AN5116-06B

Optical Line Terminal Equipment

Troubleshooting Guide

Version: A

Code: MN000001059

FiberHome Telecommunication Technologies Co., Ltd.

February 2012

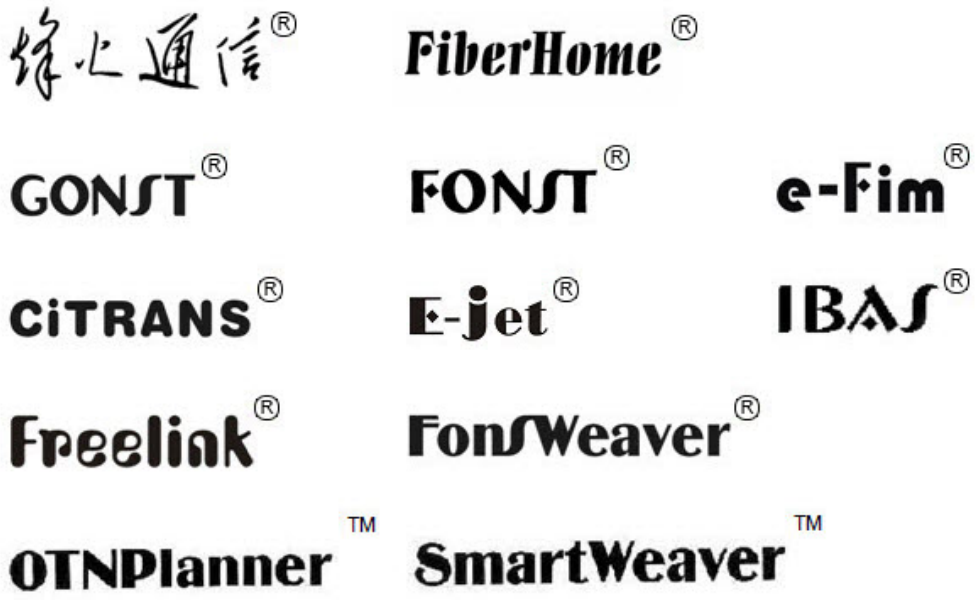
Thank you for choosing our products.

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



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 power-on 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 start-up 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 start-up 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 and Event Reference	Introduces the AN5116-06B's alarm / event information, including alarm/ event names, alarm / event levels, possible causes, 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	This manual corresponds to the AN5116-06B V3.1. Initial version

Intended Readers

This manual is intended for the following readers:

- Operation and maintenance engineers

To utilize this manual, these prerequisite skills are necessary:

- EPON technology
- Data communication technology
- Optical fiber communication technology
- Ethernet technology
- VoIP technology
- Multicast technology

Conventions

Terminology Conventions

Terminology	Convention
AN5116-06B	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	Convention	Description
	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 Overview

This chapter introduces the background knowledge about troubleshooting.

- ☑ Safety Precautions
- ☑ Requirements for Maintenance Engineers
- ☑ List of Tools and Instruments
- ☑ Principles for Troubleshooting
- ☑ General Flow of Troubleshooting
- ☑ How to Obtain Technical Support

1.1 Safety Precautions

Before troubleshooting the equipment, operators should acquaint themselves with the safety precautions for this equipment so as to ensure both human body and equipment safety.

The safety precautions cover the following aspects:

- Safety and warning symbols
- ESD protection measures
- Plugging / unplugging a card
- Precautions for operation on optical fiber and optical interface
- Electrical safety
- Safety rules for the ANM2000

1.1.1 Safety and Warning Symbols

The maintenance and commissioning staff should be familiar with the safety and warning symbols on the AN5116-06B. Location and meanings of these symbols are shown in Table 1-1.

Table 1-1 Safety and warning symbols

Symbol	Meaning	Location
	The ESD protection symbol. This symbol reminds the maintenance staff to wear the ESD protection wrist strap during the operation, so as to prevent possible damage on the equipment caused by the electrostatic discharge.	As illustrated in Figure 1-1.
	The subrack earth ground symbol. This symbol marks the location of the subrack earth ground.	

Table 1-1 Safety and warning symbols (Continued)

Symbol	Meaning	Location
	The laser class symbol. This symbol marks the optical source class of the optical interface on the card. You must prevent the optical source from entering the eyes directly to avoid bodily harm.	Located on the panel of the card that has optical interfaces.
	The Cleaning Periodically symbol, reminding the maintenance staff to clean the anti-dust screen periodically.	Located on the panel of the subrack anti-dust screen.
	The fan alarming symbol, reminding the maintenance staff not to touch the running fan blades.	Located on the panel of the fan unit.

The figure below indicates the location of the ESD protection symbol and the subrack earth ground symbol on a subrack.

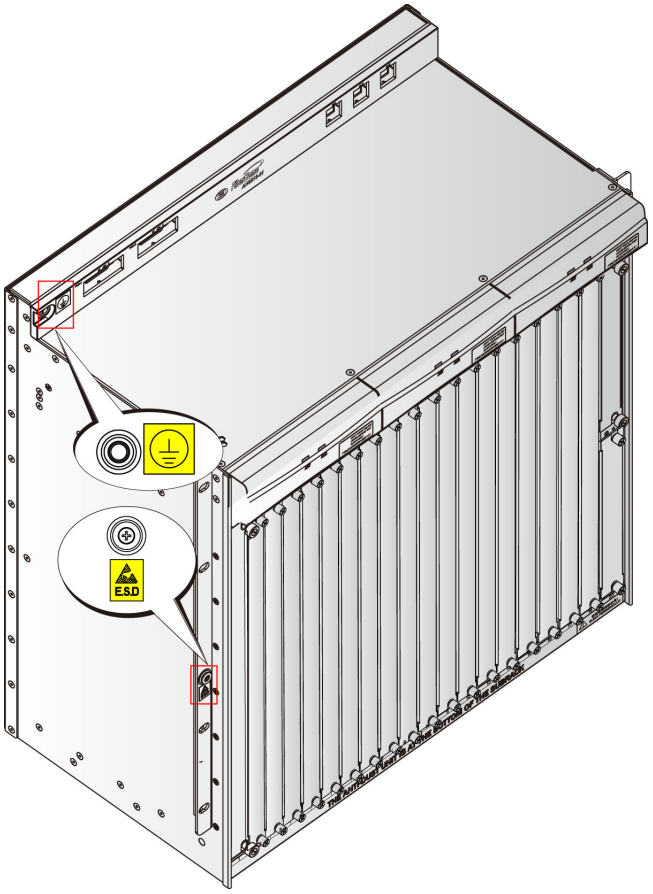


Figure 1-1 Position of the ESD protection ground fastener and subrack earth ground pole

1.1.2 ESD Protection Measures

The electrostatic discharge may damage electrostatic-sensitive components on the cards and subracks. Therefore, keep in mind that wear an ESD protection wrist strap before touching the equipment, card, or IC (Integrated Circuit) chip and use the ESD protection bags to store and transport cards.

The ESD protection wrist strap is provided as an attachment to the equipment. To wear an ESD protection wrist strap, put one end on your wrist with the metal fastener on it in close contact with the skin, and fasten the other end on the ESD protection earth ground fastener of the subrack or cabinet. Figure 1-2 illustrates how to wear an ESD protection wrist strap properly.

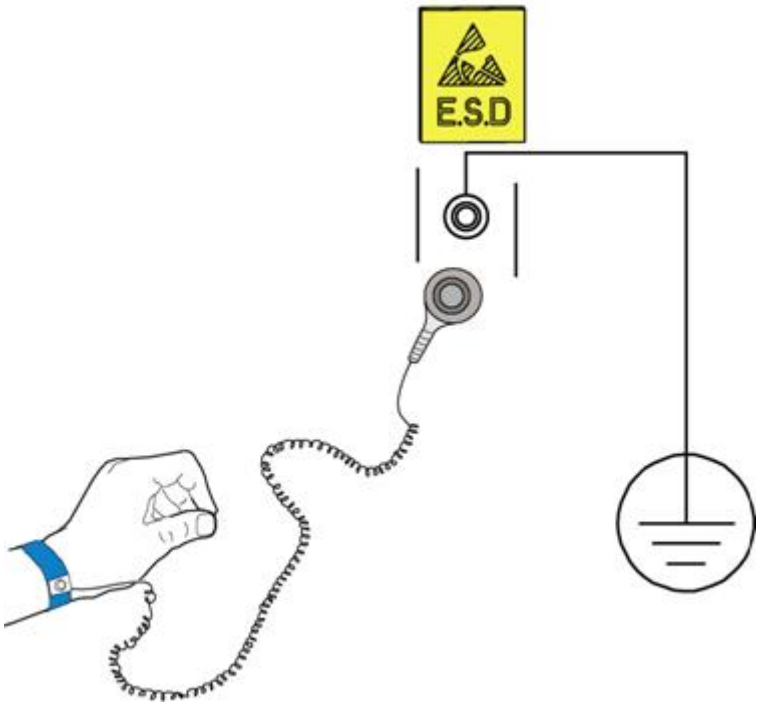


Figure 1-2 Wearing the ESD protection wrist strap

1.1.3 Plugging / Unplugging a Card

- Before plugging / unplugging a card, you need to wear ESD protection gloves or an ESD protection wrist strap, and keep your hands dry and clean.
- When holding a card, do not touch the components and wiring troughs on it.
- Before inserting a card, make sure that
  - The slot to contain this card is available.
  - The card is not connected with wires, cables or optical fibers.
  - The card is to be inserted in the right direction (do not have the card upside down), as illustrated in Figure 1-3.
- When inserting a card, make sure that
  - Operate gently to avoid distorting pins on the subrack backplane.
  - Align the edges of the card with the slide rails of the corresponding slot, and avoid contact of elements and components on the card, which may cause shorting. Figure 1-3 illustrates how to install a card.

- Before unplugging a card, make sure that the card is not carrying a service. Unplugging a card carrying services may cause service interruption.

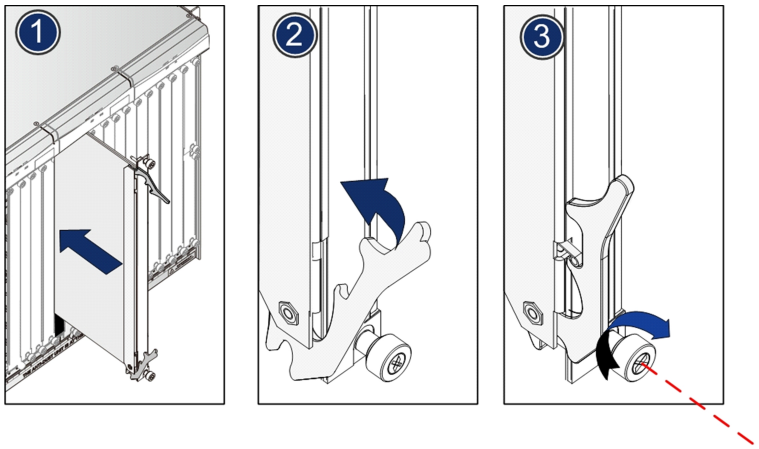


Figure 1-3 Installing a card

1.1.4 Precautions for Operation on Optical Fiber and Optical Interface

Improper operations on optical fibers or optical fiber connectors may cause hurt to hum body. This section introduces precautions in connecting optical fibers and cleaning optical fiber connectors.

Using dedicated fiber puller

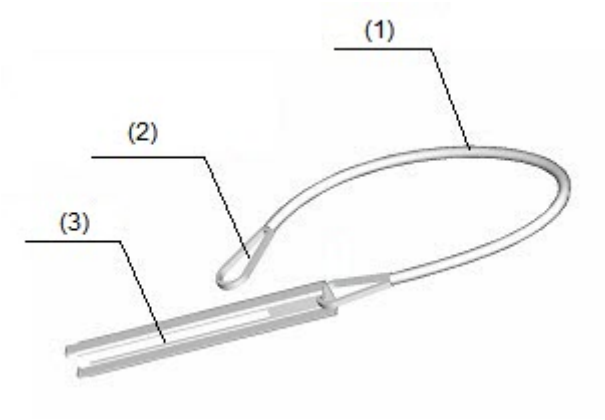
The optical fibers are liable to be damaged when plugged or unplugged by hands without use of a proper tool. Use the dedicated fiber puller to plug or unplug optical fibers to avoid damage.

Caution:

Please use the fiber puller which is provided with the equipment.

The fiber puller, as the delivery accessory, is similar to tweezers in appearance and attached with a spring cord, as shown in Figure 1-4.

The fiber puller is secured on the cabinet with the spring cord before delivery. By clipping the fiber connector with the fiber puller, you can plug or unplug the fiber very conveniently.



(1) Spring cord

(2) Attached to the mounting hole in the vertical mounting flange of the cabinet

(3) Fiber puller

Figure 1-4 Dedicated fiber puller

Protecting optical modules against high optical power

If the output power of the pigtail is unknown, you should not plug it directly into the optical interface of a card. To prevent the optical modules from being damaged by high optical power, you can just put the pigtail in the card's optical interface without connecting them or add an attenuator.

Connecting optical fibers

- Check the optical power to make sure it meets the requirement before connecting optical fibers. Refer to *AN5116-06B Optical Line Terminal Equipment Product Description* for optical power specifications of the equipment.
- Check whether the optical fiber connector matches the optical interface before connecting optical fibers. If not, use an adapter.

Protecting eyes

Prevent laser radiation from injuring the eyes. Looking directly into the optical output interface or the end surface of the pigtail connected to it will hurt your eyes.

Never bending a fiber excessively

Excessive bends or pressure on pigtails will affect the optical power. If bends are necessary, the fiber bending radius should never be less than 38mm.

Protecting optical interface and optical connector

- The unused optical interfaces and the optical connectors on pigtails should be covered with anti-dust caps, so as to protect the human eyes from being injured by looking directly into the optical interfaces or connectors, as well as to protect the optical interfaces or connectors against dust or other contamination.
- Cover the optical interfaces of the replaced card with anti-dust caps in a timely manner and keep them clean.

Cleaning

When cleaning the fiber connectors, you should use the dedicated cleaning tools and materials.

The following introduces the tools and materials available for choice.

- Dedicated cleaning solvent (the first choice is the isoamyl alcohol, followed by the propyl alcohol)
- Non-woven lens tissue
- Dedicated compressed air
- Cotton swab (cotton for medical purposes or other long-staple cotton)
- Dedicated cleaning tape

1.1.5 Electrical Safety

This section introduces the electrical safety precautions for maintenance engineers in their routine maintenance of the equipment, in order to avoid electrical accidents such as shorting and bad grounding.

Shorting

- When a shorting occurs, the excessive current surge may damage the equipment and leave potential silent failures.

- When operating the equipment, prevent conductors (such as metal filings and water) from dropping into the powered equipment, which may cause damages on the electrical equipment and components.
- Avoid the shorting caused by negligence or incorrect cable connection.
- Avoid the shorting caused by small animals entering the powered equipment.

Grounding

- Confirm that the equipment room is well-grounded.
- Confirm that the equipment is well-grounded.

Equipment power supply

- Before removing the power cable, confirm that the power supply is disconnected.
- The power cable should not be exposed. The exposed part should be wrapped with insulating tape.
- If the operation condition permits, shut down the power first and then perform other operations.

1.1.6 Safety Rules for the ANM2000

Safety rules for operations on the ANM2000 are as follows:

- The network management computer should be placed away from direct sunlight, electromagnetic interference, heat source, humidity and dust, and with at least 8cm distance from other objects in order to keep good ventilation.
- Use UPS power supply to avoid loss of network management data caused by accidental power failure.
- The computer case, UPS power supply and switch (or hub) should be connected to protection earth ground.
- To shut down the network management computer, first exit the operation system normally and then shut off the power supply.

- Do not exit the network management system when it is working normally. Exiting the network management system does not interrupt traffic in the network, but precludes centralized control of the networked equipment.
- The network management computer cannot be used for purposes other than network management. Use of unidentified memory devices should be prohibited so as to avoid computer viruses.
- Do not delete any file in the network management system randomly or copy any irrelevant file into the network management computer.
- Do not visit Internet via the network management computer. Doing so may increase data flow in the net card and hence affects normal network management data transmission or results in other accidents.

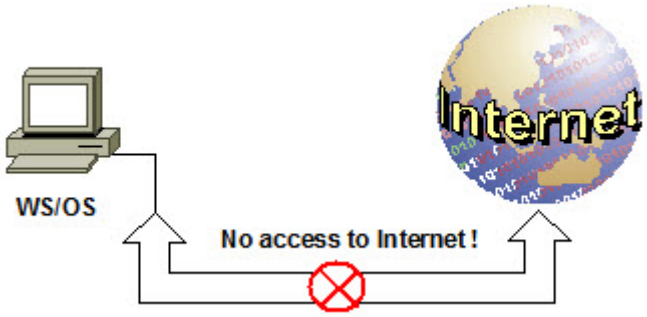


Figure 1-5 No access to Internet

- Do not perform service configuration or expansion during service busy hours via the network management system.
- Do not modify the network management computer's protocol settings, computer name or LAN settings. Doing so may result in abnormal operation of network management system.

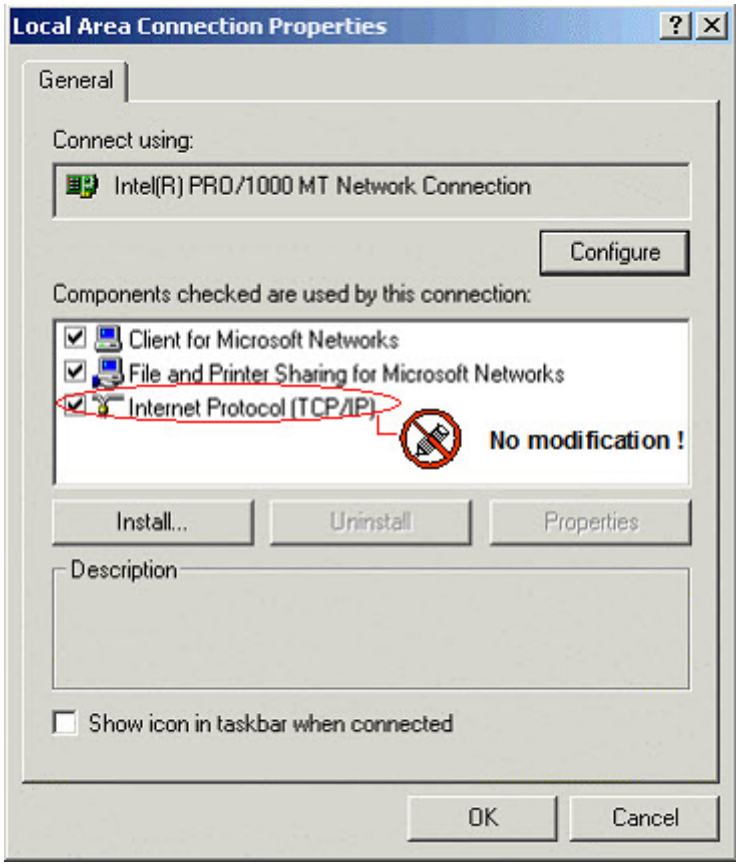


Figure 1-6 Do not modify protocol settings (1)

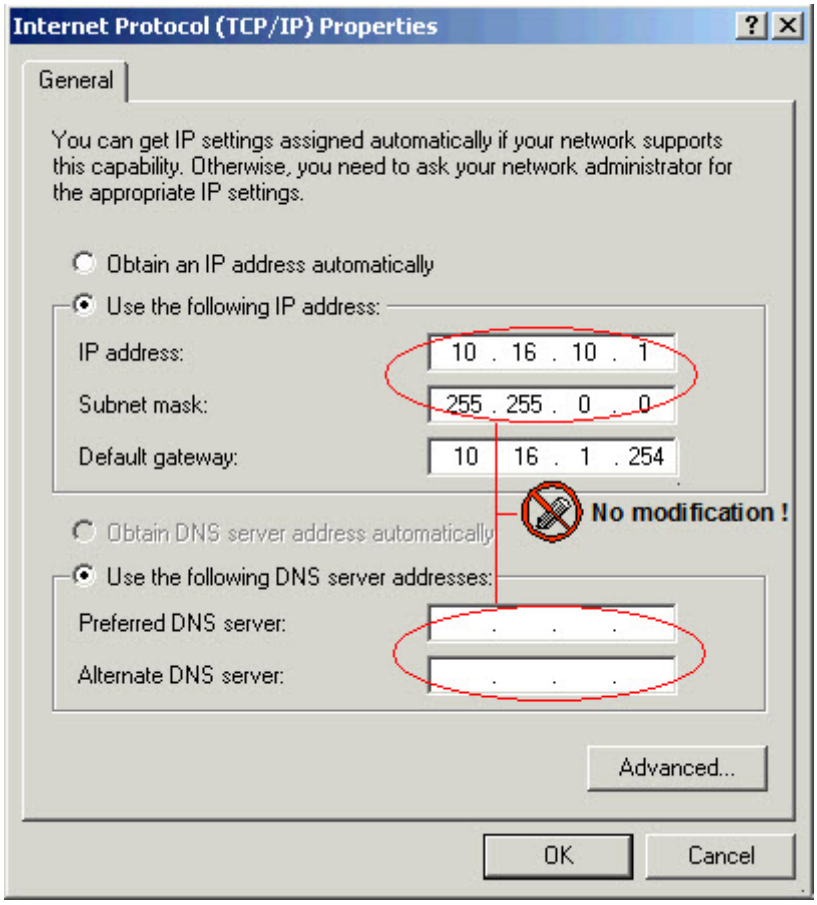


Figure 1-7 Do not modify protocol settings (2)

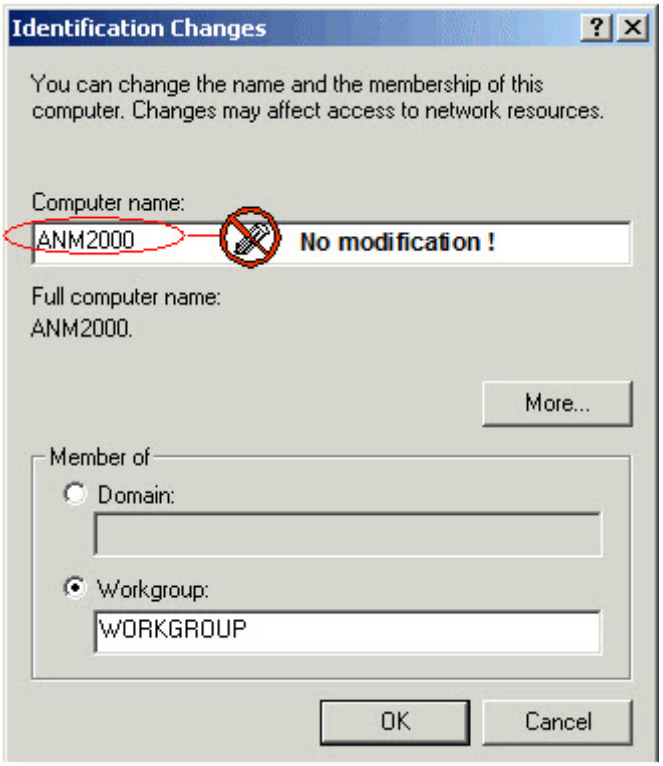


Figure 1-8 Do not modify computer name

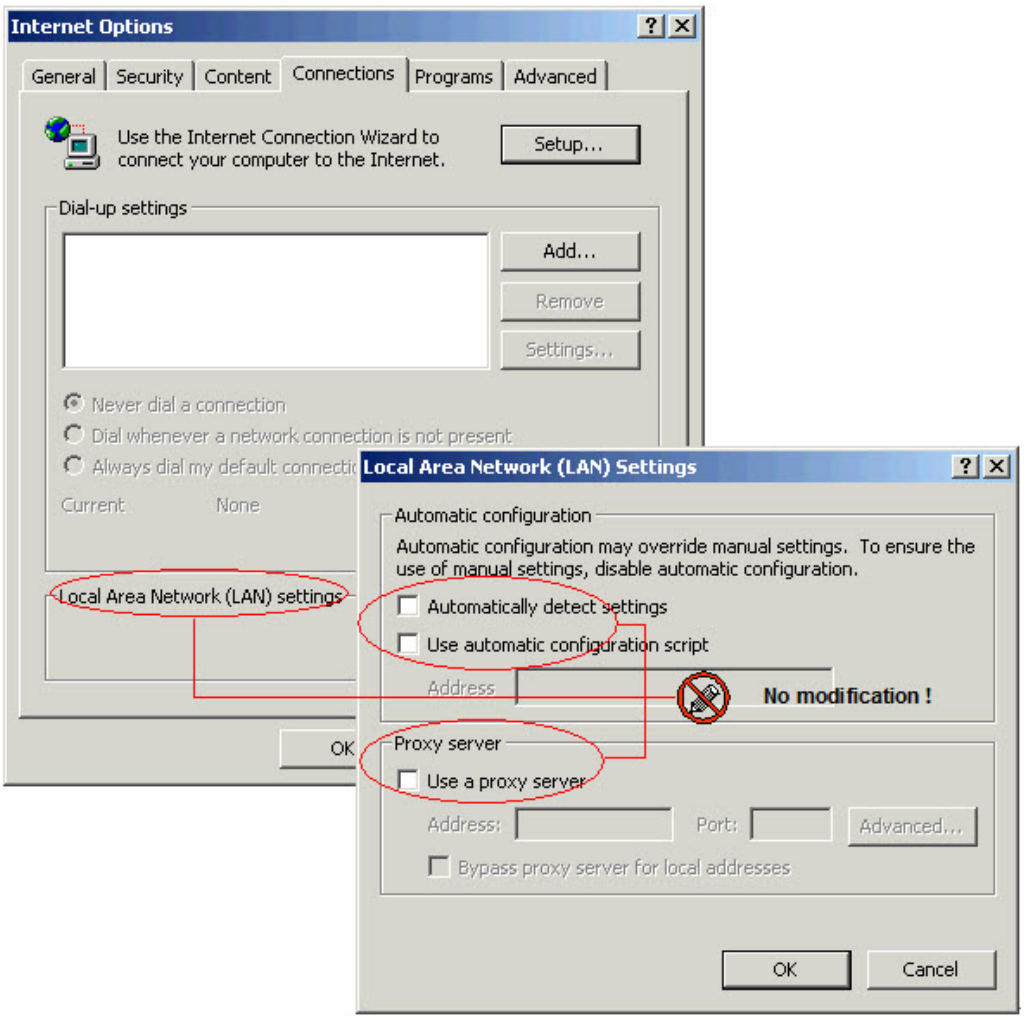


Figure 1-9 Do not modify LAN settings

1.2 Requirements for Maintenance Engineers

This section introduces requirements for maintenance engineers.

1.2.1 Theoretical Knowledge

Maintenance engineers should acquire the following theoretical knowledge:

- Ethernet protocols;
- Protocols relevant to multicast service;

- Theory of voice service;
- Fundamental principles of EPON / GPON technologies;
- MGCP, H.248 and SIP protocols;
- PBX technologies and softswitching technologies.

1.2.2 Network Information of the Project

Maintenance engineers should understand the system composition, service network and configuration data of the equipment, specifically as follows:

- Hardware configuration of the AN5116-06B;
- Functions of each card and interface of the AN5116-06B;
- Networking of the AN5116-06B;
- Physical connection of internal and external cables of the AN5116-06B;
- Network data planning and configuration of the AN5116-06B.

1.2.3 Equipment Operation

Maintenance engineers should be knowledgeable of the following basic operations:

- Basic operations on equipment such as part replacement and cleaning;
- Daily operations on the ANM2000;
- Basic operations on a computer.

1.2.4 Use of Tools and Instruments

The following tools and instruments may be used in troubleshooting the AN5116-06B:

Tool and Instrument	Purpose
Optical power meter	For testing the Rx and Tx optical power, receiving sensitivity, overload optical power, etc. at an optical interface.
Fixed optical attenuator	For attenuating the optical power received; applied in the optical interface at the Rx end to protect the optical interface against damage caused by high optical power.
Variable optical attenuator	For testing the sensitivity and overload optical power of an optical interface.
Pigtail fiber for test	For performing the loopback on an optical interface and measuring the Rx / Tx optical power.
Flange	For adaptive connection of pigtail fibers.
Fiber wiping paper dedicated for WDM device.	For cleaning the ends of optical fiber.
ESD protection wrist strap	For protecting sensitive components on the equipment against electrostatic discharge.
ESD protection bag	For holding replaced cards and other components.
Multimeter	For testing parameters such as ground resistance, input and output voltage of the PDP.
Error detector	For measuring bit error ratio of communication line in data communication and analyzing causes of line failures.
Network cable tester	For testing the connectivity of network cables.

1.2.5 Collecting and Saving Field Data

Collection of field data includes the periodic data collection during normal equipment operation and the data collection when fault occurs.

Maintenance engineers should collect and save the field data before handling faults.

1.3 List of Tools and Instruments

Maintenance engineers should know how to use the following tools and instruments to work on the equipment hardware for troubleshooting:

- Screwdriver
- Stripper
- Diagonal plier

- Network cable plier
- Optical attenuator
- Multimeter
- Optical power meter
- Error detector
- Network cable tester

1.4 Principles for Troubleshooting

You are required to comply with the following principles for troubleshooting:

- Accurately record the fault symptom and collect related information.

  Collect fault information; ascertain possible location and type of the fault by observing the alarms, performance monitoring data, signal tracing and logs on the network management system.

- Consult involved site personnel in fault isolation to collect helpful information for discovering the causes of the fault.

  For example: check whether someone has modified the configuration data, replaced a part, performed a wrong operation or whether there has been a power interruption or lightning strike.

- In the event of a severe and urgent fault, contact FiberHome or its local office for technical support while collecting fault symptoms.

- Strictly follow related rules and flow for hardware operation and data collection in troubleshooting to avoid exacerbating the fault.

1.5 General Flow of Troubleshooting

The general flow of troubleshooting the AN5116-06B is shown in Figure 1-10.

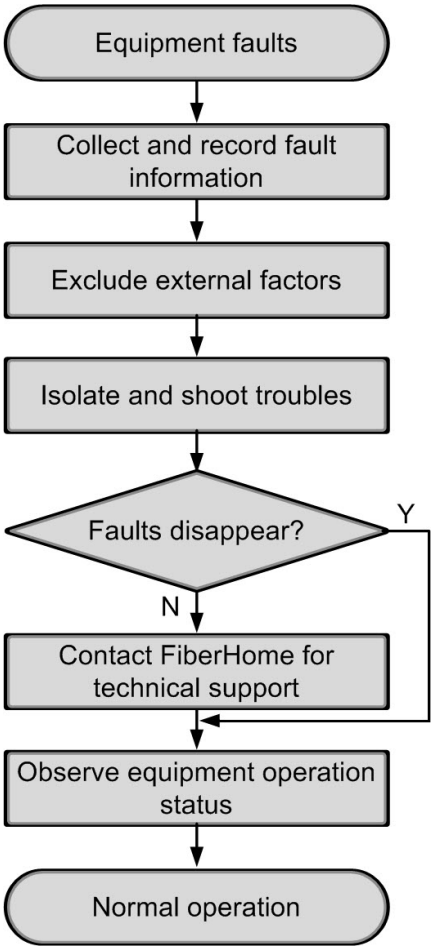


Figure 1-10 General flow of troubleshooting the AN5116-06B

The above flow describes the isolation and troubleshooting of non-urgent faults. For severe and urgent faults, contact Customer Service Department of FiberHome or its local office promptly for technical support. Instructions on how to contact the Customer Service Department are given in **How to Obtain Technical Support**.

1.5.1 Collecting and Recording Fault Information

Collecting and recording fault information is a prerequisite of fault analysis and troubleshooting. Maintenance personnel should collect and record fault information promptly when a fault occurs.

Main sources of fault information:

- Users' fault complaints;
- Faults discovered in routine maintenance;
- Alarms on the network management system.

The process for collecting and recording related fault information is as follows:

1. Record the time when the fault occurred.
2. Record the detailed fault symptoms.
3. Record any ongoing operations when the fault occurred.
4. Record the status of all equipment indicators as well as alarms, logs and performance monitoring statistics on the network management system.
5. Record the version of the network management system for the faulty equipment as well as the software and hardware versions of the equipment's cards.

1.5.2 Excluding External Factors

After collecting and recording detailed fault information, check the peripheral equipment of the AN5116-06B to see whether the fault is arising from the peripheral equipment. If it is caused by the peripheral equipment, notify related maintenance personnel for troubleshooting.

The peripheral equipment may cause failures as follows:

- A fault in the softswitch platform may cause a loss of the AN5116-06B's voice services;
- A fault in the BRAS may cause failure of the AN5116-06B's data services;
- A fault in a peripheral router or switch may cause interruption of all services carried by the AN5116-06B.

The associations between the services provided by the AN5116-06B and main peripheral equipment are shown in Table 1-2.

Table 1-2 Association between the AN5116-06B services and main peripheral equipment

Service Type	Main Peripheral Equipment
IPTV service	IPTV server, router, Ethernet switch, ONU, STB, TV
VoIP service	Softswitch platform, ONU, telephone, router, Ethernet switch
Data service	BRAS, router, Ethernet switch, ONU, HG, PC
TDM service	SDH equipment, E1 equipment (such as base station, E1 Private Line Service device), clock source device, ONU
CATV service	CATV signal source, multiplexer, TV

The process of excluding external factors are as follows:

1. Use routine methods for fault analysis and isolation to determine whether the fault is caused by peripheral equipment. Routine methods for fault analysis and isolation are shown in **Common Methods for Fault Analysis and Isolation**.
2. If the fault is caused by peripheral equipment, further check the operation status of the peripheral equipment to isolate the fault.

1.5.3 Isolating and Shooting Troubles

The step of isolating and shooting troubles focuses on analyzing and determining the fault causes and then shooting the troubles.

The following principles should be followed in the course of fault isolation:

- Inspect whether the external cables of the equipment are securely connected, and then inspect indicator LEDs;
- Check the general operation status of the equipment, and then query the status of each card via the ANM2000.

The process of trouble isolation and troubleshooting is as follows:

1. Ascertain the fault type based on the information collected.
2. Determine whether the fault is a service fault encountered by some users or by all users through analysis on fault symptoms, indicator LED status and alarms.
3. Apply routine methods for fault analysis and isolation to determine the causes of the fault. Details of routine methods for fault analysis and isolation are shown in **Common Methods for Fault Analysis and Isolation**.

1.5.4 Contacting FiberHome for Technical Support

If maintenance personnel are unable to eliminate the fault after collecting the fault information, isolating the fault and trying the troubleshooting, contact the Customer Service Department of FiberHome or the local office promptly for technical support. Details on how to contact the technical staff are given in **How to Obtain Technical Support**.

