

Access Network Products

Troubleshooting Guide

Issue 03
Date 2021-08-10



Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
 Bantian, Longgang
 Shenzhen 518129
 People's Republic of China

Website: <https://www.huawei.com>

Email: support@huawei.com

Contents

1 About This Document.....	1
2 Compliance and Safety.....	3
2.1 Regulatory Compliance Information.....	3
2.1.1 Regulatory Compliance Standards.....	4
2.1.2 European Directives Compliance.....	4
2.1.3 Japan Compliance.....	5
2.1.4 CISPR 32 Compliance.....	6
2.1.5 India RoHS hazardous substance table.....	6
2.1.6 Other Markets.....	7
2.2 Safety Information.....	7
2.2.1 General Safety Precautions.....	7
2.2.2 Installation Environment.....	11
2.2.2.1 Indoor Installation.....	11
2.2.2.2 Outdoor Installation.....	12
2.2.3 Electrical Safety.....	13
2.2.3.1 Grounding.....	13
2.2.3.2 AC/DC Operation.....	13
2.2.3.3 Cabling Requirements.....	14
2.2.3.4 TNV Circuits.....	14
2.2.3.5 ESD Requirements.....	15
2.2.4 Battery Safety.....	15
2.2.4.1 Basic Requirements.....	15
2.2.4.2 Requirements for Rechargeable Batteries.....	16
2.2.4.3 Requirements for Non-Rechargeable Batteries.....	17
2.2.5 Radiation Safety.....	17
2.2.5.1 Electromagnetic Field Exposure.....	17
2.2.5.2 Laser Radiation.....	19
2.2.6 Mechanical Safety.....	20
2.2.7 Maintenance Safety.....	22
2.2.8 Safety Signs.....	23
3 Maintenance Engineers' Must-Read.....	26
3.1 Skill Requirements.....	26

3.2 Troubleshooting Precautions.....	27
3.3 Troubleshooting Procedure.....	28
3.4 Frequently Used Methods for Troubleshooting.....	30
3.5 How to Obtain Technical Support from Huawei.....	32

4 Field Maintenance Guide.....34

4.1 Basic Principles of the Maintenance.....	35
4.2 Maintenance Recommendations for the Third-Party Device.....	37
4.3 Checking the Grounding of the Device.....	37
4.4 Checking the Hardware Status of Fans.....	39
4.5 Checking the Cabinet Appearance of the Cabinet.....	41
4.6 Checking the Battery.....	41
4.7 Cleaning the Air Filter of the Cabinet.....	43

5 Commonly Used Methods of Fault Locating and Troubleshooting.....46

5.1 Service Emulation Test.....	47
5.1.1 DHCP Emulation.....	47
5.1.1.1 DHCP Emulation Overview.....	47
5.1.1.2 DHCP Emulation Principles.....	48
5.1.1.3 DHCP Emulation Usage Scenario.....	50
5.1.1.4 Configuring DHCP Emulation.....	53
5.1.1.5 DHCP Emulation Reference Standards and Protocols.....	58
5.1.2 PPPoE Dialup Emulation.....	58
5.1.2.1 PPPoE Dialup Emulation Introduction.....	58
5.1.2.2 PPPoE Dialup Emulation Principles.....	59
5.1.2.3 PPPoE Dialup Emulation Usage Scenario.....	61
5.1.2.4 Configuring PPPoE Dialup Emulation.....	63
5.1.2.5 PPPoE Dialup Emulation Reference Standards and Protocols.....	66
5.1.3 Multicast Emulation.....	66
5.1.3.1 Introduction.....	66
5.1.3.2 Reference Standards and Protocols.....	67
5.1.3.3 Principles.....	67
5.1.3.4 Usage Scenario.....	69
5.1.3.5 Configuration.....	76
5.1.4 Call Emulation Test.....	77
5.1.4.1 Introduction to the Call Emulation Test.....	78
5.1.4.2 Principles of the Call Emulation Test.....	79
5.1.4.3 Configuring the Call Emulation Test.....	87
5.2 Common Methods of Locating Voice Service Faults.....	87
5.2.1 POTS User Circuit Test.....	88
5.2.2 POTS User Loop Line Test.....	90
5.2.3 POTS Port Loop Test.....	95
5.2.4 Search Tone Test.....	97
5.2.5 Signal Tone Test.....	99

