 802.1W：Local and metropolitan area networks - Common specifications - Part 3: Media access control (MAC) bridges; Amendment 2: Rapid reconfiguration

- IEEE 802.1D：IEEE standard for local and metropolitan area networks–Media access control (MAC) Bridges (Incorporates IEEE 802.1t-2001 and IEEE 802.1w)

Terminology

Terminology	Description
Root port	Means the port connected with the root bridge or having the best path to the root bridge.
Designated port	All ports on the root bridge are designated ports. When the designated bridges have loops, a port at the low-cost path is the designated port, and a port at the high-cost path is the non-designated port.
Alternate port	It provides an alternate path for the connection to the root bridge, and this path is not the same as the path from the port to the root bridge.
Backup port	It is used to backup the path from the designated port to the spanning tree.
Port priority	For a port, the smaller is the priority value, the higher is the priority. A port with a higher priority has more chance to act as the root port.
Port path cost	The RSTP protocol can detect the link rate of the current Ethernet port automatically, and work out the corresponding path cost.

Abbreviations

Abbreviations	Meaning
BPDU	Bridge Protocol Data Unit
RSTP	Rapid Spanning Tree Protocol
STP	Spanning Tree Protocol

8.6 Ethernet Link Aggregation

8.6.1 Definition

The link aggregation means aggregating multiple links into one link for the management, so as to meet the demands on the higher channel bandwidth and the security. The aggregated link can be connected with the equipment with higher bandwidth demands.

The link aggregation configuration modes include the manual aggregation and the dynamic aggregation. The dynamic aggregation complies with the LACP protocol. The LACP is the control protocol defined in IEEE 802.3ad to implement the link dynamic aggregation.

8.6.2 Features

- Meets the demand on the higher bandwidth. When the operator cannot construct the physical link with a high bandwidth, it can form a logical link via the link aggregation, so as to extend the link bandwidth to n times of the original link bandwidth.
- Equalizes the load. Implements the load sharing in a certain aggregation group, so as to equalize the traffic load between various ports automatically.
- Provides higher link reliability. When a certain physical link in the link aggregation has faults, its traffic will be switched to other links automatically.
- Filters the upper level protocols. When configuring the aggregated link, users do not need to modify the upper level protocols.
- If it is needed to back up the links dynamically, users can implement the manual dynamic backup between various member ports in the same aggregation group via the link aggregation configuration.

8.6.3 Specifications

The AN5116-06B has the aggregation capability as follows:

- Supports up to 16 aggregation groups, and each aggregation group includes up to 12 physical ports.
- Supports both intra- and inter- uplink card port aggregation.
- System priority: 0 to 65535.
- Port priority: 0 to 32767;
- The short LACP_timeout: 1 second to 10 seconds, with the default being 1 second.
- The long LACP_timeout: 20 seconds to 40 seconds, with the default being 30 seconds.

8.6.4 Basic Principles

Manual aggregation group

The members in a TRUNK group are configured manually by users, the LACP protocol does not run, and the system is not allowed to add or delete ports in the aggregation group automatically. Each aggregation group must include one port at least. When an aggregation group includes only one port, users can delete this port from the aggregation group only by deleting this aggregation group. A group includes one master port and several member ports. Via the configuration and management of the master port, users can configure and manage all ports in this TRUNK group.

In this mode, users need to combine random certain ports on the AN5116-06B uplink card to form an aggregation group and implement the link aggregation.

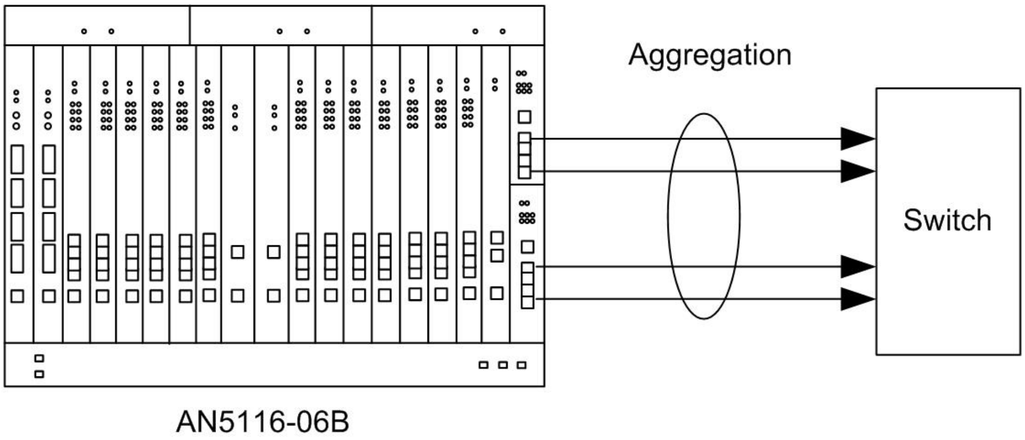


Figure 8-8 The manual aggregation group

Dynamic aggregation group

In the dynamic aggregation mode, the system creates / deletes the aggregation group and its members automatically, the LACP is running, and users are not allowed to add or delete member ports in the aggregation group. Multiple ports can be aggregated dynamically only when they have the same rate and duplex features, are connected to the same equipment, and have the same basic configurations.

The LACP protocol exchanges information with the opposite end via the LACPDU. When the LACP protocol of a certain port is enabled, this port sends LACPDU to notify the opposite end of its own system priority, system MAC address, port priority, port No., and operation key. After receiving the previous information, the opposite end compares them with the information saved by other ports to select the ports that can join the aggregation. Via this operation, the two parties can reach an agreement on a port joining or exiting a certain dynamic aggregation group.

The operation key is a configuration combination generated by the LACP protocol according to the port configuration (rate, duplex, basic configuration, management key) when the port aggregation is performed.

When running the LACP, the AN5116-06B can aggregate multiple ports on the uplink card automatically, so as to implement the link aggregation function.

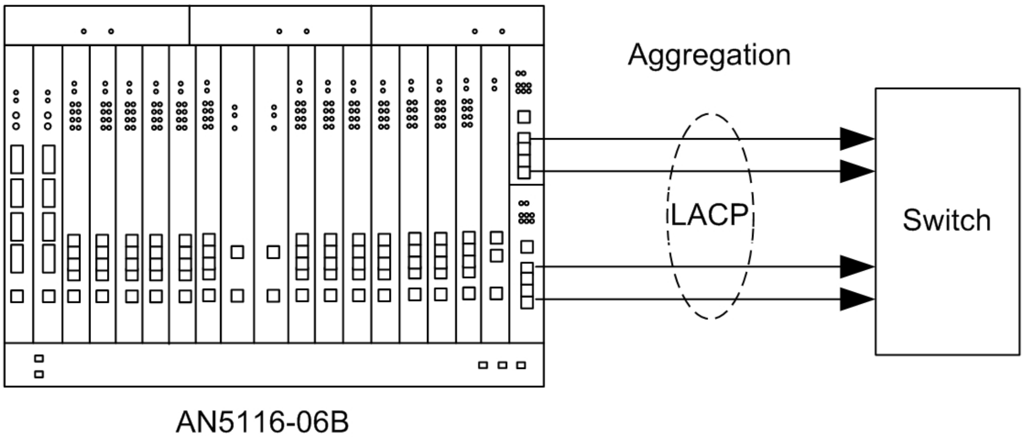


Figure 8-9 The dynamic aggregation group

8.6.5 Reference Information

Reference standard

IEEE 802.3ad：Amendment to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Access method and physical layer specifications - Aggregation of multiple link segments

Terminology

Terminology	Description
TRUNK	Port aggregation
Master port	It is the port in a certain TRUNK group to act as the representative of this group, and users can manage this group via managing this port.
Member port	Any port except for the master port in a TRUNK group.
Operation key	Is a configuration combination including rate, duplex, basic configuration, and management key.

Abbreviations

Abbreviations	Meaning
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit

8.7 Ethernet Port Mirroring

8.7.1 Definition

The port mirroring is to copy and forward all data traffics on a certain port to another port, so as to view and analyze the working status and network traffic of the mirrored port.

8.7.2 Features

- Can monitor the ingress and egress packets on a port.
- Via the data obtained from the mirroring, users can analyze the network faults and isolate faults efficiently.
- The data transmission of the monitored port is not influenced by the mirroring operation.

8.7.3 Specifications

The AN5116-06B supports the one-to-one port mirroring.

8.7.4 Basic Principles

In the port mirroring, the port whose traffics are copied is the monitored port, and the port to which the traffics are copied is the monitoring port. The monitoring port is connected with a data analyzer, and users can analyze the data of the monitored port. The connection diagram of the port mirroring is shown in Figure 15-1.

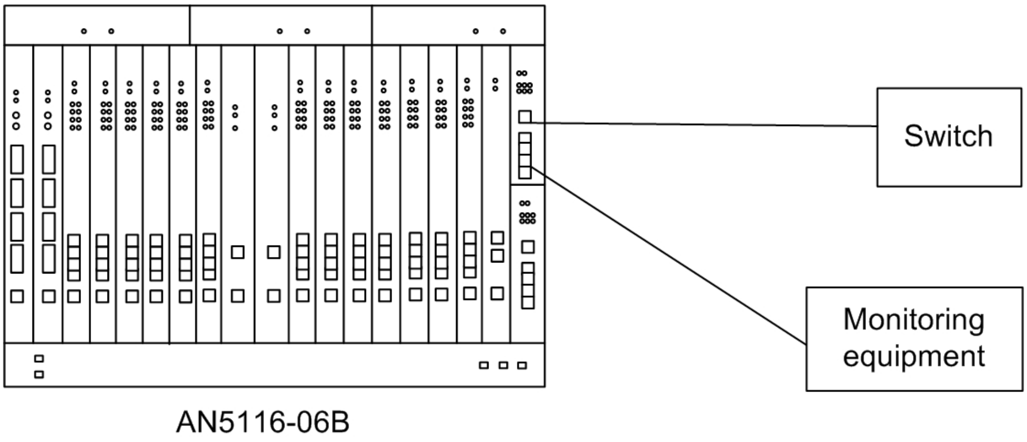


Figure 8-10 The port mirroring

The switch is connected with the monitored port, and the monitor equipment is connected with the monitoring port. The data of the monitored port can be copied to the monitoring port synchronously, so the monitoring port can monitor the data conditions of the monitored port.

The port mirroring does not influence the normal service transmission of the monitored port. It only sends the copies of the Tx / Rx packets of the monitored port to the monitoring port.

In the port mirroring, users can set the flow of the data to be monitored, and the flow can be ingress, egress, or bidirectional. But in one mirroring task, all monitored ports must have the same data flow.

Users need to pay attention that when a certain port in an aggregation group becomes a monitored port, its aggregation function will be disabled.

8.7.5 Reference Information

Terminology

Terminology	Description
Monitoring port	It is the destination port of the copied data stream, connected with the data analysis device.
Monitored port	It is the port whose data stream is copied, namely the analyzed object port.

9 Layer 3 Features

- ☑ ARP Proxy
- ☑ DHCP Relay
- ☑ OSPF
- ☑ RIP

9.1 ARP Proxy

9.1.1 Definition

ARP Proxy performs the layer 3 ARP proxy function of the AN5116-06B and provides the VoIP service intercommunication for the VoIP users accessed to the same OLT. After enabling the ARP Proxy function for the OLT, the OLT handles the received VoIP user messages.

9.1.2 Features

Performs the user VoIP service intercommunication under the same OLT.

9.1.3 Specifications

Supports the telephone intercommunication of the VoIP users under the same OLT.

9.1.4 Basic Principles

As shown in Figure 9-1, the ONU1 and ONU2 are located in different VLANs. The layer 2 is in port isolation mode. The ONU1 and ONU2 are connected using the layer 3 interface and are located within a subnet.