The flow for obtaining technical support is shown in Figure 1-11:

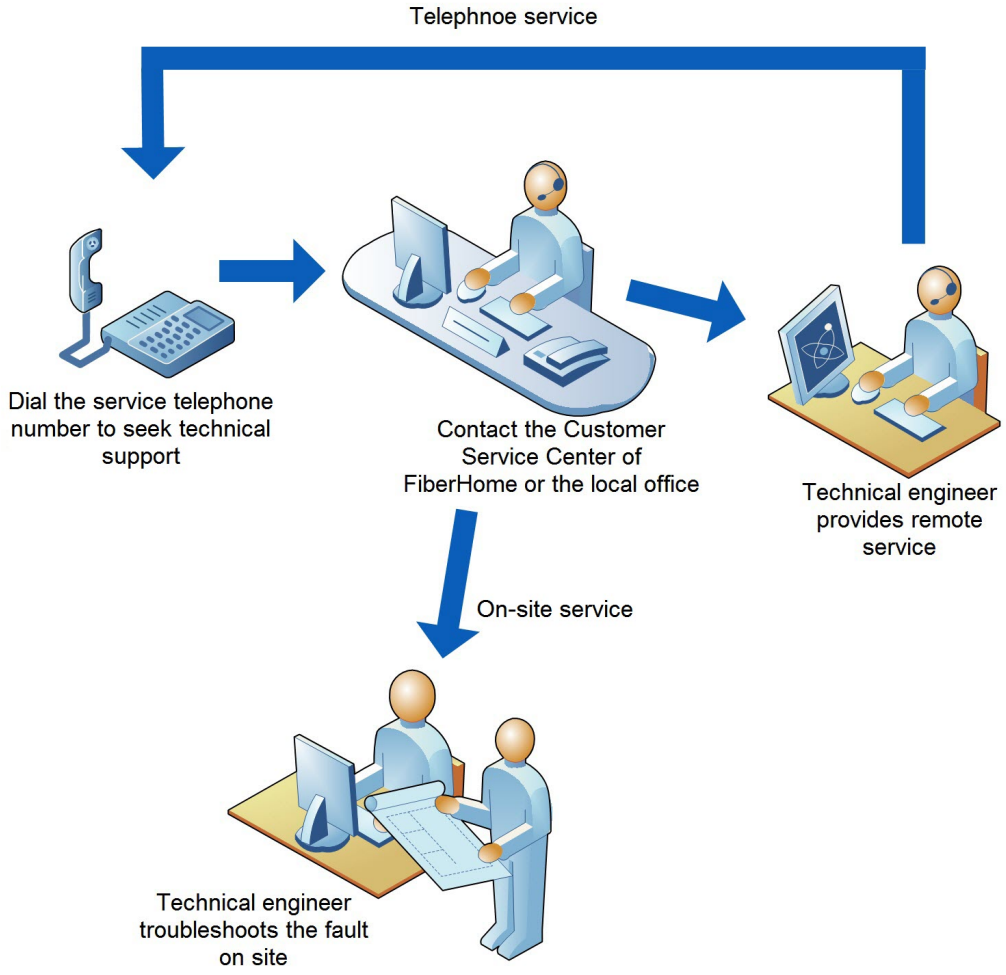


Figure 1-11 Flow for obtaining technical support

1.5.5 Observing Equipment Operation Status

After eliminating the fault, observe the equipment operation for a period of time to make sure that the equipment has resumed normal work.

1. Observe whether the equipment alarms have been eliminated. Refer to *AN5116-06B Optical Line Terminal Alarm and Event Reference* for alarm inquiry.
2. Observe whether the equipment indicator LEDs are normal. Refer to *AN5116-06B Optical Line Terminal Equipment Hardware Description* for details.
3. Check whether the hardware status information of the card is normal through the **Getting Information** command of the network management system.
4. Perform statistics of the equipment performance via the network management system, and check whether each performance item is normal.

1.6 How to Obtain Technical Support

Maintenance engineers can seek technical support from FiberHome or FiberHome local offices when they are unable to remove a fault.

See below for the contact information:

- Tel: +86 27 8769 1549
- Fax: +86 27 8769 1755
- Website: http://www.fiberhomegroup.com
- For contact information about FiberHome local offices, visit our website mentioned above.

2 Common Methods for Fault Analysis and Isolation

This chapter introduces command methods for fault analysis and isolation, so as to guide troubleshooting.

- ☑ General
- ☑ Instrument Test
- ☑ Optical Line Detection
- ☑ Status Indicator Analysis
- ☑ Alarm Analysis
- ☑ Log Inspection
- ☑ Performance Analysis
- ☑ Loopback Test
- ☑ Comparison/Substitution
- ☑ Configuration Data Analysis
- ☑ Status Call-back
- ☑ Signal Tracing

2.1 General

The routine methods for fault analysis and isolation include instrument test, indicator LED status analysis, alarm analysis, signal tracing, log inspection, performance analysis, loopback tests, comparison/substitution, configuration data analysis, status call-back and optical line detection.

The process and routing methods for fault analysis and isolation are shown in Table 2-1.

Table 2-1 Common methods for fault analysis and isolation

Fault Analysis and Isolation Process		Routine Methods	Supporting Methods
Exclude equipment peripheral factors		Instrument test	Alarm analysis
		Status indicator analysis	
		Comparison/substitution	
		Loopback test	
Trouble isolation and trouble-shooting	Ascertain the fault type	Alarm analysis	Performance analysis, configuration data analysis
		Status indicator analysis	
		Status call-back	
	Determine the fault scope	Alarm analysis	Performance analysis
		Status indicator analysis	
		Status call-back	
		Configuration data analysis	
		Comparison/Substitution	
	Determine the specific cause of the fault	Alarm analysis	Performance analysis, log inspection
		Status indicator analysis	
		Status call-back	
		Configuration data analysis	
		Comparison/substitution	
		Loopback test	
		Signal tracing (for voice service)	
		Instrument test (for system faults)	
		Optical line detection	

Table 2-1 Common methods for fault analysis and isolation (Continued)

Fault Analysis and Isolation Process	Routine Methods	Supporting Methods
Operation status observation	Alarm analysis	–
	Status indicator analysis	
	Status call-back	
	Performance analysis	

2.2 Instrument Test

Definition

Instrument test means using related instruments to measure the equipment parameters and determine fault causes by comparing the measured values with normal values.

Instruments in common use are shown in Table 2-2.

Table 2-2 Operating instructions for instruments

Item	Purpose
Multimeter	To measure voltage and current of the power system.
Network cable tester	To test the connectivity of network cables.
Error detector	To test whether the transmission link is normal.

Purpose

Instruments can show the equipment running status by providing visible and detailed data.

Application

The instrument test is used to exclude external factors and hunter for the specific cause of fault.

For example, a user on the ONU side fails to access the broadband service. In this case, you can test the network cable between the ONU and the user's computer with the network cable tester, and you will detect disconnectivity of the signal line.

2.3 Optical Line Detection

Definition

The optical line detection is applied to handle the faults in optical line, e.g. failure in registering an ONU, disconnection of a registered ONU, system loss of packets, and light leakage. Below are the main detection measures:

- Common optical power detection
- Leakage optical power detection

Purpose

- The common optical power detection is used for the purposes below:
  - Tests the Tx optical power of the OLT optical module at the central office end. Generally a normal measured value is about 0dbm (after attenuation of the optical line).
  - Tests the Tx optical power of the ONU optical module at the remote end. A normal measured value is about 0dbm to 4dbm (after attenuation of the optical line).
  - Tests the Rx optical power of the ONU at the remote end. A normal measured value is about -17dbm to -26dbm.
- The leakage optical power detection is used for the purposes below:

  Unplug the optical fiber from the optical module at the PON interface on the OLT side, and connect the optical fiber to the Rx end of the optical power meter dedicated for PON to test the uplink Tx optical power of all ONUs under the PON.

Application

The optical line detection is applied to determine the specific cause of a fault.

For example, when all the ONUs under No.1 PON interface on the EC8B card of the AN5116-06B report the fiber breakage alarm, you can use an optical power meter dedicated for PON to measure relevant optical power of the PON interface, so as to ascertain whether the optical module is working normally.

2.4 Status Indicator Analysis

Definition

The AN5116-06B has operation indicator LEDs and status indicator LEDs. These indicator LEDs directly reflect the operating status of each card, link and optical path as well as their active and standby status. These indicators are important for fault analysis and isolation.

Purpose

Status indicator analysis is used to quickly approximate the fault location or cause before the next treatment step. Through observing the indicator LEDs on the cabinet, subracks and cards, maintenance staff can initially ascertain and isolate a fault. Information provided by indicator LEDs is often insufficient; therefore, the status indicator analysis is often used together with the alarm analysis.

Application

The status indicator analysis is applied in cases where the cause of the fault is in a relatively narrow scope.

For example, when the ACT indicator LED for the EC8B card of the AN5116-06B blinks slowly, the PON interface cards are being initialized or the card software is being started, but the communication between the active and standby cards cannot be set up.

Related information

Refer to *AN5116-06B Optical Line Terminal Equipment Hardware Description* for details about indicator LEDs.

2.5 Alarm Analysis

Definition

Alarms are informative messages for various faults and events during system operation. When the equipment fails, the system will report one or more alarm messages to the network management system. Users can retrieve the current alarms, historical alarms and the time an alarm occurred via the ANM2000.

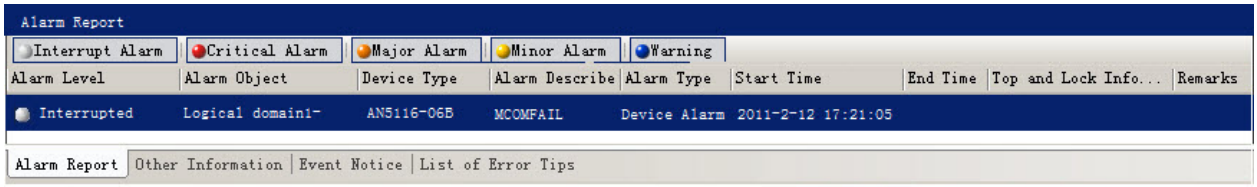
Purpose

Alarm information analysis is one of the essential operations in fault analysis and isolation.

Application

The alarm information analysis is applied in cases where the fault is relatively simple.

For example, when you check the current alarms of the AN5116-06B and find an alarm for system interruption, the communication between the equipment reporting the current alarm and the network management server is interrupted.



Related information

Refer to *AN5116-06B Optical Line Terminal Alarm and Event Reference* for details about alarm messages.

2.6 Log Inspection

Definition

The ANM2000 supports query of command logs and registration logs. In command logs, users can view the configuration data, configuration time and command execution results; in registration logs, users can view the registration name, IP address, registration time and whether a registration is successful.

Purpose

A fault may be caused by mistakes made by maintenance personnel in course of data planning and configuration. In order to isolate this type of fault quickly, maintenance personnel should view the system logs and analyze historical configuration data.

Application

The log inspection is applied to determine the specific cause of a fault.

For example, when you find an inconsistency between a configuration item and the planning data during routine maintenance of the AN5116-06B, and suspect that an illegal user has modified the equipment configuration data, you can inspect the registration name, IP address, registration time of the user by checking the logs.

2.7 Performance Analysis

Definition

Performance statistics are for monitoring the equipment operation, collecting and counting essential parameters during equipment operation.

Purpose

Through data collection and analysis, maintenance personnel can obtain adequate data on equipment operation. Performance analysis provides a powerful means of diagnosing faults.

Application

The performance analysis is applied in cases where the system operation is unstable or the transmission rate is abnormal.

For example, when the HSWA card of the AN5116-06B is restarted repeatedly or runs slowly so that you cannot perform normal operation of the equipment, you can monitor the CPU and memory utilization ratio of the HSWA card via the real-time performance statistics function. Then you can analyze the statistics data and ascertain whether the phenomenon is caused by excessive occupation of the CPU or memory by programs.

2.8 Loopback Test

Definition

The loopback test uses hardware or software methods to verify the operational status of the equipment or a transmission channel by transmitting and receiving a known signal or data pattern.

Purpose

The purpose of a loopback test is to confirm the operational status of the associated hardware or equipment and of the software parameter settings by ascertaining whether the channel is performing normally during the test. The loopback test is one of the most common ways for determining transmission problems and relay parameter settings.

Application

The loopback test is used to exclude faults in peripheral equipment.

For example, when a fault occurs in the TDM service of the AN5116-06B, you can apply the loopback test to the TDM line. Details as follows:

- Internal loopback: checks whether the line from the E1 interface of the ONU to the C155A card is faulty.
- External loopback: checks whether the line from the STM-1 interface of the SDH device to the C155A card is faulty.

2.9 Comparison/Substitution

Definition

- Comparison involves comparative analysis of faulty parts or symptoms with the normal parts or symptoms, so as to find out differences, and then locate the problem.

- Substitution involves replacing a possibly faulty part with a normal part (such as a card, an optical fiber), and then comparing the equipment operation before and after the substitution, so as to determine fault scope or location. Refer to *AN5116-06B Optical Line Terminal Equipment Component Replacement* for details.

Purpose

The comparison/substitution method is used to isolate the fault point quickly.

Application

The comparison/substitution method is generally used to exclude the fault in peripheral equipment, determine the fault scope, and find out the specific cause of the fault.

For example, when the ONU of an EPON subscriber cannot be authorized normally, you can isolate the fault by replacing the ONU or by comparing the ONU with other ONUs under the same optical splitter to see whether the same phenomenon occurs in other ONUs.

2.10 Configuration Data Analysis

Definition

Configuration data analysis entails analyzing the fault cause by viewing and analyzing current data configuration.

Purpose

When the fault has been localized to the local system, analyzing the current configuration data of the equipment can lead to identification of a configuration error.

Application

The configuration data analysis is applied in cases where the fault is relatively simple.

For example, when all subscribers under the AN5116-06B fail to use the voice phone, you can find an error with the MGC address configuration through configuration data analysis. This error contributes to abnormal registration of the ONU in the MGC address table.

2.11 Status Call-back

Definition

Status call-back can trace current equipment configuration and relevant parameters in a real-time manner.

Purpose

Maintenance personnel can acquire relevant configuration data about the equipment via status call-back, which can provide reference for subsequent analysis and troubleshooting.

Application

The status call-back is applied in cases where the cause of the fault is in a relatively narrow scope.

For example, when a subscriber under the AN5116-06B cannot access any service carried by the equipment, and the REG indicator LED on the ONU where the subscriber belongs to is extinguished, you can query the information about the unauthorized ONU via the status call-back command on the ANM2000. Accordingly, you will find that the OLT does not authorize the ONU; and when you check the ONU physical address authentication white list, you will find that the physical address of the ONU is not included into the white list.

2.12 Signal Tracing

Definition

Signal tracing can trace and save on a real time basis the voice service signaling interaction flow between the equipment and softswitch platform.

Purpose

Maintenance personnel can directly acquire the cause of a call failure by reviewing the signal trace, and thus provide valuable suggestions for subsequent analysis and troubleshooting.

For details, please see **Signal Tracing Instruction**.

Application

Signal tracing is applied in shooting troubles with voice services.

For example: a subscriber fails in making a voice phone call; signal tracing is then performed and it is found that the ONU that the subscriber belongs to fails to register in the MGC. A further inspection discovers an error in configuring the endpoint user name of the ONU.

3 Troubleshooting Common System Faults

This chapter introduces procedures for troubleshooting common system faults.

- Card Faults
- All Indicators Extinguished after Power-on
- LOS Indicator of ONU Illuminated
- REG Indicator of ONU Being Abnormal
- ONU Network Management Connection Failure
- Network Interface Indicator Extinguished
- Equipment Management IP Address Ping Timeout
- Abnormal Link between Equipment and Switch
- Link to Network Management Database Failed

3.1 Card Faults

Fault symptom

Symptoms of a card fault mainly consist of the following types:

- The working indicator LED of a card is extinguished and the alarm indicator is illuminated;
- The indicator LED remains extinguished after power-on of the card;
- The services carried by the card are interrupted;
- The active-standby communication between the card and its peer is interrupted. The services are normal but configuration commands cannot be issued;
- The card software cannot be started in a normal way.

Fault analysis

Main causes for a card fault may include the following:

- Component or subcard damage;
- Arbitrary removal and/or insertion of the card;

Troubleshooting procedure

1. Restart the card

   Remove and insert the card to restart it. If the fault does not disappear after several seconds, go to Step 2.

2. Replace the card

   - If the AN5116-06B has a standby card, replace the card. Refer to *AN5116-06B Optical Line Terminal Equipment Component Replacement* for details.
   - If the AN5116-06B has no standby card, contact FiberHome for support.

3.2 All Indicators Extinguished after Power-on

Fault symptom

All indicators on the AN5116-06B are extinguished after power-on of the equipment.

Fault analysis

Possible causes are as follows:

- A fault occurs in the power system.
- The power cables are connected incorrectly.

Troubleshooting procedure

1. Check the power system in the equipment room, and contact related maintenance personnel for repair if it has failed.
2. Turn off the head of row cabinet and the PDP. Check whether the power cables from the head of row cabinet to the PDP and from the PDP to the AN5116-06B subracks are securely and properly connected. If not, reconnect the power cables. Refer to *AN5116-06B Optical Line Terminal Equipment Installation Guide* for details.

3.3 LOS Indicator of ONU Illuminated

Fault symptom

The LOS indicator LED of the ONU is illuminated.

Fault analysis

The LOS indicator on the ONU being illuminated indicates that the ONU is not receiving the optical signal or the received optical power is too low. The possible causes are shown below:

- The optical fiber connection is incorrect;
- The received optical power of the ONU is too low;
- An OLT device at the central office end is faulty, for example, a PON interface card is faulty;
- The ONU equipment is faulty.

Troubleshooting procedure

Caution:

The laser beam at the optical interface and fiber connector can injure your eyes! Never look directly into the optical interface and fiber connector.

1. Check whether the ONU equipment operates normally or has abnormal alarms. If the ONU equipment is faulty, replace it. Refer to *AN5116-06B Optical Line Terminal Equipment Component Replacement* for operation procedures.
2. Check the connection of the optical fibers.
   - If the fiber jumper is incorrectly connected, remove and reinsert it correctly;
   - If the fiber is broken, replace it with a good fiber jumper.
3. Connect the optical fiber dedicated for PON test to the PON optical power meter and the PON port of the ONU respectively, and measure the received optical power of the ONU. The normal range of the Rx optical power of the ONU is between -24dBm and -8dBm. If the Rx optical power is measured to be normal, go to Step 6 . If not, do as follows:
   - If the fiber connector is dirty, clean it with non-woven lens tissue dampened with a small amount of dedicated detergent (the first choice is the isoamyl alcohol and the second choice is the propyl alcohol), and then reinsert the fiber into the PON port again.
   - If the fiber connector is not smooth, replace it with a good fiber jumper.
   - If the bend radius of the fiber is too small, increase the bend radius properly.
   - If there are too many optical splitter cascades, reduce the number of cascades.

   Go to Step 4 if the fault is not removed.
4. Check whether the interface card is present and whether it has abnormal alarms. If the PON interface card is faulty, replace it. Refer to *AN5116-06B Optical Line Terminal Equipment Component Replacement* for operation procedures.

5. Contact FiberHome if the above steps do not work.

3.4 REG Indicator of ONU Being Abnormal

Fault symptom

The REG indicator LED on the ONU blinks or goes out.

Fault analysis

If the REG indicator on the ONU blinks or goes out, registration of the ONU with the OLT has failed. Possible causes are as follows:

- The fiber at the uplink PON port of the ONU is loose or broken.
- The optical power at the PON port of the ONU is abnormal.

Caution:

The optical access system is sensitive to optical links. Even a slightly dirty optical connector or non-aligned adapter will cause excessive loss of optical power.

- The OLT device at the central office end is faulty; for example, the PON interface card is faulty.

Troubleshooting procedure

- If the REG indicator of the ONU is abnormal and LOS indicator is illuminated, go to Steps 1 to 5;
- If the REG indicator of the ONU is abnormal and LOS indicator is extinguished, go to Steps 3 to 5.

Caution:

The laser beam at the optical interface and fiber connector can injure your eyes! Never look directly into the optical interface and fiber connector.

1. Check the connection of the optical fibers.

- If the fiber jumper is incorrectly connected, remove it and reinsert it correctly;
- If the fiber is broken, replace it with a good fiber jumper.

2. Check the fiber jumper connector.
   - If the fiber connector is dirty, clean it with non-woven lens tissue dampened with a small amount of dedicated detergent (the first choice is the isoamyl alcohol and the second choice is the propyl alcohol), and then reinsert the fiber into the PON port again.
   - If the fiber connector is not smooth, replace it with a good fiber jumper.
3. Connect the optical fiber dedicated for PON test to the PON optical power meter and the PON port of the ONU respectively, and measure the received optical power of the ONU. The normal range of the Rx optical power of the ONU is between -24dBm and -8dBm. If the Rx optical power is measured to be normal, go to Step 6 . If not, do as follows:
   - If the optical power is too high, add an optical attenuator on the optical path for recovery;
   - If the optical power is too low, check the optical path to resume the optical power.
4. Check whether the interface card is present and whether it has abnormal alarms. If the PON interface card is faulty, replace it. Refer to *AN5116-06B Optical Line Terminal Equipment Component Replacement* for operation procedures.
5. Check whether the ONU can be normally authorized. If no, check whether the current ONU authentication mode is correct, and check whether the MAC address and the SN logical number of the ONU are in the authentication white list.
   - If the ONU authentication mode configuration is incorrect, re-configure the authentication mode according to the planning data.
   - If the MAC address or the SN logical number of the ONU is not in the authentication white list, add it to the white list and deliver the configuration data to the AN5116-06B.
6. Contact FiberHome if the above steps do not work.

3.5 ONU Network Management Connection Failure

Fault symptom

The AN5116-06B runs normally, and the ONU status indicator on the ANM2000 is grey.

Fault analysis

Below are the possible causes for the ONU's failure in connection with the network management system:

- Fiber at the PON port or at the ONU side is loose or broken;
- The optical power at the PON port is abnormal;
- The ONU equipment is faulty.

Troubleshooting procedure

Caution:

The laser beam at the optical interface and fiber connector can injure your eyes! Never look directly into the optical interface and fiber connector.

- If the fiber at the PON interface or at the ONU side is loose, broken or the optical power is abnormal, refer to **LOS Indicator of ONU Illuminated** for troubleshooting.
- Contact FiberHome if the ONU is faulty.

3.6 Network Interface Indicator Extinguished

Fault symptom

The Ethernet interface connection indicator LED of the AN5116-06B is extinguished.

Fault analysis

The Ethernet interface connection indicator LED of the AN5116-06B may be extinguished for the causes below:

- The network cable connection is incorrect;
- The AN5116-06B has a fault in hardware.

Troubleshooting procedure

1. Check peripheral equipment of the AN5116-06B, and notify related maintenance personnel for troubleshooting if it has failed. If the peripheral equipment is working normally, go to Step 2.
2. Check the network cable connection, remove and reinsert the cable again when necessary. Go to Step 3 if it does not work.
3. Examine the network cable with a network cable tester. Replace the network cable when it has a fault.
4. Contact FiberHome if the above steps do not work.

3.7 Equipment Management IP Address Ping Timeout

Fault symptom

A Ping of the core switch card via the ANM2000 fails to respond and times out.

Fault analysis

Possible causes are as follows:

- A fault in the peripheral router or switch;
- A fault in physical connection;
- An error in the management VLAN and IP address configuration for the AN5116-06B;
- An error in IP address configuration of the ANM2000 computer.

Troubleshooting procedure

1. Check whether the peripheral router or switch has failed. Notify related maintenance personnel for troubleshooting if a failure has occurred; otherwise, go to Step 2.
2. Check the physical link between the ANM2000 computer and the AN5116-06B section by section.
   - If the link is OK, go to Step 3.
   - If the link is faulty, check the network cable connection and the network card on the network management computer. If the network cable connection is incorrect or the network card is faulty, correct the network cable connection or replace the network card. If both the network cable connection and the network card are normal, go to Step 5.
3. Check whether the management VLAN configuration for the AN5116-06B is correct. Related operations are as follows:
   1) Log into the CLI network management system, enter **cd service** after the command prompt **Admin#**; then press the Enter key to access the command directory for configuring the management VLAN. Refer to *AN5116-06B Optical Line Terminal Equipment Configuration Guide* for details on how to log into the CLI network management system and enter the configuration mode.
   2) In the service directory, enter the **show manage vlan all** command to check whether the settings of the management VLAN are identical with the data planning; details of the command execution are shown below:

      For example, the uplink interface 19:2 is set to management VLAN in the untagged mode; the VLAN ID of the management VLAN is 4000; the management IP is 10.26.1.1; and the mask is 255.255.0.0.

      Return message from the CLI network management system is shown below:

```
VLAN ID:                    4000
Name:                manage
IP Address:        10.26.1.1/16
Gateway:           10.26.1.254
Mac address:       00:00:00:00:00:11
Tagged Ports:
Untagged Ports:   19:2
```

Commands for modifying the management VLAN and IP address in the CLI network management system are as follows:

Command
set manage vlan name <name> vid <vid> inputport [<portlist>|outbandport] [untagged|tagged]
set manage vlan name <name> ip <A.B.C.D/M> {<A.B.C.D>}*1

4. Perform the fault analysis and troubleshooting according to the port mode of the management VLAN.
   - If the port of the management VLAN is in the tagged mode, check the IP address configuration of the network management system computer and correct the IP address if it is incorrect.
   - If the port of the management VLAN is in the untagged mode, follow the steps below.
     a) Check whether the switch is connected to the correct uplink interface and whether the switch VLAN is configured correctly.
     b) Check whether the IP address configuration of the network management system computer is correct; if not, modify it.
5. Contact FiberHome if the above steps do not work.

3.8 Abnormal Link between Equipment and Switch

Fault symptom

The link between a GE optical interface of the AN5116-06B uplink card and the previous switch is abnormal.

Fault analysis

Possible causes are as follows:

- Fault in optical fiber connection;
- An error in the interface mode configuration;
- Unmatched optical module types.

Troubleshooting procedure

1. Check whether the optical fiber connection between the GE optical interface of the uplink card and the previous switch is normal.

   - If the fiber jumper is incorrectly connected, remove it and reinsert it correctly;
   - If the fiber is broken, replace it with a good fiber jumper.

   Go to Step 2 if the fault is not resolved.

2. Check the configuration of the uplink port properties. That is, check whether the configuration of parameters for the uplink port such as port enable / disable, port auto negotiation and port working mode is identical with that for the switch connected to it.

   Operation steps for checking the configuration of the uplink port properties are as follows:

   1) Log into the ANM2000 network management system, and right-click the **HU1A→Config→Uplink port properties** under the faulty OLT system.
   2) Click the button to read the equipment configuration. See Figure 3-1 for the configuration of port properties.

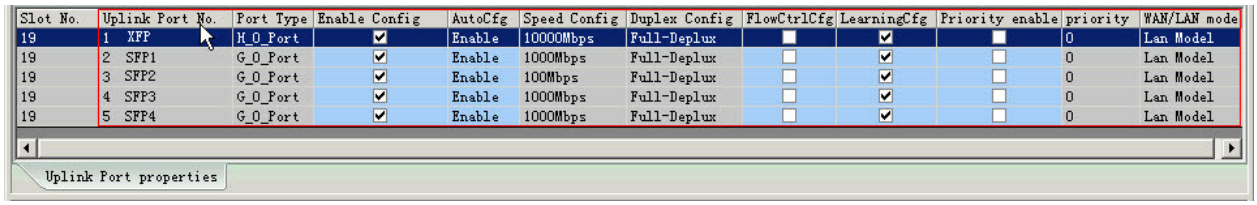


Figure 3-1 Configuring the uplink port properties

   - If the configuration of the uplink port properties is not identical with that of the previous switch connected to it, make corrections.
   - If identical, go to Step 3.

3. Check whether the type of the optical module at the uplink port of the AN5116-06B is identical with that at the switch port. If not identical, replace the optical module concerned and make them identical.

4. Contact FiberHome if the above steps do not work.

3.9 Link to Network Management Database Failed

Fault symptom

When starting the ANM2000, the user fails to enter the login window and sees a prompt of **Get data from anserver failed!** as shown in Figure 3-2.

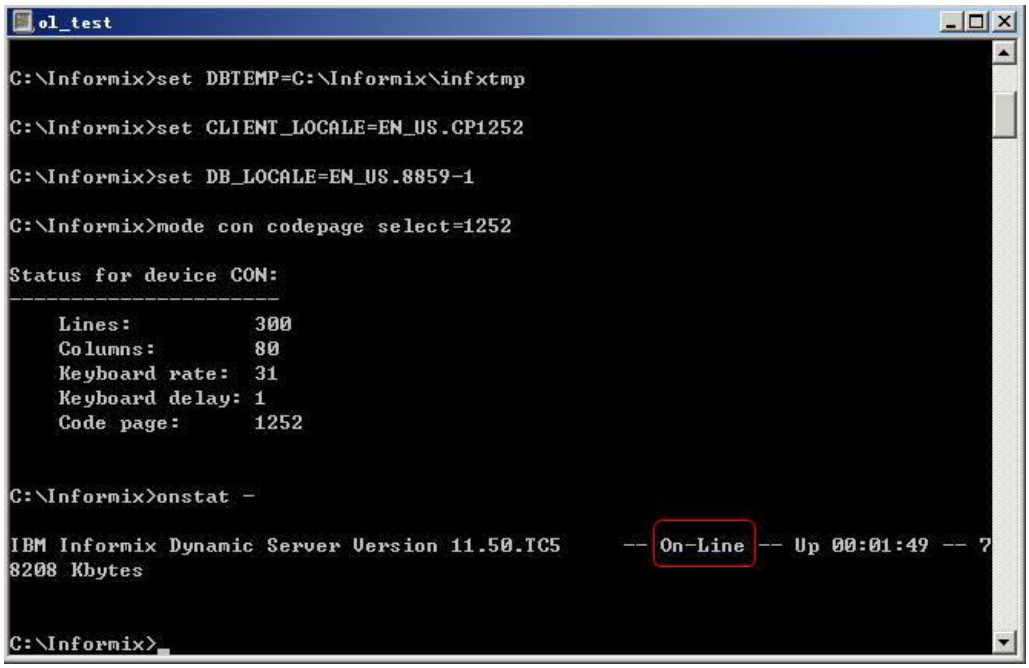
Figure 3-2 Connection failure

Fault analysis

The ANM2000 must access the database through an informix system user to get started. Add the user in the Windows system before installing the ANM2000. Deleting this user may cause failure in connection to the database.

Troubleshooting procedure

1. Check whether the database can be started normally.
   1) Click **Start→Programs→IBM Informix Dynamic Server 11.50→ol_test** (here ol_test is taken as an example).
   2) Enter **onstat_** and check whether the database can be started normally.



- If the system displays **On-Line**, the database can be started normally. Go to Step 3.
- If the database cannot be started normally, check whether the Informix IDS – ol_test service among computer services has been started. If not, start it. When the service is started normally, go to Step 2.

2. Check whether the parameter configuration for the ONCONFIG file is correct.

   Check the “onconfig.ol_test” file under the directory “C：\informix\etc”. Below is the configuration reference table:

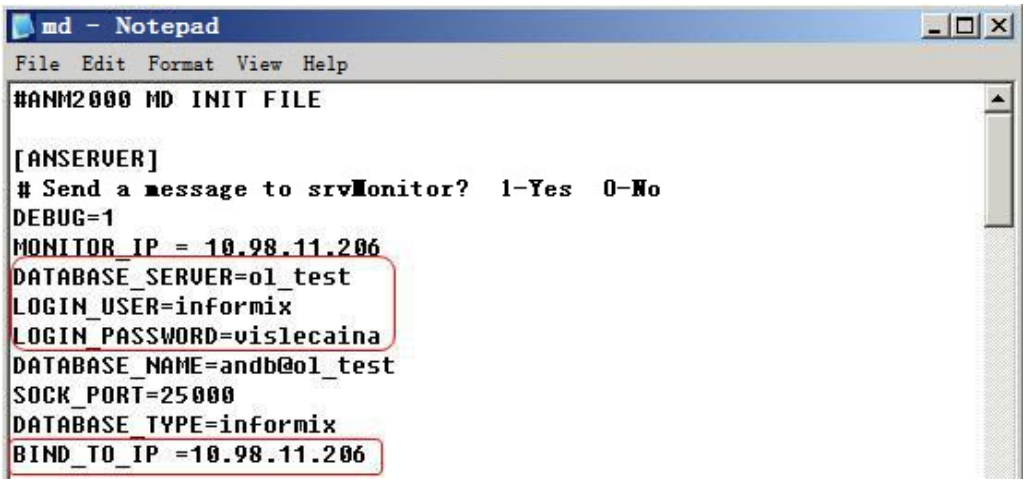
Table 3-1 ONCONFIG parameter values

Parameter	Recommended Parameter Value
ROOTSIZE	1024000
PHYSFILE	50000
LOGFILES	40
LOGSIZE	10000
SHMVIRSIZE	32656
SHMADD	8192
EXTSHMADD	8192

- If the configuration is incorrect, modify it.
- If the configuration is correct, go to Step 3.

3. Check whether the ANM2000 configuration file is correct.

   Check whether values of the parameters “DATABASE_SERVER” , “LOGIN_USER”, “LOGIN_PASSWORD” and “IP” in the md.ini file under the “D:\AEMS\Server\ini” directory are correct.



   - If not, modify the configuration, and then go to Step 4.
   - If the configuration is correct, go to Step 4.

4. Make sure that the configuration above is correct and then restart the services “AEMS-CollectionServer”, “AEMS-DBServer”, “AEMS-DumpServer” and “AEMS-Manager”.

   - If you can log into the ANM2000 normally after restarting the aforesaid services, the fault is removed.
   - If the link still fails after restarting the aforesaid services, go to Step 5.

5. Contact FiberHome if the above steps do not work.

4 Troubleshooting Data Service Faults

This chapter introduces how to troubleshoot data service faults of the AN5116-06B.

- ☑ Background Knowledge
- ☑ Troubleshooting Flow
- ☑ Troubleshooting Common Faults

4.1 Background Knowledge

This section introduces the background knowledge about data service faults.

The typical networking of the AN5116-06B for data service application is illustrated in Figure 4-1.

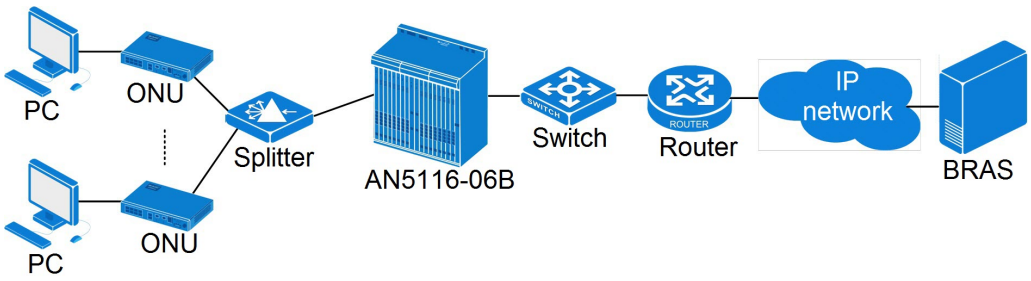


Figure 4-1 Typical networking of the AN5116-06B for data service

In the data service application network, the subscribers access the Internet using the PPPoE protocol or DHCP authentication. The ONU provides the RJ-45 interface for connection to the subscribers' computers or home gateway, and the Internet connection data packets are sent to the Internet via the OLT in a real time manner.

4.2 Troubleshooting Flow

This section introduces the procedures for troubleshooting data service faults of the AN5116-06B.

Procedures for troubleshooting data service faults is shown in Figure 4-2.

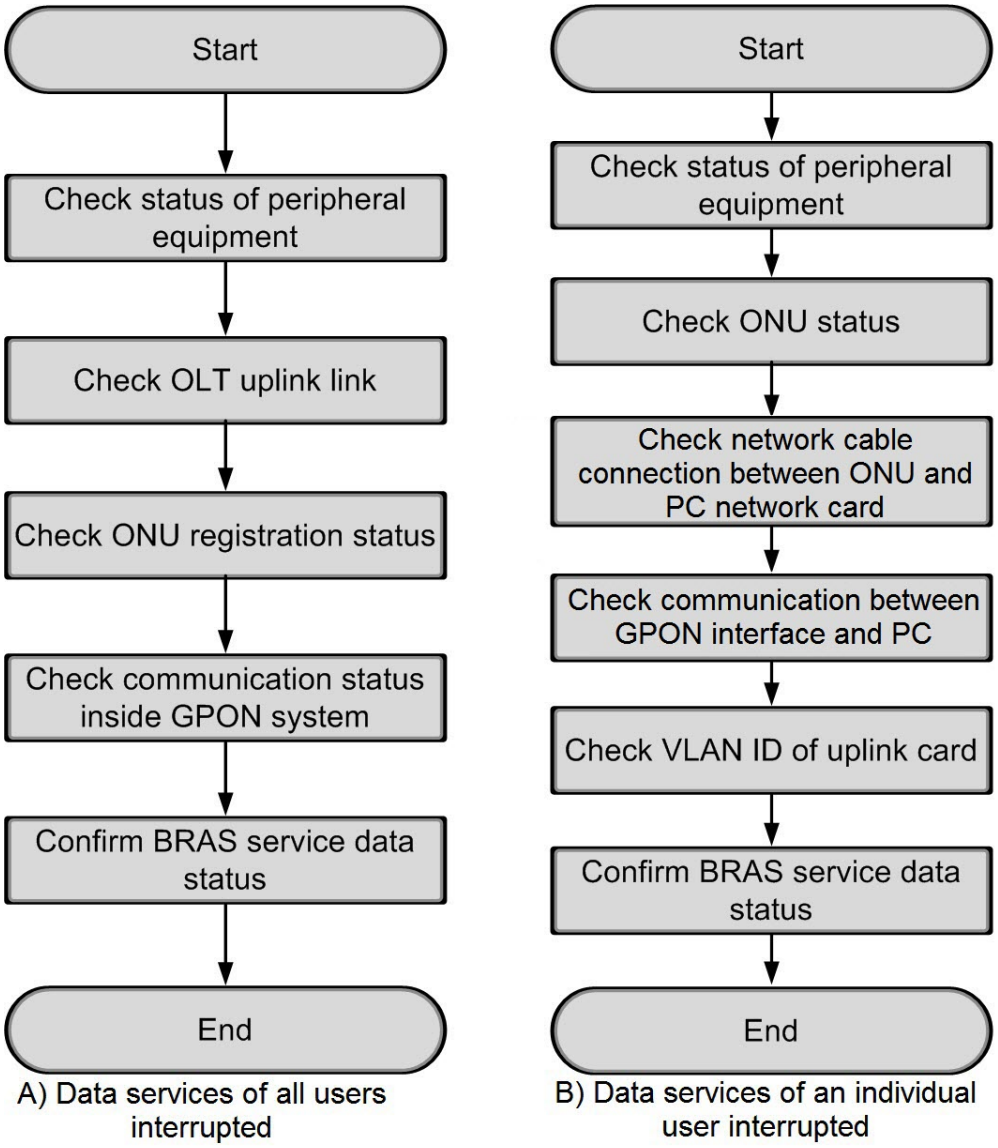


Figure 4-2 Troubleshooting flow for data service interruption

4.2.1 Troubleshooting Data Service Interruption of All Users

4.2.1.1 Checking Status of Peripheral Equipment

Analysis and troubleshooting

Consult the maintenance personnel and determine whether the interruption of all data services is arising from peripheral equipment.