5.2.6 Line Matching Test.....	101
5.3 Common Methods for Locating DSL Faults.....	103
5.3.1 Common DSL Faults.....	103
5.3.2 MELT Test.....	104
5.3.2.1 Introduction.....	104
5.3.2.2 Electrical Parameter Test.....	105
5.3.2.3 Search Tone Test.....	111
5.3.2.4 Reference Standards and Protocols.....	111
5.3.2.5 Principles.....	111
5.3.3 Loopback on a VDSL2 Port.....	113
5.3.4 Loopback on a G.fast Port.....	115
5.3.5 Changing the Line Profile (Template) Configured on a DSL Port.....	117
5.3.6 Changing the Traffic Profile of a DSL Port.....	119
5.3.7 Locating and Troubleshooting of a Vectoring Activation Failure.....	120
5.4 Common Fault Location and Rectification Methods for E1 Lines.....	121
5.4.1 Common E1 Line Faults.....	121
5.4.2 Performing a Loopback on an E1 Port.....	122
5.4.3 Performing a Loopback on an E1 Line.....	125
5.5 Diagnosing Broadband Protocol Related Faults.....	126
5.5.1 Introduction.....	126
5.5.2 Diagnosis Based on an ACL Rule.....	127
5.5.3 Diagnosis Based on a Service Port.....	129
5.5.4 Diagnosis by ACL-matched Traffic Mirroring on the Upstream Port.....	130
5.5.5 Diagnosis by Mirroring on the Upstream Port.....	130
5.5.6 Remote Diagnosis on TCP Traffic.....	131
5.6 Methods of Locating and Troubleshooting Common ODN Faults.....	132
5.6.1 Common ODN Faults.....	132
5.6.2 ODN-Related Alarms.....	141
5.6.3 Checking the Optical Power.....	141
5.6.3.1 Analyzing the Optical Power.....	141
5.6.3.2 Querying the Optical Power Using the CLI.....	144
5.6.3.3 Measuring the Upstream Optical Power Using the Optical Power Meter.....	145
5.6.3.4 Measuring the Downstream Optical Power Using the Optical Power Meter.....	147
5.6.4 Using the OTDR to Locate Abnormal Attenuation Points on the Optical Line.....	149
5.6.5 Checking Whether the Optical Fiber Is Damaged Using the Red Pointer.....	157
5.6.6 Cleaning the Connector of an Optical Fiber.....	158
5.7 Locating and Troubleshooting ONT Faults.....	162
5.7.1 ONT-Related Alarms.....	162
5.7.2 Querying ONT Information.....	163
5.7.3 Collecting ONT Performance Statistics.....	164
5.7.4 ONT Call Emulation.....	167
5.7.4.1 Introduction to ONT Call Emulation.....	167