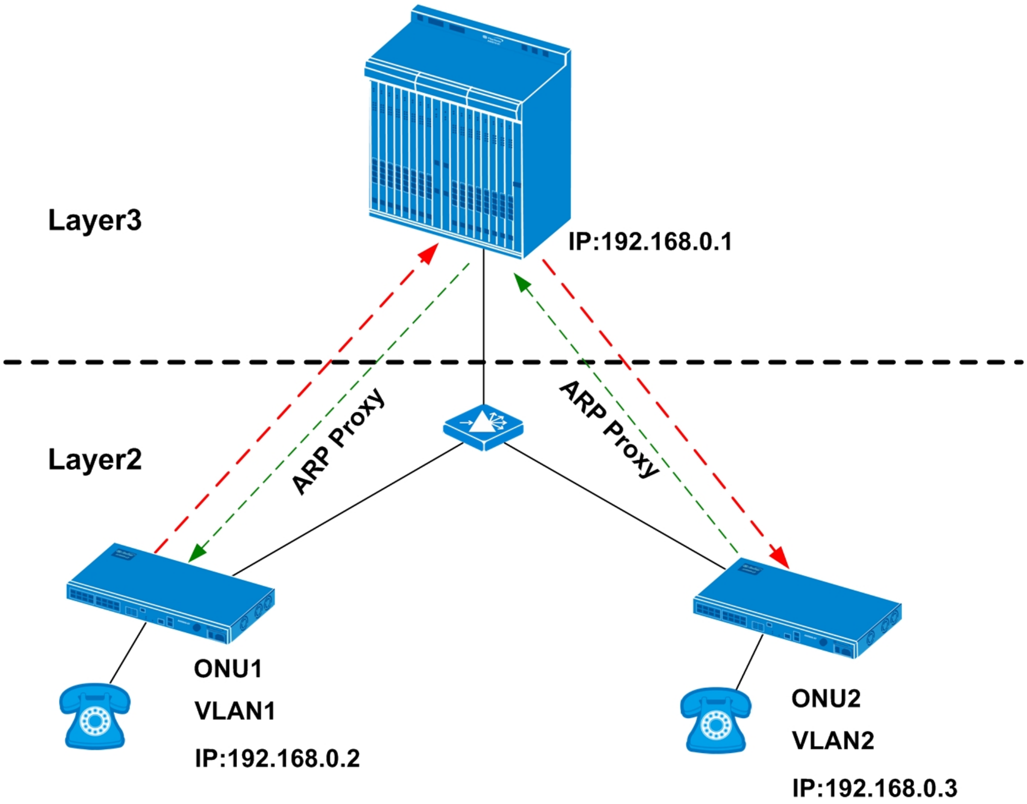


Figure 9-1 ARP Proxy principle

The AN5116-06B ARP Proxy can be performed by the methods below:

1. The ONU1 and ONU2 are located in the same subnet. When accessing the ONU2, the ONU1 will broadcast the ARP messages and request the MAC address of the ONU2.

2. Because the user ONU1 and ONU2 are isolated in the layer 2, the ARP request message will not be sent to user ONU2 directly. The ARP request messages will be sent to the AN5116-06B to handle.

3. After receiving the ARP request messages, the AN5116-06B will send its MAC address to the ONU1 and query whether the MAC address of the ONU2 exits in the APR table.

    - If the MAC address of the ONU2 exits in the APR table of the OLT, the ONU1 messages can be forwarded to the ONU2 via the AN5116-06B.

- If the MAC address of the ONU2 does not exit in the APR table of the OLT, the AN5116-06B will broadcast the ARP messages using the layer 3 interface to request the MAC address of the ONU2. After the APR of the ONU2 responds the messages, the MAC address of the ONU2 will be added into the APR table.

Then the ONU1 and ONU2 can intercommunicate via the AN5116-06B.

9.1.5 Reference Information

Reference standard

IETF RFC 1027：Using ARP to implement transparent subnet gateways

Terminology

Terminology	Description
Address resolution	Address resolution means converting the entity address of a system into two equivalent addresses existing systems.

Abbreviations

Abbreviations	Meaning
ARP	Address Resolution Protocol
ARP Proxy	Address Resolution Protocol Proxy
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol

9.2 DHCP Relay

9.2.1 Definition

The DHCP relay function performs the inter-network segment forwarding of the DHCP broadcast messages between the DHCP client end and the DHCP server. This function enables the DHCP client ends from different network segments requesting the dynamic IP addresses from the same DHCP server.

9.2.2 Features

- Performs the centralized management for the DHCP client ends to save the DHCP server resources.
- The AN5116-06B forcibly forwards the user DHCP request to the specified DHCP server to prevent the DHCP counterfeit, so as to improve the service security of the operator network.

9.2.3 Specifications

- Supports configuring 16 DHCP server groups, each group contains one working DHCP server and one standby DHCP server.
- Supports configuring the DHCP Relay working mode.

9.2.4 Basic Principles

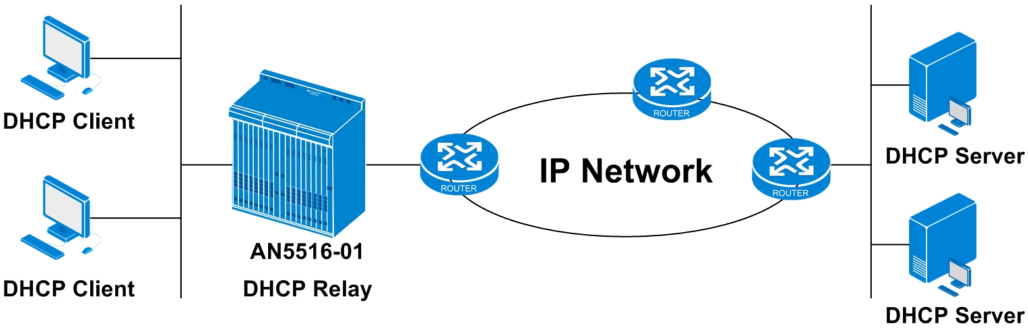


Figure 9-2 DHCP Relay principle

The working flow of the DHCP Relay is as follows:

After started, the DHCP client end will be initiated, and start broadcasting DHCP request messages within the LAN.

- If DHCP server exits within the LAN: the AN5116-06B cannot use the DHCP Relay function. The DHCP server in the LAN configures the DHCP for the DHCP client end in the network.

- If DHCP server does not exit within the LAN: the AN5116-06B will enable the DHCP Relay function. The received DHCP broadcast messages will be handled by the following methods:

  1) Select the corresponding DHCP server group;

  2) The AN5116-06B converts the user DHCP broadcast messages into unicast messages, and replace the gateway IP address (giaddr) in the DHCP message with the system IP.

  3) The AN5116-06B forwards the DHCP messages to the specified DHCP server group.

9.2.5 Reference Information

Reference standard

- IETF RFC 2131：Dynamic Host Configuration Protocol
- IETF RFC 3046：DHCP Relay Agent Information Option

Terminology

Terminology	**Description**
Dynamic distribution	When the DHCP client end first leased IP address from the DHCP server, the IP address is not permanent. After the leases expire. client end should release the IP address for other station.

Abbreviations

Abbreviations	**Meaning**
DHCP	Dynamic Host Configuration Protocol
DHCP Relay	Dynamic Host Configuration Protocol Relay Agent

9.3 OSPF

9.3.1 Definition

OSPF is a interior gateway protocol based on link status developed by the IETF.

OSPF uses the Dijkstra algorithm, also called Shortest Path First (SPF) algorithm. The SPF algorithm calculates the shortest path to the other routers in the network topology, to set up the routing table.

9.3.2 Features

- The routing overhead of the OSPF protocol is inversely proportional to the link bandwidth. Each overhead is 10^8 / link bandwidth.
- Supports various network: broadcast, non broadcast, point-to-point and point-to-multipoint.
- Non routing loopback: OSPF calculates the routing using the shortest path algorithm according to the collected link statuses.
- Fast convergence: sends updated messages immediately when the network topology structure changes to enable synchronization in the autonomous system.
- Supports area setting: allows to set areas for the autonomous system to manage, reducing the broadcast of the link status data packets within the entire network.
- Transmits and receives the protocol data using the IP multicast.
- Supports multiple equivalent routing to the same destination: when multiple routings who have the same overheads exit in the routers to the same destination, the traffic can be distributed to multiple paths.
- Supports the protocol message authentication.

9.3.3 Specifications

9.3.4 Basic Principles

OSPF message type

The OSPF message is above the IP layer with the protocol number 89.

Data Link header	IP header	OSPF header	OSPF Payload	FCS

Figure 9-3 OSPF protocol message bearer

OSPF message type

The OSPF message includes five types:

Type	Message Name	Message Function
1	Hello	Discovers and maintains the neighborhood relationship
2	Database Description	Transmits the description data packets of the link status database.
3	Link State Request	Requests the specified link status information.
4	Link State Update	Transmits the detailed link status information.
5	Link State Ack	Transmits the confirmation messages.

- Neighborhood establishing and maintaining: the neighborhood relationship is established by the Hello messages, and then the DD, LSR and LSU messages will be sent. After being established, the neighborhood relationship of the LSDBs on two ends need to be maintained by the Hello messages, which is performed by two timers.
  - Hello TIME: 10 seconds by default.
  - DEAD TIME: 4 times of the Hello TIME by default.
- The communication and database exchange will be enabled after the adjacency relation is established.

  The OSPF router generates the description data packets of the database regularly and sends the data packets to the adjacent routers. The data packet is associated with serial number. The router of adjacency relation can compare the description data packets of the database with its own database according to the serial number. If the serial number of the received data is larger than that of the database, the router of adjacency relation will send request for the data with larger serial number, and update the link status database with the requested data.

SPF algorithm

The SPF algorithm calculates the distance between the router and the destination router, taking each router as a root. Each router calculates the topology structure diagram of the router domain according to a unified database. The structure diagram resembles a tree and is called the shortest path tree in the SPF algorithm. The trunk length of the shortest path tree, the distance from the OSPF router to each destination router, is called OSPF router overhead. It is 10^8 / link bandwidth. The bigger the bandwidth is, the lower the router overhead is, and the nearer the distance between the OSPF to the destination is.

9.3.5 Reference Information

Reference standard

IETF RFC 2328：OSPF Version 2

Terminology

- AS: the entire network, composed of multiple autonomous system (AS), dynamically discovers and transmits the routing by collecting and delivering AS link statuses, so as to perform the AS information synchronization. Each AS can be set to different areas.
- Backbone area: a backbone area, which is usually Area 0, identified by 0.0.0.0, exists in the OSPF routing protocol. Other areas all connect with the backbone area directly. When being broadcasted, the routing information of an area will be first transmitted to the backbone area, and then transmitted to other area to broadcast.
- Virtual connection: the virtual connection is introduced because the backbone areas should be logically connected. Virtual connection logically connects the areas which are physically isolated. If no backbone area (Area 0) exists in the network, the virtual connection is needed between two ABRs. As a part of the backbone area, all the virtual connections belong to Area 0.
- LSA: each router notifies other routers of this area of its known link status. The notification is called link status notification. Each router sets up a complete link status database of this area.

- Router ID: uniquely identifies an OSPF router in the OSPF network, with the structure of 32-bit IP address. During neighborhood relationship establishment, the router ID acts as the ID to greet neighbors using HELLO messages; during operation algorithm, it acts as the node of the SPF tree.
- Neighborhood relationship and adjacency relationship: the neighborhood relationship means the relationship established when two OSPF routers meet specified requirements. Adjacency relationship means the relationship between two adjacent OSPF routers who can exchange LSA. Neighborhood is not always adjacency relationship.
- ABR: if one port of the router is distributed to multiple areas, this routers is called area border router. The area border router merges some routings, which share the same prefix, in the routing table of this area into one routing, and then notifies other areas.
- ASBR: the router exchanging routing information with other AS is called autonomous system border router (ASBR). The ASBR merges the routings sharing the same prefix (except AS) into one routing and notifies the entire OSPF domain.

Abbreviations

Abbreviations	Meaning
ABR	Area Border Router
AS	Autonomous System
ASBR	Autonomous System Boundary Router
LSA	Link State Advertisement
OSPF	Open Shortest Path First

9.4 RIP

9.4.1 Definition

The RIP routing protocol is the simplest dynamic routing protocol, which uses the distance vector routing algorithm to exchange the routing information via UDP.

The dynamic routing can self-adjust according to the network topology and traffic change. It can query and update the route table configuration using the dynamic routing protocol.

9.4.2 Features

- The RIP route cannot use multiple routes between two network. It selects a route which has the least routers.
- The RIP is above the UDP. The routing information received by the RIP route is encapsulated into the UDP data packet, whose port number is 520.
- Performs simple management, applicable for small-scale network.

9.4.3 Specifications

The AN5116-06B supports up to 1k RIP routings.