The data service mainly involves the following peripheral devices:

- Ethernet switches;
- Routers;
- BRAS equipment.

4.2.1.2 Checking OLT Uplink

Analysis and troubleshooting

The method for checking uplink status of the AN5116-06B is as follows:

1. Ascertain the status of the uplink by viewing the uplink card alarms on the ANM2000. Alarms relevant to the HU1A card of the AN5116-06B are shown in Table 4-1.

Note:

Refer to *AN5116-06B Optical Line Terminal Equipment Alarm and Event Reference* for causes and troubleshooting methods of different alarms.

Table 4-1 Alarms relevant to the HU1A Card

Alarms of HU1A Card	Alarm Level	Alarm Type
Card type mismatch	Urgent alarm	Equipment alarm
Card not present	Urgent alarm	Equipment alarm
Loss of optical signal	Urgent alarm	Communication alarm
Uplink / downlink CRC error threshold-crossing	Minor alarm	QoS alarm
Undersized packets reaching threshold	Minor alarm	QoS alarm
Port connection failure	Prompt alarm	Equipment alarm

2. Check whether the configuration of the uplink card port properties is identical with that of the connected switch. Check the port type, the port enabled / disabled status, port auto-negotiation status, port rate and port work mode etc.
   - If the configuration is not identical, correct it on the AN5116-06B or the switch;

- If the configuration is identical, follow the handling procedures described in Checking the Registration Status of the ONU.

Access method and GUI

- The method for viewing / modifying the uplink port properties is shown in the table below.

Operation	Access Method
View / modify the uplink port properties.	Click the **HU1A** card in the **Object Tree** pane and select **Config→Uplink Port Properties** from the shortcut menu that appears.

- The operation GUI for viewing / modifying the uplink port properties is shown in Figure 4-3.

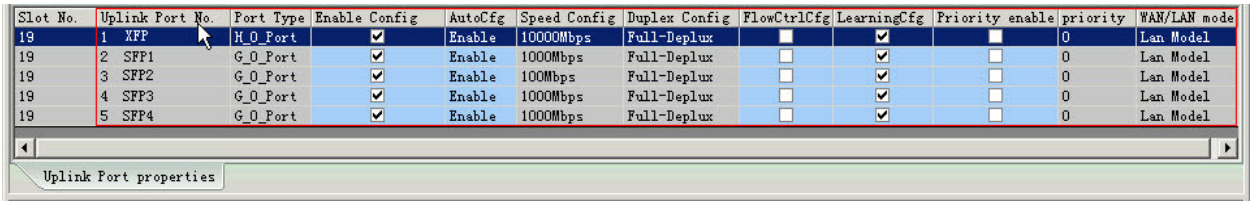


Figure 4-3 Viewing / modifying the uplink port attributes

4.2.1.3 Checking the Registration Status of the ONU

Analysis and troubleshooting

Log into the ANM2000 and check whether the ONU registration is successful or not.

- If not successful, the optical path is faulty. Check whether the fiber connection is correct and whether the Rx optical power of the ONU is in the normal range.
- If successful, follow the handling procedures described in Checking Internal Communication Status of PON System.

Access method and GUI

- The method for checking the ONU registration status is shown below:

Operation	Access Method
Check the ONU registration status.	Click the **EC4B** card on the **Object Tree** pane.

- The network management system GUI for checking the ONU registration status is shown in Figure 4-4. If the REG indicator LED in the figure is solid green, the registration is successful. If the REG indicator is grey, the registration fails.

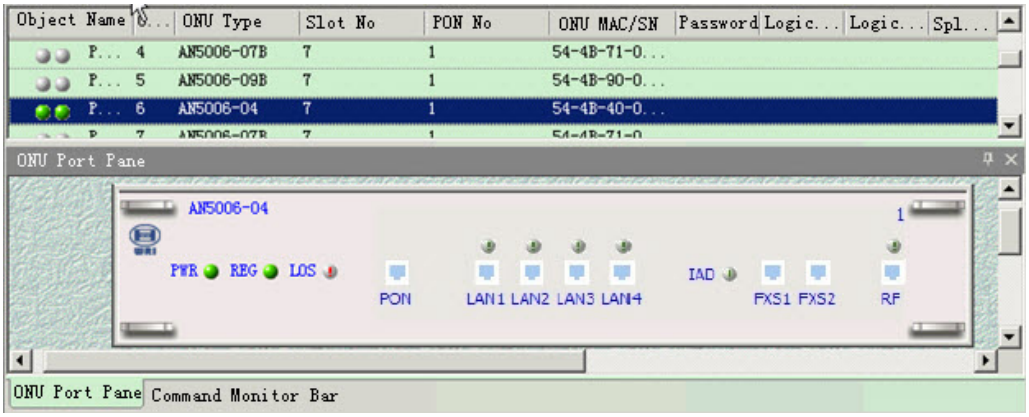


Figure 4-4 The GUI for checking ONU registration status

4.2.1.4 Checking Internal Communication Status of PON System

Analysis and troubleshooting

The method for checking the internal communication status of the PON system is shown below:

1. Select an available uplink interface from the uplink card of the AN5116-06B; use a network cable to connect the uplink interface to a test laptop or PC.
2. Select a remote end ONU and connect it to a test laptop or PC with network cable.
3. Add a service VLAN to the local end VLAN configuration for the AN5116-06B in the untagged mode; the VLAN ID value should be the same as that of the ONU at the remote end. Refer to related sections in *AN5116-06B Optical Line Terminal Equipment Configuration Guide* for details on how to configure the local service VLAN.

4. Set the local computer and the remote computer in the same network segment, and test whether the communication link between the two computers is normal using the ping command.

   - If the two computers can Ping each other, the Ethernet communication is normal in the EPON system. Then follow the handling procedures described in Confirming Status of BRAS Service Data.
   - If the Ping test turns out to be abnormal with phenomena such as loss of packets, excessive delay, and failure in Ping, please contact FiberHome for troubleshooting.

4.2.1.5 Confirming Status of BRAS Service Data

Analysis and troubleshooting

Connect the computer to an idle uplink port of the AN5116-06B, and perform the PPPoE connection test in the computer operating system.

- If a prompt of 678 error appears, the OLT uplink must be faulty. Maintenance personnel for the upper layer BRAS equipment should be notified for inspection to confirm whether the uplink service data is normal.
- If the connection is successful, it can be concluded that the fault lies inside the EPON / GPON system. Contact FiberHome for troubleshooting.

4.2.2 Troubleshooting Data Service Interruption of an Individual User

4.2.2.1 Checking Status of Peripheral Equipment

Analysis and troubleshooting

First determine whether the data service faulty of an individual user is caused by peripheral equipment by consulting the maintenance personnel of the peripheral equipment.

The data service mainly involves the following peripheral devices:

- Ethernet switches;

- Routers;
- BRAS equipment.

4.2.2.2 Checking Connection between ONU and PC

Analysis and troubleshooting

Log into the ONU CLI network management system via the PON interface card, and check whether the ONU port can normally learn the MAC address of the user's computer.

- If the ONU cannot learn the MAC address of the user's computer, a fault may exists in the communication between the user's computer and the ONU. Correct the fault of connection between the computer and the ONU.
- If the ONU can learn the MAC address of the user's computer, the connection between the user's computer and the ONU is OK. Follow the handling procedures described in Checking Communication between PON Interface Card and PC.

4.2.2.3 Checking Communication between PON Interface Card and PC

Analysis and troubleshooting

Check the OLT MAC address table to see whether the MAC address of the user's computer network card and the user's VLAN ID are included in the MAC address table of the PON interface card.

- If yes, the communication between the PON interface card and the user's computer is normal. Follow the handling procedures described in Checking VLAN ID in Uplink Card.
- If no, the communication between the PON interface card and the user's computer is abnormal. Contact FiberHome for troubleshooting.

Access method and GUI

- The method for checking the MAC address table learned by the OLT is shown below:

Operation	Access Method
Check the OLT MAC address table.	Right-click the **HSWA** card in the **Object Tree** pane and select **Get Information→OLT Mac Addr Table** from the shortcut menu that appears.

- Figure 4-5 illustrates the operation GUI for checking the OLT MAC address table.

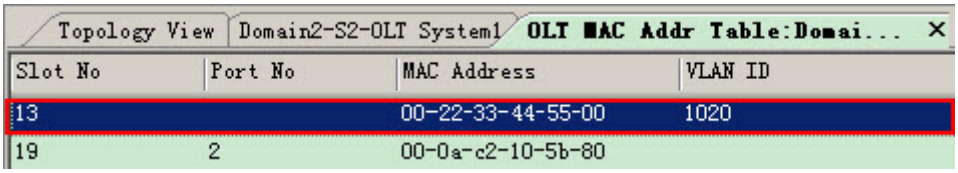


Figure 4-5 Checking the OLT MAC address table

4.2.2.4 Checking VLAN ID in Uplink Card

Analysis and troubleshooting

Check the OLT MAC address table to see whether the corresponding local end VLAN ID exists in the MAC address table of the uplink card.

- If no, the upper layer device has not been configured with this VLAN ID, so you must contact related maintenance personnel for resolution.
- If yes, follow the handling procedures described in Confirming Status of BRAS Service Data.

Access method and GUI

- The method for checking the local end VLAN ID of the uplink card is shown below:

Operation	Access Method
Check the local end VLAN ID on the uplink card.	Right-click the **HSWA** card in the **Object Tree** pane and select **Get Information→OLT Mac Addr Table** from the shortcut menu that appears.

- Figure 4-6 illustrates the operation GUI for checking the local end VLAN ID on the uplink card.

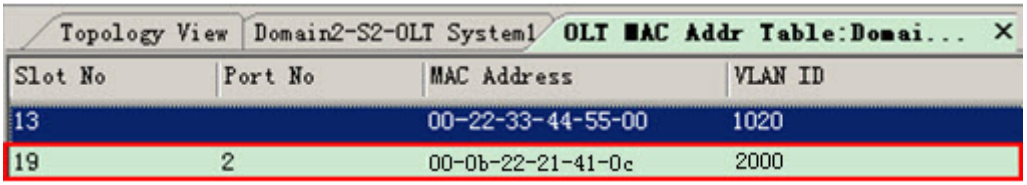


Figure 4-6 Checking the user VLAN ID of the uplink card

4.2.2.5 Confirming Status of BRAS Service Data

Analysis and troubleshooting

Connect the computer to an idle uplink port of the AN5116-06B, and perform the PPPoE connection test in the computer operating system.

- If a prompt of 678 error appears, the OLT uplink must be faulty. Maintenance personnel for the upper layer BRAS equipment should be notified for inspection to confirm whether the uplink service data is normal.
- If the connection is successful, it can be concluded that the fault lies in the EPON / GPON system. Contact FiberHome for troubleshooting.

4.3 Troubleshooting Common Faults

This chapter introduces how to troubleshoot some common faults.

4.3.1 Windows Operating System Prompting a 678 Error

Fault symptom

The Windows operating system prompts a 678 error when connecting a user terminal with PPPoE.

Fault analysis

The prompt of 678 error indicates no response from the remote computer; fault analysis and isolation are shown as follows:

- In the event an individual user encounters the problem, the possible causes are as follows:
  1) Error in the configuration data on the ONU;
  2) Error in the user data on the BRAS.
- In the event that all users of the equipment encounter the problem, the possible causes are as follows:
  1) Uplink interface link failure;
  2) Fault in optical path of PON;
  3) BRAS failure.

Troubleshooting procedure

See **Troubleshooting Data Service Interruption of All Users** and **Troubleshooting Data Service Interruption of an Individual User** for details.

4.3.2 Windows Operating System Prompting a 691 Error

Fault symptom

The Windows operating system prompts a 691 error when connecting a user terminal with PPPoE.

Fault analysis

Possible causes are as follows:

- Computer hardware failure;
- Incorrect PPPoE username or password;
- The BRAS has bound the username with VLAN, port or MAC address.

Troubleshooting procedure

1. Check the computer hardware. Remove the fault with the computer if there is any.
2. Check the PPPoE user name and password, making sure that you are using correct username and code for verification.

3. Check whether the user’s status on BRAS is bound or not and notify BRAS maintenance personnel for troubleshooting.
4. Contact FiberHome if the above steps do not work.

5 Troubleshooting Voice Service Faults

This chapter introduces how to troubleshoot voice service faults of the AN5116-06B.

- Background Knowledge
- Troubleshooting Flow
- Troubleshooting Common Faults

5.1 Background Knowledge

The AN5116-06B networking for voice service is shown in Figure 5-1.

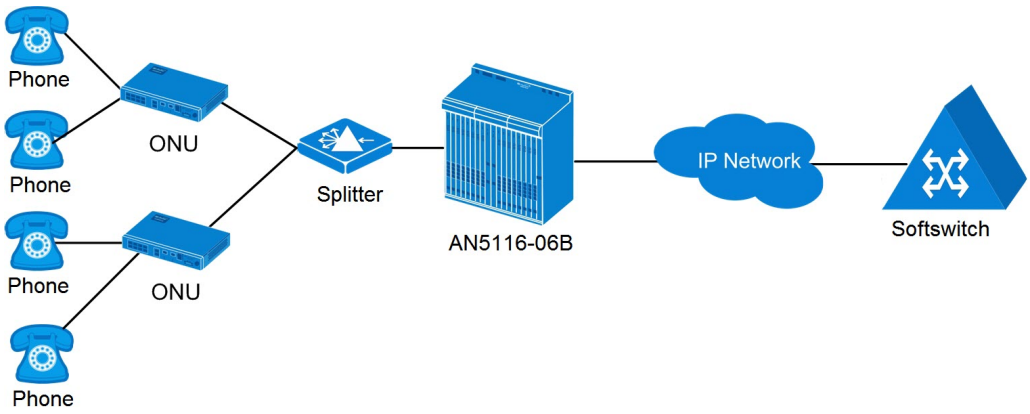


Figure 5-1 The AN5116-06B networking for voice service

In the voice service application network, the ONUs provide POTS ports for the telephone connection. The ONUs compress and encode the voice signals to implement analog to digital conversion, and then transfer the voice data to the IP network through the OLT in the form of IP data package. The softswitch platform controls the call for the voice service.

5.2 Troubleshooting Flow

This section introduces the procedures for troubleshooting voice service faults.

Figure 5-2 illustrates the flow for troubleshooting voice service faults.

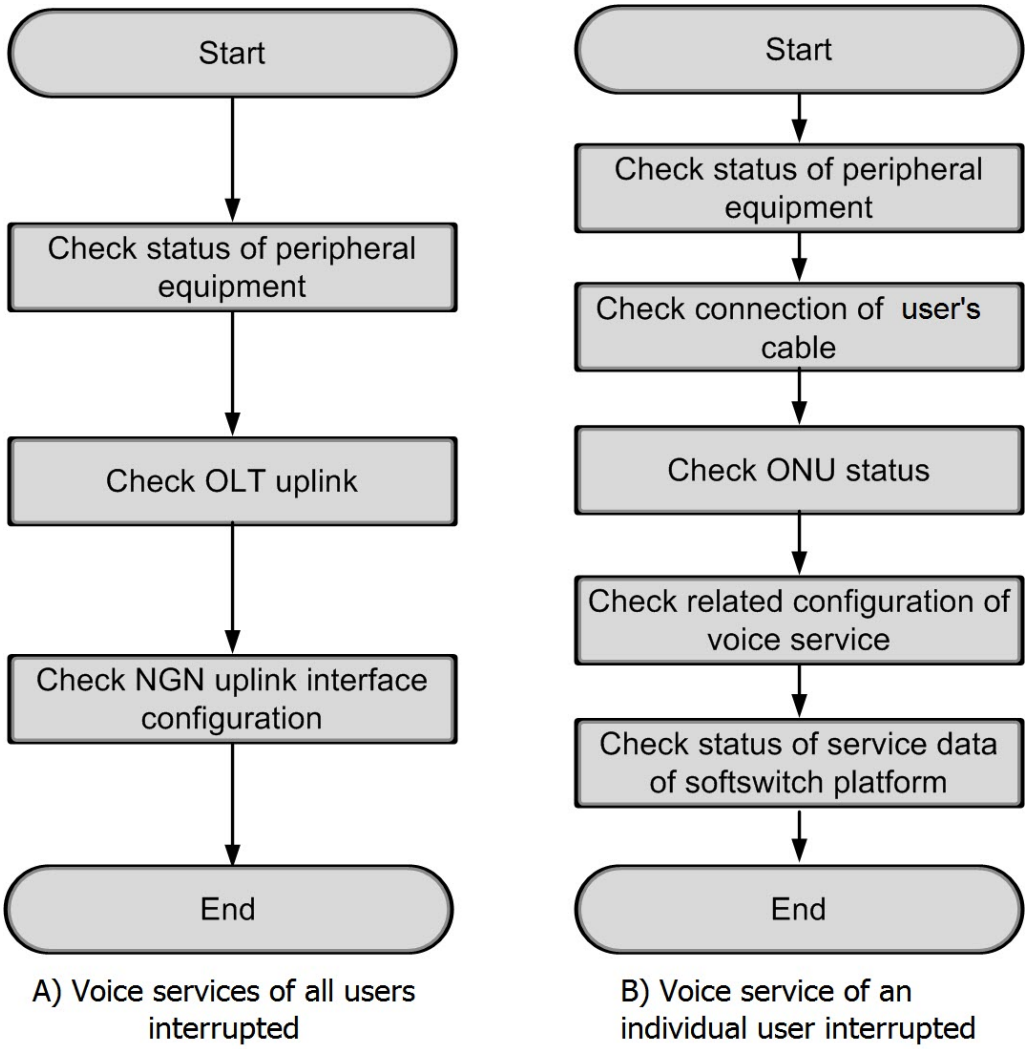


Figure 5-2 Troubleshooting flow for voice service interruption

5.2.1 Troubleshooting Voice Service of All Users

5.2.1.1 Checking Status of Peripheral Equipment

Analysis and troubleshooting

When all users' voice service is interrupted, consult maintenance personnel of the peripheral equipment to initially determine whether the fault is caused by the peripheral equipment.

Main peripheral equipment involved in voice service is shown below:

- Ethernet switch;
- Router;
- Softswitch platform.

Access method and GUI

None.

5.2.1.2 Checking OLT Uplink

Analysis and troubleshooting

The OLT voice uplink bears all voice RTP flow messages and signal messages of the ONU. Check the OLT uplink status after troubleshooting the peripheral equipment. peripheral equipment.

Refer to Step 2 of Troubleshooting Voice Service of All Users for details of checking and troubleshooting the uplink of the AN5116-06B.

Access method and GUI

None.

5.2.1.3 Checking Local End Service VLAN Data

Analysis and troubleshooting

Check the local end service VLAN data configuration to see whether the configuration of parameters such as starting VLAN ID / VLAN ID end, TAG / UNTAG, Interface No. or TRUNK Group No. is identical with the planning data.

- If the configuration is incorrect, modify it according to the planning data;
- If the configuration is correct, follow the troubleshooting procedures described in Checking Configuration of NGN Uplink Interface.

Access method and GUI

- Method for checking the local end service VLAN data is shown as follows:

Operation	Access Method
Check local end service VLAN data configuration.	Right-click the **HSWA** card in the **Object Tree** pane, and select **Config→Local VLAN→Local End Service VLAN**.

- Figure 5-3 shows the GUI for checking local end service VLAN data configuration.

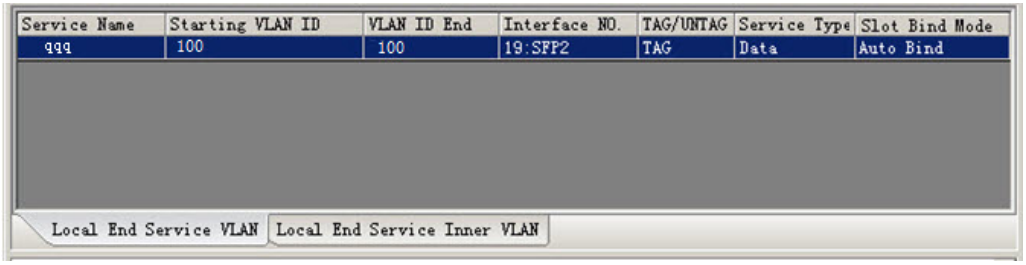


Figure 5-3 Checking local end service VLAN data configuration

5.2.1.4 Checking Configuration of NGN Uplink Interface

Analysis and troubleshooting

An error in configuring the IP address of the softswitch platform of the ONU will cause failure in establishing the link between the ONU and MGC. Log into the ONU CLI network management system via the PUBA card. Test the network connection between the ONU and the softswitch platform with the Ping command, and check whether the link between the ONU and MGC is normal.

When the ONU heartbeat is disabled, the ONU will be disconnected from the softswitch platform, and users will be unable to access the voice service.

Check configuration of the NGN uplink interface to see whether parameters such as softswitch protocol type, MGC IP address and heartbeat switch are correctly configured.

- If the configuration is incorrect, modify it according to the planning data;
- If the configuration is correct, contact FiberHome for troubleshooting.

Access method and GUI

- Method for checking the NGN uplink interface configuration data is shown below:

Operation	Access Method
Check the NGN uplink interface configuration data.	Right-click the **HSWA** card in the **Object Tree** pane and select **Voice Config→NGN Interface**.

- Figure 5-4 shows the GUI for checking the NGN uplink interface configuration data.

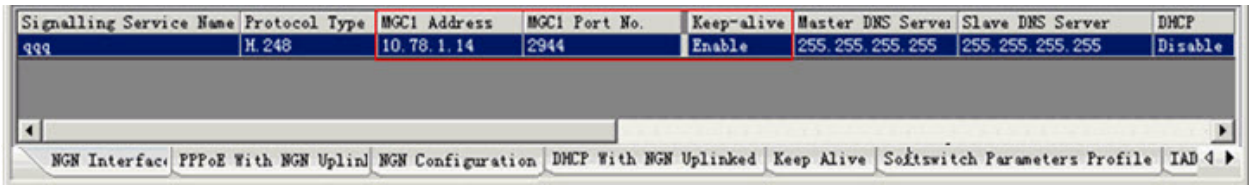


Figure 5-4 Checking the NGN uplink port configuration

5.2.2 Troubleshooting Voice Service of an Individual User

5.2.2.1 Checking Status of Peripheral Equipment

Analysis and troubleshooting

When the voice service of an individual user is interrupted, consult maintenance personnel of the peripheral equipment to initially ascertain whether the fault is caused by the peripheral equipment.

Main peripheral equipment involved in voice service is shown below:

- Softswitch platform;
- Voice gateway;
- Telephones.

Access method and GUI

None.

5.2.2.2 Checking Connection of Subscriber Line

Analysis and troubleshooting

Check whether the subscriber voice line is electrically short-circuited or broken, and whether the wiring scheme is correct.

- If the subscriber line is faulty, notify the maintenance personnel for inspection and repair;
- If the subscriber line is normal, follow the troubleshooting procedures described in Checking ONU Status.

Note:

Faults in close connection with the subscriber line include the following ones:

- No feed after off-hook;
- Excessive noise during calls;
- Connection to a wrong phone number.

Access method and GUI

None.

5.2.2.3 Checking ONU Status

Analysis and troubleshooting

Check the registration and authorization of the ONU. Refer to Checking the Registration Status of the ONU for details.

- If the ONU is not legally registered or authorized, refer to Checking the Registration Status of the ONU for troubleshooting;
- If the ONU is legally registered and authorized, refer to Checking Related Configuration of Voice Service for troubleshooting.

Access method and GUI

None.

5.2.2.4 Checking Related Configuration of Voice Service

Analysis and troubleshooting

For voice service fault encountered by an individual user, check related data configuration of the voice service after troubleshooting the subscriber line and the ONU.

- If the data configuration is incorrect, modify the configuration data via the ANM2000;
- If the configuration is correct, refer to Confirming Service Data of SoftSwitch Platform for troubleshooting.

Parameters to be checked and their influences are shown in Table 5-1.

Table 5-1 Main parameters and their influences

Main Parameter	Influence
ONU public network IP address, mask, gateway	A configuration error will cause failure in connection between the ONU and the MGC.
Endpoint domain name	A configuration error will cause a registration failure of the media gateway.
ONU protocol port	A configuration error will cause a registration failure of the media gateway.
Endpoint username	A configuration error will cause a registration failure of the port.
RTP tag format	The parameter must be configured when using H.248 protocol. A configuration error will cause a busy tone after dialing. After being configured, the intercommunication parameter template of the softswitch platform should be bound to the ONU so that the parameter can be valid. If the template is incorrectly bound or not bound to the ONU, the configured RTP resource will be invalid. Refer to *AN5116-06B Optical Line Terminal Equipment GUI Reference* for details.
Digit map	The parameter must be configured when using SIP protocol. A configuration error will cause a busy tone after dialing.

Table 5-1 Main parameters and their influences (Continued)

Main Parameter	Influence
DigitMap timer duration	A configuration error will cause abnormal receiving of the phone number on the platform, so that the call cannot be connected.
SIP telephone	The parameter must be configured when using SIP protocol. The user cannot use the telephone if the parameter is incorrectly configured.
SIP protocol attested username	The parameter must be configured when using SIP protocol. The user cannot use the telephone if the parameter is incorrectly configured.
SIP protocol attested user password	The parameter must be configured when using SIP protocol. The user cannot use the telephone if the parameter is incorrectly configured.

Access method and GUI

- The method for checking parameters such as **ONU Public IP**, **ONU Public IP Subnet**, **ONU Public IP Gateway**, **Endpoint Domain Name / SIP**, **ONU Protocol Port No.** and **Endpoint User** is shown as follows:

Operation	Access Method
Check NGN uplink user's data	Right-click the **HSWA** card in the **Object Tree** pane and select **Voice Config→NGN Configuration** from the shortcut menu.

- The GUIs for checking parameters such as **ONU Public IP**, **ONU Public IP Subnet**, **ONU Public IP Gateway**, **Endpoint Domain Name / SIP**, **ONU Protocol Port No.** and **Endpoint User** are shown in Figure 5-5 and Figure 5-6.

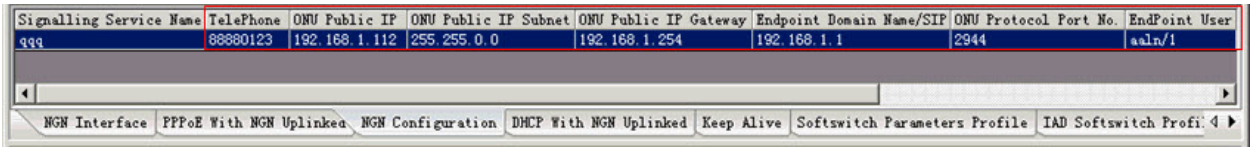


Figure 5-5 Checking NGN uplink user data (using the H.248 protocol)

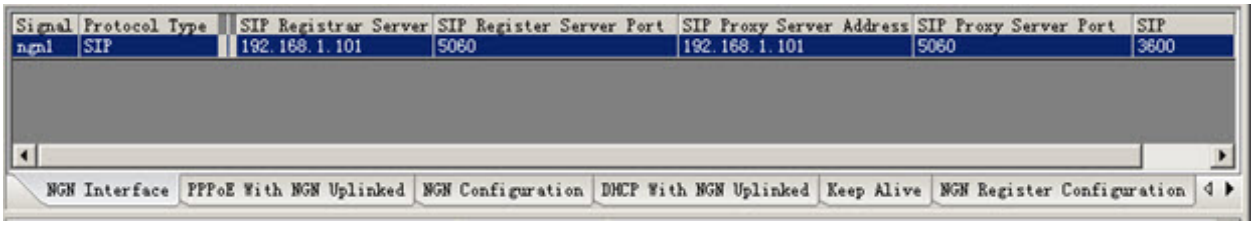


Figure 5-6 Checking NGN uplink port (using the SIP)

- The method for checking intercommunication parameter template of the softswitch platform via the network management system is shown below:

Operation	Access Method
Check the softswitch intercommunication template configuration.	Right-click the system in the **Object Tree** pane and select **Config→Profile Definition→Softswitch Parameters Profile** from the shortcut menu.

- The GUI for checking the configuration of the RTP resource tag format is shown in Figure 5-7.

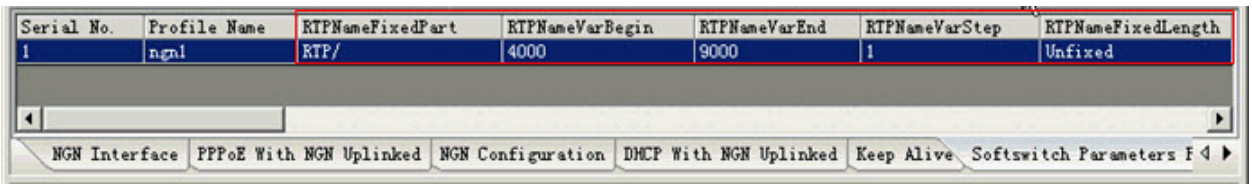


Figure 5-7 Checking the softswitch intercommunication template configuration (RTP resource)

- The GUI for checking the configuration of DigitMap timer is shown in Figure 5-8.

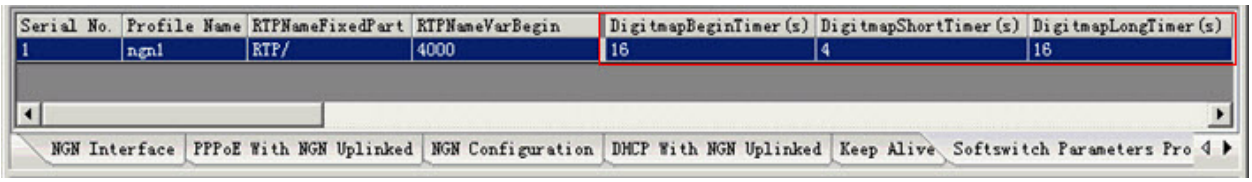


Figure 5-8 Checking the softswitch intercommunication template configuration (DigitMap timer)

5.2.2.5 Confirming Service Data of SoftSwitch Platform

Analysis and troubleshooting

Ask the maintenance personnel of the core network to check whether the data configuration on the softswitch platform is correct. Number analysis error on the MGC and abnormal user's data on HSS/SDC will influence individual user's service.

- If the softswitch platform of the core network has failed, notify the maintenance personnel for troubleshooting;
- If the softswitch platform of the core network is normal, contact FiberHome for troubleshooting.

Access method and GUI

None.

5.3 Troubleshooting Common Faults

5.3.1 Busy Tone or No Tone after Picking Up the Telephone

Fault symptom

The user hears a busy tone or no tone after picking up the telephone.

Fault analysis

- Configuration of the heartbeat parameter is incorrect. If heartbeat timeout is set to 0, the ONU will send a port registration message together with a heartbeat command. This will cause the endpoint status reset. Then the user will hear a busy tone after picking up the telephone.
- Configuration of the ONU endpoint domain name is incorrect, which results in unsuccessful registration on the softswitch platform.
- The endpoint user's port name for the ONU POTS port is not identical with that on the softswitch platform.

Troubleshooting procedure

1. Check the heartbeat mechanism settings. Set the heartbeat time-out to 3. If the fault persists after this operation, go to Step 2.

   The access method is shown in the table below.

Operation	Access Method
Check the NGN heartbeat parameter.	Right-click the **HSWA** card in the **Object Tree** pane and select **Voice Config→Keep Alive** from the shortcut menu.

   The operation GUI is shown in Figure 5-9.

Figure 5-9 Checking the NGN heartbeat parameter

2. Check the domain name of the ONU endpoint and configuration of the port domain name. See Checking Related Configuration of Voice Service for details.
3. Contact FiberHome if the above steps do not work.

5.3.2 Dial Tone Cannot Be Cut Off After Dialing

Fault symptom

The dial tone cannot be cut off after dialing.

Fault analysis

- The telephone dial mode is set to pulse dialing while the ONU voice port only supports DTMF dialing;
- A telephone extension on this line has not been hung up.

Troubleshooting procedure

1. Check the telephone dialing mode. The P on the switch key indicates pulse dialing; and the T indicates DTMF dialing. If the switch is at the option P, switch it to the option T. If the fault persists after this operation, go to Step 2.
2. Check all telephones (including extensions) on this line to see whether they have been hung up. After making sure that all telephones have been hung up, dial again. If the fault persists after this operation, go to Step 3.
3. Contact FiberHome if the above steps do not work.

5.3.3 Busy Tone after Calling Dial

Fault symptom

The user hears a busy tone after dialing a phone number, which is not busy then.

Fault analysis

- An error in configuration of RTP resource name;
- Incorrect configuration of the DigitMap timer, long timer and short timer;
- Incorrect configuration of telephone numbers for the voice service on the FTTH-type ONU;
- Incorrect DigitMap configuration when the SIP protocol is used.

Troubleshooting procedure

1. Check the configuration of the fixed part of the RTP resource name, long and short dialing timers. In case of inconsistency, modify the configuration accordingly. See Checking Related Configuration of Voice Service for details.
2. Check whether the voice service telephone number configured on the FTTH–type ONU is identical with that on the softswitch platform; if not, modify it accordingly. See Checking Related Configuration of Voice Service for details.
3. When using SIP protocol, check whether the dialing rules in the DigitMap configuration is reasonable; if not, make corrections. See Checking Related Configuration of Voice Service for details.
4. Contact FiberHome if the above steps do not work.

5.3.4 One-way Call Phenomenon

Fault symptom

Only one side of the telephone can hear the voice of the other side after the connection is made.

Fault analysis

- A network IP address conflict;

- A media server configuration error;
- A line fault;
- A telephone fault.

Troubleshooting procedure

1. Mirror the uplink port data of the AN5116-06B to an idle uplink port, conduct packet capture via a corresponding software, and check the RTP data messages.
   - Go to Step 3 if the RTP flow is bidirectional;
   - If the RTP flows are unidirectional, check whether the valid IP address of the equipment conflicts with the IP address of other equipment. The MAC address associated with the IP address can be viewed on the softswitch platform. Check whether this MAC address is identical with the actual MAC address of the equipment. Inconsistency between the MAC addresses indicates that the IP address of the equipment conflicts with other equipment. Modify the equipment IP address accordingly. If the fault persists after this operation, go to Step 2.
2. Troubleshoot unidirectional RTP flow.
   - If the ONU equipment can send RTP data messages normally but cannot receive RTP data messages,

     contact the maintenance personnel of the softswitch platform to check and determine whether the media server has filtered the RTP data messages.
   - If the ONU equipment can receive RTP data messages normally but cannot send RTP data messages,
     - mirror the uplink port data of the AN5116-06B to an idle uplink port, conduct packet capture via a corresponding software, and check whether the ONU equipment ends RTP data messages. If the ONU sends RTP data messages but receives no response, contact the related party to find out the causes.
     - Test the network connection between the ONU and the far end voice gateway equipment via a Ping command. If the connection is normal, but the ONU does not send RTP data messages, check whether the far end softswitch platform changes the RTP mode into the transmit mode.