5.7.4.2 Principles of ONT Call Emulation.....	169
5.7.4.3 Configuring ONT Call Emulation.....	173
5.7.5 ONT Loop-Line Test.....	177
5.7.5.1 Introduction to ONT Loop Test.....	177
5.7.5.2 Principles of ONT Loop Test.....	177
5.7.5.3 Configuring ONT Loop Test.....	178
5.7.5.4 Reference Documents of ONT Loop Test.....	181
5.7.6 Pinging from an ONT Remotely.....	181
5.7.7 Restoring Factory Defaults.....	181
5.7.8 Resetting an ONT.....	182
5.7.9 Detecting a Rogue ONT.....	183
5.7.10 Replacing an ONT.....	187
5.8 Traffic Burst Detection.....	188
5.8.1 Traffic Burst Detection Overview.....	188
5.8.2 Traffic Burst Detection Principle.....	188
5.8.3 Traffic Burst Detection Application Scenario.....	190
5.8.4 Configure Traffic Burst Detection.....	192
5.9 Packet Loss Query.....	194
5.10 PPPoE Echo Packet Monitoring on the Upstream Port.....	199
6 GPON ONU Abnormal State.....	201
6.1 Failure to Go Online of a GPON ONU.....	201
6.1.1 Fault Identification and Demarcation.....	202
6.1.2 Alarming Handling.....	203
6.1.3 OLT Fault.....	204
6.1.4 ODN Fault.....	206
6.1.5 ONU Fault.....	210
6.2 Failure to Recover GPON ONU Configurations.....	213
6.2.1 Fault Identification and Demarcation.....	213
6.2.2 Alarming Handling.....	214
6.2.3 OLT Fault.....	214
6.2.4 ONU Fault.....	215
6.3 GPON ONU Profile Match state is Mismatch.....	215
6.3.1 Fault Identification and Demarcation.....	215
6.3.2 Fault of a Single ONU.....	216
6.3.3 Fault of All ONUs.....	217
6.4 Failure to Auto Discover a GPON ONU.....	217
6.4.1 Fault Identification and Demarcation.....	217
6.4.2 OLT Fault.....	219
6.4.3 ODN Fault.....	220
6.4.4 ONU Fault.....	224
6.5 GPON ONU Frequently Goes Online and Offline.....	226
6.5.1 Fault Identification and Demarcation.....	227

6.5.2 Alarming Handling.....	228
6.5.3 OLT Fault.....	229
6.5.4 ODN Fault.....	229
6.5.5 ONU Fault.....	232

7 Troubleshooting the FTTH Service..... 234

7.1 Troubleshooting the Internet Access Service.....	234
7.1.1 Internet Access Service Fails.....	235
7.1.1.1 Fault Identification and Demarcation.....	235
7.1.1.2 User's PC Is Faulty.....	236
7.1.1.3 DNS Server Is Faulty.....	237
7.1.2 Internet Access Is Interrupted Frequently.....	237
7.1.2.1 Fault Identification and Demarcation.....	237
7.1.2.2 User's PC Is Faulty.....	239
7.1.2.3 Residential Router Is Faulty.....	239
7.1.2.4 User's ONT Is Faulty.....	239
7.1.2.5 Packet loss of OLT Occurs.....	240
7.1.2.6 OLT Is Faulty.....	240
7.1.2.7 OLT Has MAC Address Duplication.....	240
7.1.2.8 The Upper-layer Device Loss Packet	241
7.1.3 Low Internet Access Rate.....	241
7.1.3.1 Fault Identification and Demarcation.....	241
7.1.3.2 User's PC Is Faulty.....	242
7.1.3.3 Residential Router Is Faulty.....	243
7.1.3.4 User's ONT Is Faulty.....	243
7.1.3.5 The Limited Rate of the OLT Is Faulty.....	243
7.1.3.6 Large Volume of Traffic Cause Packet Loss.....	244
7.1.3.7 Unknown Traffic Occupies User's Bandwidth.....	244
7.1.3.8 OLT Is Faulty.....	244
7.1.3.9 The Rate Limited on the BRAS is Lower Than the Applied Rate.....	245
7.1.3.10 The Upper-layer Device Loss Packet	245
7.1.4 PPPoE Dialup Failure.....	245
7.1.4.1 Fault Identification and Demarcation.....	245
7.1.4.2 User's PC Is Faulty.....	247
7.1.4.3 Residential Router Is Faulty.....	248
7.1.4.4 User's ONT Is Faulty.....	248
7.1.4.5 PTP Configuration Is Incorrect.....	248
7.1.4.6 User Number Reaches the Maximum Number of Learned MAC Addresses.....	249
7.1.4.7 OLT Discards the Interaction Packets.....	249
7.1.4.8 OLT Is faulty.....	250
7.1.4.9 User's Account Is Restricted on the BRAS.....	250
7.1.4.10 The Upper-layer Device Loss Packet	250
7.1.5 Failure to Obtain an IP Address in the DHCP Mode.....	250