9.4.4 Basic Principles

Forming process of the RIP protocol table

The RIP protocol uses hops to measure the distance to the destination network, which is called routing metric. In the RIP, the hop number from the router to the network it directly connected to is 0; the hop number from the router to the network via another router is 1, and so on. To limit the convergence time, the RIP sets the rule that the metric value should be within 0 to 15; the hop number equals or larger than 16 is defined as infinite, which means the destination network or host cannot be reached.

Note:

Each router updates its routing table according to the routing information received from the adjacent router.

1. When started, the RIP routing's initiate routing table only contains the straight-through port routings of the router.

2. After started, the RIP routing broadcasts a Request message to each interface every 30 seconds by default.
3. After receiving the Request message from the interface, the adjacent router forms the Response messages according to its routing table, and then broadcasts the messages to the network corresponding to the interface.
4. The RIP routing receives the Response message responded by the adjacent router, which contains the routing table of the adjacent router, and then forms its routing table. If the router has not received the Response message from the opposite end in 180 seconds, it will identify the routing information from this router as unreachable; after that, if the router has not received the updating message in 120 seconds, this routing will be deleted from the routing table.

Routing loop

When maintaining the routing table information, if the topology changes, the routing loop may be faulty because the slow convergence of network generates the uncoordinated or contradictory entries. As the router ignores the routing that cannot reach the network, the user's packet will be transmitted repeatedly in the network and thus a large quantity of network resources will be consumed.

Assume three router A, B and C exist. The router C connects with the network 11.4.0.0 directly (hop number is 0). The router B reaches the network 11.4.0.0 via the router C (hop number is 1). The router B reaches the network 11.4.0.0 via the router B (hop number is 2). The routing loop may be generated between routers if the network 11.4.0.0 is faulty.

The RIP prevent the routing loop using the following mechanism:

- Defines the maximum value: defines the overhead value 16 as unreachable to prevent the infinite routing weight when routing loop occurs and correct the incorrect routing information. The routing loop may still exist before the overhead value reaches the maximum value.
- Split horizon: does not allow the router transmitting the updating routing information back to the port which transmits the routing information. That is, after learning the routing to the network 11.4.0.0 from the router C, the router B does not transmit the routing information to the network 11.4.0.0 back to the router C. So that the bandwidth consumption is reduced and the routing loop is also prevented.

- Route poisoning: when the network 11.4.0.0 cannot be accessed, the router C will transmit the updating routing information to the adjacent routers and identify routing weight of the network to infinite, so as to inform that it is unreachable. After receiving the route poisoning information, the router B identifies the link item in the routing table to infinite to indicate this routing is unavailable; and then the router B informs the adjacent router A and other routers in sequence that the network 11.4.0.0 is unavailable. So that the routers will no longer receive the updating information, which prevents the routing loop.
- Triggered update: when discovering that the network 11.4.0.0 is faulty, the router C informs the adjacent routers that the network 11.4.0.0 is unavailable immediately without waiting for the updating period.

9.4.5 Reference Information

Reference standard

- IETF RFC1058：Routing Information Protocol
- IETF RFC1723：RIP Version 2 - Carrying Additional Information

Terminology

No

Abbreviations

Abbreviations	Meaning
RIP	Routing Information Protocol
UDP	User Datagram Protocol
IP	Internet Protocol

10 Traffic Management

☑ Traffic Classification

☑ Traffic Strategy

10.1 Traffic Classification

10.1.1 Definition

Traffic classification means classifying user data messages according to the features and rules, and handling them using different methods and providing different services, so as to improve the data transmission capacity.

10.1.2 Features

Performs service traffic differentiation to provide different QoS guarantees for each user service.

10.1.3 Specifications

The AN5116-06B supports the following traffic classification rules:

- Source MAC address;
- Destination MAC address;
- Classification based on source IP address;
- Classification based on destination IP address;
- Classification based on VLAN ID;
- Classification based on Ethernet type;
- Classification based on IP protocol type;
- Classification based on Ethernet priority;
- Classification based on IPv4 ToS / DSCP;
- Classification based on L4 source port;
- Classification based on L4 destination port;
- Classification based on TTL.

10.1.4 Basic Principles

The AN5116-06B's traffic classification means classifying the user services on the ONU according to the user data message features so as to provide QoS guarantee for each user service traffic on the ONU side.

After the entering into the ONU, the messages will be classified according to the traffic classification rules, and then the classified data traffic will be bound with different traffic strategies.

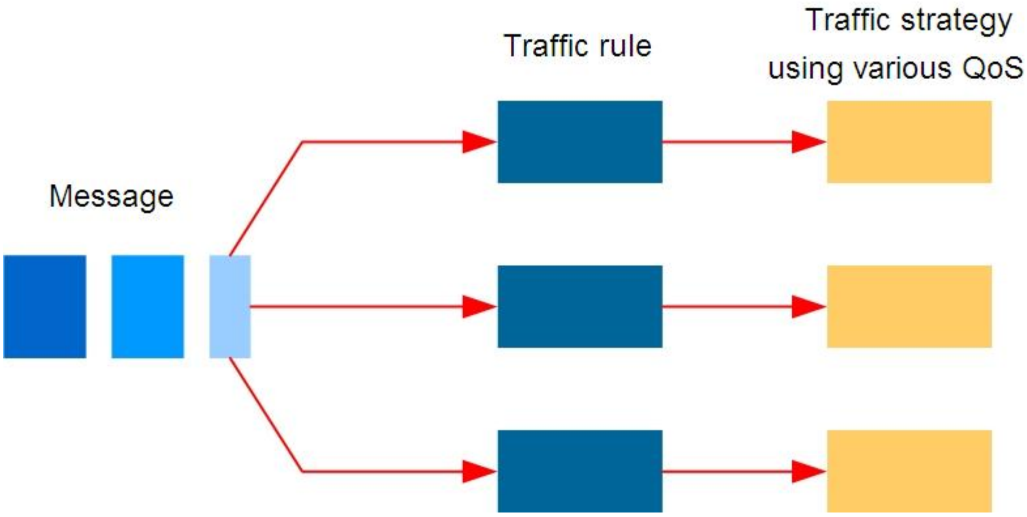


Figure 10-1 The principle of the flow rule

10.1.5 Reference Information

Abbreviations

Abbreviations	Meaning
QoS	Quality of Service
ToS	Type of Service

10.2 Traffic Strategy

10.2.1 Definition

The traffic strategy provides the end-to end QoS guarantee for user services, including traffic classification, priority marking, traffic rate control and monitoring, and queue scheduling management.

10.2.2 Features

Uses the techniques such as the priority marking, traffic rate control and monitoring, and queue scheduling to provide end-to-end QoS guarantee for users.

10.2.3 Specifications

- Supports re-marking the priority.
- Supports traffic rate control; supports configuring the parameters such as guaranteed rate, burst size, excess burst size and peak cell rate.
- Supports mapping to eight queue for scheduling.

10.2.4 Basic Principles

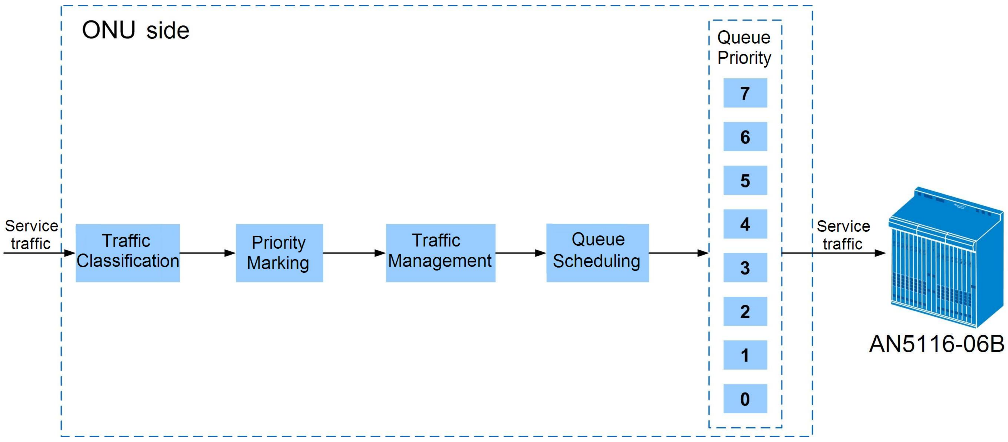


Figure 10-2 The principle of the flow strategy

The handling methods for the AN5116-06B traffic strategy are as follows:

1. Traffic classification;

   Classifies the user services on the ONU according to the user data message features so as to provide QoS guarantee for each user service traffic on the ONU side.

2. Priority marking

   The service traffic of different types will be scheduled according to their priorities.

3. Traffic management;

   Limits the burst traffic entering into the equipment. When the message traffic entering the ONU is excessive, the traffic management will limit and discard the message according to the pre-set guaranteed rate and each burst size, so as to keep the port at a relatively stable ratio and prevent the equipment of lower level from strike.

4. Queue scheduling.

   Manages the export messages of the ONU port, that is, the messages of different priority enters the queue of different priority, and schedules according to the PQ, WRR and mixed priority algorithm, so as to resolve the equipment congestion.

10.2.5 Reference Information

Reference standard

- IETF RFC 2481：A Proposal to add Explicit Congestion Notification(ECN) to IP
- IETF RFC 2474：Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers
- IETF RFC 1349：Type of Service in the Internet Protocol Suite

Terminology

None

Abbreviations

Abbreviations	Meaning
PQ	Strict-Priority Queue
WRR	Weighted Round Robin

11 Line Identifier

☑ DHCP Option82

☑ DHCP Option60

11.1 DHCP Option82

11.1.1 Definition

The DHCP Option 82 is called the relay agent information option, and it includes the position information of the DHCP client. The Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers recognizing the Relay Agent Information option may use the information to implement IP address or other parameter assignment policies.

11.1.2 Features

The Option 82 can record the address information of the DHCP client and the DHCP relay agent in the DHCP packet. A DHCP packet passing through the DHCP realy equipment will be tagged with the unique address information, and the format of the information can be defined via the network management system.

11.1.3 Specifications

- Supports the Option 82 enabling / disabilng function.
- The local basic information (access node ID, cabinet No., and subrack No.) can be configured.
- Provides 22 types of ID parameters, and supports the user defined relay ID information.

11.1.4 Basic Principles

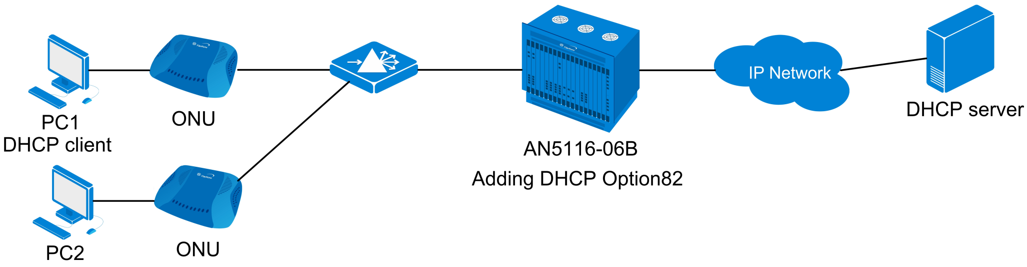


Figure 11-1 The principle of the DHCP Option 82

The AN5116-06B addes the Option 82 information in the user DHCP request packet and the user access point information, and reports to the DHCP server.

The DHCP server can allocate different IP addresses or provide different parameter values for PC1 and PC2 according to the Option 82 option information and the pre-configured policy provided by the packet, to configure and manage the client.

11.1.5 Reference Information

Reference standard

- IETF RFC 2131：Dynamic Host Configuration Protocol
- IETF RFC 3046：DHCP Relay Agent Information Option

Terminology

Terminology	Description
Option 82	The Option 82 is called the relay agent information option, and it records the position information of the DHCP client.
DHCP Relay	The DHCP relay forwards the user DHCP request to the designated DHCP server.

Abbreviations

Abbreviations	Meaning
DHCP Option 82	DHCP Relay Agent Information Option

11.2 DHCP Option60

11.2.1 Definition

The DHCP Option 60 obtains an IP address for the voice service in the DHCP mode, and the Option 60 field is used to identify the user IAD information. The AN5116-06B identifies the Option 60 field in the user DHCP packet and forwards the packet to different DHCP servers; this enables each IAD to obtain a dedicated IP address and perform the authentication and accounting operations via this DHCP server.

11.2.2 Features

In the same VLAN, the AN5116-06B forwards the DHCP packets to different DHCP servers according to the Option 60 field in the IAD DHCP packet and the configurations of the AN5116-06B, so as to obtain different IP addresses.