- If the far end platform is in the transmit mode and the equipment still does not send RTP data messages, contact FiberHome for troubleshooting.

3. In the event that the telephone is faulty, substitute a known good telephone for the suspected one.
   - If the voice service recovers after substitution, the telephone must be faulty.
   - If the voice service is still abnormal, the fault may be caused by cross or electrical short-circuit of the external subscriber lines. Contact related maintenance personnel for troubleshooting.
4. Contact FiberHome if the above steps do not work.

5.3.5 Intra-system Users Disconnected

Fault symptom

The voice user can hear a dial tone after picking up the telephone. But the ONU fails to get connected with another user in the AN5116-06B system.

Fault analysis

- The subscriber number of the called ONU is incorrectly configured;
- The ONU is not registered with the PUBA card of the AN5116-06B;
- The ONU equipment is faulty.

Troubleshooting procedure

1. Check whether the number of the called party has been assigned to the expected ONU. If the number is not assigned or is incorrectly configured, reconfigure the ONU voice service. Refer to *AN5116-06B Optical Line Terminal Equipment EPON Configuration Guide* and *AN5116-06B Optical Line Terminal Equipment GPON Configuration Guide* for details.
2. If the ONU is faulty or cannot be registered with the PUBA card of the AN5116-06B (the REG LED on the ONU keeps blinking or blacks out), contact FiberHome for troubleshooting.

5.3.6 The Dialed Number Not Existing

Fault symptom

When calling a subscriber telephone, the caller receives a prompt that “The subscriber you have dialed does not exist.”

Fault analysis

The softswitch platform has not configured the subscriber’s number.

Troubleshooting procedure

Ask maintenance personnel of the softswitch platform to configure the subscriber’s number.

5.3.7 No Dial Tone When Picking Up Telephone

Fault symptom

A voice service subscriber picks up the telephone and hears no dial tone.

Fault analysis

Possible causes are as follows:

- A fault occurs in the subscriber's telephone;
- The cable connection at the POTS port is incorrect;
- Communication between the MGC and the ONU is interrupted;
- The ONU voice service configuration is incorrect.

Troubleshooting procedure

1. Check the telephone.
   - If the telephone is faulty, replace it.
   - If the telephone is normal, go to Step 2.
2. Check the cable connection at the POTS port.

- If the cable connection is abnormal, ask the external line maintenance personnel to recover the normal cable connection at the port.
- If the cable connection is normal, go to Step 3.

3. Check whether the communication between the MGC and the ONU is normal by logging into the ANM2000 and checking the registration of the ONU with the MGC and the NGN user's port status.
   - If the MGC registration is unsuccessful or the port is in an abnormal status, check the configuration of the NGN uplink interface and the uplink user's data.
   - If the ONU has registered successfully and the port is in a normal status, go to Step 4.

   The method for checking the MGC and port status is shown below:

Operation	Access Method
Show the status of the MGC registration server.	Right-click the **HSWA** card in the **Object Tree** pane, select **Get Information→NGN Status** from the shortcut menu, and click the **MGC/Registrar Server Status** tab.
Show NGN user's port status.	Right-click the **HSWA** card in the **Object Tree** pane, select **Get Information→NGN Status** from the shortcut menu, and click the **NGN User Port Status** tab.

The operation GUIs are shown in Figure 5-10 and Figure 5-11.

Figure 5-10 Showing status of the MGC registration server

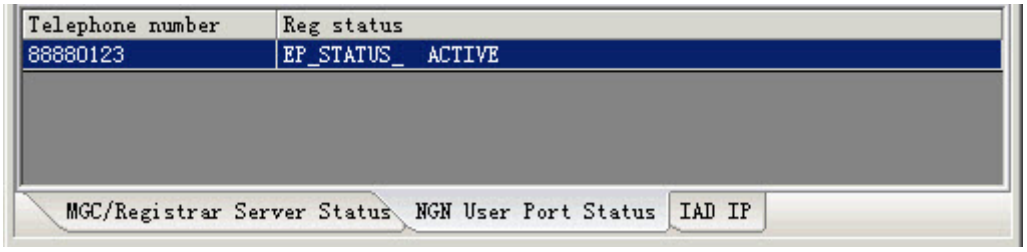


Figure 5-11 Showing NGN user's port status

4. Check the voice service configuration. Refer to Troubleshooting Voice Service of an Individual User for details.
5. Contact FiberHome if the above steps do not work.

5.3.8 Excessive Noise During Calls

Fault symptom

A subscriber hears excessive noise during calls.

Fault analysis

- A fault occurs in the subscriber's telephone;
- Silence suppression algorithm is set for the ONU POTS port. This leads to the packet jitter in the network which can raise the noise level;
- The protection earth ground cable for the ONU equipment is poor. This causes current noise.

Troubleshooting procedure

1. Check the subscriber's telephone. Replace the telephone to see whether the fault is eliminated. If there is still too much noise, go to Step 2.
2. Disable the silence suppression and check whether the fault is eliminated. If there is still too much noise, go to Step 3.

   The method for disabling the silence suppression is shown below:

Operation	Access Method
Turn off the silence suppression.	Click the EPON interface card in the **Object Tree** pane, and then right-click the ONU AN5006-04, select **Config→Port Service Config** from the shortcut menu, then click the **Voice Config** tab in the window that appears.

   The operation GUI is shown in Figure 5-12.

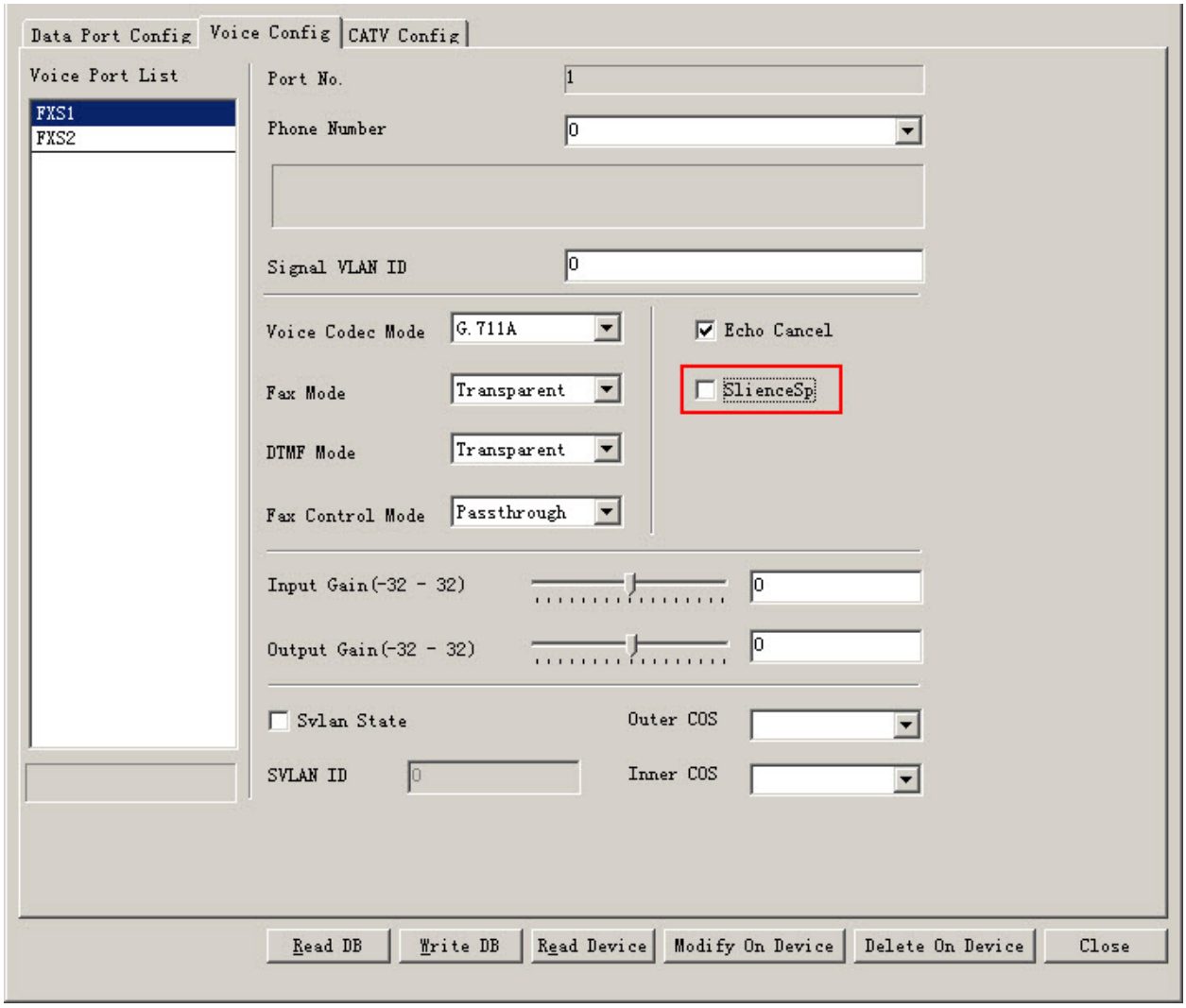


Figure 5-12 Disabling silence suppression

3. Check the corridor type ONU, and make sure that the earth grounding for the ONU is proper. If excessive noise remains, go to Step 4.
4. Contact FiberHome if the above steps do not work.

5.3.9 Echo During Conversation

Fault symptom

The subscriber can hear his or her own voice after a few seconds' delay in a call.

Fault analysis

The echo suppression function of the equipment is not activated.

Troubleshooting procedure

1. Log into the ANM2000 and activate the echo suppression function of the ONU.

   The method for configuring the echo suppression is shown below:

Operation	Access Method
Activate echo suppression (taking the AN5006-04 as an example).	Click the EPON interface card in the **Object Tree** pane, and then right-click the ONU AN5006-04, select **Config→Port service config** from the shortcut menu, then click the **Voice Config** tab in the window that appears.

   The operation GUI is shown in Figure 5-13.

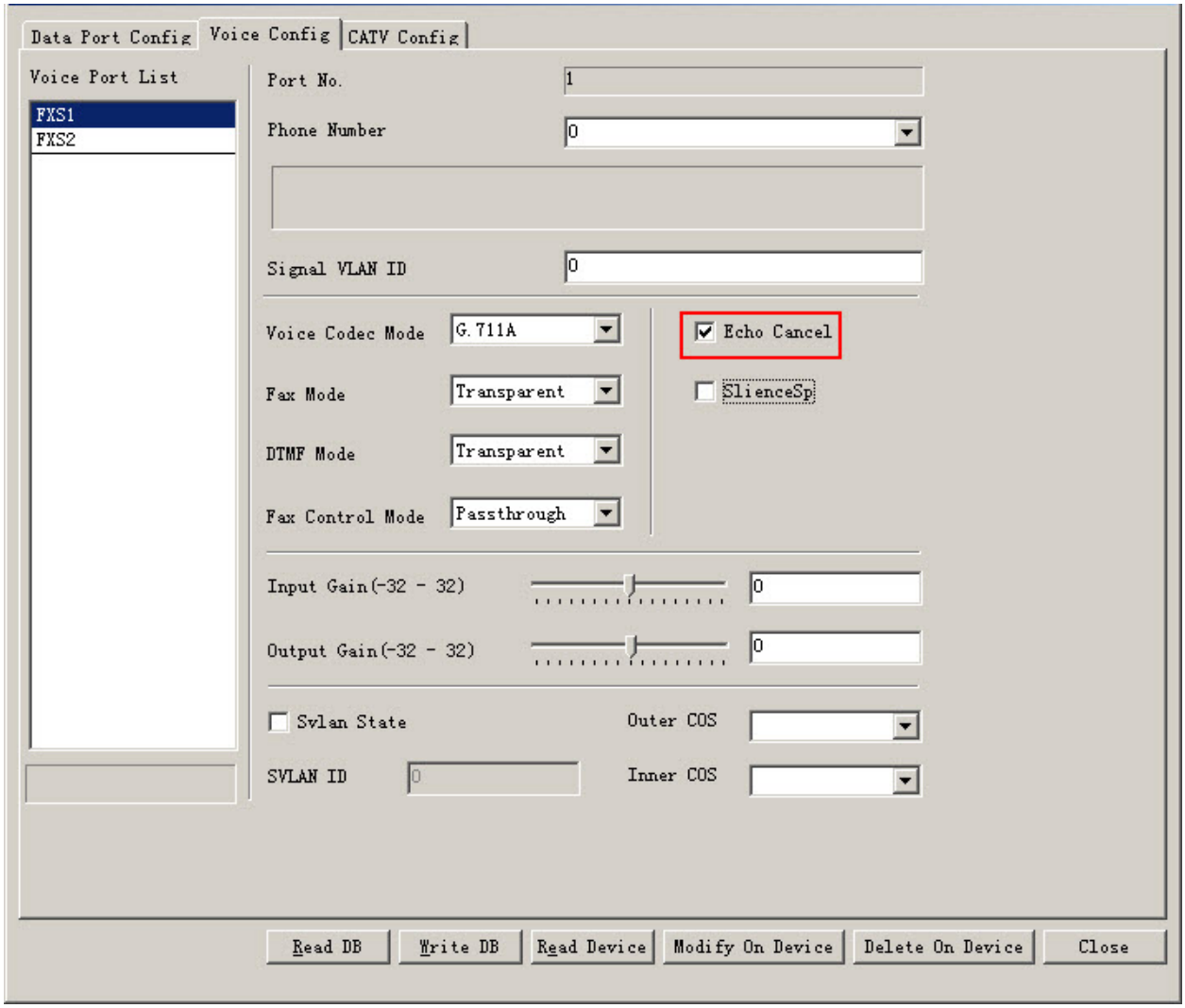


Figure 5-13 Enabling echo suppression

2. Contact FiberHome if the above steps do not work.

5.3.10 Abnormal Interruption in Long-Term Conversation

Fault symptom

The call is automatically and regularly interrupted after establishing normal communication for a period.

Fault analysis

Heartbeat settings for the ONU and the softswitch platform MGC are not identical.

Troubleshooting procedure

Modify the heartbeat settings of the ONU and make them identical with those of the MGC. Refer to Busy Tone or No Tone after Picking Up the Telephone for details on how to make the heartbeat settings.

5.3.11 Abnormal Ring Back Tone

Fault symptom

When the subscriber is making a call, he or she can not hear the ring back tone or the ring back tone is abnormal. However, when the called party pick up the telephone, the two parties can communicate normally with each other.

Fault analysis

- The subscriber's telephone is faulty;
- The external line is faulty;
- The signaling interaction between the ONU and the MGC is abnormal.

Troubleshooting procedure

1. Check whether the subscriber's telephone is faulty. If so, replace the faulty telephone with a good one. If the fault remains after this operation, go to Step 2.
2. Use a telephone to test whether the POTS port of the ONU equipment is normal.
   - If the ring back tone at the ONU port is normal, the external line is faulty, go to Step 3.
   - If the ring back tone at the ONU port is abnormal, the fault exists in the POTS port of the ONU equipment. Replace the ONU. If the fault persists after this operation, go to Step 5.
3. Check whether the external line is short-circuited or incorrectly connected.

- If the external line is faulty, contact related maintenance personnel for troubleshooting;
- If the external line is normal, go to Step 4.

4. Mirror the uplink port data of the AN5116-06B to an idle uplink port, conduct packet capture via a corresponding software, and check whether the softswitch platform delivers the ring back tone signaling messages.
   - If the softswitch platform does not deliver the ring back tone signaling messages, contact the softswitch platform maintenance personnel for troubleshooting;
   - If the softswitch platform delivers the ring back tone signaling messages, contact FiberHome for troubleshooting;
5. Contact FiberHome if the above steps do not work.

5.3.12 Abnormal Three-Party Service

Fault symptom

- Symptom 1: The two-way conversation can be established. However, there is no dial tone after the caller sends a flash hook signal to establish a three-party conversation;
- Symptom 2: The two-way conversation can be established, and there is a dial tone after the caller sends a flash hook signal to establish a three-party conversation. But no response is received after dialing;
- Symptom 3: The three-party conversation can be established. However, when the caller only needs to talk with one party, he or she cannot switch between the two called parties after sending a flash hook signal and dialing the 2 key.

Fault analysis

- The ONU equipment does not report the flash-hook event to the softswitch platform correctly.
- The softswitch platform does not deliver the dialing plan or dial tone after the ONU equipment reports the flash-hook event.

Troubleshooting procedure

1. Mirror the uplink port data of the AN5116-06B to an idle uplink port, and perform packet capture via a corresponding software to analyze the signaling flow during the three-party service.
   - In Symptom 1, the ONU equipment does not report the flash-hook event to the softswitch platform. The fault lies in the ONU equipment. Contact FiberHome for troubleshooting;
   - In Symptom 2, the ONU equipment reports the flash-hook event but the softswitch platform does not deliver the dialing plan and dial tone. The fault lies in the softswitch platform. Contact related softswitch platform maintenance personnel for repair;
   - In Symptom 3, the ONU equipment does not report the phone number correctly or the softswitch platform does not response correctly after the calling party sends the flash hook signal and dials the 2 key. Contact related maintenance personnel for repair.

5.3.13 Fax Service Failure

Fault symptom

In faxing, the caller dials the fax number and sends a fax after the called party rings. However, the called party fails to receive the fax, and the fax machine gives the prompt message **received failed**.

Fault analysis

- A fault occurs in the voice service;
- The fax modes set for the calling and called parties are inconsistent. The fax modes include the transparent fax mode (T.30) and the T.38 mode.
  - In the T.30 mode, VBD can be enabled or disabled, and the default setting is enabled. The T.30 mode supports the G711A/U encoding mode only.
  - In the T.38 mode, the G711A/U, G.723 and G.729 encoding modes are supported.
- The intervals of VBD transmitting / receiving packets are inconsistent.

Troubleshooting procedure

1. Set up a voice call and check whether the voice service is normal.
   - If no, refer to the relevant section in troubleshooting voice service faults with the same fault symptom to resume the normal voice service.
   - If yes, go to Step 2.
2. Check the fax modes of the calling and called parties.
   - If the fax modes on the two parties are inconsistent, make modifications accordingly.
   - If the fax modes on the two parties are consistent, go to Step 3.

   The method for checking the fax mode is shown below:

Operation	Access Method
Port service configuration	Click the **EC8B** card in the **Object Tree** pane, and then right-click the ONU, select **Config→Port Service Config** from the shortcut menu, and then click the **Voice Config** tab in the window that appears.

   The operation GUI is shown in Figure 5-14.

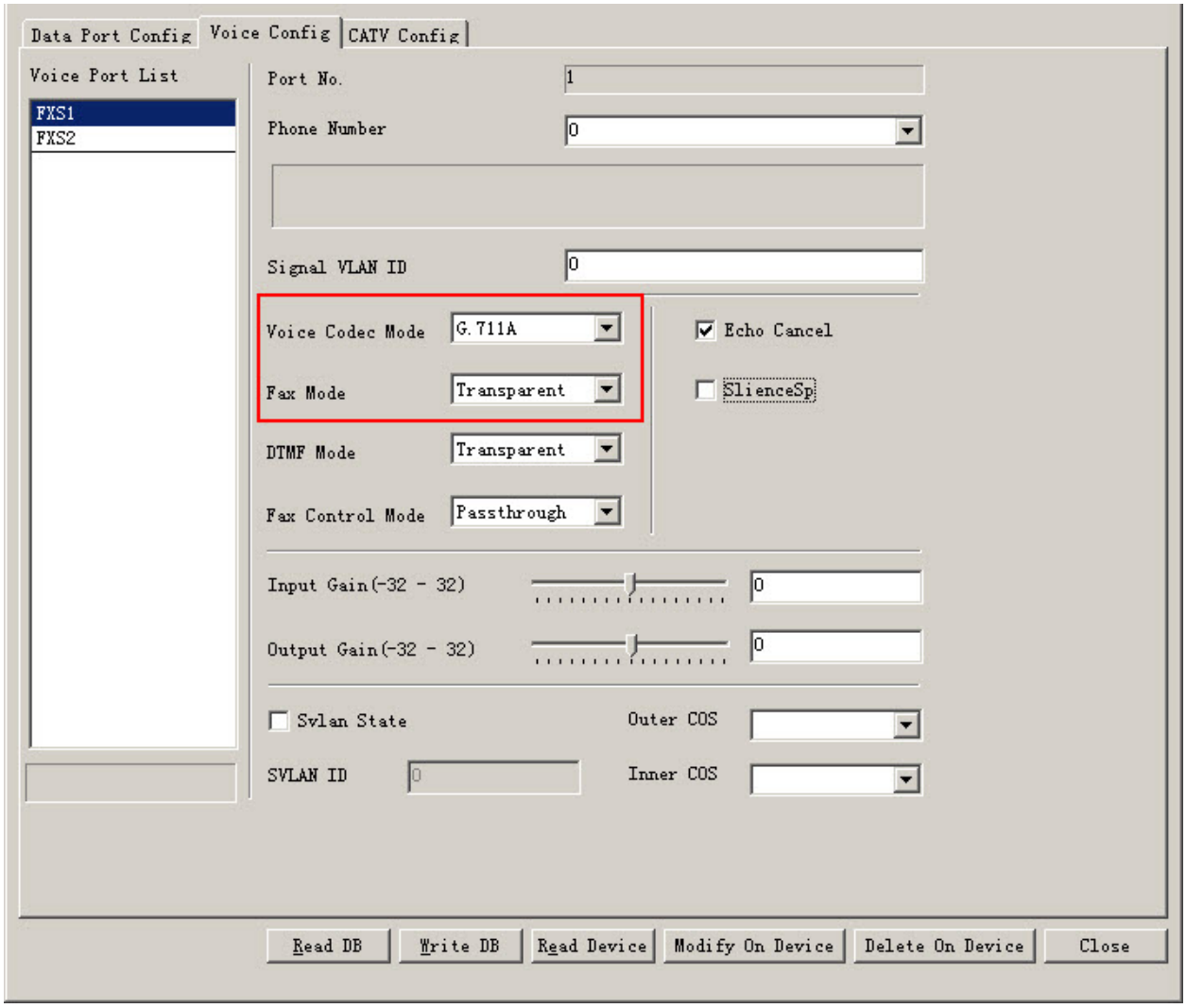


Figure 5-14 Port service configuration (fax mode)

3. Check VBD receiving / transmitting packet interval.

   Mirror the AN5116-06B's uplink port data to an idle uplink port, and perform the packet capture test via the packet capture software, checking whether the encoding mode of the RTP flow packets and interval of receiving / transmitting packets are consistent with those set for the AN5116-06B.

   Check the remote end media packet interval. If the fax machine switches to the T.30 mode and the packet receiving interval of the remote end voice gateway equipment changes, the VBD mode of the ONU should be enabled.

Caution:

In the T.30 mode, the packet receiving / transmitting interval of the Huawei softswitch platform is 20 ms and that of Bell is 10 ms. To achieve intercommunication between FiberHome and Huawei and Bell, the VBD mode of the ONU should be enabled. And the packet intervals should be set to 10ms and 20 ms correspondingly.

The VBD mode configuration method is shown below:

Operation	Access Method
Configure packet receiving / transmitting interval	Right-click the system in the **Object Tree** pane and select **Config→Profile Definition→Softswitch Parameters Profile**.

The operation GUI is shown in Figure 5-15.

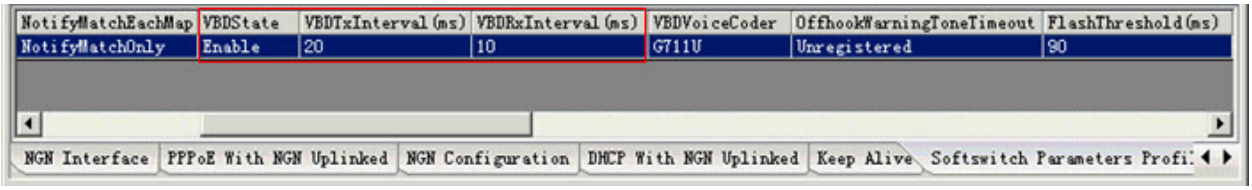


Figure 5-15 Packet transmitting interval

4. Contact FiberHome if the above steps do not work.

6 Troubleshooting Multicast Service Faults

This chapter introduces how to troubleshoot multicast service faults of the AN5116-06B.

☑ Background Knowledge

☑ Troubleshooting Flow

☑ Troubleshooting Common Faults

6.1 Background Knowledge

Multicast service network of the AN5116-06B is shown in Figure 6-1.

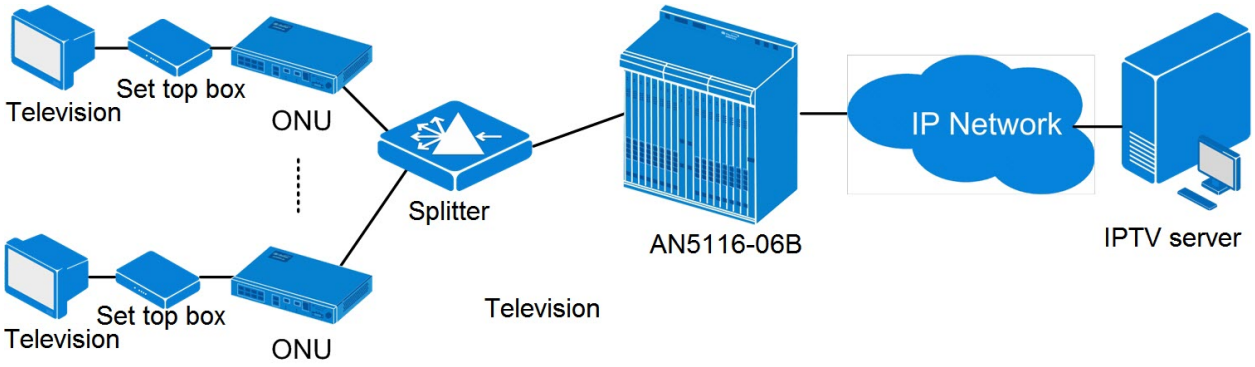


Figure 6-1 Multicast service networking

There are multiple modes for delivering multicast service using the AN5116-06B system, as shown in Table 6-1.

Table 6-1 The multicast service modes using the AN5116-06B

Multicast Service Mode	Card and ONU Work Mode		
	Core Switch Card	PON Interface Card	ONU
IGMP Proxy-proxy	Proxy	Proxy	Snooping
IGMP Proxy-snooping	Proxy	None	Snooping
IGMP Snooping	Snooping	None (broadcast)	Snooping
Controllable multicast	Proxy	Proxy	None, transfer based on rules
IGMP Disable	Disable	Snooping	Snooping

6.2 Troubleshooting Flow

The AN5116-06B provides multicast services in five modes. This section uses the controllable mode as an example. Troubleshooting of multicast faults in other modes can follow the same troubleshooting procedure.

The troubleshooting flow for multicast service interruption is shown in Figure 6-2.

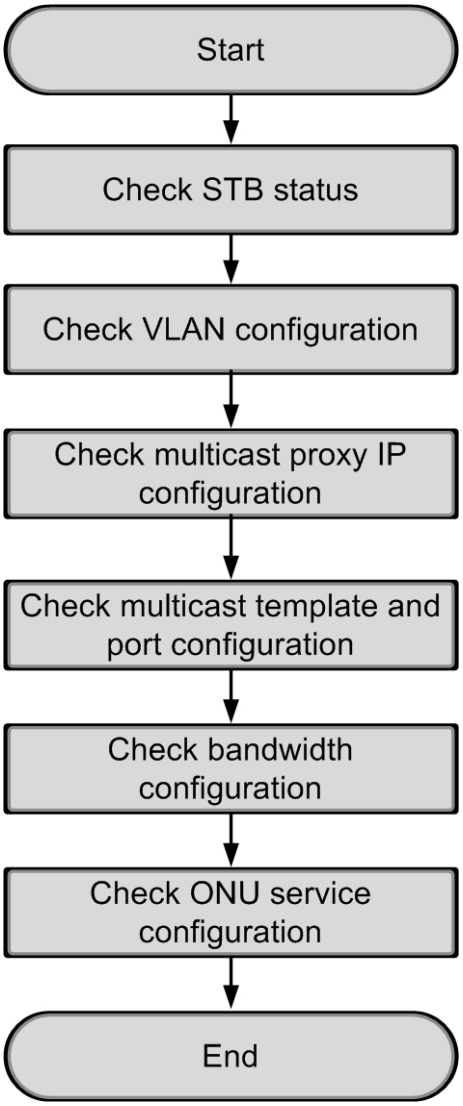


Figure 6-2 Troubleshooting flow for multicast service

6.2.1 Checking STB Status

Analysis and troubleshooting

Check the user's STB and isolate the fault by substituting a known good STB.

- If the STB is abnormal, repair or replace the STB;
- If the STB is normal, refer to Checking VLAN Configuration for troubleshooting.

6.2.2 Checking VLAN Configuration

Analysis and troubleshooting

Check whether the configuration of the user's multicast VLAN ID and service VLAN ID is identical with the planning data. The multicast VLAN ID should be within the service VLAN ID scope.

- If the configuration is unreasonable, modify it via the ANM2000.
- If the configuration is correct, refer to Checking Configuration of Multicast Proxy IP Address for troubleshooting.

Access method and GUI

- The method for checking the local end service VLAN data is shown as follows:

Operation	Access Method
Checking Local End Service VLAN Data	Right-click the HSWA card in the **Object Tree** pane and select **Config→Local VLAN→Local End Service VLAN**.

- Figure 6-3 shows the GUI for checking the local end service VLAN data.

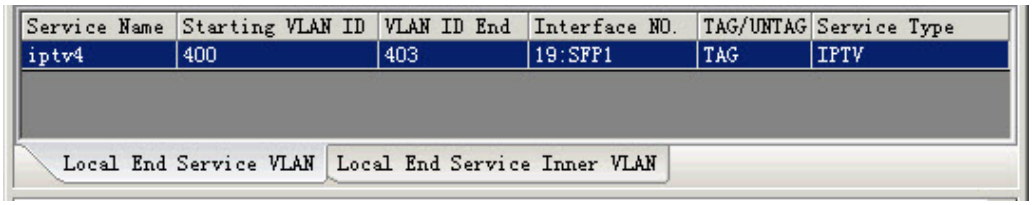


Figure 6-3 Checking local end service VLAN data

- The method for checking the multicast VLAN data is shown below:

Operation	Access Method
Checking multicast VLAN configuration	Right-click the HSWA card in the **Object Tree** pane and select **Config→IGMP Config→Multicast VLAN**.

- The operation GUI for checking the multicast VLAN data is shown in Figure 6-4.

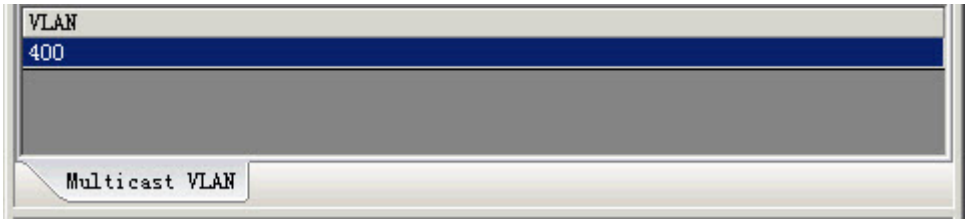


Figure 6-4 Checking multicast VLAN configuration

6.2.3 Checking Configuration of Multicast Proxy IP Address

Analysis and troubleshooting

When the core switch card works under the proxy mode, check the proxy IP address of the core switch card. The multicast proxy IP address and the IP address of the previous device should be in the same network segment.

- If the configuration is incorrect, modify it via the network management system.
- If the configuration is correct, refer to Checking Multicast Profile and Port Configuration for troubleshooting.

Access method and GUI

- The method for checking the service multicast proxy IP address is shown below:

Operation	Access Method
Checking configuration of multicast proxy IP address	Right-click the HSWA card in the **Object Tree** pane and select **Config→IGMP Config→Multicast Proxy IP**.

- The operation GUI for checking the service multicast proxy IP address is shown in Figure 6-5.

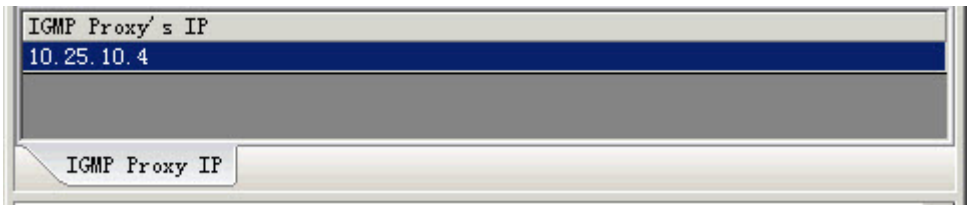


Figure 6-5 Checking configuration of multicast proxy IP address

6.2.4 Checking Multicast Profile and Port Configuration

Analysis and troubleshooting

Check the settings of the following parameters:

- The multicast group IP address and the corresponding authority settings;
- The preview duration and times of controllable multicast;
- The port bandwidth configuration of the ONU and the maximum number of online groups.

If the settings are incorrect, make corrections; if the settings are correct, follow Checking Bandwidth Configuration for troubleshooting.

Access method and GUI

- The method for checking the multicast profile and port configuration is shown below:

Operation	Access Method
Checking multicast profile and port configuration	Right-click the HSWA card in the **Object Tree** pane and select **Config→IGMP Config→IGMP Profile and Port**.

- The operation GUIs for checking the multicast profile, group parameter configuration and port parameter configuration are shown in Figure 6-6, Figure 6-7 and Figure 6-8. The main parameters are shown in the red frame.

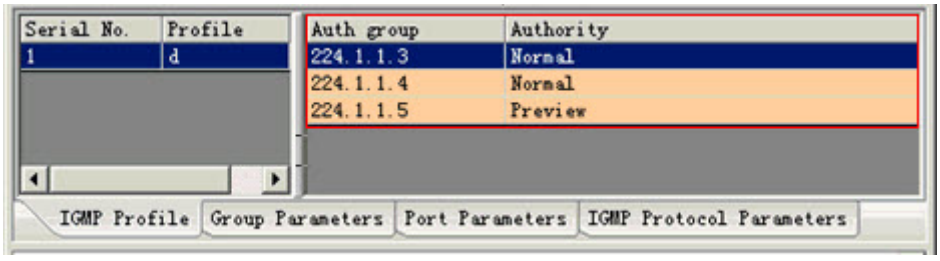


Figure 6-6 Checking multicast profile configuration

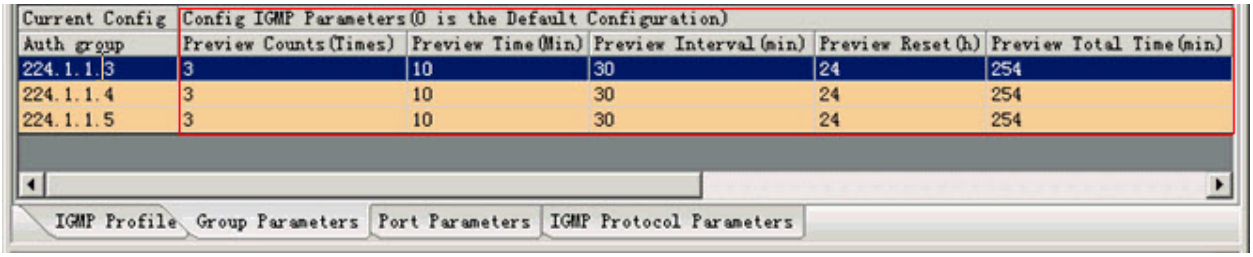


Figure 6-7 Checking group parameter configuration

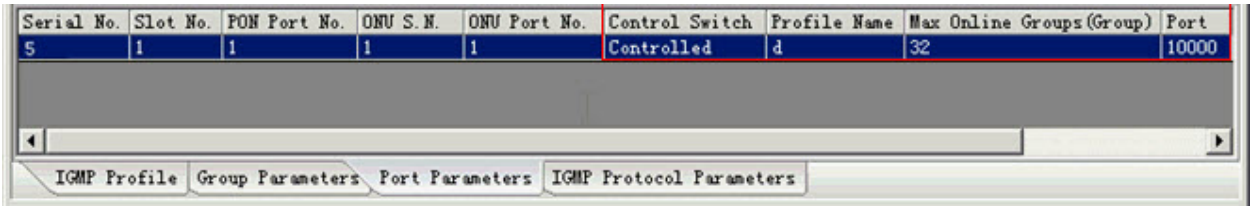


Figure 6-8 Checking port parameter configuration

6.2.5 Checking Bandwidth Configuration

Analysis and troubleshooting

Check the uplink interface bandwidth configuration. The set bandwidth should be greater than the total of program bandwidths. Otherwise, the uplink interface will not be able to carry the programs.