11.2.3 Specifications

- Supports adding the line ID format.
- Supports adding the ONU ID of the access point.

11.2.4 Basic Principles

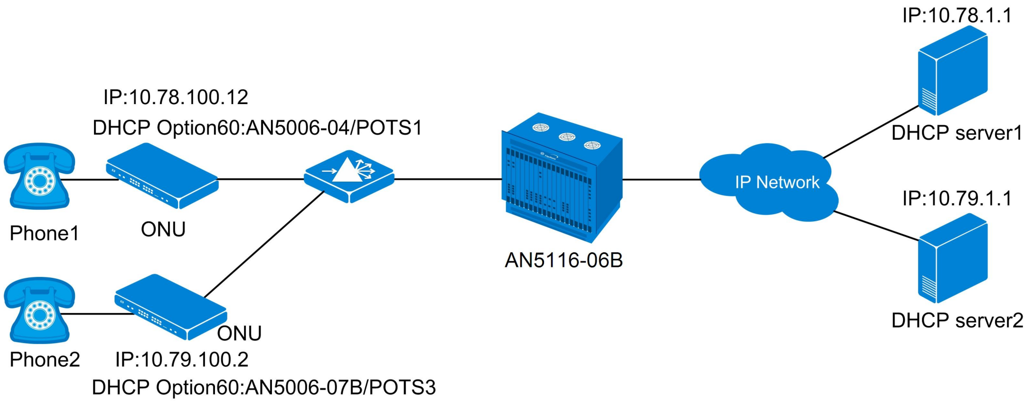


Figure 11-2 The principle of the DHCP Option 60

Two types of ONUs exist at the AN5116-06B user side to access the voice service: the AN5006-04 and the AN5006-07B; the AN5006-04 uses POTS port 1, and the AN5006-07B uses POTS port 3. The system uses the Option 60 field to identify the IAD modules in the two ONUs; the AN5006-04 IAD obtains the IP address 10.78.100.12 via DHCP server 1, and the AN5006-07B IAD obtains the IP address 10.79.100. 2 via DHCP server 2.

As the DHCP relay, the AN5116-06B finds the corresponding DHCP server according to the DHCP Option 60 field from the IAD to enable the IAD to obtain the IP address.

11.2.5 Reference Information

Reference standard

IETF RFC 2131：Dynamic Host Configuration Protocol

Terminology

Terminology	Description
Option 60	The DHCP Option 60 field is used to identify the information of the user ONU .
DHCP Relay	The DHCP relay forwards the user DHCP request to the designated DHCP server.

Abbreviations

Abbreviations	Meaning
DHCP Option 60	Vendor Class Identifier

12 QoS

☑ Priority ID

☑ Mapping between the CoS Priority and the Queue Scheduling

☑ Congestion Control

☑ Rate Limitation Based on the Flow and the Port

12.1 Priority ID

12.1.1 Definition

The priority ID includes the IP ToS, the DSCP, the 802.1P, etc., and these priority IDs are used to identify different QoS models.

- The CoS priority ID means identifying the CoS priority based on the flow.
- The DSCP priority ID is described as follows: In the ToS field at the IP header of each data packet, the occupied six bits and non-occupied two bits are used to distinguish the priority via the coding value.

12.1.2 Features

- Modification of multiple priority types

  The AN5116-06B supports modifying the CoS and DSCP priorities.

- Modification of multipoint priorities

  The AN5116-06B supports modifying the priorities at the OLT side and the ONU side.

12.1.3 Specifications

- Supports the default CoS priority.
- Supports the priority mapping.
- Supports the CoS copy (copying the CoS value of the C-VLAN to the S-VLAN).
- Supports modifying the DSCP according to the CoS.
- Supports CoS remarking.

12.1.4 Basic Principles

The commonly used modifations on the priority in the QoS include the DSCP and the 802.1P.

- The DSCP priority is indicated by the first six bits (bits 0 to 5) in the ToS field at the IP packet header, and the value ranges from 0 to 63; the last two bits (bits 6 and 7) are reserved.
  - The two-byte tag protocol identifier, with the value being 8100.
  - The two-byte tag control information.
- The 802.1P priority is based on the layer 2 switch QoS / CoS protocol related to the traffic priority. In the 802.1Q protocol, a four-byte 802.1Q header is added after the source address in the Ethernet frame header. This four-byte 802.1Q header includes the following contents:

A three-bit priority field exists in the TCI field, and this field is the 802.1P priority, whose value ranges from 0 to 7 (meaning eight priorities); it is mainly used to determine which packet is sent first under the network congestion condition.

By default, the priorities of various services in the system are arranged as follows: VoIP = TDM > IPTV > data.

12.1.5 Reference Information

Reference standard

IETF RFC 2474：Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers

Terminology

Terminology	Description
CoS priority	Refers to the priority in the 802.1P domain of an Ethernet frame, whose value ranges from 0 to 7.
ToS priority	Refers to the priority in the ToS domain of an IP packet header field, whose value ranges from 0 to 7.
DSCP priority	In the ToS ID byte at the IP header of each data packet, the occupied six bits and non-occupied two bits are used to distinguish the priority via the coding value.

Abbreviations

Abbreviations	Meaning
ToS	Type Of Service
DSCP	Differentiated Services Code Point
TPID	Tag Protocol Identifier
TCI	Tag Control Information
802.1p	LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization

12.2 Mapping between the CoS Priority and the Queue Scheduling

12.2.1 Definition

The mapping between the CoS priority and the queue scheduling refers to sending a packet with a certain priority to the designated queue.

12.2.2 Features

The AN5116-06B can configure the mapping relationships between the priority and the queue as requried, so as to control the QoS. For example, if the voice service whose CoS priority is 6 has a relatively better QoS, users can map this service to queue 7, so as to ensure that the voice service can be scheduled first.

12.2.3 Specifications

Supports the priority mapping.

12.2.4 Basic Principles

When a packet is to enter a queue for the scheduling operation, it needs to enter the corresponding queue according to the mapping relationship between the packet priority and the queue.

In queues 0 to 7, queue 7 has the highest priority, and queue 0 has the lowest priority.

By default, a fixed mapping relationship exists between the priority of a packet and the queue that it is to enter. For example, a packet whose priority is 1 will enter queue 1.

The mapping relationship also can be re-configured according to the actual network conditions. For example, CoS priority 2 indicates the data service, CoS priority 3 indicates the IPTV service, and CoS priority 5 indicates the VoIP service; the three services enter queues 1, 4, 6 respectively. The mapping relationship between the priority and the queue is listed in Table 12-1.

Table 12-1 The mapping relationship between the priority and the queue

CoS Priority	**Queue**		
	Default	**Application Condition**	**Corresponding Service**
0	0	—	—
1	1	—	—
2	2	1	DATA
3	3	4	IPTV
4	4	—	—
5	5	6	VoIP
6	6	—	—
7	7	—	—

12.2.5 Reference Information

Reference standard

- IETF RFC 2474：Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers
- IETF RFC 1349：Type of Service in the Internet Protocol Suite

Terminology

Terminology	Description
CoS Priority	Refers to the priority in the 802.1P domain of an Ethernet frame, whose value ranges from 0 to 7.
Priority queue	Means another queue mode different from the first-in first-out queue. In this mode, a queue with a higher priority is usually schduled first.

Abbreviations

Abbreviations	Meaning
CoS	Class of Service

12.3 Congestion Control

12.3.1 Definition

The congestion control means the method to implement the management, control, and processing operations when the network congestion occurs. It is described as follows: Uses the queue technology to schedule the packets to be sent from the same interface into multiple queues, and processes these queues according to their priorities. The system uses different queue algorithms to solve different problems and obtain the required results.

When network congestion occurs, various queues will compete for the use of resources. Under this condition, the system usually uses the queue scheduling to meet the requirements of various services.

◆ Strict-priority queue scheduling (SP): Processes the packets in each queue according to the priority of this queue. The system first allows the packets in the highest-priority queue to leave and sends them; after the packets in the highest-priority queue are all sent, the system sends the packets in other queues with lower priorities.

- Weighted round robin scheduling (WRR): The system assigns a dedicated weight value for each queue. Depending on the weight, the packets in a high-weight priority queue have more chance to be processed than the packets in a low-weight priority queue, and each queue uses the bandwidth resource according to its weight proportion.
- Mixed-mode scheduling (SP + WRR): The high-priority queues use the SP mode, and the low-priority queues use the WRR mode. In this mode, the system first sends the packets in the high-priority queues; after the packets in the high-priority queues are all sent, each low-priority queue uses the bandwidth resource according to its weight proportion.

12.3.2 Features

The AN5116-06B supports the SP, WRR, and mixed-mode queue scheduling.

12.3.3 Specifications

- Each AN5116-06B port supports eight priority queues.
- Supports the queue scheduling in the SP mode.
- Supports the queue scheduling in the WRR mode.
- Supports the queue scheduling in the SP + WRR mode.

12.3.4 Basic Principles

SP mode

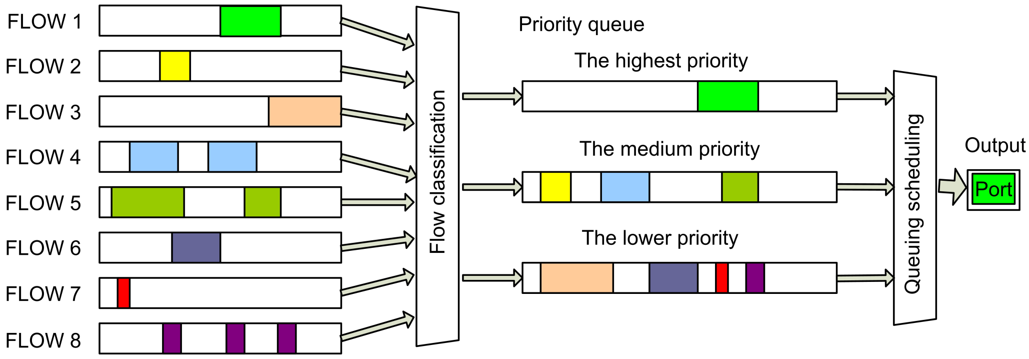


Figure 12-1 The principle of the queue scheduling in the SP mode

1. The system first marks the priorities of and classifies the packets in the eight flows via the configured flow classification rules and flow policies.
2. Performs the priority mapping, and arranges the packets into different priority queues.
3. The system sends the packets strictly according to the queue priority: First sends the packets in the high-priority queues, then sends the packets in the medium-priority queues, and finally sends the packets in the low-priority queues.

WRR mode

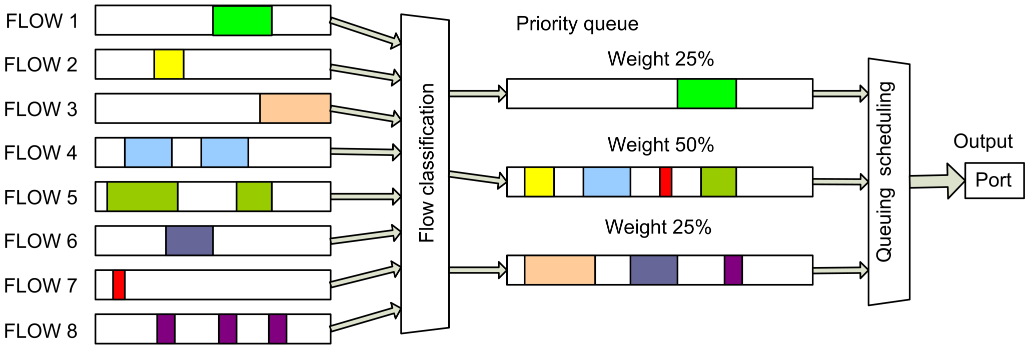


Figure 12-2 The principle of the queue scheduling in the WRR mode

1. The system first marks the priorities of and classifies the packets in the eight flows via the configured flow classification rules and flow policies.
2. Performs the priority mapping, and arranges the packets into different priority queues.
3. In each scheduling circle, each priority queue sends its packets according to the weight proportion 1: 2: 1.

SP + WRR mode

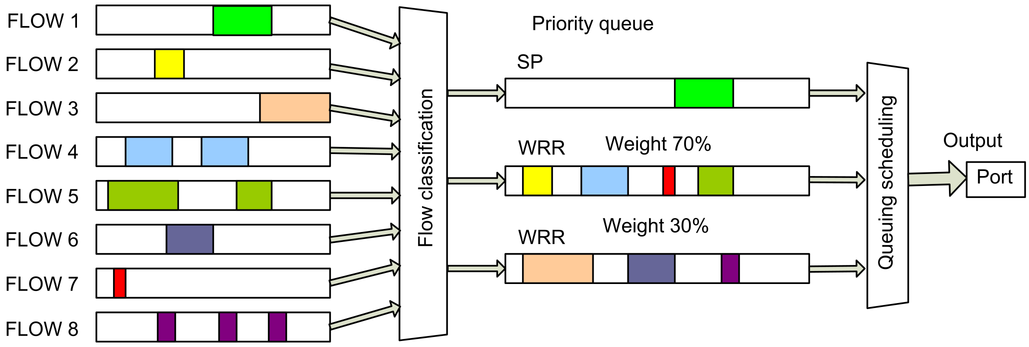


Figure 12-3 The principle of the queue scheduling in the SP+WRR mode

1. The system first marks the priorities of and classifies the packets in the eight flows via the configured flow classification rules and flow policies.
2. Performs the priority mapping, and arranges the packets into different priority queues.
3. For the high-priority queues, the system uses the SP scheduling mode; this means that the system sends the packets in them first.
4. For other priority queues, the system uses the WRR scheduling mode; in this example, each priority queue sends its packets according to the weight proportion 7: 3.

12.3.5 Reference Information

Reference standard

IETF RFC 2481：A Proposal to add Explicit Congestion Notification(ECN) to IP

Terminology

Terminology	Description
Weight	The weight means the proportion of a queue to occupy resources.
Congestion	Congestion is described as follows: If the number of the packets reaching a certain part in the communication subnet is so many that this part of network cannot process these packets in a timely manner, and this causes the performance degradation of this part and even the entire network; under the worst conditions, the communication services in the network will be interrupted (this is called dead lock).

Abbreviations

Abbreviations	Meaning
PQ	Priority Queuing
WRR	Weighted Round Robin
SP	Strict Priority

12.4 Rate Limitation Based on the Flow and the Port

12.4.1 Definition

To manage the bandwidth of each service, users can configure the rate limitation parameters based on the port and the flow. The purpose of this operation is to ensure that a certain port or flow does not occupy too much bandwidth.

12.4.2 Features

None.

12.4.3 Specifications

- Supports the service bandwidth limitation.

- Supports the port bandwidth limitation.

12.4.4 Basic Principles

Port-based and flow-based rate limitation of the uplink service

- At the ONU side, if each logic link bears only one type of service, users can perform the flow-based rate limitation according to the LLID. If a certain logic link bears multiple types of services, the flow-based rate limitation is not supported. Under this condition, users only can perform the rate limitation of a certain type of services or use the port-based rate limitation for the ONU.
- At the OLT side, the interface card can distinguish the uplink service flow and perform the flow-based rate limitation of the service flow in each PON.

Port-based and flow-based rate limitation of the downlink service

- At the ONU side, the rate limitation principle is the same as that of the uplink service. An FTTB ONU supports the downlink port-based and flow-based rate limitation, and an FTTH ONU only supports the downlink port-based limitation.
- At the OLT side, the core switch card can distinguish the downlink service flow and perform the flow-based rate limitation of each flow type; in addition, the core switch card supports the downlink port-based limitation.

12.4.5 Reference Information

Terminology

Terminology	Description
LLID	Means the logical link identification. When an OLT broadcasts and sends the downlink signals continuously, the ONU will receive the downlink signals selectively according to the LLID.

Abbreviations

Abbreviations	Meaning
LLID	Logical Link Identification

13 DBA

☑ Definition

☑ Features

☑ Specifications

☑ Basic Principles

☑ Reference Information

13.1 Definition

The DBA is the dynamic bandwidth assignment mechanism. It is used to increase the utilization ratio of the system uplink bandwidth and assure the service fairness and QoS, and can assign the bandwidth authorization according to the queuing status information reported by the LLID.

13.2 Features

- Utilizes the idle bandwidth effectively and increases the bandwidth utilization ratio.
- Accommodates to variable traffics and the burst service.
- Provides high-speed connection service and better QoS for users.

13.3 Specifications

- The bandwidth allocation granularity of the DBA is in steps of 256 kbit/s.
- The minimum configurable bandwidth of the DBA is no more than 512 kbit/s.
- The accuracy of the DBA is better than ±5%.

13.4 Basic Principles

Bandwidth assignment types

The DBA has three bandwidth assignment types as follows:

- Fixed bandwidth: The fixed bandwidth is reserved for a dedicated ONU or the dedicated service of an ONU. Even if the ONU does not have the fixed-bandwidth uplink service traffic, the AN5116-06B still assigns the authorization corresponding to this fixed bandwidth, and this fixed bandwidth cannot be used by other ONUs. The fixed bandwidth is mainly used for the ONUs (or LLIDs) with the TDM service, so as to guarantee a smaller transmission delay of the TDM service. Generally, the fixed bandwidth is implemented by the AN5116-06B via sending the authorizations of fixed number to the ONU in a smaller polling period and higher authorization frequency.

- Assured bandwidth: The assured bandwidth is the bandwidth that that an ONU is assured to obtain, and is authorized by the AN5116-06B according to the report information of each ONU. When the actual traffic of an ONU does not reach the assured bandwidth, the AN5116-06B DBA mechanism can assign the unused bandwidth to services of other ONUs. If the actual traffic of an ONU exceeds the assured bandwidth, the AN5116-06B also can guarantee that this ONU obtains the bandwidth at least equal to the assured bandwidth, even if the traffic congestion occurs in the uplink direction of the system.
- Best effort bandwidth: It is also called the maximum bandwidth. When the bandwidth of a PON port is not used by other high-priority services, the ONU can use it. For the best effort bandwidth, the AN5116-06B assigns the authorization for an ONU according to the reports information of all online ONUs in the PON system and the bandwidth using conditions of the PON port, and the system does not guarantee the bandwidth size that is obtained by this ONU or the dedicated service of the ONU.

For a dedicated ONU, the AN5116-06B DBA mechanism supports combinations of the three bandwidth assignment types mentioned previously.

Polling and authorization mechanism

The AN5116-06B DBA mechanism supports using different polling and authorization periods for different ONUs under one PON port. For example, for an ONU with the TDM service, the AN5116-06B can select a shorter polling period and a higher authorization frequency than those of other ONUs.

Fairness mechanism

The AN5116-06B DBA algorithm supports the fairness mechanism, and it can guarantee that the remaining bandwidth is assigned fairly according to the SLA. The AN5116-06B assigns the remaining bandwidth in the weighted mode according to the SLA assured bandwidth for each user.

13.5 Reference Information

Reference standard

ITU-T G.983.4：A broadband optical access system with increased service capability using dynamic bandwidth assignment

Terminology

Terminology	Description
Fixed bandwidth	The fixed bandwidth is reserved for a dedicated ONU or the dedicated service of an ONU. Even if the ONU does not have the fixed-bandwidth uplink service traffic, the OLT still assigns the authorization corresponding to this fixed bandwidth, and this fixed bandwidth cannot be used by other ONUs either.
Assured bandwidth	The assured bandwidth is the bandwidth that that an ONU is assured to obtain, and is authorized by the OLT according to the report information of each ONU.
Best effort bandwidth	When the bandwidth of a PON port is not used by other high-priority services, the ONU can use the best effort bandwidth.

Abbreviations

Abbreviations	Meaning
DBA	Dynamic Bandwidth Assignment
LLID	Logic Link Identifier
QoS	Quality of Service
SLA	Service-Level Agreement
TDM	Time Division Multiplexing

14 System Security

☑ Anti-DoS Attack

☑ MAC Address Filtering

☑ Packet Suppression

14.1 Anti-DoS Attack

14.1.1 Definition

The denial of service (DoS) attack refers to an attack from a malicious user who sends a large number of protocol packets, which results in denying service requests of normal users by the system.

The anti-DoS attack feature refers to the defensive measures taken by the system to control and limit the number of protocol packets sent from a user.

14.1.2 Features

The equipment can prevent users from launching the DoS attack with various types of control packets, so as to increase its anti-attack performance and guarantee the security.

14.1.3 Specifications

Supports preventing users from launching the DoS attack with various types of control packets, and the attack packets include IP packet, ARP packet, DHCP packet, ICMP packet, IGMP packet, BPDU packet, etc.

14.1.4 Basic Principles

After the CPU / memory utilization ratio classification function of the core switch card is enabled, the system determines whether the DoS attack has occurred or stopped according to the following steps:

1. The switch chip of the AN5116-06B core switch card analyzes the arrived control packet and determines whether this packet is related to the DoS attack; at the same time, it observes the CPU utilization in the collected real time performance data. If the CPU utilization becomes too high suddenly, this indicates that the AN5116-06B has encountered the DoS attack.

2. When the DoS attack occurs, the system enables the anti-DoS attack function via the core switch card, so as to prevent the control packets transferred to the switch chip of the core switch card.

3. When the CPU utilization in the collected real time performance data reaches a value lower than the standard threshold, this indicates that the equipment is not DoS-attacked by the users any more.

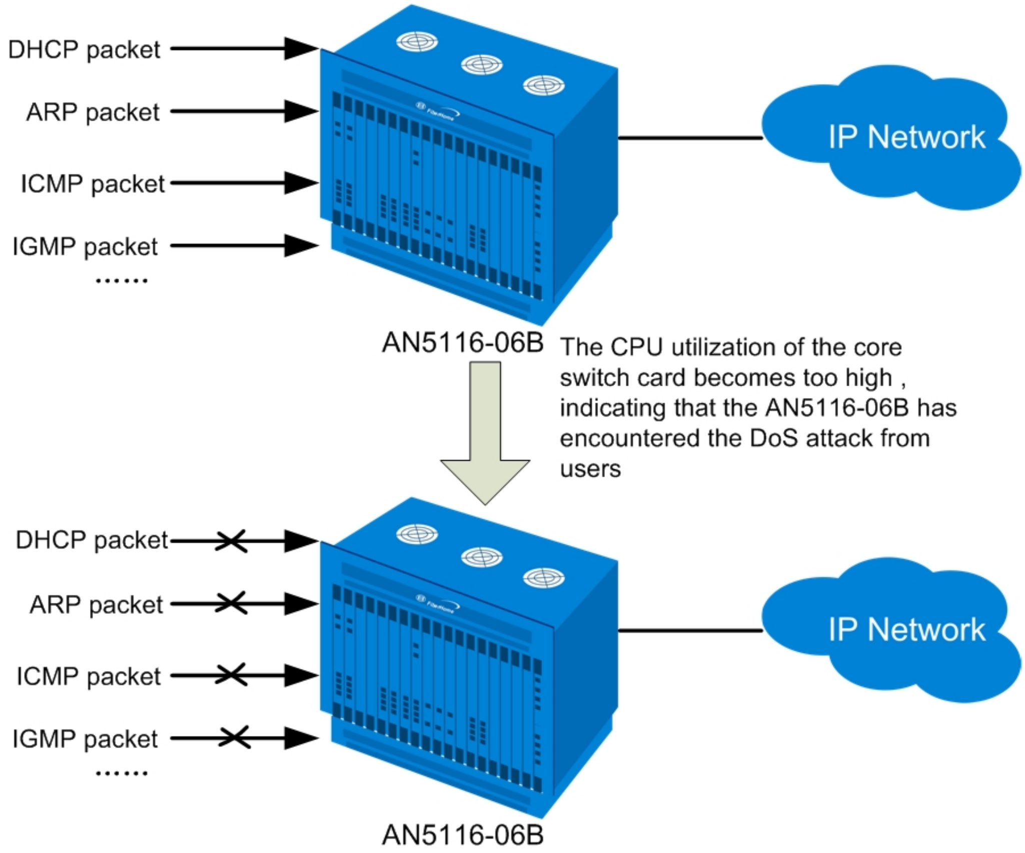


Figure 14-1 The working principle of the anti-DoS attack

14.1.5 Reference Information

Reference standard

None.

Terminology

None.

Abbreviations

Abbreviations	Meaning
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol

14.2 MAC Address Filtering

14.2.1 Definition

Filters MAC addresses by configuring the QoS profile. Its purpose is to control the source or destination MAC addresses of user packets, and discard the packets from a malicious user .