- If the set bandwidth is too low, make corrections;
- If the set bandwidth is reasonable, follow Checking ONU Service Configuration for troubleshooting.

Access method and GUI

- The method for checking the uplink interface bandwidth is shown below:

Operation	Access Method
Checking the maximum multicast bandwidth of the uplink interface	Right-click the HSWA card in the **Object Tree** pane and select **Config→IGMP Config→GMP Cascade Ports** from the shortcut menu. Then click the **Max. Uplink IGMP Bandwidth** tab.

- Figure 6-9 shows the GUI for checking the he uplink interface bandwidth.

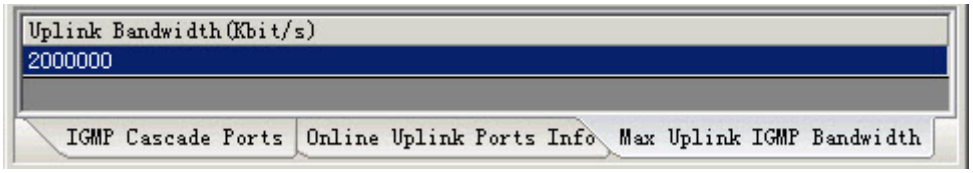


Figure 6-9 Checking total bandwidth configuration of uplink port

6.2.6 Checking ONU Service Configuration

Analysis and troubleshooting

Check the VLAN mode, multicast VLAN ID and VLAN translation on the ONU.

The AN5116-06B system handles VLAN tags in the following ways:

- For an FTTB Type ONU, the VLAN mode is **tag**, and a VLAN ID added to the message via the home gateway is translated into a multicast VLAN ID;
- For an FTTH Type ONU, the VLAN mode is **tag**; and the ONU adds a multicast VLAN ID as service VLAN.

If the configuration is incorrect, make corrections; if the configuration is correct and the fault persists after the aforesaid operations, contact FiberHome for troubleshooting.

Access method and GUI

- The method for checking the ONU multicast service configuration is shown below:

Operation	Access Method
Checking ONU service configuration	In the **Object Tree** pane, right-click the PON interface card to display all ONUs connected to the PON interface card in the right pane. Right-click the object ONU and select **Config→Port Service Config** from the shortcut menu. Then select the **Data Port Config** tab.

- The GUIs for checking the ONU multicast service are shown in Figure 6-10 and Figure 6-11.

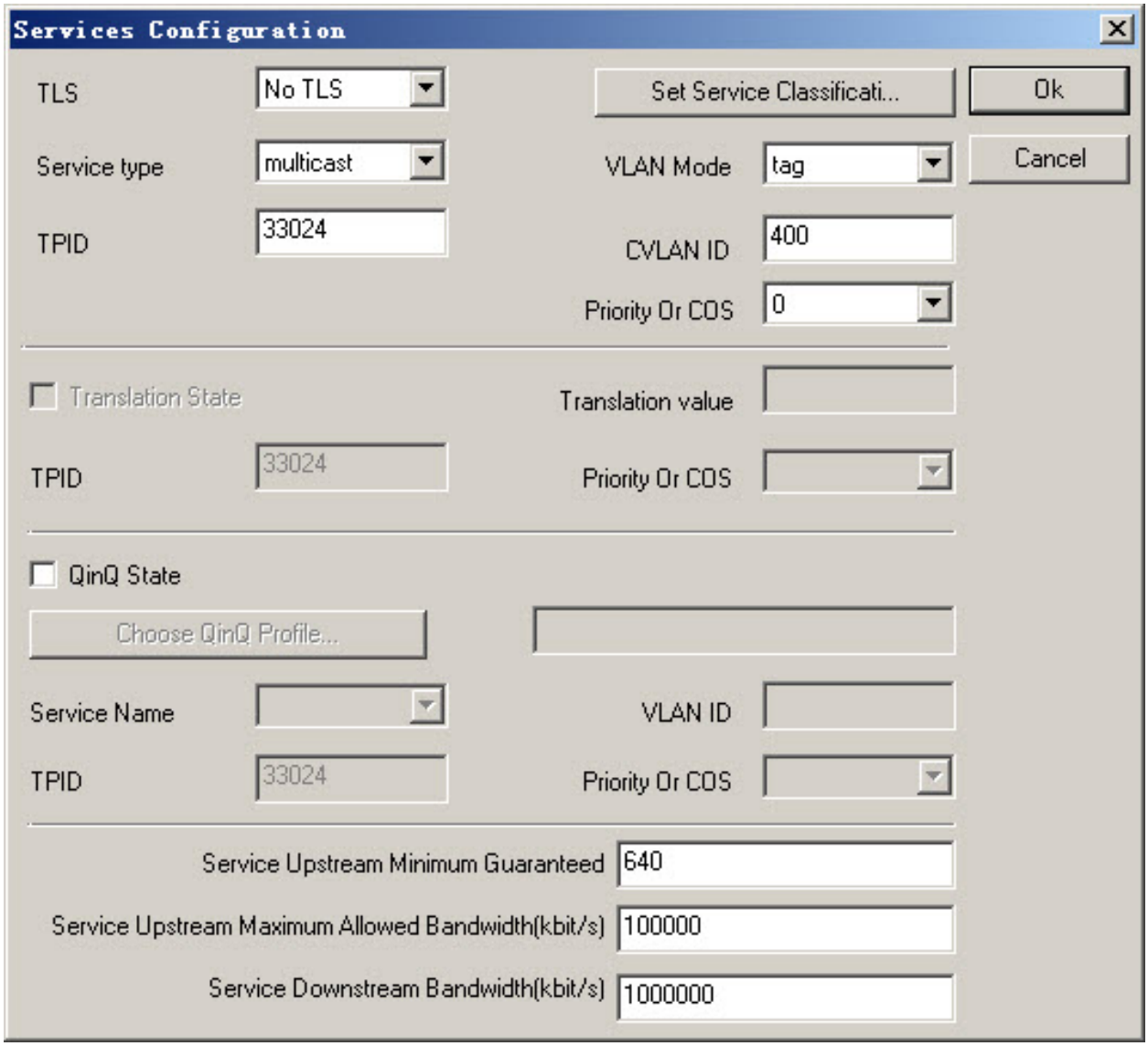


Figure 6-10 Checking ONU multicast service configuration (taking the FTTH mode as an example)

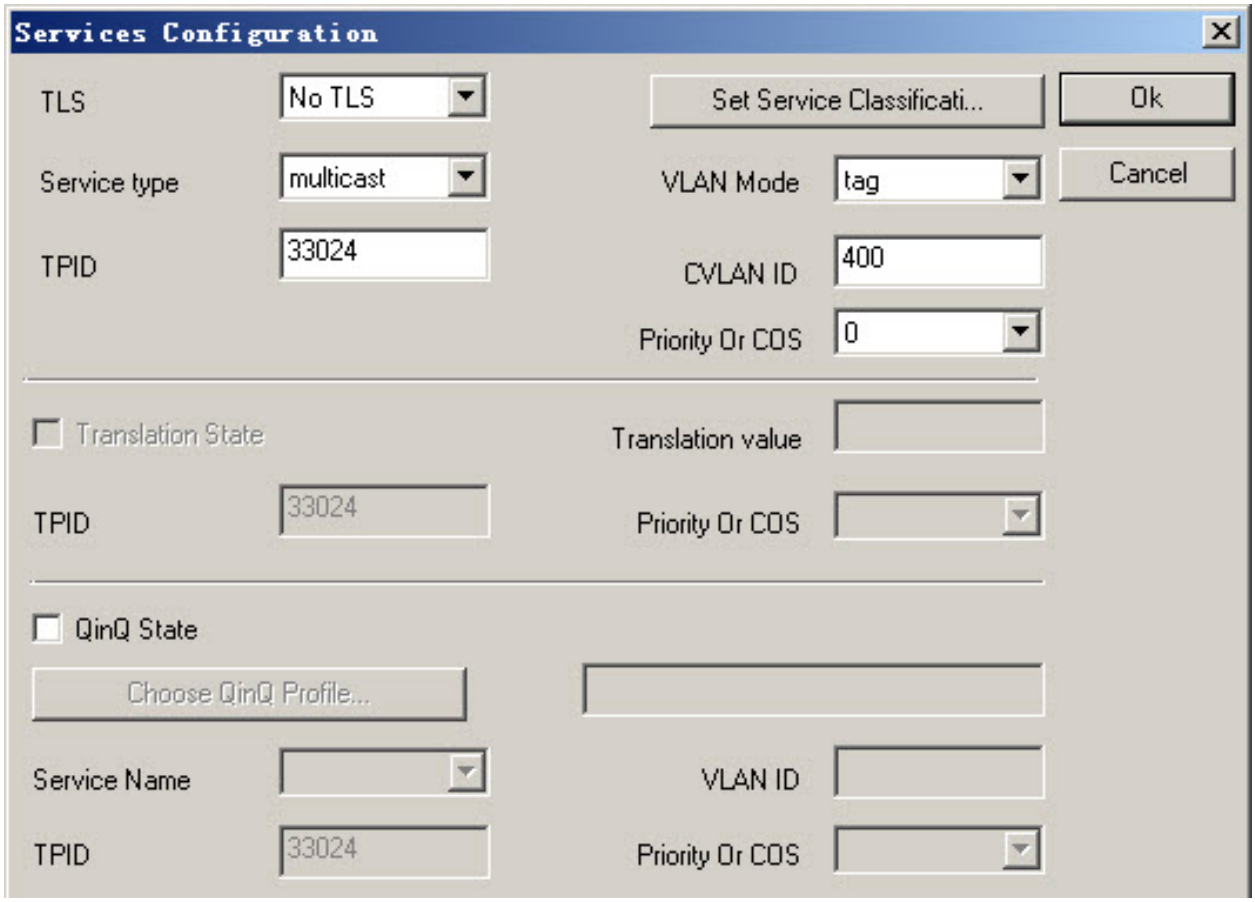


Figure 6-11 Checking ONU multicast service configuration (taking the FTTB mode as an example)

6.3 Troubleshooting Common Faults

This section introduces common faults in multicast service, and procedures for fault analysis and troubleshooting.

6.3.1 Failure to Go Online

Fault symptom

The subscriber fails to go online.

Fault analysis

- A fault occurs in the ONU.
- The subscriber terminal is faulty.
- Configuration of the multicast program or the group VLAN is incorrect.
- In the controllable mode, the subscriber has no authority to watch the program.
- In the controllable mode, the subscriber has the authority for watching the program, but the viewing time and number of times that the user views the program cross the preset value.
- In the controllable mode, the configuration of the ONU port multicast bandwidth is unreasonable.

Troubleshooting procedure

1. Check whether the ONU is working normally.
   - If yes, go to Step 2;
   - If no, check and repair the ONU or replace it.
2. Check whether the subscriber terminal is working normally.
   - If yes, go to Step 3;
   - If no, check and repair the subscriber terminal or replace it.
3. Check whether the multicast program is correctly configured, and whether the VLAN of the multicast uplink protocol message is consistent with the VLAN of the multicast stream.
   - If this multicast program is incorrectly configured, check whether the VLAN of this multicast stream is consistent with the multicast global VLAN. Only when the two VLANs are consistent can the multicast path be established.
   - If the multicast program is correctly configured, check whether the VLAN of the multicast uplink protocol message is consistent with the VLAN of this multicast stream. Only when the two VLANs are consistent can the multicast path be established.
4. If the multicast service of the AN5116-06B is in the controllable mode, check whether the subscriber has the watching authority.

5. If the AN5116-06B is in the controllable mode and the subscriber has the preview authority, check the preview time and the number of times that the user previews the program via the multicast log command.
   - Within the interval for resetting the subscriber preview authority, check whether the time that the subscriber previews the program crosses the threshold. If yes, the subscriber cannot watch the programs any more.
   - Within the interval for resetting the subscriber preview authority, check whether the number of times that the subscriber previews the program crosses the threshold. If yes, the subscriber cannot watch the programs any more.
   - Within the interval for resetting the subscriber preview authority, if neither the viewing time nor the number of times that the user previews the program crosses the threshold, check whether the interval between this time and last time that the subscriber previews the program. If the interval is shorter than the preview interval threshold, the subscriber cannot watch the program any more.
6. If the AN5116-06B is in the controllable mode, check whether the multicast bandwidth configuration for the ONU port is reasonable. If the ONU port multicast stream bandwidth plus the multicast joining message bandwidth is larger than the ONU port multicast bandwidth, the user cannot watch the program.

6.3.2 Failure to Watch a Multicast Program

Fault symptom

The subscriber cannot watch the multicast program.

Fault analysis

- The multicast subscriber cannot get online.
- The multicast server configuration is incorrect or the multicast server is in an abnormal status.
- The PON interface card operates abnormally.
- The subscriber terminal operates abnormally.

- The IP address of the VLC video software is inconsistent with the network card IP address.

Troubleshooting procedure

1. Check whether the multicast user is online.
   - If the multicast user is not online, follow Failure to Go Online for troubleshooting.
   - If the multicast user is online, go to Step 2.
2. Mirror the multicast data message of the uplink port to an idle uplink port, then perform the packet capture at the uplink port to check whether the multicast message reaches the uplink port.
   - If the multicast message does not reach the uplink port, check the configuration of the multicast server and multicast routing.
   - If the multicast message reaches the uplink port, go to Step 3.
3. Mirror the multicast message of the PON interface to the debug port (FE port) on the PON interface card, and then perform the packet capture at the debug port via packet capture software to check whether the multicast stream reaches the PON interface.
   - If the multicast message does not reach the PON interface, check whether the PON interface card works normally.
   - If the multicast message reaches the PON interface, go to Step 4.
4. Check whether the multicast message reaches the subscriber terminal. Substitute a computer for the subscriber terminal, and use video software such as VLC to view the program. Check whether the multicast stream reaches the subscriber terminal by performing packet capture at the subscriber side.
   - If the multicast message does not reach the subscriber terminal, check whether the physical link between the ONU and the subscriber terminal is normal.
   - If the multicast message reaches the subscriber terminal, check whether the subscriber terminal is working normally.

6.3.3 Failure to Watch a Program after Successful Access to the Program

Fault symptom

The user is online but fails to watch a program.

Fault analysis

- The uplink port of the AN5116-06B works abnormally.
- The VLAN configuration of the local end is different from that of the previous router.
- The multicast packet suppression function is enabled on the uplink port.
- The multicast server does not transmit the video streams to the AN5116-06B normally.
- The TTL value of the multicast program is smaller than the number of hops from the video server to the subscriber.

Troubleshooting procedure

1. Check whether the uplink port of the AN5116-06B works normally and whether the LINK indicator LED is illuminated or blinking quickly.
2. Check whether the local end VLAN configuration of the AN5116-06B's uplink port is correct.
   - If the previous router receives the messages with the VLAN Tag, check whether the VLAN range in the VLAN configuration at the local end matches the VLAN received by the previous router.
   - If the messages received by the previous router is in the Untag mode, check whether the attribute of the uplink port is set to untag in VLAN configuration at the local end.
3. Check whether the multicast packet suppression function is disabled at the uplink port. Before starting the multicast service, make sure that you have disabled the multicast packet suppression function of the uplink port.
4. Check whether the multicast server transmits the video streams to the AN5116-06B normally. Make sure that the uplink is normal.

5. Check whether the TTL value of the multicast program is appropriate. This value should be larger than the number of hops from the video server to the subscriber.

7 Troubleshooting Cases

This chapter introduces how to troubleshoot typical faults.

- System Fault Cases
- Voice Service Fault Case
- Fax Service Fault Case
- Data Service Fault Case

7.1 System Fault Cases

This section introduces system fault cases.

7.1.1 “651”, “619”, or “31” Error Reported during ONU Connection

Fault symptom

The system prompts a **651**, **619**, or **31** error when connecting the subscriber with PPPoE via the ONU. The connection can be successful after multiple attempts, and no off-line occurs after the subscriber gets online.

Fault analysis

- The optical power between the OLT and the ONU is abnormal;
- The ONU has hardware faults;
- The packet transmitting delay of the splitter in the uplink direction is overlong.

Troubleshooting procedure

1. Log into the PON interface card and ping the remote ONU. The Ping operation is normal and no packet loss occurs.
2. Measure the optical power of the PON interface and ONU with a dedicated optical power meter. The optical power values measured are normal. The ONU may have a hardware fault.
3. Replace the ONU, and the fault persists.
4. Analyze the PPPoE connection process with the packet capture software. It is found via data message analysis that the BRAS server cannot receive the PPPoE connection signal transmitted by the subscriber in a timely manner, so that the BRAS server transmits the PADT termination message to the subscriber. Based on the above analysis, it is ascertained that the fault is caused by the overlong packet transmitting delay of the splitter in the uplink direction.
5. After replacing the optical splitter, the service is restored.

Conclusion

Hunter for the cause of fault step by step with the substitution method. Exclude the fault with the ONU first, and then determine that the fault lines in the splitter.

7.1.2 Frequent Restart of Endpoint

Fault symptom

A subscriber of voice service hears no dial tone after off-hook and fails in dialing. Several minutes later, the subscriber is able to dial. Then the dialing switches frequently between the normal and abnormal statuses.

Fault analysis

The IP address the ONU equipment is identical with the IP address other equipment.

Troubleshooting procedure

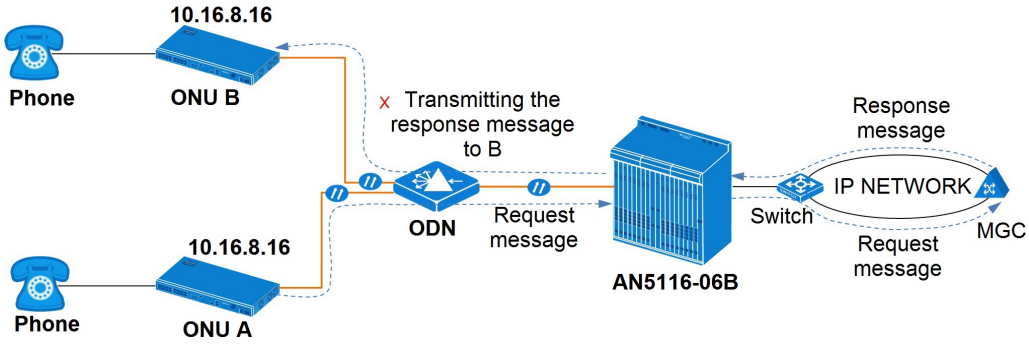


Figure 7-1 Frequent restart of endpoint

1. Via the packet capture analysis, we find the on-hook and off-hook signaling of the ONU equipment A that connects with the subscriber is normal at the initial stage. Several minutes later, the ONU A begins to transmit the cold boot registration packets to the platform repeatedly.
2. Through analyzing the records in the packets, we find that the ONU equipment B that has the same IP address as ONU equipment A transmits the cold boot registration packet to the MGC platform. As a result, the ARP address table of the softswitch platform is changed.

- Since then, for any request received from ONU equipment A, the platform replies to ONU equipment B. Since equipment A cannot receive any response from the platform, it continues to send the message requiring service recovery message to the platform.
- And the platform continues to reply to ONU equipment B.
- So ONU equipment A determines that the platform is not in service and starts to send the cold boot message to the platform. Since it cannot receive any response from the platform, ONU equipment A keeps transmitting the cold boot registration message to the platform.

3. Change the IP address of either ONU equipment A or ONU equipment B, and the fault is eliminated.

Conclusion

Make data planning carefully before starting the voice service, and make sure that the IP address is not repeatedly configured for ONUs or IADs.

7.1.3 Working Mode Inconsistency between the Uplink Port of the Local Equipment and Previous Device Causing Physical Connection Fault

Fault symptom

The uplink port of the AN5116-06B is connected to the previous device via LC/PC fiber. The interface indicator LED on the uplink card's panel is extinguished.

Fault analysis

The working mode of the AN5116-06B's uplink port is inconsistent with that of the previous device's port.

Troubleshooting procedure

1. Log into the ANM2000 and disable the auto-negotiation function of the SFP1 interface on the uplink card, and the panel indicator LED becomes illuminated.
2. Log into the CLI network management system and access the device directory; then execute the show port command. The system shows that the link status is up.

3. Log into the ANM2000 and set the rate of the uplink port to **1000Mbps**; then the connection becomes normal, and the fault is eliminated.

Conclusion

The working mode of the upper level switch port is set to forced, while that of the uplink port of the AN5116-06B is set to auto-negotiation. Inconsistency of the working modes leads to failure in connection.

7.1.4 A Majority of PON Broadband Subscribers under an OLT Encountering Faults in Internet Service

Fault symptom

The AN5116-06B connects about 2000 broadband subscribers. A majority of the subscribers encounter overlow downlink rate and problems such as discarding of messages and long delay in network.

Fault analysis

- The AN5116-06B has a fault;
- A device (such as BRAS) in the distribution layer has a fault;

Troubleshooting procedure

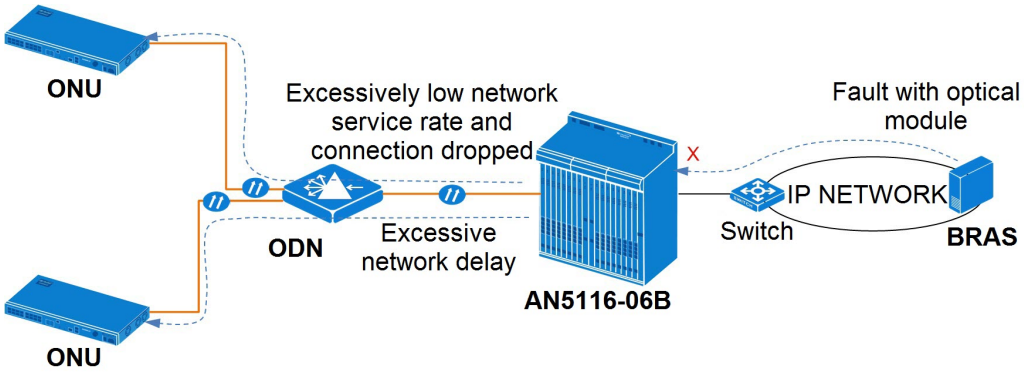


Figure 7-2 A majority of PON broadband subscribers under an OLT encountering faults in Internet service

1. Check whether the equipment has so many broadband subscribers that the bandwidth becomes insufficient, which results in network congestion and

packet loss. By analyzing the monthly traffic statistics via the BRAS, we find that the maximum bandwidth is 591Mbps. So the bandwidth insufficiency is excluded from the fault causes.

2. Modify the broadband route for the subscribers, set the subscribers to private line subscribers, and distribute fixed IP addresses for the users. The services of users pass through the SR instead of the BRAS. Then the services become normal.
3. Ping the BRAS from the broadband subscriber, and we find the delay is normal, no packet loss occurs. When we Ping the broadband subscriber from the BRAS, packet loss occurs.
4. Check the AN5116-06B's uplink port that is connected to the BRAS, and the status of the uplink port is normal.
5. Check the MAC address learning status of the AN5116-06B, and we find no loop.
6. Check the BRAS configuration data, which is found to be normal.
7. It is ascertained that the optical module of the BRAS is aged or faulty. Replace the BRAS optical module. Then the fault is eliminated.

Conclusion

An aged or faulty optical module of the BRAS will lead to overlong network delay in receiving data message or loss of packets.

7.1.5 ONU Network Access Fails to be Reported

Fault symptom

When a new ONU accesses the network, the OLT can authorize the ONU, but the network access of some ONUs cannot be reported to the ANM2000 and recorded in the log.

Fault analysis

- The ANM2000 has a fault in service process;
- The polling interval of the ANM2000 is not reasonable.

Troubleshooting procedure

1. The ANM2000 operates normally, and the status and alarms can be reported in a timely manner. So we perform the packet capture operation of the ONUs with network access report failure on the gathering server, application server and the interface server. And we find the ONU network access information on both the gathering server and the application server. No ONU network access information is found on the interface server. We initially determine that a fault occurs in the anserver or the anmws process.
2. Save the userdump.exe file under the root directory of any disk on the local computer. Run the cmd command and access the directory of userdump.exe. Enter userdump <process name>, and press Enter.

   For example, `D:\>userdump anserver.exe`. An anserver.dmp file will be generated under the corresponding directory. This operation backs up the memory data of anserver.
3. By analyzing the ANserver.dmp file, we find that the polling of the ANM2000 is too frequent. So we modify the **heartbeat interval** item in the md.ini file under the D:\AEMS\md\ini directory of the gathering server. The original value 30s is modified to 600s.
4. After restarting the ANM2000 services, the ONU network access can be reported normally.

Conclusion

Since the equipment polling interval of the ANM2000 background is too short, too much polling data waits to be processed by the background program. So the ONU network access request cannot have immediate response, and the fault occurs. With the heartbeat interval for polling modified, when there are many ONUs, the normal system reporting can be guaranteed, and the reporting operation does not interfere with the normal processing of other commands.

7.1.6 Fault in Configuration of Received Command Buffer Area on Gathering Server

Fault symptom

Users can log in the ANM2000 via the client end normally; but the alarms generated by the AN5116-06B cannot be reported to the network management system. The ANM2000 shows that the OLT status is unknown. The data of all the ANM2000 users in the **User Data Check** GUI are all displayed as **Unauth in DB, Auth in Device.** And the equipment user data is blank.

Fault analysis

- The ANM2000 gathering server is faulty;
- Configuration of the gathering server's buffer area on the ANM2000 is not reasonable.

Troubleshooting procedure

1. Log into the AN5116-06B via the Telnet command, and find that an ONU is connected to the PON interface card.
2. The ANM2000 cannot gather the AN5116-06B equipment status and alarms. Check the gathering server by visiting the gathering server via the Windows remote desktop function.
3. Save the userdump.exe file under the root directory of any disk on the local computer. Run the cmd command and access the directory of userdump.exe. Enter userdump <process name>, and press Enter.

   For example, `D:\>userdump admaems.exe`.An admaems.dmp file will be generated under the corresponding directory. This operation backs up the memory data of admaems.
4. By analyzing the admaems.dmp file, we find that the buffer area for receiving commands from the background ANSERVER service on the Manager server is too small. When the data volume in the buffer area crosses the threshold, the excessive data are discarded. So we modify the parameter in the configuration file of the Manager server, setting the value of the ANSERVERRECVBUFFERLEN to 1048576, so as to guarantee that the

memory reading / writing of the ANM2000 is normal when multiple systems are used.

5. Restart the services of the ANM2000, and the ANM2000 recovers to normal work.

Conclusion

The buffer area for commands received of the ANM2000 is set so small that a plenty of messages are discarded. By modifying the size of the buffer area to a proper one, we can guarantee that the memory reading / writing of the ANM2000 is normal.

7.1.7 Upgrading Firmware and CPU Merge File for Multiple FTTB ONUs Failed

Fault symptom

While upgrading software for multiple FTTB ONUs at the same time, the system prompts that upgrading of the firmware and CPU merge file is unsuccessful, and reports the alarm for communication fault.

Fault analysis

The CPU versions of the FTTB ONUs to be upgraded are old.

Troubleshooting procedure

1. Check the software version of the AN5116-06B as well as the ONU firmware and CPU version to see whether software inconsistency exists.
2. Check the network connection between the AN5116-06B and the ONUs to be upgraded. Log into the PON interface card and PUBA card, and use the Ping command to check the network connection between the AN5116-06B and the ONUs. It is found that the network connection is normal.
3. Upgrade other FTTB ONUs under the AN5116-06B using the firmware and CPU merge file. The upgrade is successful.
4. Analyze the versions of the CPU and firmware of the two types of FTTB ONUs and find that the ONU that can be successfully upgraded has a higher version than that of the CPU of the ONU that fails in upgrading. Upgrade the CPU of the

ONU that fails in upgrading, and then upgrade the ONU with the firmware and CPU merge file. The system shows that the upgrading is successful.

Conclusion

Compare the CPU and firmware versions of the two types of the ONUs to find out the cause of failure in ONU upgrading.

7.1.8 Network Management Server Time Asynchronous with the Client End Time in Alarm Report

Fault symptom

When the AN5116-06B reports an alarm, the alarm time shown on the ANM2000 and that shown on the client end are asynchronous.

Fault analysis

The time of the ANM2000 server and the time on the client end are asynchronous or the configuration of the time zone is incorrect.

Troubleshooting procedure

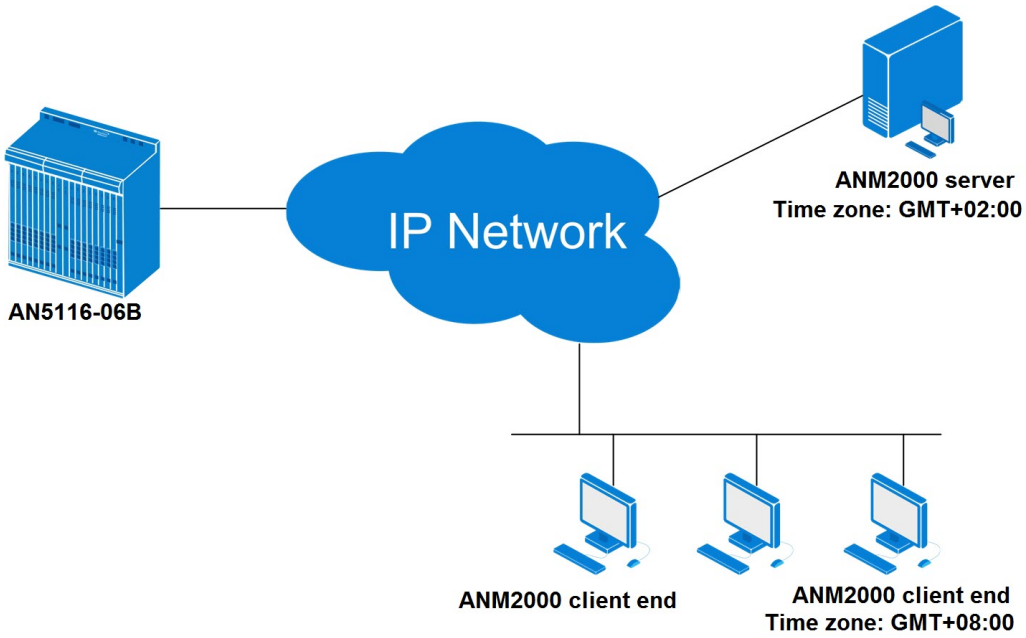
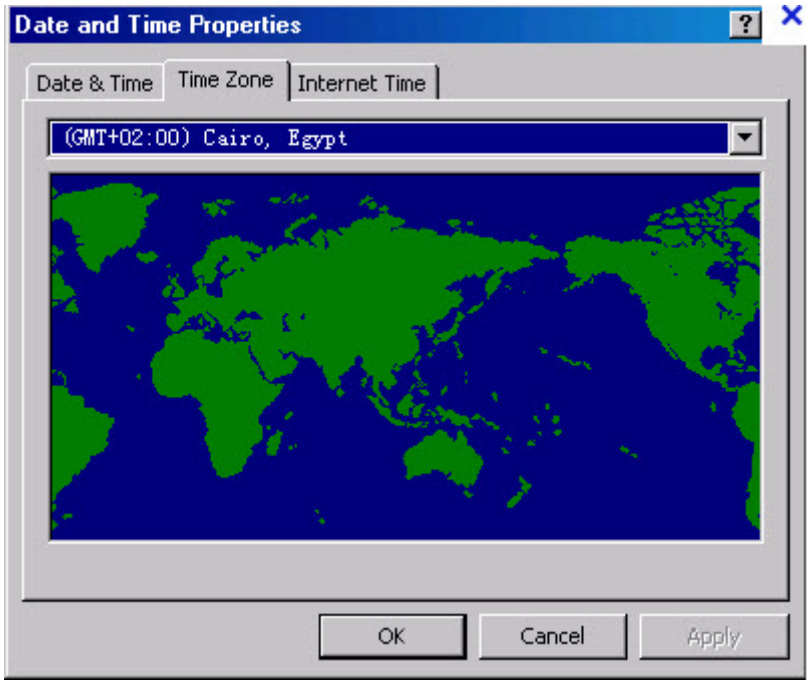


Figure 7-3 Network management server time asynchronous with the client end time in alarm report

1. Check whether the time on the ANM2000 is consistent with the time on the client end. If not, modify the time accordingly.
2. Check whether the time zone set on the ANM2000 is consistent with that on the client end, details as follows:
   1) Click the Start button the computer, and select **Control panel** on the shortcut menu that appears; then double-click **Date and Time** in the control panel window that appears.
   2) Click the **Time Zone** tab to check the configuration of time zone. It is found that the time zone on the ANM2000 server is set to **(GMT+02:00) Cairo**; while the time zone on the client end is set to **(GMT+08:00) Beijing, Chongqing, Hong Kong SAR, Urumqi**.



3. Modify the time zone of the ANM2000 server to **(GMT+08:00) Beijing, Chongqing, Hong Kong SAR, Urumqi**, and then restart the network management server, the alarm time for the AN5116-06B becomes normal.

Conclusion

Configuration of time zone for the ANM2000 server and the client end should be consistent. Inconsistency of the time zone will cause asynchronous alarm time shown on the ANM2000 server.

7.2 Voice Service Fault Case

This section introduces voice service fault cases.

7.2.1 Gateway Address Error Causing Fault in Voice Service

Fault symptom

The voice service under an ONU fails. Check the configuration of the uplink subscribers under the ONU via the ANM2000, and find that the ONU gateway IP address is **10.32.160.2**.

Fault analysis

Configuration of the ONU gateway IP address is incorrect.

Troubleshooting procedure

1. Log into the ANM2000, enable the signal tracing function, and check the ONU uplink subscriber configuration. It is found that the ONU returns a **510 UNKOWN ENDPOINT** message when MGC (IP address: 10.0.55.2) is auditing the ONU (IP address: 10.32.160.2).
2. The ONU returns a normal message after using a test IP address to replace its original IP address, and the subscriber's calling becomes normal.
3. Analysis of the signal tracing result shows that an extra space character was added after the original gateway IP address **10.32.160.2** during configuration.
4. Delete the space character following the gateway IP address, and the ONU voice subscriber can make a call normally. The fault is eliminated.

Conclusion

Pay attention to the rules for entering a parameter value while configuring service, for fear that a typing error may cause fault in service.

7.2.2 Voice Encoding Inconsistency Causes Abnormal Connection of the Subscriber as a Called Party

Fault symptom

A voice subscriber can call normally. But the subscriber often fails to have normal conversation when he / she is called, and hears busy tone after off-hook.

Fault analysis

The voice encoding method for the softswitch platform MGC is different from that for the ONU.

Troubleshooting procedure

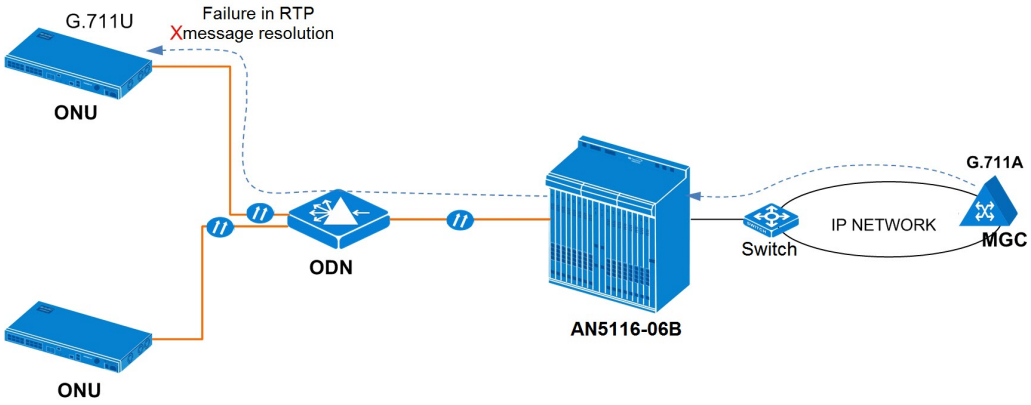


Figure 7-4 Voice encoding inconsistency causing abnormal connection of the subscriber as a called party

1. Log into the ANM2000, enable the signal tracing function, and repeat the faulty operation. Then check the signal tracing result. It is found that the voice encoding method for the softswitch platform MGC is different from that of the ONU. The voice encoding mode used by MGC is G.711A and that used by the ONU is G.711U.
2. Modify the voice encoding method for the ONU, details as follows:
   1) Click the corresponding PON interface on the EC8B card in the Object Tree pane, and select the corresponding ONU in the right pane. Right-click the target ONU, and select **Config→Port Service Config** from the shortcut menu appears, and then click the **Voice Config** tab.
   2) Modify the voice encoding mode for the ONU to G.711A.