14.2.2 Features

This feature, which supports configuring the user packets without the source MAC address or destination MAC address, is mainly to prevent the carriers' networks from being attacked by a malicious user who forges the legal MAC address.

14.2.3 Specifications

- Supports binding / unbinding with the QoS profile, so as to filter the uplink packets based on the source or destination MAC address.
- The maximum number of the MAC addresses that can be filtered is 2000.

14.2.4 Basic Principles

The principles to implement the MAC address filtering function are described as follows.

- In the uplink direction:

  1) To prevent a user from forging the MAC address of the network side equipment, the system sets the MAC address of the network side equipment as the source MAC address to be filtered in the QoS profile, and binds this profile with the card in the corresponding slot.

  2) When a user packet from this slot is transferred in the uplink direction, the AN5116-06B will check the source MAC address of this packet; if the source MAC address is the same as a certain MAC address to be filtered configured in the QoS profile, the AN5116-06B will discard this packet.

- In the downlink direction:

  1) To avoid the packet attack from the network side equipment, the system sets the MAC address of the network side equipment as the source MAC address to be filtered in the QoS profile, and binds this profile with the corresponding uplink port.

  2) When a packet is transferred to this uplink port in the downlink direction, the AN5116-06B will check the source MAC address of this packet; if the source MAC address is the same as a certain MAC address to be filtered configured in the QoS profile, the AN5116-06B will discard this packet.

14.2.5 Reference Information

Reference standard

None.

Terminology

None.

Abbreviations

Abbreviations	**Meaning**
MAC	Medium Access Control
QoS	Quality of Service

14.3 Packet Suppression

14.3.1 Definition

The AN5116-06B supports compressing the excessive and illegal data packet, so as to ensure the system and user security.

Since the group network is out of control, if users send excessive multicast data packets and unknown data packets no matter the packets are legal or not, the equipment resource will be greatly consumed. This may lead to the performance degradation or even system crash.

14.3.2 Features

14.3.3 Specifications

- Excessive multicast packets.
- Excessive unknown packets.

14.3.4 Basic Principles

In the uplink direction, the equipment performance will be degraded or the service will even be stopped if malicious users send excessive multicast and broadcast data packets, no matter the packets are legal or not, which consumes massive system resource.

In the downlink direction, the AN5116-06B is within the controllable network. However it may send excessive data packet because of the network complexity, which need to be compressed.

The processing methods for the excessive multicast and unknown data packets are as follows:

- Match the data packet features of specified type: specified multicast and unknown data packet.
- Get the statistics of the transmission ratio of the specified data packets.

- Discard the data packets if the transmission ratio exceeds the pre-defined ratio.

14.3.5 Reference Information

Reference standard

None.

Terminology

None.

Abbreviations

Abbreviations	Meaning
DOS	Deny of Service

15 User Security

- ☑ Anti MAC Spoofing
- ☑ Data Encryption of an EPON User
- ☑ Data Encryption of a GPON User

15.1 Anti MAC Spoofing

15.1.1 Definition

MAC spoofing means that the malicious users forge the MAC addresses and attack the network by transmitting packets. Malicious users can forge the MAC addresses of common users to damage the services of these users. Malicious users can also transmit a large number of forged packets that contain different MAC addresses to the system, which affects the normal operation of the system or even causes the system crash.

15.1.2 Features

- Increases the security of the operator network.
- Increases the security of the user services.

15.1.3 Specifications

Supports obtaining the binding relationship between the source MAC address and the user port during the PPPoE accessing process.

15.1.4 Basic Principles

The AN5116-06B monitors the PPPoE accessing flow. During the process of a PPPoE user accessing, the AN5116-06B obtains the binding relationship between the source MAC address and the user port. If other ONU ports forge this MAC address to send packets to the AN5116-06B, the AN5116-06B will prevent these ports from doing so.

15.1.5 Reference Information

Reference standard

None.

Terminology

None.

Abbreviations

Abbreviations	Meaning
MAC	Media Access Control
PPPoE	Point to Point Protocol over Ethernet

15.2 Data Encryption of an EPON User

15.2.1 Definition

In the downlink direction, an EPON system uses the broadcast mode, and malicious users can easily obtain the information of other users in the system. So the EPON system uses the AES to perform the encryption of the user data. The AES is a block password algorithm, and is operated based on the 16-byte (128-bit) data block. The AN5116-06B uses the AES128 encryption algorithm, adopting the 128-bit key.

Note:

Currently only partial ONUs support the triple churning encryption.

15.2.2 Features

Increases the security of the EPON user data.

15.2.3 Specifications

Supports the encryption function based on each LLID.

15.2.4 Basic Principles

AES encryption

The AES algorithm uses the symmetric packet password mechanism, the shortest key length is 128 / 192 / 256 bits, and the packet length is 128 bits; the algorithm should be easy to perform by various hardware and software types. For the iteration symmetric packet encryption algorithm with variable-length key, its encryption and decryption uses the same key, and the key exchange is initiated by the AN5116-06B. Before an ONU accesses the network, the AN5116-06B and the ONU can pre-configure an SSK as the key seed for the data encryption of downlink users. As soon as the key seed is configured and the ONU is started, the AN5116-06B can initiate the key exchange and modification flow as required.

Triple churning

The triple churning algorithm adds the time domain association of the churned data base on the single churning algorithm, so as to increase the security of the user data.

The triple churning uses three concatenated churners. Each churner performs the single churning operation, and each churning uses a different key. The level 1 churning of the triple churning uses the primal 24-bit key (X1 to X8, P1 to P16), the level 2 churning uses the key (P9 to P16, X1 to X8, P1 to P8) generated by rotating the primal 24-bit key to the right by 8 places, the level 3 churning uses the key (P1 to P16, X1 to X8) generated by rotating the primal 24-bit key to the right by 16 places.

15.2.5 Reference Information

Reference standard

None.

Terminology

None.

Abbreviations

Abbreviations	Meaning
AES	Advanced Encryption Standard
EPON	Ethernet Passive Optical Network
LLID	Logical Link Identifier
OAM	Operation, Administration and Maintenance
OAMPDU	OAM Protocol Data Unit
ONU	Optical Network Unit
SSK	Share Secrect Key

15.3 Data Encryption of a GPON User

15.3.1 Definition

The GPON system uses the AES to perform the encryption of the user data. The AES is a block password algorithm, and is operated based on the 16-byte (128-bit) data block. The AN5116-06B uses the AES128 encryption algorithm, adopting the 128-bit key.

15.3.2 Features

Increases the security of the GPON user data.

15.3.3 Specifications

Supports the encryption function based on the GEM port.

15.3.4 Basic Principles

Encryption algorithm

The AES algorithm generates a 16-byte pseudorandom code block flow, called the AES cipher block or key. The AES cipher block performs the exclusive OR (XOR) operation operation with the input plain text to output the cipher text, and the cipher text performs the XOR operation with the same AES cipher block to generate the plain text again.

For a GEM segment, the encryption algorithm only encrypts its payload, but does not encrypt its Port_ID frame header. The AES cipher block is arranged at the starting position of the packet payload. Because a GEM segment is not always the integral times of an AES cipher block, the data block trailer whose length is less than 16 bytes performs the XOR operation with the most significant bit of the AES cipher block trailer. And the redundant parts of the AES cipher block trailer are discarded.

Key exchange

The AN5116-06B initiates the key exchange. Before an ONU accesses the network, the AN5116-06B and the ONU can pre-configure an SSK as the key seed for the data encryption of downlink users. As soon as the key seed is configured and the ONU is started, the AN5116-06B can initiate the key exchange and modification flow as required. The detailed flow is described as follows:

1. The AN5116-06B sends a key modification request via the Request Key Message broadcast or unicast in the downlink PLOAM channel.
2. After receiving the key update request, the ONU generates a 128-bit-long random number RAND (its length should be the same as the key length).
3. The ONU sends the RAND to the AN5116-06B via the uplink PLOAM message (Encryption Key Message). To ensure the redundancy, the ONU sends for three times repeatedly.
4. Ensures that the AN5116-06B can receive the same RAND for three times repeatedly.
5. The ONU calculates the key using the formula Key = f (SSK, RAND).

6. After receiving the RAND, the AN5116-06B also calculates the key using the formula Key = f (SSK, RAND).

7. The AN5116-06B selects a certain frame No. as the first frame No. of the new key, and transfers the multiframe No. of this frame to the ONU via the Key_switching_time message. The Key_switching_time message is sent for three times, and the ONU only needs to receive the correct copy for once to know the modification time.

8. The ONU acknowledges its response via the Acknowledge message.

9. The AN5116-06B and the ONU start to use the new key to perform the encryption and decryption of the downlink data.

15.3.5 Reference Information

Reference standard

ITU-T G.984.3：Gigabit-capable Passive Optical Networks (GPON): Transmission convergence layer specification

Terminology

None.

Abbreviations

Abbreviations	Meaning
AES	Advanced Encryption Standard
GEM	GPON Encapsulation Method
GPON	Gigabit Passive Optical Network
PLOAM	Physical Layer OAM
SSK	Share Secrect Key

16 Redundancy backup

☑ Redundancy Backup of the Core Switch Card

☑ Redundancy Backup of the Uplink Port

☑ Redundancy Backup of the PON Port

16.1 Redundancy Backup of the Core Switch Card

16.1.1 Definition

The redundancy backup of the core switch card is described as follows: The AN5116-06B can be configured with two core switch cards (active and standby), so as to implement the 1+1 protection switching of the core switch card.

16.1.2 Features

- Increases the security of the core switch card.
- Ensures the equipment safety and the normal running of services effectively.

16.1.3 Specifications

- Supports the 1+1 protection switching of the core switch card.
- Supports the configuration data synchronization between the active and standby core switch cards.
- Supports the automatic switching and manual switching of the core switch card.
- The switching time of the core switch card is less than 50 ms.

16.1.4 Basic Principles

The AN5116-06B supports the configuration of two core switch cards (active and standby) and the 1+1 protection switching of the core switch card. When the switching of the core switch card occurs, all services are switched to the standby core switch card; the standby core switch card is activated, and it takes over the work of the active one.

Configuration synchronization

The AN5116-06B supports the configuration information real time synchronization function between the active and standby core switch cards. When executing any commands / operations (except for the query operation), the active core switch card sends the command to the standby card, and the standby card performs no configurations of other cards; this can guarantee the real time active / standby switching and avoid influencing services when the active / standby switching is performed.

Active / standby switching module

The active / standby switching module is abbreviated as the HSS module. This module makes the core switch card have a good fault-tolerance feature, and when the system has faults, the card can respond rapidly to reduce the influence on services. It performs the following functions:

- Determines the identity of the active / standby core switch cards. The corresponding operations vary with the identities. The active card not only modifies its own data structure, but also delivers the specific configuration command to the corresponding service card to execute it; the standby card only needs to modify its own data structure, but does not need to configure the service cards.
- Determines the switching time. The switching can be classified into two conditions: the automatic switching and the manual switching. The active / standby switching module should determine the switching time rapidly and accurately, so as to ensure the normal running of the entire system and reduce the influence on services.

Active / standby switching time

When one of the following conditions occurs, the active / standby switching will be performed:

- The active core switch card has faults, including the hardware or software abnormality.
- The active core switch card is unplugged.
- The network management system delivers a forced switching command.

16.1.5 Reference Information

Reference standard

None.

Terminology

None.

Abbreviations

Abbreviations	Meaning
HSS	Hot Standby Switching

16.2 Redundancy Backup of the Uplink Port

16.2.1 Definition

The redundancy backup of the uplink port is described as follows: The AN5116-06B supports setting the master and slave uplink ports as a protection group; depending on the uplink port status, it performs the switching between the master and slave uplink ports, so as to ensure the safety of the uplink line.

16.2.2 Features

- Increases the security of the uplink line.
- Ensures the reliability of the uplink service.

16.2.3 Specifications

- Supports the dual-homed protection function of the uplink port.
- When the active up link is abnormal, the equipment supports switching to the standby up link automatically.

- When the active up link resumes normal state, the equipment supports two working modes: recovering to the active up link automatically and not recovering to the active up link automatically.
- The uplink port protection switching time is less than 50 ms.
- Supports the card protection of the uplink card. When users set the card protection of the uplink card, the uplink cards must be of the same type, and the master / slave uplink port protection groups should be established in turn according to the port sequence.
- Supports the port protection of the uplink card. When users set the port protection of the uplink card, the two uplink ports forming the protection group can be located at either one uplink card or two uplink cards. The uplink card types can be either the same or different, but the uplink port types must be the same.

16.2.4 Basic Principles

Network of the master and slave up links

The AN5116-06B supports the dual-homed protection of the uplink port. This is described as follows: Two AN5116-06B up links are connected to two uplink equipment sets respectively; when the AN5116-06B detects that one active up link is abnormal, services are switched to another standby up link.

The connection diagrams of the master and slave up links are shown in Figure 16-1 and Figure 16-2.

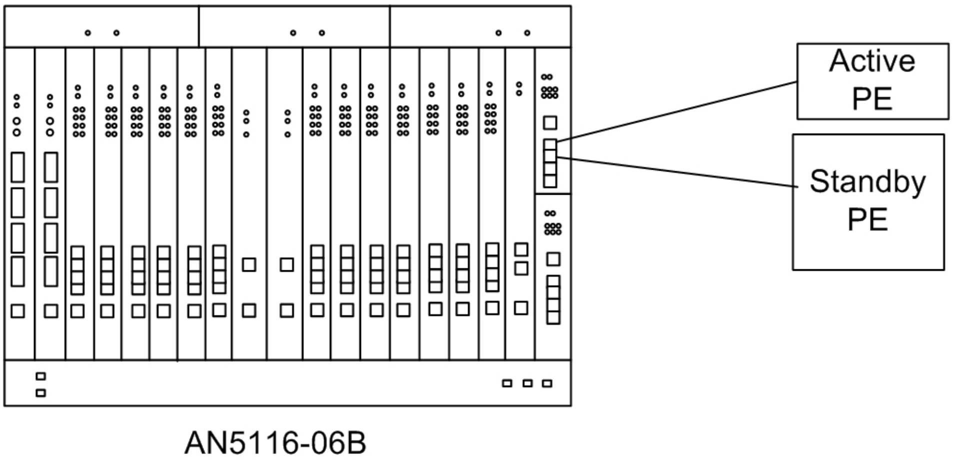


Figure 16-1 The connection of the master and slave up links on the same uplink card

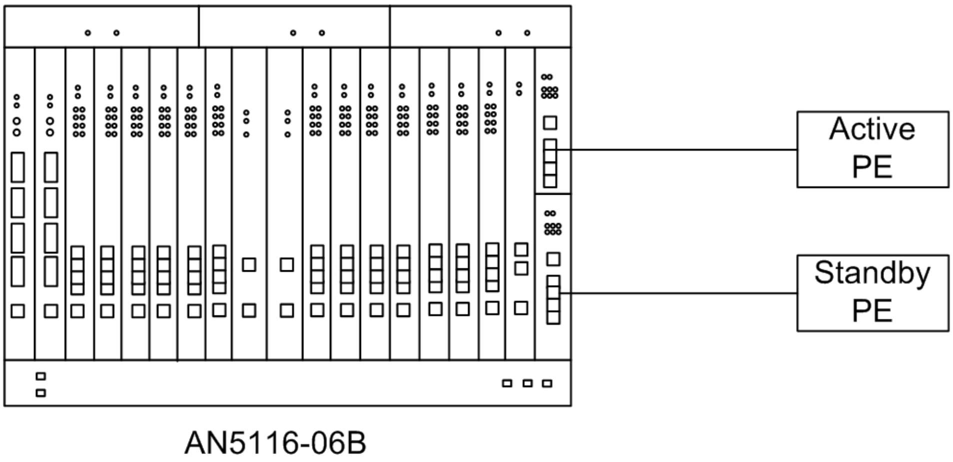


Figure 16-2 The connection of the master and slave up links on different uplink cards

Master and slave ports

One protection group includes the master port and the slave port.

- Master port: It enters the active status (namely the forwarding status) first.
- Slave port: Under normal conditions, it is in the standby status (namely the blocking status).

When the link of the master port has faults and the link of the slave port is normal, the links will be switched, and the slave port will enter the active status.

Switching mechanism

When the dual-homed protection is enabled, the master port first enters the forwarding status. The link monitoring module of the uplink card monitors the working conditions of the master port in real time. If the link monitoring module of the uplink card finds that the master port fails, it will generate an interruption on the CPU of the core switch card via the interruption bus of the backplane. Then the software of the core switch card responds to the interruption immediately; this means blocking the master port and setting the slave port to the forwarding status. The configuration information of the master port (including VLAN, Trunk, port priority, port rate, duplex mode, etc.) will be synchronized to the slave port in real time, so as to implement the seamless switching.

After the switching occurs, the equipment continues to detect the status of the master port. When detecting that the master port has resumed normal state, the equipment runs as follows: if it is set as recovering to the master link automatically, the master port will enter the forwarding status, and the slave port will enter the blocking status; if it is set as not recovering to the master link automatically, the current master and slave ports will not change.

The master / slave uplink port switching flow is shown in Figure 16-3. In this figure, the automatically recovering to the master link mode is taken as an example.

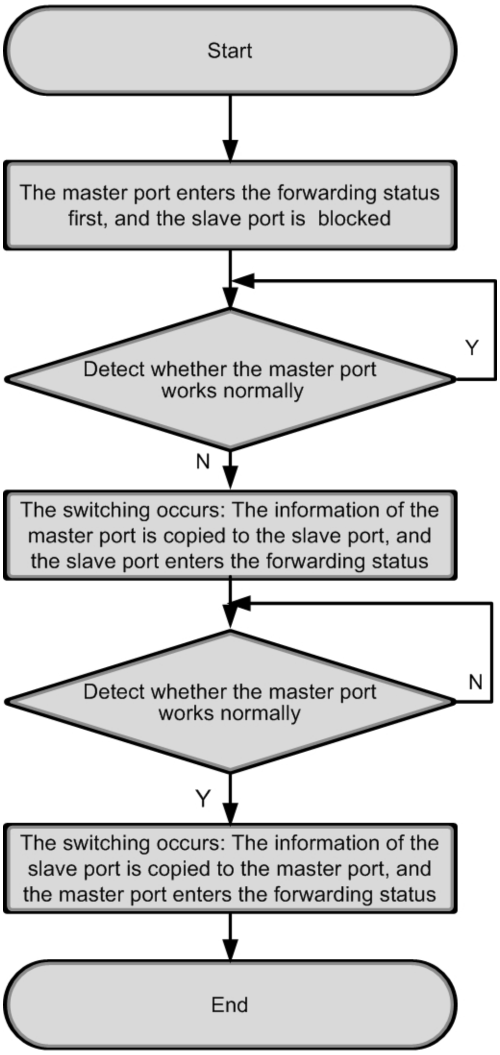

Start
The master port enters the forwarding status first, and the slave port is blocked
Detect whether the master port works normally
Y
N
The switching occurs: The information of the master port is copied to the slave port, and the slave port enters the forwarding status
Detect whether the master port works normally
N
Y
The switching occurs: The information of the slave port is copied to the master port, and the master port enters the forwarding status
End

Figure 16-3 The master / slave uplink port switching flow (recovering to the master link automatically)

16.2.5 Reference Information

Reference standard

None.

Terminology

Terminology	Description
Dual-homed	Means that dual nodes and routes are adopted, and offer redundancy mutually.

Abbreviations

Abbreviations	Meaning
PE	Provider Edge
VLAN	Virtual Local Area Network

16.3 Redundancy Backup of the PON Port

16.3.1 Definition

The redundancy backup of the PON port is described as follows: The AN5116-06B supports setting the master and slave PON ports as a PON port protection group; when the optical circuit has faults, the service data switching can be completed rapidly in the protection group, so as to protect the user services.

16.3.2 Features

- Increases the security of the PON port and the optical fiber line.
- Ensures the reliability of the service.

16.3.3 Specifications

- The equipment supports up to 64 PON port protection groups.
- The equipment supports types B, C, D and hand-in-hand PON port protection.
- Supports both the intra- and inter- interface card PON port protection.

16.3.4 Basic Principles

PON port protection group mode

The AN5116-06B supports types B, C, D and hand-in-hand PON port protection.

- Type B: Provides the redundancy protection for the OLT PON port and the optical fiber between the splitter and the OLT. The AN5116-06B supports the PON port protection on the same PON interface card or between two PON interface cards.
    - OLT: The standby PON port is under the cold standby status; the OLT detects the line status and PON port status, and completes the PON port switching.
    - Splitter: One 2: N splitter is used.
    - ONU: No special requirements exist.

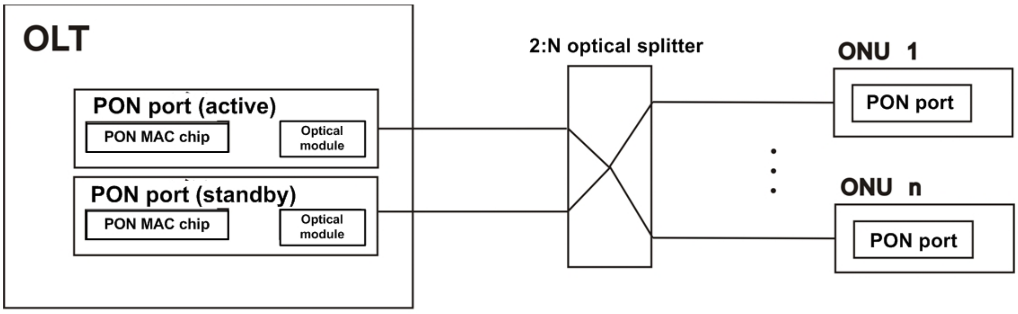


Figure 16-4 Principle of type B of the PON port protection

- Type C: Provides dual OLT PON ports, dual ONU optical modules, dual optical fibers between the splitter and OLT, dual splitters and distribution optical fibers for redundancy protection. The AN5116-06B supports the PON port protection on the same PON interface card or between two PON interface cards.
    - OLT: The active and standby PON ports are both under the working status; the OLT should guarantee that the service information of the active PON port can be backed up to the standby PON port synchronously so that the standby PON port can maintain the service attributes of the ONU in course of protection switching.
    - Splitter: Two 1: N splitters are used.

- ONU: Uses one PON chip and two different optical modules. The standby optical module is under the cold standby status.

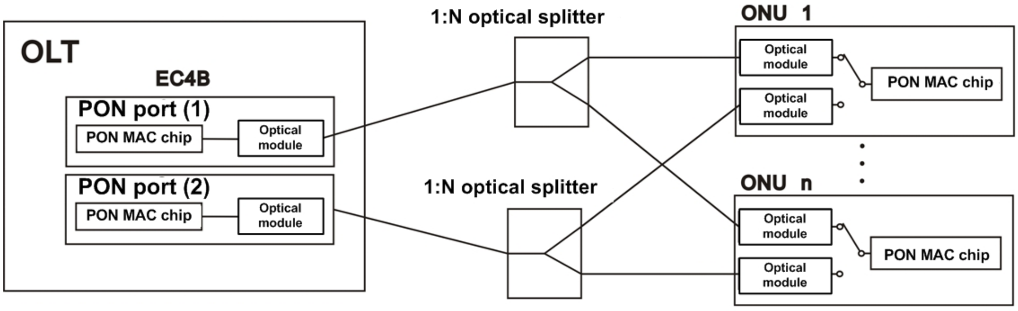


Figure 16-5 Principle of type C of the PON port protection

- Type D: Provides dual OLT PON ports, dual ONU optical modules, dual optical fibers between the splitter and OLT, dual splitters and distribution optical fibers for redundancy protection. The AN5116-06B supports the PON port protection on the same PON interface card or between two PON interface cards.
  - OLT: The active and standby PON ports are both under the working status; the OLT should guarantee that the service information of the active PON port can be backed up to the standby PON port synchronously so that the standby PON port can maintain the service attributes of the ONU in course of protection switching.
  - Splitter: Two 1: N splitters are used.
  - ONU: Uses two PON chips and two different optical modules. The standby optical module is under the hot standby status.