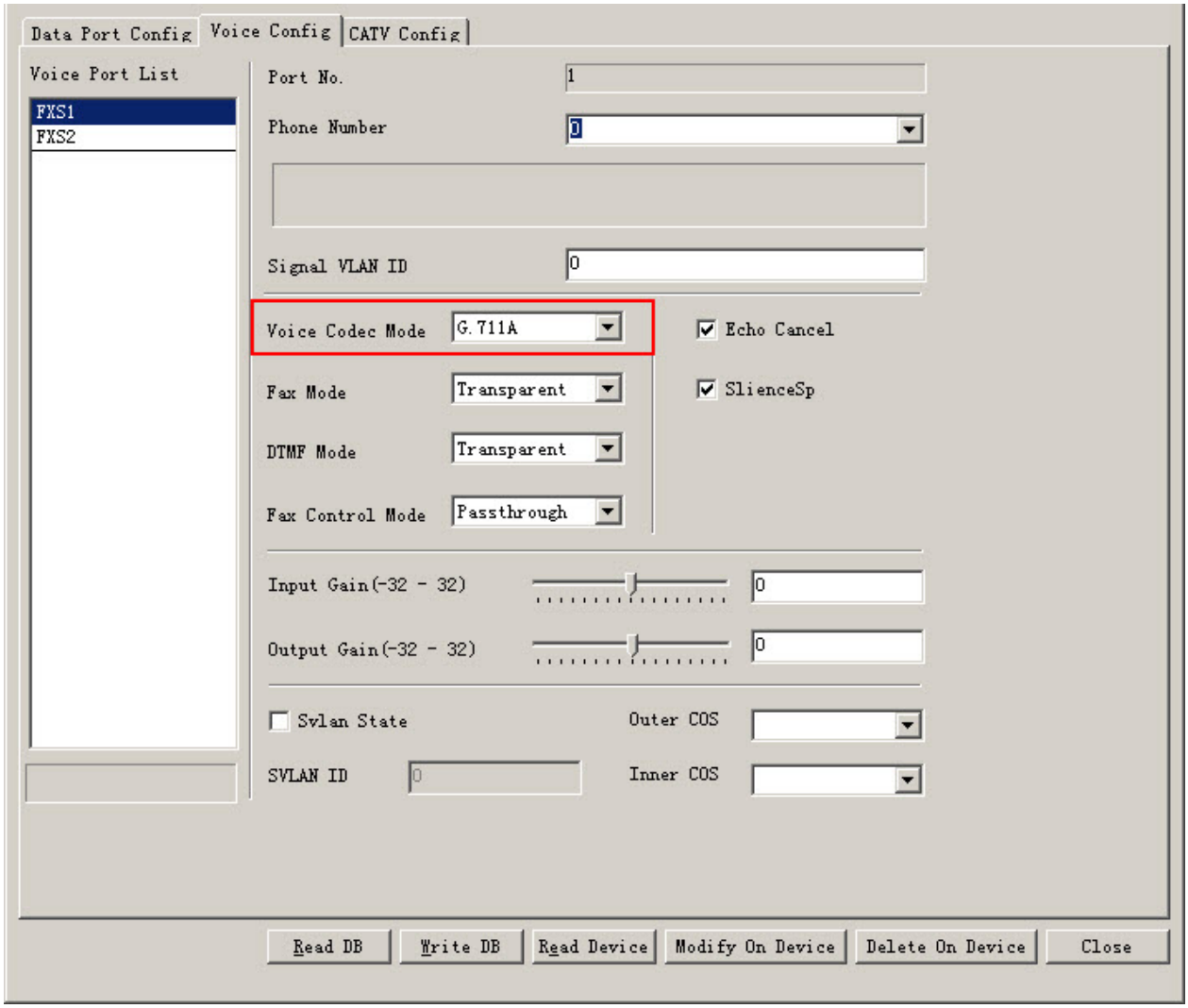


Figure 7-5 Configuring ONU voice encoding / decoding

3. Make a phone call to the subscriber, and the subscriber is connected and has normal communication after he pick up the telephone. The fault is eliminated.

Conclusion

Inconsistency in voice encoding mode between the softswitch platform MGC and the ONU causes the ONU's failure in encapsulating voice RTP data message. Accordingly, the call fails.

7.2.3 DNS Configuration Error Causes Connection Failure of External SIP Terminal Voice Service

Fault symptom

Video telephone service is started at an ONU port, and the SIP protocol is used at the telephone terminal. However, the video telephone cannot access the server after the service configuration is completed.

Fault analysis

- The service configuration is incorrect;
- The uplink device is faulty;
- The SIP terminal is faulty.

Troubleshooting procedure

1. Log into the ANM2000 and check the service configuration. It is found that the configuration is correct.
2. Check whether the OLT and the uplink link are normal, details as follows:
    1) Connect a laptop to an idle port on the uplink card of the AN5116-06B. Log into the ANM2000 to add the port to the video telephone service VLAN, and set the uplink port to untag mode.
    2) Use the laptop to Ping the uplink switch and its gateway, and it is found that the network connection between them are normal. The fault may exist at the section between the OLT and the ONU, or between the ONU and the SIP terminal.
3. Substitute a laptop for the SIP terminal and test if the laptop can Ping the laptop connected to the uplink card and the uplink switch. It is found that the network connection between them are normal. The fault lies in the SIP terminal.
4. Check the SIP terminal configuration and DNS address configuration, and it is found that the DNS address configuration is incorrect. After modifying the DNS address, the video call service recovers to normal, and the fault is eliminated.

Conclusion

Hunter for the fault section by section from the uplink to the ONU subscriber side. It is found that the configuration of the DNS address at the SIP terminal is incorrect, as a result of which, the system fails in resolution of the SIP terminal domain name, and the video telephone fails to work.

7.2.4 Intelligent Telephone Fault in Long Distance Call

Fault symptom

The subscriber subscribes the intelligent public telephone service. When the intelligent public telephone is connected with a 600m subscriber line, the subscriber can call and be called normally. When the telephone is connected with a 1500m subscriber line, the subscriber can only be called, and cannot make calls.

Fault analysis

- The resistance value for the voice port is inappropriate;
- The gain value for the voice port is inappropriate;
- The echo suppression function for the voice port is enabled.

Troubleshooting procedure

1. Perform the packet capture operation on the AN5116-06B, and make sure that the number is reported. When the subscriber line is 600m long, the calling is normal, and when the subscriber line is 1500m long, the calling fails. Therefore, we can initially determine the fault is caused by the signal attenuation as a result of the increase in the subscriber line distance.
2. Restore the RTP data message, and we find that when the subscriber line is 600m long, the number is fully reported; and when the subscriber line is 1500m long, the number cannot be fully reported.
3. Log into the ANM2000 and check the POTS resistance value. Modify the resistance value from 600Ω to 680Ω, and the fault is eliminated.

Conclusion

When the subscriber line is over long, inappropriate POTS resistance value will cause so strong reflection signal that the DSP number reporting is interfered, and the call fails.

7.2.5 Noises Occurring during Conversation

Fault symptom

When the voice service subscriber is making a call, the called party hears sharp noises but the calling party cannot hear the noises.

Fault analysis

- The line is in poor quality;
- The ONU equipment is faulty.
- The mute function at the voice port is enabled.

Troubleshooting procedure

1. Check the quality of the line with a line analyzer, and no problem is found.
2. Check the operation status of the ONU, and no problem is found.
3. When a subscriber under this ONU calls the telephone numbers starting with the same number segment in a business building, the called party hears the noises.
4. When the user calls other urban telephone numbers, the called party hears no noise. Therefore, it is determined that the fault is caused by the mismatch between the ONU and the access network equipment for the business building.
5. Enable the voice signal tracing function and check whether loss of packets occurs during calls.
6. Check the configuration of the **SilenceSp** item, details as follows:
   1) Click the corresponding PON interface on the EC4B/GC4B card in the Object Tree pane, and select the corresponding ONU in the right pane. Right-click the target ONU, and select **Config→Port Service Config** from the shortcut menu appears, and then click the **Voice Config** tab.

2) Disable the **SilenceSp** function.

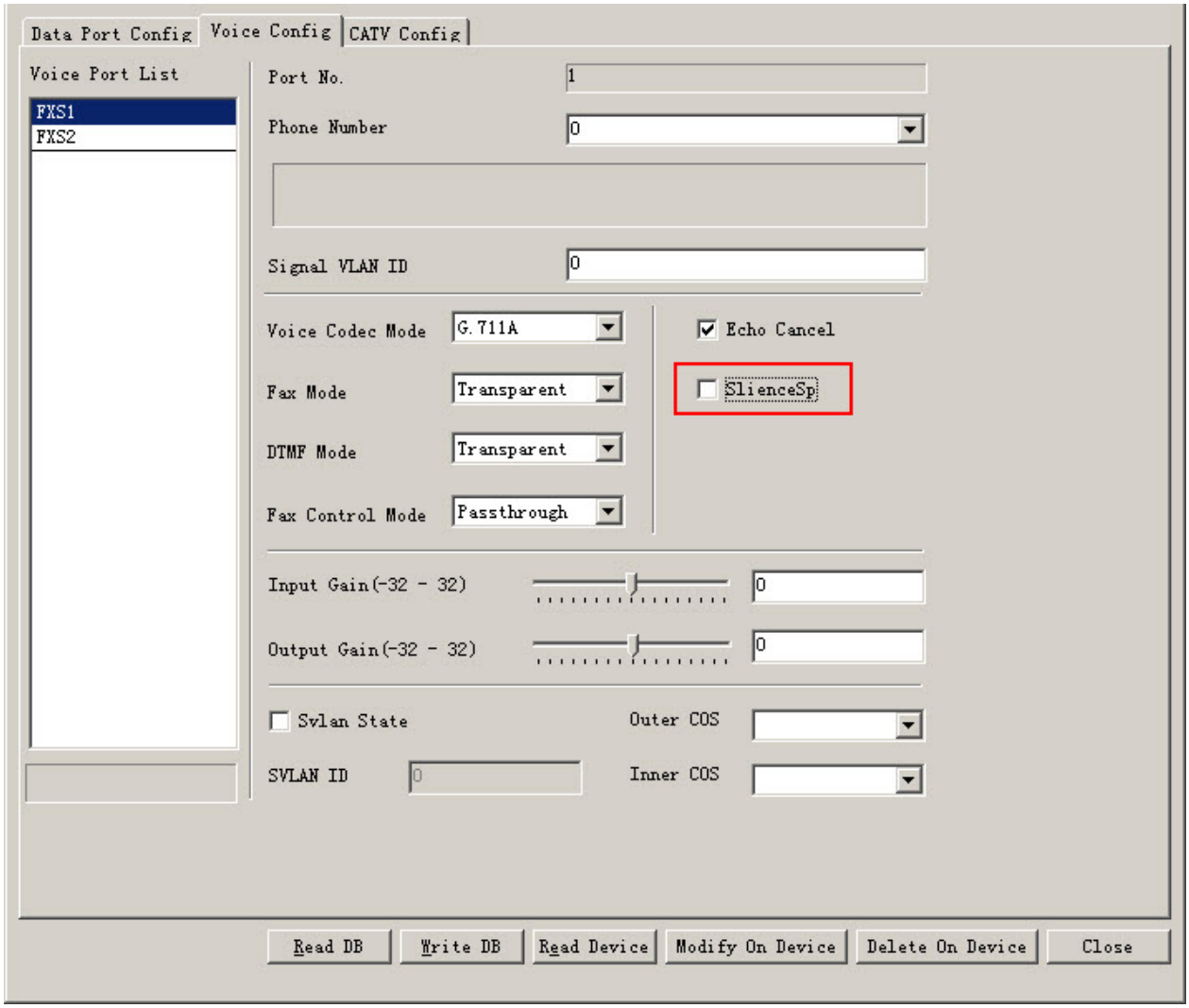


Figure 7-6 Configuring the mute switch

7. After disabling the silence suppression function, the subscriber dial the numbers started with the same segments again. The noises disappear and the fault is eliminated.

Conclusion

Use the substitution method and dial other phone numbers in the urban area to narrow down the fault scope. The mismatch of the access network equipment for the business building and the ONU causes noises in calls.

7.2.6 Multiple Subscribers under an AN5006-07 ONU Failing to Make Calls Simultaneously

Fault symptom

Some subscribers under an AN5006-07 ONU have an unstable voice service. The call failure rate is relatively high.

Fault analysis

Configuration of RTP resource name is incorrect.

Troubleshooting procedure

1. Checking the subscribers failing in call, we find that these subscribers belong to the same ONU. Further checking the voice service configuration of the ONU, we find that the configuration is correct.
2. Check the telephone communication states of the subscribers in the NGN RTP Resource GUI of the corresponding ONU.
   - It never occurs that any two or more telephones have been in the communication state at the same time.
   - No matter which telephone is in call, the corresponding RTP Resource Name is always RTP/0.
   - When no telephone under this ONU is in call, a subscriber can call and be called normally after off-hook. However, when this subscriber is making a call, all the subscribers will fail in calling and can only hear the busy tone after off-hook either as the calling party or as the called party.
3. Log into the ANM2000 to check the configuration of the softswitch interconnection profile, and we find that the items for the starting and ending RTP resource names are blank. Modify the RTP resource names to be from RTP/0 to RTP/15. Accordingly, the subscribers' voice service becomes normal, and the fault is eliminated.

Conclusion

The AN5006-07 ONU provides16 voice ports, so its corresponding softswitch interconnection profile should be configured with 16 RTP resources (RTP/0 to RTP/15). The subscribers will use the RTP resources in the sequence as they make calls.

That is, the telephone making a call first will extracts the RTP/0 resource. As long as this telephone is in call, the RTP/0 resource will not be released. The next telephone to make a call should search for the RTP/1 resource. If the RTP/1 resource is missing in the voice gateway, the situation that one online telephone prevents other telephones from calling or being called will occur.

7.2.7 Digitmap Configuration Error Causing Toll Call Failure

Fault symptom

The subscriber cannot make toll calls to the telephone numbers staring with the area code 0660. The voice service uses the SIP (Session Initiation Protocol).

Fault analysis

The digitmap configuration is faulty.

Troubleshooting procedure

1. Have a test subscriber call 0660-3363130 and perform the packet capture operation.
2. By analyzing the signal tracing result, we find that the area code reported by the ONU is 066. So we determine that the incompletely reported area code causes the dialing failure.
3. Check the SIP digitmap configuration, and we find it to be**06【36】【38】xxxsxxxx**. So the subscriber can only make toll calls to the telephone numbers staring with the area code 0663 or 0668, but cannot call the telephone numbers with the area code of 0660.
4. Modify the digitmap configuration to **06【36】【038】xxxsxxxx**. The fault is eliminated. Now users can make toll calls to the telephone numbers staring with the area code 0660.

Conclusion

The SIP digitmap configuration is unreasonable, so that the subscriber fails to call phone numbers starting with a specified area code. Add the number segment that the subscriber fails to be connected to the digitmap, and the fault is eliminated.

7.2.8 Subscribers under AN5006-20 ONU Failing to Hear Opposite Party

Fault symptom

The AN5116-06B has been expanded and an AN5006-20 ONU is added. The voice service uses the SIP H.248 protocol. The subscribers of the AN5006-20 cannot hear the opposite part either as the called party or the calling party. The opposite party can hear the subscribers of the AN5006-20.

Fault analysis

The VLAN configuration of the voice service is incorrect.

Troubleshooting procedure

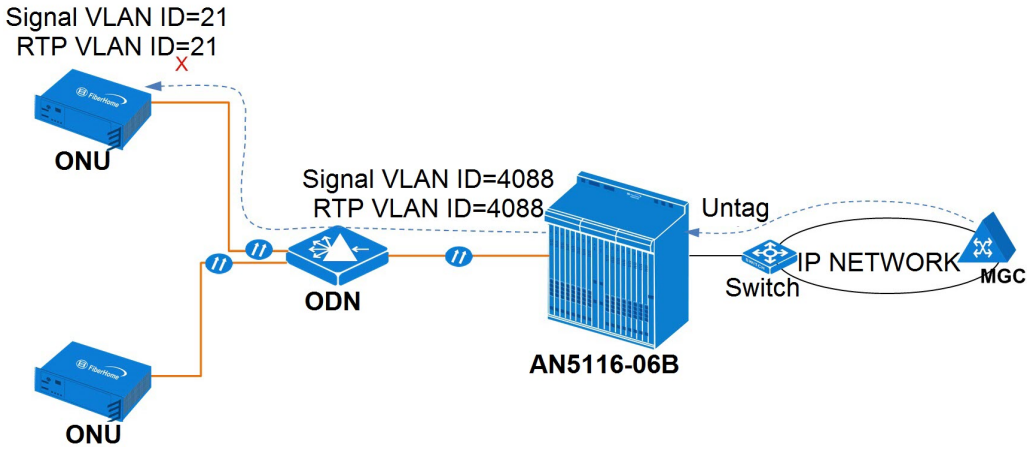


Figure 7-7 Subscribers under AN5006-20 ONU failing to hear the opposite party

1. Perform the packet capture tests on the AN5006-20 uplink port respectively with a test subscriber serving as the calling party and the called party respectively. The following items are checked:
   - The H.248 uplink signaling message–the uplink signaling message is normal and the VLAN ID of the signaling is 21.
   - The H.248 downlink signaling message–the downlink signaling message is normal and has no VLAN ID.
   - The uplink / downlink RTP data message–the uplink RTP data message has the VLAN ID of 21; while the downlink RTP data message has no VLAN.

- Whether interactive messages between the CPU of the MCU card and the RTP stream of the DSP exist–the RTP data message whose source MAC address is the CPU MAC address and destination MAC address is the DSP MAC address can be captured at the uplink port. This indicates that the RTP stream message cannot be transmitted from the CPU of the MCU card to the DSP chip; instead, it is converted into unknown messages and broadcast to the uplink port.

2. Check the FDB address table of the AN5116-06B's core switch card, and we find that the voice service VLAN ID of the uplink card is 4088, which means that the voice data message sent by the previous switch to the AN5116-06B's uplink card is in the Untag mode.
3. Modify the voice service VLAN of the previous device to 21, and the fault is eliminated.

Conclusion

For the AN5006-20 ONU, the voice signaling messages are processed by the CPU of the MCU card, and the RTP stream messages need to be processed by the DSP chip of the MCU card.

The voice service signaling messages and RTP stream messages reach the CPU of the MCU card directly. The signaling messages can interact with the softswitch platform normally; while the RTP stream messages, whose default VLAN ID is 4088, are inconsistent with the configuration of the ONU uplink port, and will not be forwarded to the DSP of the MCU card. Accordingly, the subscriber cannot hear the voice of the opposite party.

7.2.9 AN5006-04 ONU Displaying Wrong Incoming Call Time

Fault symptom

The AN5006-04 ONU uses the SIP protocol to interconnect with the softswitch equipment. Set the telephone time to Beijing time, e.g., 14:48 on May 13th. And when the telephone receives a call, the time displayed changes to 12:05 on February 7th. Replace the telephone and the error persists.

Fault analysis

- The voice signaling flow cannot be established;
- The caller ID display configuration of the ONU is different from that of the softswitch platform.

Troubleshooting procedure

1. Log into the CLI network management system, and issue the show time command. We find that the time of the OLT system is correct.
2. Long into the ANM2000, enable the signal tracing function, and analyze the SIP call flow. We find that the flow is correct. We also find that the caller ID display signaling transmitted from the platform has time signals, and the ONU transmits the time signals to the telephone. So when the telephone receives the incoming call, the time displayed changes to the time of the caller ID display signaling.
3. Check the configuration status of the caller ID display mode. Log into the ONU via the CLI network management system, and use the codec command to check the caller ID display mode. The default displaying mode of the ONU is FSK, which is different from that of the softswitch platform.
4. Change the caller ID display mode of the ONU with the following method:
   - Modify the caller ID display mode via the CLI network management system, and save the modification.

```
codec> cid dtmf
codec> exit

Changes found, please select the operations:
 [1] Discard changes.
 [2] Save changes without taking effect.
 [3] Save changes with taking effect instantly.
Your choice? (Press Ctrl-C or Enter to cancel exiting):
```

   - Modify the caller ID display mode via the ANM2000, and save the modification.
     a) Log into the ANM2000, right-click the system in the Object Tree pane, and select **Config→Profile Definition→Softswitch Parameters Profile** from the shortcut menu that appears.
     b) In the **Softswitch Parameters Profile** window that appears, change the **CallerIDmode** of the softswitch interconnection profile binding to

the ONU to DTMF (The default setting is FSK). Then deliver the configuration to the equipment.

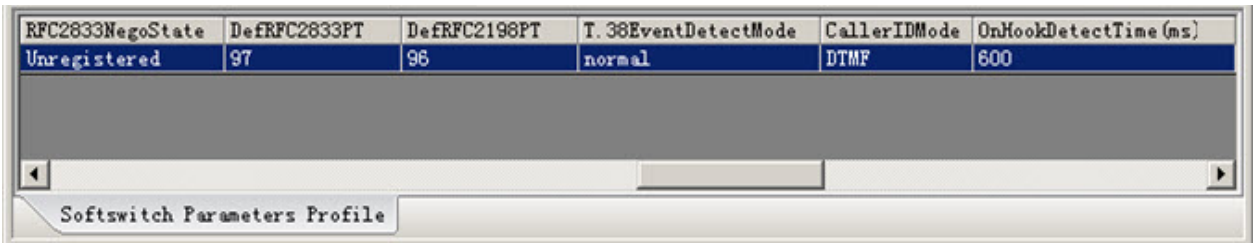


Figure 7-8 Configuration of the caller ID display mode

5. Call the subscriber again and find that the incoming call time of the telephone can be normally displayed. The fault is eliminated.

Conclusion

- When the caller ID display mode of the ONU is configured as FSK, the softswitch platform will send both the telephone number and the time signals to the telephone. The time signals transmitted from the softswitch platform are inconsistent with the time of the telephone. So when the telephone receives a call, the time displayed on the telephone will be changed to the time transmitted from the softswitch platform.
- When the caller ID display mode of the ONU is configured as DTMF, the softswitch platform will send only the calling telephone number to the telephone. Under this mode, the time displayed on the telephone will not be changed.

7.2.10 Incorrect DSP Profile Parameter Configuration Causing Card Swiping Failure on POS Machine

Fault symptom

Both the data service and the normal voice service of the subscriber are normal, but the subscriber's POS machine does not operate normally.

Fault analysis

- The software version of the ONU is incorrect;
- The earth ground cable of the equipment is not well grounded;

- The server number of the POS machine is incorrectly configured;
- The DSP profile configuration is incorrect.

Troubleshooting procedure

1. Check the software version of the ONU, and find that the software version is correct.
2. Check whether the ONU is well grounded, and find that the earth ground protection cable for the ONU is properly connected.
3. Check the configuration of the POS machine server number, and find that the POS machine cannot connect to the server. After modifying the configuration, the POS machine still fails to connect to the server.
4. Check the ONU DSP profile configuration, and find that parameters of the new DSP profile is different from those of the default DSP profile. The DSP profile usually uses the default settings unless otherwise specified.
5. Modify the DSP profile binding configuration, and change the bound profile to the default profile. Then the POS machine can connect to the server and the card swiping becomes successful. The fault is eliminated.

Conclusion

Use default settings for the DSP profile unless otherwise specified for voice encoding, and bind the default profile to the ONU.

7.2.11 ONU Reporting MGC Disconnection Alarm Frequently

Fault symptom

The AN5116-06B is configured with additional AN5006-07B and AN5006-10B ONUs. After configuration, the alarm for MGC link disconnection is reported, and the voice service is in a flashing state.

Fault analysis

- The configuration of the local VLAN is incorrect.
- The MGC configuration for the OLT voice service is unreasonable.

Troubleshooting procedure

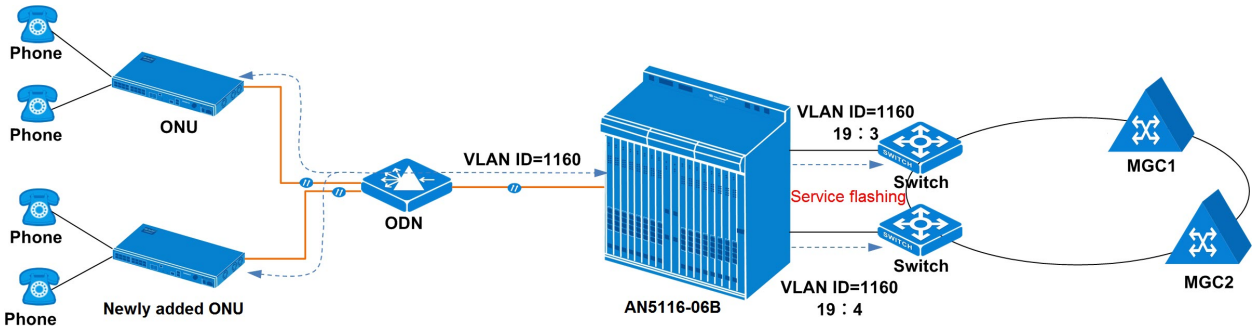
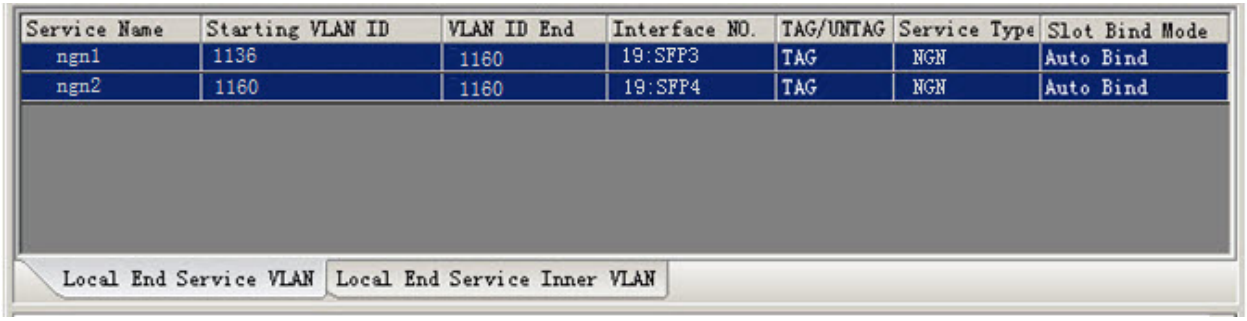
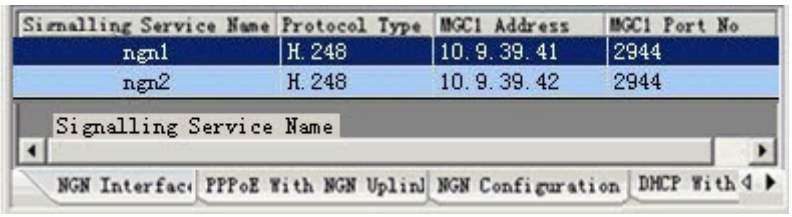


Figure 7-9 ONU reporting MGC disconnection alarm frequently

1. Check whether the voice service configuration data has been delivered to the ONU and validated.
2. Check the configuration of the local VLAN, details as follows:
   1) Log into the network management system, right-click the HSWA card on the Object Tree pane, and select **VLAN Config→Local VLAN→Local End Service VLAN**;
   2) The voice service on the original ONU is connected to the upper layer network via the uplink port 19:SFP3; while the voice service on the added ONUs is connected to the upper layer network via the port 19:SFP4.



3. Check the uplink port for the voice service, details as follows:
   1) Log into the network management system, right-click the HSWA card on the Object Tree pane, and select **Voice Config→NGN Interface**;
   2) Different MGC addresses have been assigned to the added ONUs and the original ONU.



4. Both the 19:SFP3 and the 19:SFP4 optical interfaces on the uplink card of the AN5116-06B have transparently transmitted the voice service flow with the VLAN ID of 1160. The added ONUs and the original ONU use different MGC addresses. The voice service flow is continuously switched via the two uplink ports, and the voice data packets with different MGC addresses are sent to different routes, so as to cause flashing of the voice service.
5. Modify the uplink port for the voice service on the added ONUs to 19:SFP3 optical interface, and the voice service becomes normal.

Conclusion

When load sharing is configured for the voice service, the voice data flow is encapsulated with VLAN and sent to different softswitch platforms (MGCs). The voice data flow can only be forwarded via one uplink port on the OLT. When multiple uplink ports are used to forward the voice data flow, the core switch card will forward the voice data packets by switching between these uplink ports. This causes flashing of the connection between the voice data flow and the MGC server.

7.3 Fax Service Fault Case

This section introduces fax service fault cases.

7.3.1 Dial Mode Setting Error Causing Fax Service Fault

Fault symptom

When a subscriber makes a voice call on the fax machine, the softswitch platform sends a warning tone for a dialing mistake and it cannot send a fax. But using the same port as an ordinary telephone port, the subscriber can both call and be called normally.

Fault analysis

The dialing mode set for the fax machine is incorrect.

Troubleshooting procedure

1. Perform a packet capture test at the uplink port and find that the displayed caller ID of the fax machine is longer than that of the ordinary telephone.
2. Check the dialing mode of the fax machine and find that the fax machine is set to the pulse dialing mode. The default mode is DTMF dialing mode.
3. Modify the dialing mode to the DTMF dialing mode on the fax machine; the call resumes and the fault is eliminated.

Conclusion

In the pulse dialing mode, electronic circuit is used to simulate the work of the mechanical dial plate. Modern telephones generally use the DTMF dialing mode. If the fax machine is set to the pulse dialing mode, while the voice gateway recognizes the DTMF dialing mode only, the telephone number reported by the voice gateway to the softswitch platform will be abnormal.

7.3.2 Incorrect Uplink Port Mode Configuration Causing Connection Failure in Fax Service

Fault symptom

An ONU is connected to the AN5116-06B. The subscribers under the ONU have normal voice services but fail to send or receive faxes.

Fault analysis

- The fax service configuration is incorrect.
- The working mode of the uplink port is different from that of the previous switch.

Troubleshooting procedure

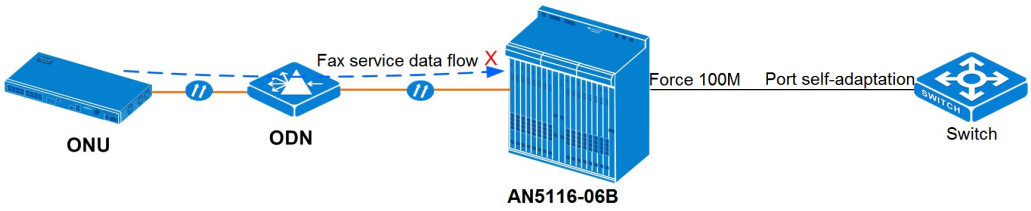


Figure 7-10 Incorrect uplink port mode configuration causing connection failure in fax service

1. Check the fax service configuration of the ONU, and find that the fax mode is set to transparent.
2. Perform packet capture on the uplink port of the AN5116-06B. By analyzing the data, we find that when the media gateway server interacts with the voice gateway, a 6% packet loss rate occurs. So we isolate the fault between the AN5116-06B and the upper layer network.
3. Check the working mode of the previous switch port and find it to be**Auto-negotiate**. Check the uplink port working mode of the AN5116-06B and find it to be **100Mbps and Full-Duplex**. The working modes of the two sets of equipment do not match.
4. Modify the working mode of the AN5116-06B uplink port to **Auto-negotiate**; the fax service resumes and the fault is eliminated.

Conclusion

The working mode of the AN5116-06B's uplink port should be consistent with that of the previous switch interface, so as to ensure the normal transmission of data.

7.4 Data Service Fault Case

7.4.1 Video Monitoring Interrupted after Power Supply Recovery

Fault symptom

In the urban security video monitoring project, the AN5116-06B and the ONU equipment work together to provide video signal transmission for the video camera. Suddenly, the power supply is interrupted. When the power supply recovers, some of the video cameras can work normally, while other video cameras cannot be connected to the video monitoring platform.

Fault analysis

When the power supply recovers from failure, the ONU and the video cameras are started at the same time. The video cameras send ARP messages applying for joining the video monitoring platform. The ONUs then interact with the OLT to generate the logical links. There are multiple ONUs under the PON interface; therefore, it takes a certain period of time to generate the logical links. Some of the video cameras send the ARP messages before the logical links are generated; accordingly, these ARP messages cannot reach the video monitoring platform, and these video cameras are out of the management of the network management system.

Troubleshooting procedure

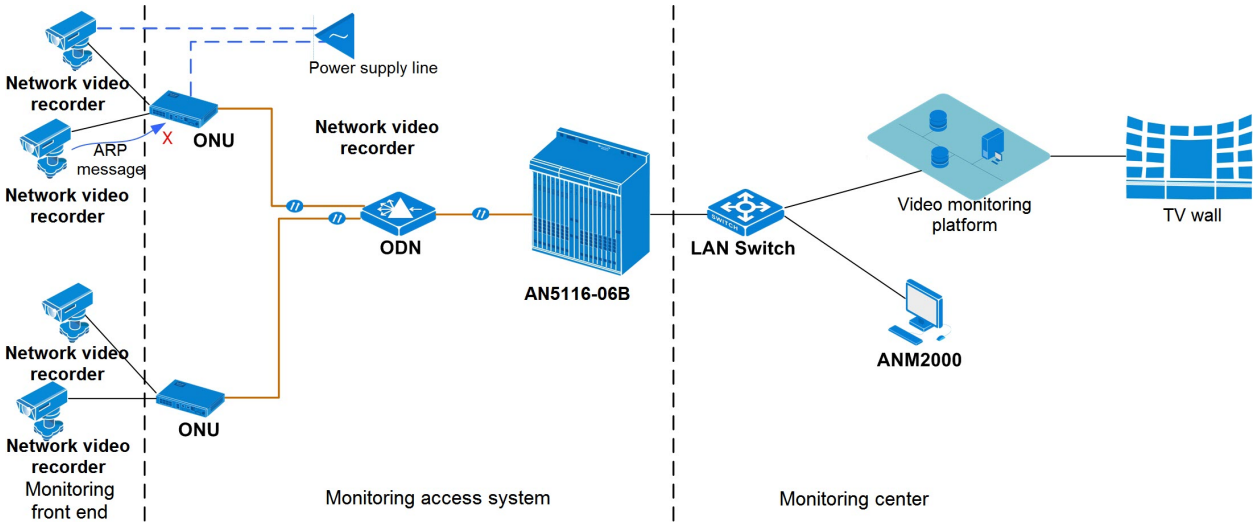


Figure 7-11 Video monitoring interrupted after power supply recovery

1. Check the VLAN configuration of the AN5116-06B system to see whether it is consistent with the planning data.
2. Check the FDB table of the AN5116-06B system and the MAC address learning table of the uplink switch to see whether the MAC addresses of the faulty video cameras have been learned.
3. Use the Ping command to test the network connection between the video monitoring platform and the faulty video cameras. The network connection is normal. During the test, the faulty video cameras recover and begin to send images.
4. Perform the packet capture test for the faulty video cameras, and check how many times that the ARP messages have been sent and when the messages have been sent. It is found that some video cameras send the ARP messages before the ONUs generate the logical links, so that the ARP messages cannot reach the video monitoring platform.
5. Contact the video camera manufacturer to modify the times and time that the video cameras have sent the ARP packets. After that, the fault is eliminated, and all the faulty video cameras recover to upload images.