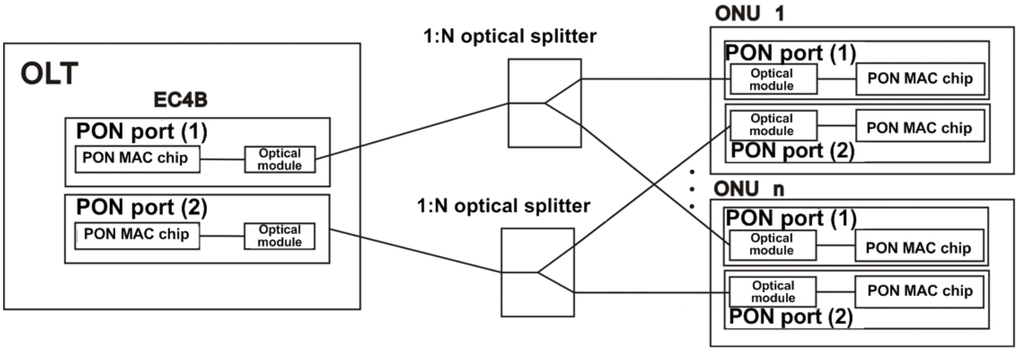


Figure 16-6 Principle of type D of the PON port protection

- Hand in hand protection: The slot numbers and PON port numbers of the PONs protecting each other on two OLTs should be the name. The authorization numbers of two OLTs on one ONU should be the same.

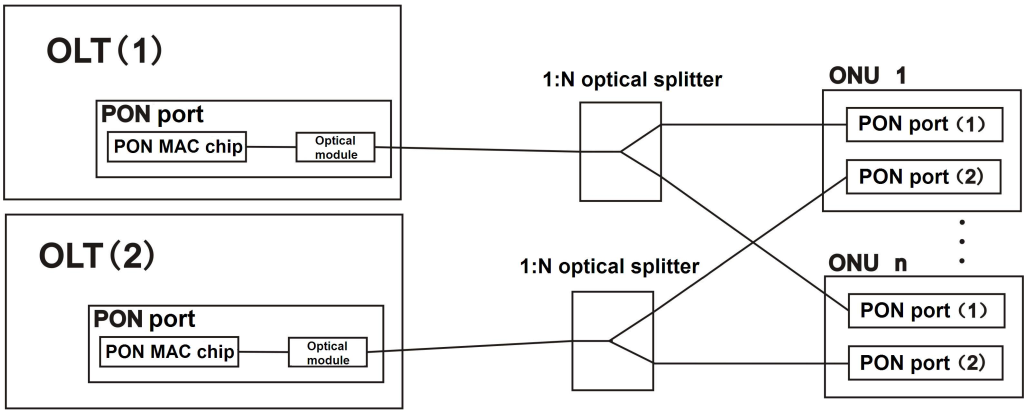


Figure 16-7 Principle of hand in hand PON port protection

Switching trigger conditions

The AN5116-06B PON protection control module monitors the optical modules under the active status; if the optical signals of a certain optical module is interrupted, the line card CPU controls and starts the switching.

16.3.5 Reference Information

Reference standard

- ITU-T G.984.3：Gigabit-capable Passive Optical Networks (GPON): Transmission convergence layer specification
- IEEE 802.3-2005：IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks–Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

Terminology

None.

Abbreviations

Abbreviations	Meaning
CPU	Central Processing Unit
OLT	Optical Line Termination
ONU	Optical Network Unit
PON	Passive Optical Networrk

17 ACL

☑ Definition

☑ Features

☑ Specifications

☑ Basic Principles

☑ Reference Information

17.1 Definition

The access control list (ACL) refers to the feature in which the IP matching rule filters the computers accessing the equipment. Only the specified computers are allowed to access the equipment, so as to ensure the system security.

17.2 Features

The ACL filtering function can increase the system security effectively.

17.3 Specifications

The AN5116-06B supports controlling the computers accessing the equipment according to the IP matchinig rule.

17.4 Basic Principles

Principle diagram

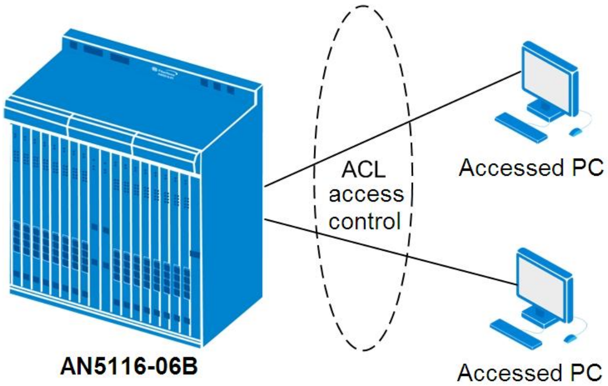


Figure 17-1 ACL function

Working flow

1. The AN5116-06B acquires the IP address and mask of the accessing computer.
2. Match the IP address and the mask of the accessing computer with the IP address in the ACL accessing control IP address list of the AN5116-06B.

3. If the IP address and the mask match the IP address in the ACL accessing control IP address list, the computer can access the AN5116-06B; if not, the access will be denied.

17.5 Reference Information

Reference standard

IETF RFC 4314：IMAP4 Access Control List (ACL) Extension

Terminology

No

Abbreviations

Abbreviations	**Meaning**
ACL	Access Control List

18 NTP

☑ Definition

☑ Features

☑ Specifications

☑ Basic Principles

☑ Reference Information

18.1 Definition

The Network Time Protocol (NTP) is an application layer protocol in the TCP/IP protocol suite. NTP is used to synchronize the time between the distributed time server and the client. The implementation of NTP is based on IP and UDP. NTP involves the Time Protocol and the ICMP Timestamp Message, with special design on accuracy and robustness.

18.2 Features

The AN5116-06B can implement the time synchronization between the NTP client and the NTP server, working with second-level accuracy.

18.3 Specifications

Supports the selection of clock modes.

18.4 Basic Principles

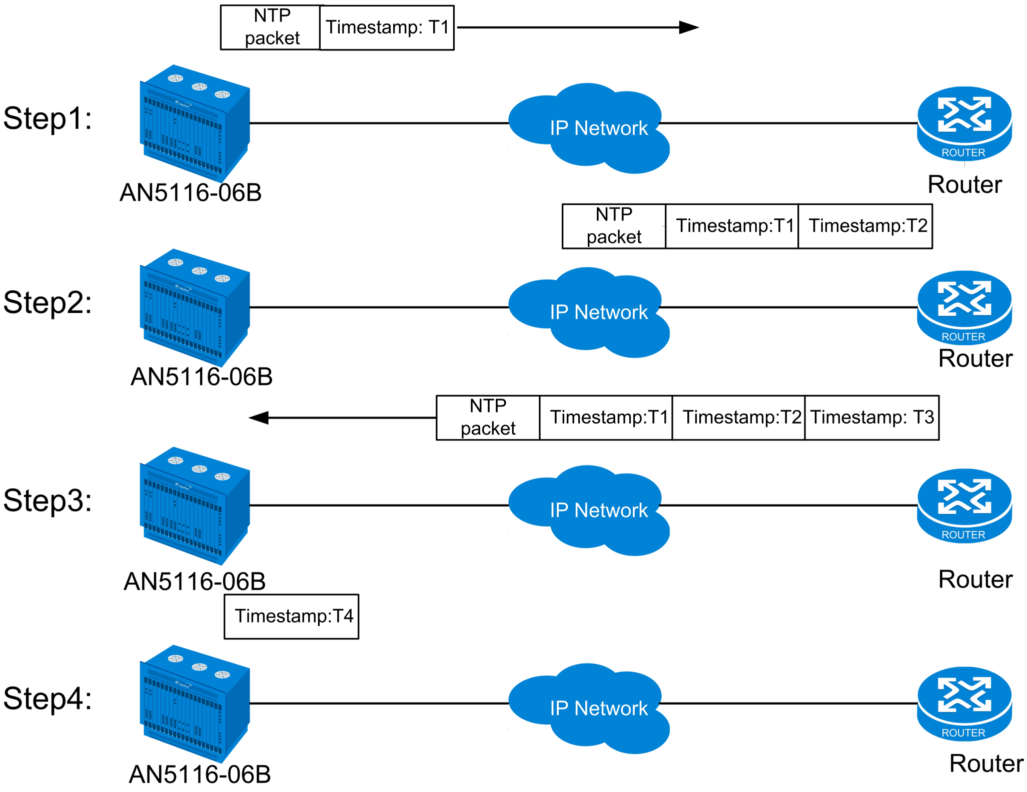


Figure 18-1 The principle of the NTP function

As the NTP client, the AN5116-06B keeps to the following working flow:

1. The AN5116-06B sends an NTP packet to the router. This packet contains the timestamp T1 when it leaves the AN5116-06B.

2. When the NTP packet arrives at the router, the router adds its timestamp T1 to the packet. Assume that the timestamp is T2.

3. When the NTP packet leaves the router, the router adds another timestamp to the packet. Assume that the timestamp is T3.

4. When the AN5116-06B receives the response packet, it adds a new timestamp to the packet. Assume that the timestamp is T4.

5. The AN5116-06B works out the transmission delay (DELAY) and clock offset (OFFSET) between the AN5116-06B and the router. In this way, the AN5116-06B can set its clock according to the information and thus keeps its clock synchronized with that of the router (the router acts as the NTP server).

6. DELAY=(T4-T1)–(T3-T2)
7. OFFSET=[(T2-T1)+(T3-T4)]/2

18.5 Reference Information

Reference standard

IETF RFC 1305：Network Time Protocol(Version 3) Specification, Implementation

Terminology

Terminology	Description
Timestamp	The timestamp means the number of seconds from 00:00:00 (GMT), January 1st, 1970. It is the base for the NTP to implement the clock synchronization.
The number of a layer	The number of a layer means the network layer number of an NTP server in the NTP protocol. The clock whose layer number is 0 has the highest accuracy, the NTP server whose layer number is 1 synchronizes with the NTP server whose layer number is 0, the NTP server whose layer number is 2 synchronizes with the NTP server whose layer number is 2. The accuracy of the clock decreases from 0 to 14.

Abbreviations

Abbreviations	Meaning
NTP	Network Time Protocol

Product Documentation Customer Satisfaction Survery

Thank you for reading and using the product documentation provided by FiberHome. Please take a moment to complete this survey. Your answers will help us to improve the documentation and better suit your needs. Your responses will be confidential and given serious consideration. The personal information requested is used for no other purposes than to respond to your feedback.

Name	
Phone Number	
Email Address	
Company	

To help us better understand your needs, please focus your answers on a single documentation or a complete documentation set.

Documentation Name	
Code and Version	

Usage of the product documentation:

1. How often do you use the documentation?

☐ Frequently ☐ Rarely ☐ Never ☐ Other (please specify) ____________________

2. When do you use the documentation?

☐ in starting up a project ☐ in installing the product ☐ in daily maintenance ☐ in trouble shooting ☐ Other (please specify) ____________________

3. What is the percentage of the operations on the product for which you can get instruction from the documentation?

☐ 100% ☐ 80% ☐ 50% ☐ 0% ☐ Other (please specify) ____________________

4. Are you satisfied with the promptness with which we update the documentation?

☐ Satisfied ☐ Unsatisfied (your advice) ____________________

5. Which documentation form do you prefer?

☐ Print edition ☐ Electronic edition ☐ Other (please specify) ____________________

Quality of the product documentation:

1. Is the information organized and presented clearly?

☐ Very ☐ Somewhat ☐ Not at all (your advice) ____________________

2. How do you like the language style of the documentation?

☐ Good ☐ Normal ☐ Poor (please specify) ____________________

3. Are any contents in the documentation inconsistent with the product?

____

4. Is the information complete in the documentation?

□ Yes

□ No (Please specify) ______________________________

5. Are the product working principles and the relevant technologies covered in the documentation sufficient for you to get known and use the product?

□ Yes

□ No (Please specify) ______________________________

6. Can you successfully implement a task following the operation steps given in the documentation?

□ Yes (Please give an example) ______________________________

□ No (Please specify the reason) ______________________________

7. Which parts of the documentation are you satisfied with?

____

8. Which parts of the documentation are you unsatisfied with?Why?

____

9. What is your opinion on the Figures in the documentation?

□ Beautiful □ Unbeautiful (your advice) ______________________________

□ Practical □ Unpractical (your advice) ______________________________

10. What is your opinion on the layout of the documentation?

□ Beautiful □ Unbeautiful (your advice) ______________________________

11. Thinking of the documentations you have ever read offered by other companies, how would you compare our documentation to them?

Product documentations from other companies:______________________________

Satisfied (please specify) ______________________________

Unsatisfied (please specify) ______________________________

12. Additional comments about our documentation or suggestions on how we can improve:

____

____

Thank you for your assistance. Please fax or send the completed survey to us at the contact information included in the documentation. If you have any questions or concerns about this survey please email at edit@fiberhome.com.cn