Conclusion

In the urban security monitoring project, you need to check the video cameras. If the time when the video cameras send the ARP packets conflicts with the time when the ONUs generate the logical links, contact the manufacturer of the video cameras to modify the configuration data of the cameras accordingly.

7.4.2 Wireless Network Access Indicating Windows Failing to Find a Certificate for Logging into Network

Fault symptom

When the subscriber accesses the ONU or home gateway via wireless network, the computer displays the prompt message that **windows fails to find the certificate for you to log into the network**.

Fault analysis

- The IEEE 802.1x authentication configuration is incorrect.
- The configuration of wireless network authentication mode is incorrect.

Troubleshooting procedure

1. Check the IEEE 802.1x authentication configuration, and shut down the IEEE 802.1x authentication, details as follows:
   1) Right-click **Wireless network connection**, and select **Properties**, to bring up the **Wireless network configuration** window.
   2) Select the network to be connected, and click **Properties** to bring up the **Wireless network property** window.
   3) Click the **Authentication** tab, and click to clear the section of the **Activate IEEE 802.1x authentication for the network** check box to disable the IEEE 802.1x authentication.
2. Check the configuration of the wireless network authentication mode, details as follows:
   1) In the **Wireless network property** window, click the **Association** tab, and find that the network authentication mode is set to **Open**.

2) Modify the network authentication mode to **Shared**, and the wireless network link resumes.

Conclusion

The wireless network cards of some computers do not match the network authentication and encryption configuration. Settle the problem by modifying the relevant settings of the wireless network cards of the computers.

Appendix A Signal Tracing Instruction

A.1 Overview

A.1.1 Operation Flow

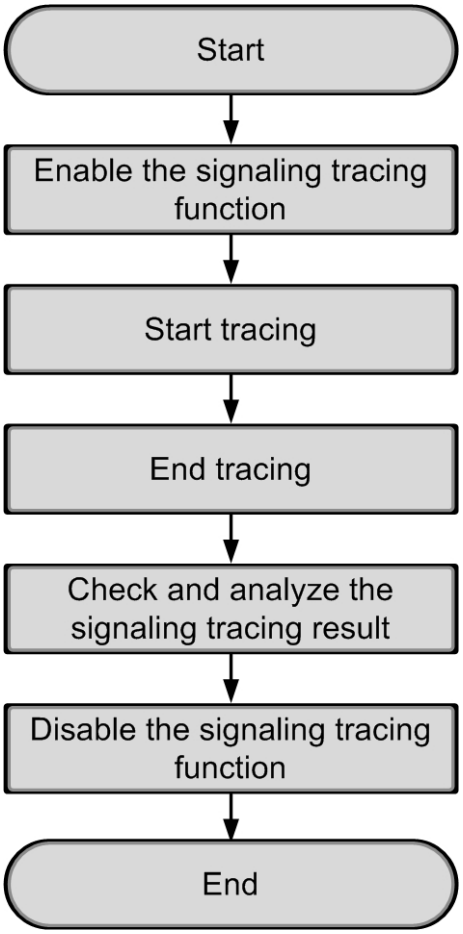


Figure A -1 Operation flow of signal tracing

A.1.2 Enabling / Disabling Signal Tracing

Command function

This command is used to enable or disable the signaling tracing function.

Note:

Enabling the signaling tracing function does not affect the subscriber services. Since the signaling tracing operation occupies the system memory, you should turn off the signal tracing switch after the signaling tracing operation is completed, so as not to impact the equipment performance.

Command access

In the ANM2000 GUI, right-click the HSWA card in the Object Tree pane, and select **Config→Signal Trace** from the shortcut menu to open the Signal Trace window.

Parameter description

Name	Meaning	Value Range	Attribute	Configuration Method
IP	Source or destination IP address of the data packet. The data packet whose source or destination IP address is this IP address will be transmitted to the network management server.	–	Compulsory	Double-click the blank under this item to input the IP address of the data packet.
L4 Src. Port No	The layer 4 source port number of the data packet. The data packet whose source port number is this port number will be transmitted to the network management server.	1 to 65534	Compulsory	Double-click to input the layer 4 source port number.

Name	Meaning	Value Range	Attribute	Configuration Method
L4 Dst. Port No.	The layer 4 destination port number of the data packet. The data packet whose destination port number is this port number will be transmitted to the network management server.	1 to 65534	Compulsory	Double-click to input the layer 4 destination port number.
Enable Status	Signal tracing enabling switch. The options include Enable and Disable.	–	Compulsory	Click the pulldown menu to select an enabling status.

Configuration example

Perform the tracing operation of the signaling packet whose source and destination port numbers are both 2944 and destination IP address is 192.168.1.1 on the AN5116-06B.

1. Access the ANM2000 GUI, right-click the HSWA card in the Object Tree pane, and select **Config→Signal Trace** from the shortcut menu to open the Signal Trace window.
2. Click the  button, input 1 in the Please Input the Rows For Add dialog box that appears to add one entry.
3. Configure the parameters in turn.
4. Click the  button to deliver the configuration to the equipment. See Figure A-2.

Figure A -2 Enabling / disabling signal tracing

A.1.3 Signal Trace Window

This section introduces the layout of the Signal Trace window.

Access the ANM2000 GUI, click **Configuration→Signal Trace** in the main menu and open the Signal Trace window, as shown in Figure A-3.

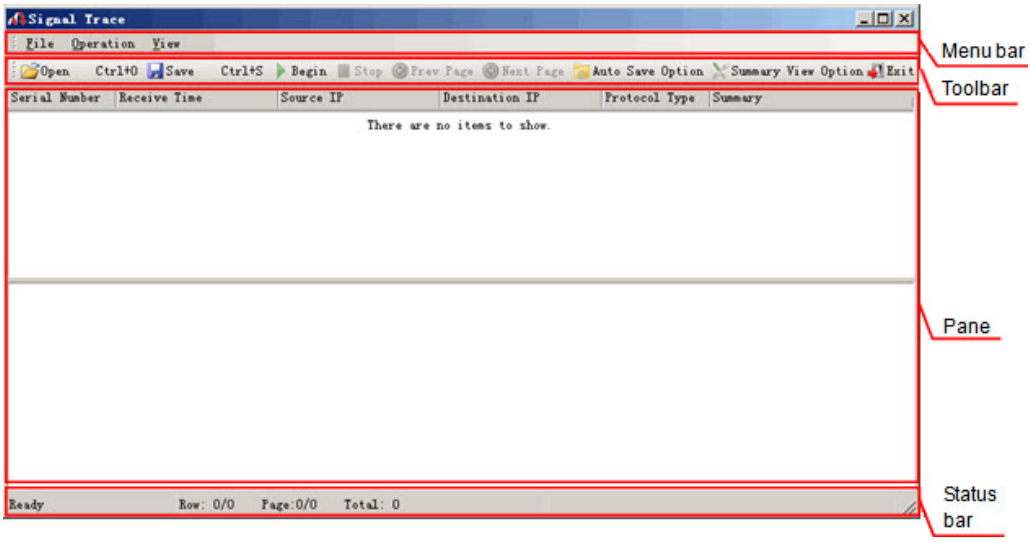


Figure A -3 Signal tracing

Menu bar

Menu Option		Function
File	Open	Opens the signaling tracing document saved under the designated directory.
	Save	Saves the signaling tracing document to the designated directory.
	Exit	Quits the Signal Trace window.
Opera-tion	Begin	Starts the signaling tracing.
	Stop	Stops the signaling tracing.
	Auto Save Option	Configures the function of automatically saving the signaling tracing document.
	Summary View Option	Configures the related parameters of the summary view.

Toolbar

Button	Function
Open	Opens the signaling tracing document saved under the designated directory.
Save	Saves the signaling tracing document to the designated directory.
Begin	Starts the signaling tracing.

Button	Function
Stop	Stops the signaling tracing.
Auto Save Option	Configures the function of automatically saving the signaling tracing document.
Summary View Option	Configures the related parameters of the summary view.
Exit	Quits the Signal Trace window.

Pane

Area	Parameter	Description
Upper pane	Serial Number	The number of the signaling packet.
	Receive Time	The time when the signaling packet is received by the network management server.
	Source IP	The source IP address of the transmitting signaling packet.
	Destination IP	The destination IP address of the transmitting signaling packet.
	Protocol Type	Protocol type of the signaling packet.
	Summary	The summary of the contents in the signaling packet.
Lower pane	–	Displays the original code stream of the signaling packet.

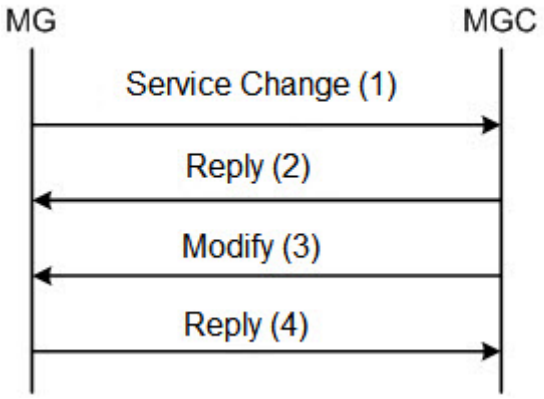
Status bar

Displays the information of the signaling tracing status.

A.2 H.248 Signaling Flow Analysis

A.2.1 MG Registering to MGC

The MG (IP address being 132.108.95.20) registers to the MGC (IP address being 132.108.95.1).



1. The MG sends the ServiceChange message to the MGC for registration. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.20]:2944.
```

// The protocol type is H.248; the version is 1; the IP address of the MG is 132.108.95.20; the protocol port number is 2944.

```
Transaction=1{Context=-
```

// The transaction number is 1, the context encapsulated in the transaction is blank.

```
ServiceChange=ROOT{Services{Method=Restart, Reason="902 Warm Boot",
Version=1}}}}
```

// TerminationID of the ServcieChange message is Root. (It means the ServcieChange command applies to the entire gateway.) The ServcieChangeMethod is Restart. The ServiceChangeReason is 902. (902 stands for hot start; 901 stands for cold start.)

2. The MGC sends the Reply message informing the success of registration back to the MG. Below is the signal tracing example:

```
[132.108.95.1]:2944.
```

// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.

```
P=1{C=-{SC=ROOT{SV{AD=2944}}}}.
```

// The MGC receives the registration message from the MG, and replies the MG with the Reply message informing the success of registration.

3. The MGC sends the Modify message to the MG, asking the MG to check the off-hook of all users. Below is the signal tracing example:

```
T=53{C=-
```

// The transaction number is 53, the context encapsulated in the transaction is blank.

```
{MF=a2{E=1{al/of}}}}.
```

// The MGC sends the Modify message to the MG to check the off-hook of user a2.

```
T=54{C=-
```

// The transaction number is 54, the context encapsulated in the transaction is blank.

```
{MF=a1{E=1{al/of}}}}.
```

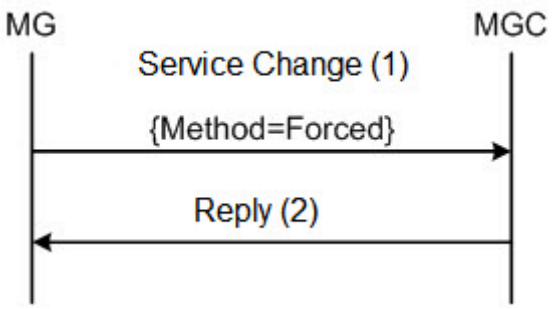
// The MGC sends the Modify message to the MG to check the off-hook of user a1.

4. The MG responds to the Reply message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.20]:2944. Reply=53{Context=-{Modify=a2}}
// The MG responds to the Reply message for checking the off-hook of user a2.
MEGACO/1 [132.108.95.20]:2944. Reply=54{Context=-{Modify=a1}}
// The MG responds to the Reply message for checking the off-hook of user a1.
```

A.2.2 MG Logging Out Actively

The MG (IP address being 132.108.95.20) applies to the MGC (IP address being 132.108.95.1) for logout actively.



1. The MG sends the ServiceChange message to the MGC for logout. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.20]:2944.
// The protocol type is H.248; the version is 1; the IP address of the MG is 132.108.95.20; the protocol port number is 2944.
Transaction=48{Context=-
// The transaction number is 48, the context encapsulated in the transaction is blank.
{ServiceChange=ROOT{Services{Method=Forced, Reason="908 MG Impending Failure"}}}}
// TerminationID of the ServcieChange message is Root. (It means the ServcieChange command applies to the entire gateway.) The ServcieChangeMethod is Forced. The ServiceChangeReason is 908 (the MG will have faults).
```

2. The MGC sends the Reply message informing the success of logout back to the MG. Below is the signal tracing example:

```
[132.108.95.1]:2944.
// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.
P=48{C=-{SC=a1{SV{AD=132.108.95.1}}}}
// The MGC receives the logout message from the MG, and replies the MG with the Reply message informing the success of logout.
```

A.2.3 Endpoint Exiting from Service

The subscriber a1 of the MG (IP address being132.108.95.20) exits from service. The IP address of the MGC is 132.108.95.1.

1. The MG sends the ServiceChange message to the MGC for logout. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.20]:2944.
```

// The protocol type is H.248; the version is 1; the IP address of the MG is 132.108.95.20; the protocol port number is 2944.

```
Transaction=11{Context=-
```

// The transaction number is 11, the context encapsulated in the transaction is blank.

```
{ServiceChange=a1{Services{Method=Graceful, Reason="905 Termination taken out of service"}}}}
```

// TerminationID of the ServcieChange message is a1. The ServcieChangeMethod is Graceful (It means that subscriber a1 will exit from service after the preset ServiceChangeDelay time. And Forced means that subscriber a1 will be removed from service immediately). The ServiceChangeReason is 905 (the endpoint is removed from service).

2. The MGC replies with a Reply message. Below is the signal tracing example:

```
[132.108.95.1]:2944.
```

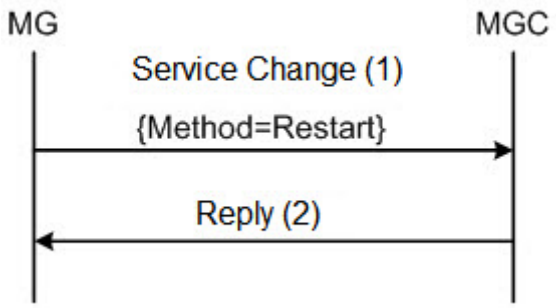
// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.

```
P=11{C= - {SC=a1{SV{AD=132.108.95.1}}}}
```

// The MGC receives the message requesting taking the endpoint out of service from the MG, and replies the MG with a Reply message.

A.2.4 Restoring Endpoint to Service

Restore the subscriber a1 of the MG (IP address being 132.108.95.20) to service. The IP address of the MGC is 132.108.95.1.



1. The MG sends the ServiceChange message to the MGC for registration. Below is the signal tracing information:

```
MEGACO/1 [132.108.95.20]:2944.
```

// The protocol type is H.248; the version is 1; the IP address of the MG is 132.108.95.20; the protocol port number is 2944.

```
Transaction=28{Context=-
```

// The transaction number is 28, the context encapsulated in the transaction is blank.

```
{ServiceChange=a1{Services{Method=Restart, Reason="900 Service
Restored"}}}}
```

// TerminationID of the ServcieChange message is a1. The ServcieChangeMethod is Restart. The ServiceChangeReason is 900 (service restoration).

2. The MGC replies with a Reply message. Below is the signal tracing example:

```
[132.108.95.1]:2944.
```

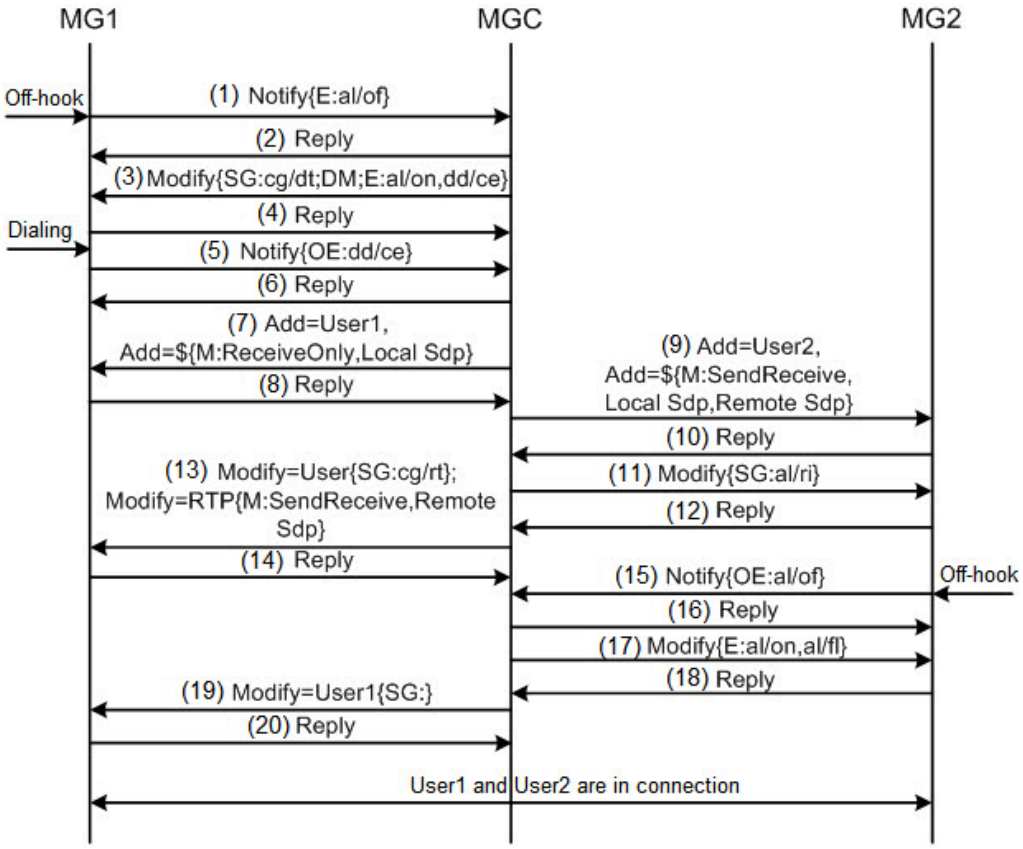
// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.

```
P=28{C=-{SC=a1{SV{AD=132.108.95.1}}}}
```

// The MGC receives the message requesting restoring the endpoint to service from the MG, and replies the MG with a Reply message.

A.2.5 Establishing a Normal Call

Establish a normal call between the subscriber a2 of MG1 (IP address being 132.108.95.20) and subscriber a1 of MG2 (IP address being132.108.95.30). The IP address of the MGC is 132.108.95.1.



1. MG1 detects the off-hook of User1 and reports the off-hook to the MGC via a Notify message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.20]:2944.
```

// The protocol type is H.248; the version is 1; the IP address of the MG1 is 132.108.95.20; the protocol port number is 2944.

```
Transaction=11{Context= -
```

// The transaction number is 11, the context encapsulated in the transaction is blank.

```
{Notify=a2{ObservedEvents=1{20000101T00024105:al/of{init=False}}}}}
```

// TerminationID in the Notify message is a2. MG1 (gateway of subscriber a2) detects the off-hook of subscriber a2 and reports it to the MGC.

2. The MGC replies MG1 with a Reply message. Below is the signal tracing example:

```
[132.108.95.1]:2944.
```

// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.

```
P=11{C=-{N=a2}}
```

// The MGC's response to the Notify message.

3. The MGC sends a Modify message to MG1. Below is the signal tracing example:

```
T=63{C= -
```

// The transaction number is 63, the context encapsulated in the transaction is blank.

```
{MF=a2{E=1{al/on,dd/ce{DigitMap=dialplan0}},SG{cg/dt},DM=dialplan0
{xxxxxxxx}}}}
```

// TerminationID in the Modify message is a2. The MGC checks the on-hook (al/on) and the digit collection completion (dd/ce) events. The MGC sends the digit map (Digitmap) which is xxxxxxxx to MG1 and requests MG1 to play the dial tone.

4. MG1 replies the MGC with a Reply message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.20]:2944.Reply=63{Context=-{Modify=a2}}
```

// MG1's response to the Modify message transmitted from MGC.

5. Below is the signal tracing example: User1 of MG1 dials a number. After MG1 completes the digit collection, it matches the number with the digit map delivered by the MGC. MG1 reports the number dialed by User1 and the result of matching to the MGC with a Notify message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.20]:2944.
```

// The protocol type is H.248; the version is 1; the IP address of the MG1 is 132.108.95.20; the protocol port number is 2944.

```
Transaction=12{Context= -
```

// The transaction number is 12, the context encapsulated in the transaction is blank.

```
{Notify=a2{ObservedEvents=1{20000101T00024631:dd/ce{ds="88880001",
Meth=UM}}}..}.}
```

// User1 of MG1 dials the number 88880001. The MG1 performs the digit collection according to the digit map delivered by the MGC and determine that the dialed number perfectly matches the digit map (Meth=UM). MG1 reports the number dialed by User1 and the result of matching to the MGC with a Notify message.

6. The MGC replies MG1 with a Reply message. Below is the signal tracing example:

```
[132.108.95.1]:2944.P=12{C=-{N=a2}}
```

// The MGC's response to the Notify message transmitted from MG1.

7. The MGC sends an Add message to MG1. Below is the signal tracing example:

```
T=64{C=$
```

// The transaction number is 64. The MGC requests MG1 to create a new context. Since the context is indefinite, $ is used here.

```
{A=a2,
```

// Add user a2 to the new context.

```
A=${M{L{.v=0.c=IN IP4 $.m=audio $ RTP/AVP 8.a=ptime:20},O{MO=RC,nt/
jit=40}}}}}
```

// Add RTP termination of user a2 to the new context. The new RTP termination is a temporary termination. Since the descriptor of RTP termination is not settled, $ is used here. v=0 means the SDP

protocol version is 0. c=IN IP4 $ indicates the related information of the RTP termination: The related network identifier is Internet; the related address type is IPv4; $ means that the local IP address is unknown currently. m=audio $ RTP/AVP 8 indicates the media description recommended by the MGC for the new RTP termination. audio means the media type of the RTP termination is audio; $ means the media port number of the RTP termination is unknown currently; RTP/AVP is the transport layer protocol, whose value is related to the address type in the "c=" field. For IPv4, most of the media traffic streams are transmitted by RTP/UDP. The following two types of protocols have been defined: RTP/AVP denotes RTP used under the RTP Profile for Audio and Video Conferences with Minimal Control running over UDP; Udp denotes an unspecified protocol running over UDP. As to the RTP Profile for Audio and Video Conferences with Minimal Control, 8 stands for the media payload type. It means that G.711A is recommended as the RTP stream compression encoding format by the MGC. a=ptime:20 means the length of time in milliseconds represented by the media in a packet is 20ms. MO=RC means the RTP mode is ReceiveOnly. The maximum jitter buffer (nt/jit) is 40ms.

Note:

The mapping correspondences between the RTP payload type number and the encoding format defined by the H.248 protocol are: G.711U=0; G.726=2; G.723=4, G.723.1=4; G.711A=8; G.729=18, G.729A=18.

8. MG1 distributes resources for the RTP, and replies the MGC with a Reply message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.20]:2944.
```

// The protocol type is H.248; the version is 1; the IP address of the MG1 is 132.108.95.20; the protocol port number is 2944.

```
Reply=64{Context=1
```

// The transaction number is 64. MG1 creates a new context; and the context ID is 1.

```
{Add=a2, ...Add=RTP/0
```

// Confirm that user a2 and its RTP termination is added to the context.

```
{Media{.Local{.v=0..c=IN IP4 132.108.95.20..m=audio 4010 RTP/AVP 8..
a=ptime:20..}}}}}
```

// Media descriptor, which indicates that the IP address of the RTP is 132.108.95.20, the RTP port number is 4010, and the compression encoding mode is G.711A.

9. The MGC sends an Add message to MG2 to create a new context on MG2. Below is the signal tracing example:

```
[132.108.95.1]:2944.
```

// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.

```
T=65{C=$
```

// The transaction number is 65. The MGC requests MG2 to create a new context, which is identified by $.

```
{A=a1
```

// Add user a1 in the new context.

```
{M{O{MO=SR}},
// RTP mode of User2 is configured as SendReceive (MO=SR).
E=1{al/of},
// The MGC detects the off-hook of user a1 (al/of).
A=${M{L{.v=0.c=IN IP4 $.m=audio $ RTP/AVP 8.a=ptime:20..},
// The RTP termination descriptor of user a1. See Step 7 for details.
R{.v=0.c=IN IP4 132.108.95.20.m=audio 4010 RTP/AVP 8.a=ptime:20..},
// The RTP termination descriptor of user a2 (the remote end of user a1). See Step 7 for details.
O{MO=SR,nt/jit=40}}}}}
// The RTP mode of user a1 is SendReceive, the maximum jitter buffer (nt/jit) is 40ms.
```

10. MG2 replies the MGC with a Reply message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.30]:2944.
// The protocol type is H.248; the version is 1; the IP address of MG2 is 132.108.95.30; the protocol port number is 2944.
Reply=65{Context=2
// MG2 replies to the MGC with a Reply message and creates a context, whose ID is 2.
{Add=a1,...Add=RTP/1{....Media{.Local{.v=0..c=IN IP4 132.108.95.30..
m=audio 4000 RTP/AVP 8..a=ptime:20..}}}}}.
// Add user a1 and its RTP to the newly created context 2. The IP address of RTP is 132.108.95.30; the RTP port number is 4000; and the compression encoding mode is G.711A.
```

11. The MGC sends a Modify message to MG2. Below is the signal tracing example:

```
[132.108.95.1]:2944.
// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.
T=66{C=2
// The transaction number is 66. The ID of the context encapsulated in the transaction is 2.
{MF=a1{SG{al/ri}}}.
// The MGC sends a Modify message to MG2, requesting MG2 to send the ring tone to the called party a1 (al/ri).
```

12. MG2 replies the MGC with a Reply message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.30]:2944.Reply=66{..Context=2{Modify=a1}.}.
// MG2’s response to the Modify message.
```

13. The MGC sends a Modify message to MG1. Below is the signal tracing example:

```
[132.108.95.1]:2944.
// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.
T=67{C=1
// The transaction number is 67. The ID of the context encapsulated in the transaction is 1.
```

```
{MF=a2{SG{cg/rt}},MF=RTP/0{M{R{.v=0.c=IN IP4 132.108.95.30.m=audio 4000
RTP/AVP 8.a=ptime:20..}}}}}.
```

// The MGC sends a Modify message to MG1, requesting user a2 to play the ring back tone as well as report it to MGC that the RTP IP address of user a1 is 132.108.95.30, the RTP port number of user a1 is 4000; and the compression encoding mode of user a1 is G.711A.

14. MG1 replies the MGC with a Reply message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.20]:2944.
```

// The protocol type is H.248; the version is 1; the IP address of the MG1 is 132.108.95.20; the protocol port number is 2944.

```
Reply=67{Context=1
```

// The transaction number is 67. The ID of the context encapsulated in the transaction is 1.

```
{Modify=a2,...Modify=RTP/0{Media{.Local{.v=0..c=IN IP4 132.108.95.20..
m=audio 4010 RTP/AVP 8..a=ptime:20..}}}}}
```

// TerminationID of the Modify message is a2, and the RTP termination description information of user a2.

15. MG2 detects the off-hook of user a1 and reports the off-hook event to the MGC with a Notify message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.30]:2944.
```

// The protocol type is H.248; the version is 1; the IP address of MG2 is 132.108.95.30; the protocol port number is 2944.

```
Transaction=13{Context=2
```

// The transaction number is 13. The ID of the context encapsulated in the transaction is 2.

```
{Notify=a1{ObservedEvents=1{20000101T00025542:al/of{init=False}}}..}.}
```

// TerminationID of the Notify message is a1. MG2 (gateway of user a1) detects the off-hook of user a1.

16. The MGC replies MG2 with a Reply message. Below is the signal tracing example:

```
[132.108.95.1]:2944.P=13{C=2{N=a1}}.
```

// The MGC’s response to the Notify message.

17. The MGC sends a Modify message to MG2. Below is the signal tracing example:

```
T=68{C=2
```

// The transaction number is 68. The ID of the context encapsulated in the transaction is 2.

```
{MF=a1{E=1{al/on,al/fl},SG{}}}}.
```

// The MGC sends a Modify message to MG2 (gateway of user a1), requesting MG2 to check the on-hook (al/on) and hook-flash (al/fl) events of user a1 as well as stop user a1’s ringing (SG{}).

18. MG2 replies the MGC with a Reply message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.30]:2944.Reply=68{Context=2{.Modify=a1}}
```

// MG2’s response to the Modify message.

19. The MGC sends a Modify message to MG1. Below is the signal tracing example:

```
[132.108.95.1]:2944.
```

// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.

```
T=69{C=1
```

// The transaction number is 69. The ID of the context encapsulated in the transaction is 1.

```
{MF=a2{E=1{al/on},SG{}},MF=RTP/0{M{O{MO=SR}}}}.
```

// The MGC sends Modify message to MG1 (gateway of user a2), requesting MG1 to check the on-hook (al/on) event of user a2, stop user a1's ring back tone (SG{}), and set the RTP mode of user a2 to SendReceive (MO=SR).

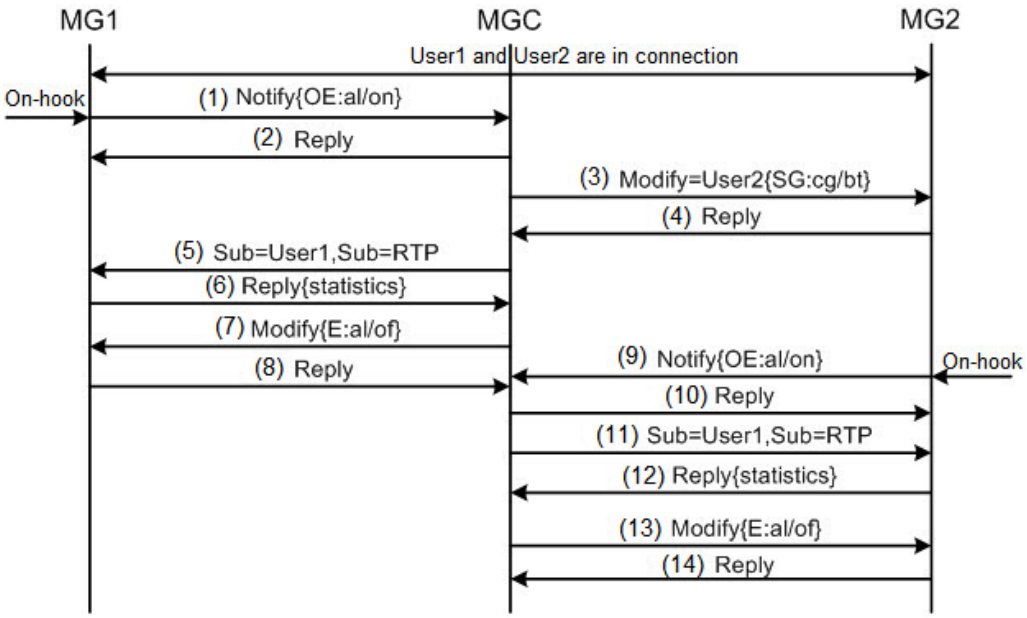
20. MG1 replies the MGC with a Reply message. A normal call is established between User1 and User2. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.20]:2944.Reply=69{Context=1{Modify=a2,Modify=RTP/
0}}
```

// MG1's response to the Modify message.

A.2.6 NOC First Party Release

The call established between user a1 of MG1 (IP address being 132.108.95.20) and user a2 of MG2 (IP address being 132.108.95.30) is released. The IP address of the MGC is 132.108.95.1.



1. MG1 detects the off-hook of user a1 and reports the off-hook event to the MGC with a Notify message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.20]:2944.
// The protocol type is H.248; the version is 1; the IP address of the MG1 is 132.108.95.20; the protocol port number is 2944.
Transaction=30{Context=5
// The transaction number is 30. The ID of the context encapsulated in the transaction is 5.
{Notify=a1{ObservedEvents=1{20000101T06255847:al/on{init=False}}}}}
// MG1 (gateway of user a1) sends a Notify message to the MGC, reporting the on-hook (al/on) event of user a1.
```

2. The MGC replies MG1 with a Reply message. Below is the signal tracing example:

```
[132.108.95.1]:2944.
// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.
P=30{C=5{N=a1}}.
// The MGC’s response to the Notify message.
```

3. The MGC sends a Modify message to MG2. Below is the signal tracing example:

```
T=45{C=6
// The transaction number is 45. The ID of the context encapsulated in the transaction is 6.
{MF=a2{SG{cg/bt}}}}
// The MGC sends a Modify message to MG2 (gateway of user a2), requesting MG2 to play the busy tone (cg/bt) to user a2.
```

4. MG2 replies the MGC with a Reply message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.30]:2944.
// The protocol type is H.248; the version is 1; the IP address of MG2 is 132.108.95.30; the protocol port number is 2944.
Reply=45{Context=6{Modify=a2}}
// The transaction number is 45. MG2’s response to the Modify message.
```

5. The MGC sends a Subtract message to MG1, releasing user a1 and its RTP. Below is the signal tracing example:

```
[132.108.95.1]:2944.
// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.
T=46{C=5
// The transaction number is 46. The ID of the context encapsulated in the transaction is 5.
{S=a1,S=RTP/4}}
// The MGC sends a Subtract message to MG1 to delete user a1 and its RTP from context 5.
```

6. MG1 replies the MGC with a Reply message, releases the resources, and reports the media stream statistics of calling to the MGC. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.20]:2944.
```

// The protocol type is H.248; the version is 1; the IP address of the MG1 is 132.108.95.20; the protocol port number is 2944.

```
Reply=46{Context=5
```

// The transaction number is 46. The ID of the context encapsulated in the transaction is 5.

```
{Subtract=a1{Statistics{amet/cpc=0,amet/pcslr=0}},
```

// MG1 replies to the Subtract message. It releases user a1 and reports the statistics of user a1 to the MGC. The current pulse count (cpc) is 0; the pulse count since last report (pcslr) is 0.

```
Subtract=RTP/4{Statistics{nt/or=183065, nt/os=172000, rtp/delay=0, rtp/
jit=13, rtp/pl=0, rtp/pr=1169, rtp/ps=1075}}}}
```

// MG1 replies to the Subtract message. It releases the RTP of user a1 and reports the RTP statistics of user a1 to the MGC. The received byte number is 183065 (nt/or=183065); the transmitted byte number is 172000 (nt/os=172000); the average delay is 0 (rtp/delay=0); the jitter is 13ms (rtp/jit=13); the packet loss rate is 0 (rtp/pl=0); the received packet number is 1169 (rtp/pr=1169) and the transmitted packet number is 1075 (rtp/ps=1075).

7. The MGC sends a Modify message to MG1. Below is the signal tracing example:

```
[132.108.95.1]:2944.
```

// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.

```
T=47{C=-
```

// The transaction number is 47, the context encapsulated in the transaction is blank.

```
{MF=a1{E=1{al/of}}}}
```

// The MGC sends a Modify message to MG1, requesting MG1 to check the off-hook event (al/of) of user a1.

8. MG1 replies the MGC with a Reply message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.20]:2944.Reply=47{Context=-{Modify=a1}}
```

// MG1’s response to the Modify message.

9. MG2 detects the on-hook of user a2 and reports the on-hook event to the MGC with a Notify message. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.30]:2944.
```

// The protocol type is H.248; the version is 1; the IP address of MG2 is 132.108.95.30; the protocol port number is 2944.

```
Transaction=31{Context=6
```

// The transaction number is 31. The ID of the context encapsulated in the transaction is 6.

```
{Notify=a2{ObservedEvents=1{20000101T06260445:al/on{init=False}}}}}
```

// MG2 (gateway of user a2) sends a Notify message to the MGC, reporting the on-hook (al/on) event of user a2.

10. The MGC replies MG2 with a Reply message. Below is the signal tracing example:

```
[132.108.95.1]:2944.P=31{C=6{N=a2}}
```

// The MGC’s response to the Notify message.

11. The MGC sends a Subtract message to MG2, releasing user a2 and its RTP. Below is the signal tracing example:

```
[132.108.95.1]:2944.
```

// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.

```
T=48{C=6
```

// The transaction number is 48. The ID of the context encapsulated in the transaction is 6.

```
{S=a2,S=RTP/5}}
```

// The MGC sends a Subtract message to MG2 to delete user a2 and its RTP from context 6.

12. MG2 replies the MGC with a Reply message, and reports the media stream statistics of calling to the MGC. Below is the signal tracing example:

```
MEGACO/1 [132.108.95.30]:2944.
```

// The protocol type is H.248; the version is 1; the IP address of MG2 is 132.108.95.30; the protocol port number is 2944.

```
Reply=48{Context=6
```

// The transaction number is 48. The ID of the context encapsulated in the transaction is 6.

```
{Subtract=a2{Statistics{amet/cpc=0, amet/pcslr=0}},
```

// MG2 replies to the Subtract message. It releases user a2 and reports the statistics of user a2 to the MGC. The current pulse count (cpc) is 0; the pulse count since last report (pcslr) is 0.

```
Subtract=RTP/5{Statistics{nt/or=151360, nt/os=237946, rtp/delay=0, rtp/
jit=7, rtp/pl=0, rtp/pr=946, rtp/ps=1513}}}}
```

// MG2 replies to the Subtract message. It releases the RTP of user a2 and reports the RTP statistics of user a2 to the MGC. The received byte number is 151360 (nt/or=151360); the transmitted byte number is 237946 (nt/os=237946); the average delay is 0 (rtp/delay=0); the jitter is 7ms (rtp/jit=7); the packet loss rate is 0 (rtp/pl=0); the received packet number is 946 (rtp/pr=946) and the transmitted packet number is 1513 (rtp/ps=1513).

13. The MGC sends a Modify message to MG2. Below is the signal tracing example:

```
[132.108.95.1]:2944.
```

// The IP address of the MGC is 132.108.95.1, the protocol port number is 2944.

```
T=49{C=-
```

// The transaction number is 49, the context encapsulated in the transaction is blank.

```
{MF=a2{E=1{al/of}}}}
```

// The MGC sends a Modify message to MG1, requesting MG1 to check the off-hook event (al/of) of user a1.

14. MG2 replies the MGC with a Reply message. Below is the signal tracing example:

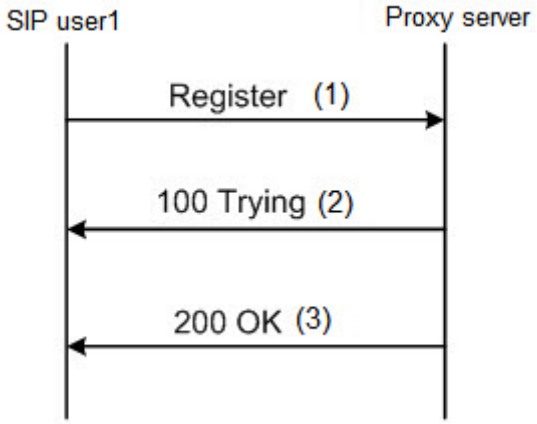
```
MEGACO/1 [132.108.95.30]:2944.Reply=49{Context=-{Modify=a2}}
```

// MG2’s response to the Modify message.

A.3 SIP Signaling Flow Analysis

A.3.1 SIP User Terminal Registration

SIP user1 (telephone number being 77770001) registers to the proxy server (IP address being 32.108.95.1).



1. Before the first call attempt, SIP user1 should send the Register registration request to the proxy server. Below is the signal tracing example:

```
REGISTER sip:132.108.95.1 SIP/2.0..
```

// Start line of the registration request. It means that the SIP user is initiating a registration to the proxy server whose IP address is 132.108.95.1. The SIP version number is 2.0.

```
From:<sip:77770001@132.108.95.1>;tag=10095010-505f6c84-13c4-386d43b7-7951437d-386d43b7..
```

// The "From" header field. This field indicates the logical identity of the initiator of the request. The above field shows that the request message is initiated by the SIP user1 (telephone number being 77770001) of the proxy server (IP address being 132.108.95.1).

```
To: <sip:77770001@132.108.95.1>..
```

// The "To" header field. This field shows the address to receive the request message. Here it refers to the IP address of the proxy server.

```
Call-ID: 1009c068-505f6c84-13c4-386d43b7-2e101815-386d43b7..
```

// The "Call-ID" header field. This field is a globally unique identifier identifying a particular invitation.

```
CSeq: 5 REGISTER..
```

// The "CSeq" header field. This field is used to match a response to the request it refers to. It consists of a sequence number and a method. The "CSeq" header field serves to order transactions within a dialog, to provide a means to uniquely identify transactions, and to differentiate between new requests and request retransmissions.

Via: SIP/2.0/UDP132.108.95.80:5060; branch=z9hG4bK-386d476a-6adef794-6dcf9c84..

// The "Via" header field. This field indicates the path taken by the request so far and indicates the path that should be followed in routing responses. SIP/2.0/UDP indicates the transmission protocol: The protocol is SIP, the version is 2.0, the transport layer is UDP, and the IP address of the SIP user that sends the request message is 132.108.95.80.

Max-Forwards: 70..

// The "Max-Forwards" header field. This field serves to limit the number of hops a request can transit on the way to its destination. The default value is 70.

Supported: 100rel,replaces,timer..

// The "Supported" header field. This field enumerates all the extensions supported by the UA. If empty, it means that no extensions are supported.

Contact: <sip:77770001@132.108.95.80:5060>..

// The "Contact" header field. In a registration request, this field specifies the location reachable from the user. Here it means that the SIP user's current IP address is 132.108.95.80 and the telephone number is 77770001.

Expires: 3600..

// The "Expires" header field. This field gives the relative time after which the message (or content) expires. Here it means this registration request will expire after 3600 seconds.

Content-Length: 0........

// The "Content-Length" header field. This field means the length of the message body is 0. This field has no dialog description.

2. The proxy server sends a response message 100 Trying to SIP user1. The message means that the proxy server is processing the request. Below is the signal tracing example:

SIP/2.0 100 Trying..

// Start line of the 100 Trying message.

Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d476a-6adef794-6dcf9c84..

// The "Via" header field. Here 132.108.95.80 is the IP address of the SIP user that sends the request message.

From:<sip:77770001@132.108.95.1>;tag=10095010-505f6c84-13c4-386d43b7-7951437d-386d43b7..

// The "From" header field. This field indicates the logical identity of the initiator of the request.

To:<sip:77770001@132.108.95.1>..

// The "To" header field. This field shows address to receive the request message.

Call-ID: 1009c068-505f6c84-13c4-386d43b7-2e101815-386d43b7..

// The "Call-ID" header field. This field uniquely identifies the invitation sent from SIP user1, and it is globally unique.

CSeq: 5 REGISTER..

// The "CSeq" header field, which is used to match a response to the request it refers to.

Content-Length: 0........

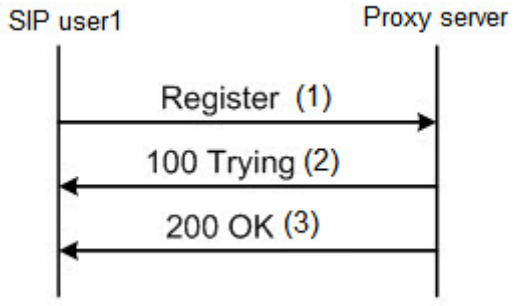
// The "Content-Length" header field. This field means the length of the request's message body is 0.

3. The proxy server sends a response message 200 OK to SIP user1, which means the registration is successful. Below is the signal tracing example:

```
SIP/2.0 200 OK..
```
// Start line of the 200 OK message.
```
Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d476a-6adef794-6dcf9c84..
```
// The "Via" header field. Here 132.108.95.80 is the IP address of the SIP user that sends the request message.
```
From:<sip:77770001@132.108.95.1>;tag=10095010-505f6c84-13c4-386d43b7-7951437d-386d43b7..
```
// The "From" header field. This field indicates the logical identity of the initiator of the request.
```
To:<sip:77770001@132.108.95.1>;tag=1282621041031-812906075..
```
// The "To" header field. This field shows address to receive the request message.
```
Call-ID: 1009c068-505f6c84-13c4-386d43b7-2e101815-386d43b7..
```
// The "Call-ID" header field. This field uniquely identifies the invitation sent from SIP user1, and it is globally unique.
```
CSeq: 5 REGISTER..
```
// The "CSeq" header field, which is used to match a response to the request it refers to.
```
Contact: <sip:77770001@132.108.95.80:5060>;expires=3600;q=1.0..
```
// The "Contact" header field. In a registration request, this field specifies the location reachable from the user.
```
Content-Length: 0.....
```
// The "Content-Length" header field. This field means the length of the request's message body is 0.

A.3.2 SIP User Terminal Logout

SIP user1 (telephone number being 77770001) applies to the proxy server (IP address being 132.108.95.1) for logout.



1. SIP user1 sends a Register message to the proxy server requesting logout. In the logout message, the "Expires" header field is 0. Below is the signal tracing example:

```
REGISTER sip:132.108.95.1 SIP/2.0..From: <sip:77770001@132.108.95.1>;
tag=10095010-505f6c84-13c4-386d43b7-7951437d-386d43b7..To:
<sip:77770001@132.108.95.1>..Call-ID: 1009c068-505f6c84-13c4-386d43b7-
2e101815-386d43b7..CSeq: 4 REGISTER..Via: SIP/2.0/UDP 132.108.95.80:5060;
branch=z9hG4bK-386d4757-6adeabf0-6b4d112f..Max-Forwards: 70..Supported:
100rel,replaces,timer..Contact: <sip:77770001@132.108.95.80:5060>..
Expires: 0..Content-Length: 0........
```

2. The proxy server sends a response message 100 Trying to SIP user1. The message means that the proxy server is processing the request. Below is the signal tracing example:

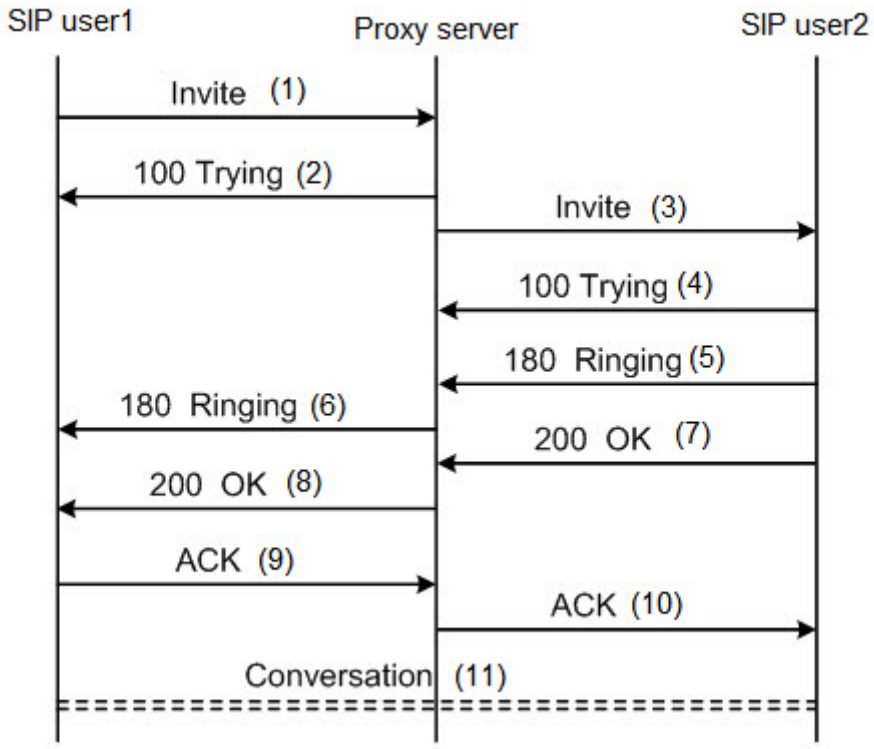
```
SIP/2.0 100 Trying..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-
386d4757-6adeabf0-6b4d112f..From: <sip:77770001@132.108.95.1>;
tag=10095010-505f6c84-13c4-386d43b7-7951437d-386d43b7..To:
<sip:77770001@132.108.95.1>..Call-ID: 1009c068-505f6c84-13c4-386d43b7-
2e101815-386d43b7..CSeq: 4 REGISTER..Server: Brekeke OnDO SIP Server
(rev.172)..Content-Length: 0....H...
```

3. The proxy server sends a response message 200 OK to SIP user1, and clears the data related to SIP user1 in the database. Below is the signal tracing example:

```
SIP/2.0 200 OK..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-
386d4757-6adeabf0-6b4d112f..From: <sip:77770001@132.108.95.1>;
tag=10095010-505f6c84-13c4-386d43b7-7951437d-386d43b7..To:
<sip:77770001@132.108.95.1>;tag=1282621021671-931396014..Call-ID:
1009c068-505f6c84-13c4-386d43b7-2e101815-386d43b7..CSeq: 4 REGISTER..
Contact: <sip:77770001@132.108.95.80:5060>;expires=0;q=1.0..Server:
Brekeke OnDO SIP Server (rev.172)..Content-Length: 0.....
```

A.3.3 Establishing a Normal Call

Establish a normal call between SIP user1 (telephone number being 77770002) and SIP user2 (telephone number being 77770001) of the proxy server (IP address being 132.108.95.1).



1. The SIP user1 initiates an Invite request to the proxy server. The “Allow” field of the request message lists the methods supported by the SIP user terminal, including Invite, ACK and Cancel; the “Content-Type” header field identifies the media type of the message body transmitted to the opposite party. Below is the signal tracing example:

```
INVITE sip:77770001@132.108.95.1 SIP/2.0..From:
<sip:77770002@132.108.95.1>;tag=10097110-505f6c84-13c4-386d48df-
eef7cc7-386d48df..To: <sip:77770001@132.108.95.1>..Call-ID: 1009af80-
505f6c84-13c4-386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 1 INVITE..
Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d48df-6ae4a798-
1ead2944..Allow: INVITE,ACK,CANCEL,BYE,REGISTER,REFER,NOTIFY,PRACK,
CANCEL,SUBSCRIBE,OPTIONS,INFO,UPDATE..Max-Forwards: 70..Supported:
100rel,replaces,timer..Contact: <sip:77770002@132.108.95.80:5060>..
Content-Type: application/SDP..Content-Length: 226....v=0..o=77770002
946686175 946686175 IN IP4 132.108.95.80..s=-..c=IN IP4 132.108.95.80..t=0
0..m=audio 4010 RTP/AVP 8 0 18 4..a=rtpmap:8 PCMA/8000..a=rtpmap:0 PCMU/
8000..a=rtpmap:18 G729/8000..a=rtpmap:4 G723/8000..a=ptime:20..*b..
```

2. The proxy server sends a response message 100 Trying to SIP user1. The message means that the proxy server is processing the request. Below is the signal tracing example:

SIP/2.0 100 Trying..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d48df-6ae4a798-1ead2944..From: <sip:77770002@132.108.95.1>;tag=10097110-505f6c84-13c4-386d48df-eef7cc7-386d48df..To: <sip:77770001@132.108.95.1>..Call-ID: 1009af80-505f6c84-13c4-386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 1 INVITE..Server: Brekeke OnDO SIP Server (rev.172)..Content-Length: 0....7[..

3. After confirming the SIP user1 has passed the authentication, the proxy server forwards the Invite request to the terminal user indicated by the “To” header field of the Invite message. Below is the signal tracing example:

INVITE sip:77770001@132.108.95.80:5060 SIP/2.0..From: <sip:77770002@132.108.95.1>;tag=10097110-505f6c84-13c4-386d48df-eef7cc7-386d48df..To: <sip:77770001@132.108.95.1:5060>..Call-ID: 1009af80-505f6c84-13c4-386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 1 INVITE..Via: SIP/2.0/UDP 132.108.95.1:5060;rport;branch=z9hG4bKccd69d69154f8bac.1..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d48df-6ae4a798-1ead2944..Allow: INVITE,ACK,CANCEL,BYE,REGISTER,REFER,NOTIFY,PRACK,CANCEL,SUBSCRIBE,OPTIONS,INFO,UPDATE..Max-Forwards: 69..Supported: 100rel,replaces,timer..Contact: <sip:77770002@132.108.95.1:5060>..Record-Route: <sip:132.108.95.1:5060;lr>..Content-Type: application/sdp..Content-Length: 226....v=0..o=77770002 946686175 946686175 IN IP4 132.108.95.80..s=-..c=IN IP4 132.108.95.80..t=0 0..m=audio 4010 RTP/AVP 8 0 18 4..a=rtpmap:8 PCMA/8000..a=rtpmap:0 PCMU/8000..a=rtpmap:18 G729/8000..a=rtpmap:4 G723/8000..a=ptime:20......

4. The SIP user2 sends a response message 100 Trying to the proxy server. Below is the signal tracing example:

SIP/2.0 100 Trying..From: <sip:77770002@132.108.95.1>;tag=10097110-505f6c84-13c4-386d48df-eef7cc7-386d48df..To: <sip:77770001@132.108.95.1:5060>..Call-ID: 1009af80-505f6c84-13c4-386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 1 INVITE..Via: SIP/2.0/UDP 132.108.95.1:5060;rport=5060;branch=z9hG4bKccd69d69154f8bac.1..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d48df-6ae4a798-1ead2944..Supported: 100rel,replaces,timer..Contact: <sip:77770001@132.108.95.80:5060>..Content-Length: 0....>T..

5. The SIP user2 rings and sends the ringing message 180 Ringing to the proxy server. Below is the signal tracing example:

SIP/2.0 180 Ringing..From: <sip:77770002@132.108.95.1>;tag=10097110-505f6c84-13c4-386d48df-eef7cc7-386d48df..To: <sip:77770001@132.108.95.1:5060>;tag=10097950-505f6c84-13c4-386d48df-2c64722-386d48df..Call-ID: 1009af80-505f6c84-13c4-386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 1 INVITE..Via: SIP/2.0/UDP 132.108.95.1:5060;

rport=5060;branch=z9hG4bKccd69d69154f8bac.1..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d48df-6ae4a798-1ead2944.. Supported: 100rel,replaces,timer..Contact: <sip:77770001@132.108.95.80:5060>..Record-Route: <sip:132.108.95.1:5060; lr>..Content-Length: 0........

6. The proxy server forwards the ringing message to SIP user1. Below is the signal tracing example:

SIP/2.0 180 Ringing..From: <sip:77770002@132.108.95.1>;tag=10097110-505f6c84-13c4-386d48df-eef7cc7-386d48df..To: <sip:77770001@132.108.95.1>;tag=10097950-505f6c84-13c4-386d48df-2c64722-386d48df..Call-ID: 1009af80-505f6c84-13c4-386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 1 INVITE..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d48df-6ae4a798-1ead2944.. Supported: 100rel,replaces,timer..Contact: <sip:77770001@132.108.95.1:5060>..Record-Route: <sip:132.108.95.1:5060; lr>..Content-Length: 0........

7. The SIP user2 picks up the telephone and sends a response message 200 OK indicating the success of connection to the proxy server. SDP description is included in the message. Below is the signal tracing example:

SIP/2.0 200 OK..From: <sip:77770002@132.108.95.1>;tag=10097110-505f6c84-13c4-386d48df-eef7cc7-386d48df..To: <sip:77770001@132.108.95.1:5060>; tag=10097950-505f6c84-13c4-386d48df-2c64722-386d48df..Call-ID: 1009af80-505f6c84-13c4-386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 1 INVITE.. Allow: INVITE,ACK,CANCEL,BYE,REGISTER,REFER,NOTIFY,PRACK,CANCEL, SUBSCRIBE,OPTIONS,INFO,UPDATE..Via: SIP/2.0/UDP 132.108.95.1:5060; rport=5060;branch=z9hG4bKccd69d69154f8bac.1..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d48df-6ae4a798-1ead2944.. Supported: 100rel,replaces,timer..Contact: <sip:77770001@132.108.95.80:5060>..Record-Route: <sip:132.108.95.1:5060; lr>..Content-Type: application/SDP..Content-Length: 238....v=0.. o=77770001 946686176 946686176 IN IP4 132.108.95.80..s=-..c=IN IP4 132.108.95.80..t=0 0..m=audio 4000 RTP/AVP 8 0 18 4..a=rtpmap:8 PCMA/8000.. a=rtpmap:0 PCMU/8000..a=rtpmap:18 G729/8000..a=rtpmap:4 G723/8000.. a=ptime:20..a=sendrecv...d..

8. The proxy server forwards the connection success message to SIP user1. Below is the signal tracing example:

SIP/2.0 200 OK..From: <sip:77770002@132.108.95.1>;tag=10097110-505f6c84-13c4-386d48df-eef7cc7-386d48df..To: <sip:77770001@132.108.95.1>; tag=10097950-505f6c84-13c4-386d48df-2c64722-386d48df..Call-ID: 1009af80-505f6c84-13c4-386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 1 INVITE.. Allow: INVITE,ACK,CANCEL,BYE,REGISTER,REFER,NOTIFY,PRACK,CANCEL,

SUBSCRIBE,OPTIONS,INFO,UPDATE..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d48df-6ae4a798-1ead2944..Supported: 100rel,replaces,timer..Contact: <sip:77770001@132.108.95.1:5060>..Record-Route: <sip:132.108.95.1:5060;lr>..Content-Type: application/sdp..Content-Length: 238....v=0..o=77770001 946686176 946686176 IN IP4 132.108.95.80..s=-..c=IN IP4 132.108.95.80..t=0 0..m=audio 4000 RTP/AVP 8 0 18 4..a=rtpmap:8 PCMA/8000..a=rtpmap:0 PCMU/8000..a=rtpmap:18 G729/8000..a=rtpmap:4 G723/8000..a=ptime:20..a=sendrecv..;...

9. After the SIP user1 receives the connection success message, it sends an ACK acknowledgement message to the proxy server. Below is the signal tracing example:

ACK sip:77770001@132.108.95.1:5060 SIP/2.0..From: <sip:77770002@132.108.95.1>;tag=10097110-505f6c84-13c4-386d48df-eef7cc7-386d48df..To: <sip:77770001@132.108.95.1>;tag=10097950-505f6c84-13c4-386d48df-2c64722-386d48df..Call-ID: 1009af80-505f6c84-13c4-386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 1 ACK..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d48e1-6ae4b05e-5f47e4cc..Max-Forwards: 70..Contact: <sip:77770002@132.108.95.80:5060>..Route: <sip:132.108.95.1:5060;lr>..Content-Length: 0....D...

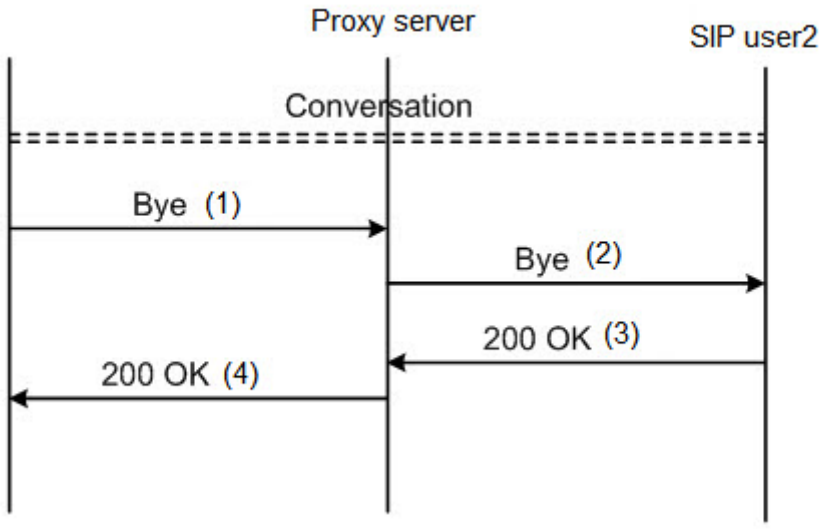
10. The proxy server forwards the ACK acknowledgement message to SIP user2. Below is the signal tracing example:

ACK sip:77770001@132.108.95.80:5060 SIP/2.0..From: <sip:77770002@132.108.95.1>;tag=10097110-505f6c84-13c4-386d48df-eef7cc7-386d48df..To: <sip:77770001@132.108.95.1:5060>;tag=10097950-505f6c84-13c4-386d48df-2c64722-386d48df..Call-ID: 1009af80-505f6c84-13c4-386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 1 ACK..Via: SIP/2.0/UDP 132.108.95.1:5060;rport;branch=z9hG4bKfcdef8b04d989bac.1..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d48e1-6ae4b05e-5f47e4cc..Max-Forwards: 69..Contact: <sip:77770002@132.108.95.1:5060>..Record-Route: <sip:132.108.95.1:5060;lr>..Content-Length: 0........

11. The communication connection is established between the calling and called users. A normal dialog starts.

A.3.4 Performing a Normal Call Release

The SIP user1 (telephone number being 77770002) hooks on and releases the connection.



1. After the dialog is ended, the calling party SIP user1 hooks on and sends a Bye message to the proxy server. Below is the signal tracing example:

```
BYE sip:77770001@132.108.95.1:5060 SIP/2.0..From:
<sip:77770002@132.108.95.1>;tag=10097110-505f6c84-13c4-386d48df-
eef7cc7-386d48df..To: <sip:77770001@132.108.95.1>;tag=10097950-505f6c84-
13c4-386d48df-2c64722-386d48df..Call-ID: 1009af80-505f6c84-13c4-
386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 2 BYE..Via: SIP/2.0/UDP
132.108.95.80:5060;branch=z9hG4bK-386d48e2-6ae4b61c-357664e0..Max-
Forwards: 70..Supported: 100rel,replaces,timer..Route:
<sip:132.108.95.1:5060;lr>..Content-Length: 0....P...
```

2. The proxy server transmits the Bye message to the called party SIP user2. Below is the signal tracing example:

```
BYE sip:77770001@132.108.95.80:5060 SIP/2.0..From:
<sip:77770002@132.108.95.1>;tag=10097110-505f6c84-13c4-386d48df-
eef7cc7-386d48df..To: <sip:77770001@132.108.95.1:5060>;tag=10097950-
505f6c84-13c4-386d48df-2c64722-386d48df..Call-ID: 1009af80-505f6c84-
13c4-386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 2 BYE..Via: SIP/2.0/
UDP 132.108.95.1:5060;rport;branch=z9hG4bK954f3aac5d14dbac.1..Via: SIP/
2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d48e2-6ae4b61c-357664e0..
Max-Forwards: 69..Supported: 100rel,replaces,timer..Record-Route:
<sip:132.108.95.1:5060;lr>..Content-Length: 0........
```

3. SIP user2 sends a response message 200 OK to the proxy server confirming the on-hook. Below is the signal tracing example:

```
SIP/2.0 200 OK..From: <sip:77770002@132.108.95.1>;tag=10097110-505f6c84-
13c4-386d48df-eef7cc7-386d48df..To: <sip:77770001@132.108.95.1:5060>;
tag=10097950-505f6c84-13c4-386d48df-2c64722-386d48df..Call-ID: 1009af80-
505f6c84-13c4-386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 2 BYE..Via:
```

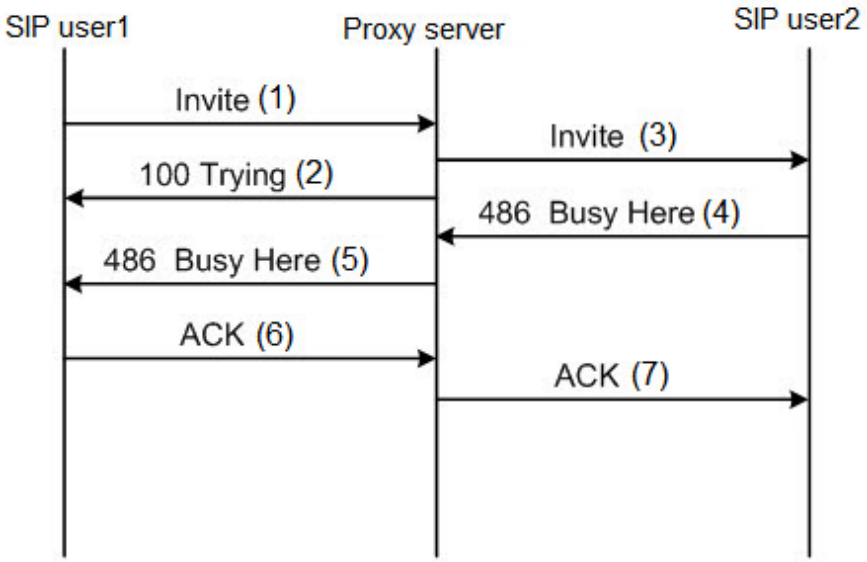
```
SIP/2.0/UDP 132.108.95.1:5060;rport=5060;
branch=z9hG4bK954f3aac5d14dbac.1..Via: SIP/2.0/UDP 132.108.95.80:5060;
branch=z9hG4bK-386d48e2-6ae4b61c-357664e0..Supported: 100rel,replaces,
timer..Content-Length: 0.....E..
```

4. The proxy server forwards the response message to SIP user1. Below is the signal tracing example:

```
SIP/2.0 200 OK..From: <sip:77770002@132.108.95.1>;tag=10097110-505f6c84-
13c4-386d48df-eef7cc7-386d48df..To: <sip:77770001@132.108.95.1>;
tag=10097950-505f6c84-13c4-386d48df-2c64722-386d48df..Call-ID: 1009af80-
505f6c84-13c4-386d48df-23f0cd46-386d48df@132.108.95.1..CSeq: 2 BYE..Via:
SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d48e2-6ae4b61c-
357664e0..Supported: 100rel,replaces,timer..Content-Length: 0.....]..
```

A.3.5 The Called Party Being Busy

SIP user1 (telephone number being 77770001) of the proxy server (IP address being 132.108.95.1) calls SIP user2 (telephone number being 77770002). Since SIP user2 is busy, SIP user1 releases the connection.



1. The SIP user1 initiates an Invite request to the proxy server. SIP user1 (77770001@132.108.95.1) of the proxy server (IP address being 132.108.95.1) calls SIP user2 (77770002@132.108.95.1). Below is the signal tracing example:

```
INVITE sip:77770002@132.108.95.1 SIP/2.0..From:
<sip:77770001@132.108.95.1>;tag=10097950-505f6c84-13c4-386d450f-
```

248cde39-386d450f..To: <sip:77770002@132.108.95.1>..Call-ID: 10098f00-505f6c84-13c4-386d450f-5756a230-386d450f@132.108.95.1..CSeq: 1 INVITE..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d450f-6ad5c37a-168c62ce..Allow: INVITE,ACK,CANCEL,BYE,REGISTER,REFER,NOTIFY,PRACK,CANCEL,SUBSCRIBE,OPTIONS,INFO,UPDATE..Max-Forwards: 70..Supported: 100rel,replaces,timer..Contact: <sip:77770001@132.108.95.80:5060>..Content-Type: application/SDP..Content-Length: 226....v=0..o=77770001 946685199 946685199 IN IP4 132.108.95.80..s=-..c=IN IP4 132.108.95.80..t=0 0..m=audio 4000 RTP/AVP 8 0 18 4..a=rtpmap:8 PCMA/8000..a=rtpmap:0 PCMU/8000..a=rtpmap:18 G729/8000..a=rtpmap:4 G723/8000..a=ptime:20......

2. The proxy server sends a response message 100 Trying to SIP user1 indicating that the request is in process. Below is the signal tracing example:

SIP/2.0 100 Trying..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d450f-6ad5c37a-168c62ce..From: <sip:77770001@132.108.95.1>;tag=10097950-505f6c84-13c4-386d450f-248cde39-386d450f..To: <sip:77770002@132.108.95.1>..Call-ID: 10098f00-505f6c84-13c4-386d450f-5756a230-386d450f@132.108.95.1..CSeq: 1 INVITE..Server: Brekeke OnDO SIP Server (rev.172)..Content-Length: 0........

3. After receiving the request message, the proxy server forwards the Invite request message to SIP user2. Below is the signal tracing example:

INVITE sip:77770002@132.108.95.80:5060 SIP/2.0..From: <sip:77770001@132.108.95.1>;tag=10097950-505f6c84-13c4-386d450f-248cde39-386d450f..To: <sip:77770002@132.108.95.1:5060>..Call-ID: 10098f00-505f6c84-13c4-386d450f-5756a230-386d450f@132.108.95.1..CSeq: 1 INVITE..Via: SIP/2.0/UDP 132.108.95.1:5060;rport;branch=z9hG4bKf527779acf7c6bac.1..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d450f-6ad5c37a-168c62ce..Allow: INVITE,ACK,CANCEL,BYE,REGISTER,REFER,NOTIFY,PRACK,CANCEL,SUBSCRIBE,OPTIONS,INFO,UPDATE..Max-Forwards: 69..Supported: 100rel,replaces,timer..Contact: <sip:77770001@132.108.95.1:5060>..Record-Route: <sip:132.108.95.1:5060;lr>..Content-Type: application/sdp..Content-Length: 226....v=0..o=77770001 946685199 946685199 IN IP4 132.108.95.80..s=-..c=IN IP4 132.108.95.80..t=0 0..m=audio 4000 RTP/AVP 8 0 18 4..a=rtpmap:8 PCMA/8000..a=rtpmap:0 PCMU/8000..a=rtpmap:18 G729/8000..a=rtpmap:4 G723/8000..a=ptime:20......

4. The calling request message is sent to SIP user2. The called party is busy, so SIP user2 transmits a called party busy message 486 Busy Here to the proxy server. Below is the signal tracing example:

SIP/2.0 486 Busy Here..From: <sip:77770001@132.108.95.1>;tag=10097950-505f6c84-13c4-386d450f-248cde39-386d450f..To: <sip:77770002@132.108.95.1:5060>;tag=10097ab0-505f6c84-13c4-386d450f-

5b608f4c-386d450f..Call-ID: 10098f00-505f6c84-13c4-386d450f-5756a230-386d450f@132.108.95.1..CSeq: 1 INVITE..Via: SIP/2.0/UDP 132.108.95.1:5060;rport=5060;branch=z9hG4bKf527779acf7c6bac.1..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d450f-6ad5c37a-168c62ce..Supported: 100rel,replaces,timer..Content-Length: 0....X...

5. The proxy server forwards the called party busy response to SIP user1. Below is the signal tracing example:

SIP/2.0 486 Busy Here..From: <sip:77770001@132.108.95.1>;tag=10097950-505f6c84-13c4-386d450f-248cde39-386d450f..To: <sip:77770002@132.108.95.1>;tag=10097ab0-505f6c84-13c4-386d450f-5b608f4c-386d450f..Call-ID: 10098f00-505f6c84-13c4-386d450f-5756a230-386d450f@132.108.95.1..CSeq: 1 INVITE..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d450f-6ad5c37a-168c62ce..Supported: 100rel,replaces,timer..Content-Length: 0....uB..

6. After SIP user1 receives the message, it sends an ACK acknowledgement message to the proxy server. Below is the signal tracing example:

ACK sip:77770002@132.108.95.1 SIP/2.0..From: <sip:77770001@132.108.95.1>;tag=10097950-505f6c84-13c4-386d450f-248cde39-386d450f..To: <sip:77770002@132.108.95.1>;tag=10097ab0-505f6c84-13c4-386d450f-5b608f4c-386d450f..Call-ID: 10098f00-505f6c84-13c4-386d450f-5756a230-386d450f@132.108.95.1..CSeq: 1 ACK..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d450f-6ad5c37a-168c62ce..Max-Forwards: 70..Contact: <sip:77770001@132.108.95.80:5060>..Content-Length: 0....J...

7. The proxy server forwards the ACK acknowledgement message to SIP user2, and this call is released. Below is the signal tracing example:

ACK sip:77770002@132.108.95.80:5060 SIP/2.0..From: <sip:77770001@132.108.95.1>;tag=10097950-505f6c84-13c4-386d450f-248cde39-386d450f..To: <sip:77770002@132.108.95.1:5060>;tag=10097ab0-505f6c84-13c4-386d450f-5b608f4c-386d450f..Call-ID: 10098f00-505f6c84-13c4-386d450f-5756a230-386d450f@132.108.95.1..CSeq: 1 ACK..Via: SIP/2.0/UDP 132.108.95.1:5060;rport;branch=z9hG4bKf527779acf7c6bac.1..Via: SIP/2.0/UDP 132.108.95.80:5060;branch=z9hG4bK-386d450f-6ad5c37a-168c62ce..Max-Forwards: 69..Contact: <sip:77770001@132.108.95.1:5060>..Record-Route: <sip:132.108.95.1:5060;lr>..Content-Length: 0....e...

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