7.1.5.1 Fault Identification and Demarcation.....	251
7.1.5.2 User's PC Is Faulty.....	253
7.1.5.3 Residential Router Is Faulty.....	254
7.1.5.4 User's ONT Is Faulty.....	254
7.1.5.5 ONT Configuration Is Incorrect.....	254
7.1.5.6 User Number Reaches the Maximum Number of Learned MAC Addresses.....	255
7.1.5.7 OLT is faulty.....	255
7.1.5.8 User's Account Is Restricted on the BRAS.....	256
7.1.5.9 The Upper-layer Device Loss Packet	256
7.2 IPTV Service Failure.....	256
7.2.1 Online Access Failures.....	257
7.2.1.1 Symptoms.....	257
7.2.1.2 Fault Identification and Demarcation.....	257
7.2.1.3 Handling Process.....	259
7.2.1.3.1 Multicast User Is Blocked.....	259
7.2.1.3.2 The User Fails to Pass Bandwidth CAC.....	259
7.2.1.3.3 Number of Specific Videos Ordered Has Reached the Upper Limit.....	260
7.2.1.3.4 Total Number of Ordered Videos Has Reached the Upper Limit.....	261
7.2.1.3.5 User Has No Rights to Watch a Video.....	261
7.2.1.3.6 Match Program Fail.....	263
7.2.1.3.7 IGMP Has Been Incorrectly Configured.....	264
7.2.1.3.8 Subscriber Line or Terminal Is Faulty.....	265
7.2.2 Blank Screens on the Multicast Service.....	265
7.2.2.1 Symptoms.....	266
7.2.2.2 Fault Identification and Demarcation.....	266
7.2.2.3 Handling Process.....	268
7.2.2.3.1 The User Fails to Pass Bandwidth CAC.....	268
7.2.2.3.2 Number of Specific Videos Ordered Has Reached the Upper Limit.....	268
7.2.2.3.3 Total Number of Ordered Videos Has Reached the Upper Limit.....	269
7.2.2.3.4 User Has No Rights to Watch a Video.....	270
7.2.2.3.5 Match Program Fail.....	271
7.2.2.3.6 Prejoined Videos Use an Excessively High Bandwidth.....	273
7.2.2.3.7 Maximum Downstream Bandwidth Allocated to a PON Port Is Excessively Low.....	274
7.2.2.3.8 Poor Video Source Quality.....	275
7.2.2.3.9 User Terminal Is Faulty.....	277
7.2.3 Multicast Video Artifacts and Intermittent Video Stops.....	278
7.2.3.1 Symptoms.....	278
7.2.3.2 Fault Identification and Demarcation.....	279
7.2.3.3 Handling Process.....	280
7.2.3.3.1 Poor Video Source Quality.....	280
7.2.3.3.2 Poor OLT's Upper-Layer Network Quality.....	282
7.2.3.3.3 Poor ODN Line Quality.....	284

7.2.3.3.4 User Bandwidth Is Insufficient.....	285
7.2.3.3.5 User Terminal Is Faulty.....	287
7.3 Troubleshooting Voice Service Faults.....	289
7.3.1 No Power Feed After Offhook.....	290
7.3.2 No Tone After Offhook.....	291
7.3.3 Busy Tone After Off-hook.....	293
7.3.4 One-Way Audio in a Voice Call.....	298
7.3.5 Noise in a Voice Call.....	300
7.3.6 Voice Interruptions in a Voice Call.....	303
7.3.7 Failure to Dial Certain Phone Numbers.....	305

8 Troubleshooting the xPON power distribution service.....307

8.1 Troubleshooting Ethernet Access Services.....	307
8.1.1 Troubleshooting Video Surveillance Data Transmission Services.....	307
8.1.2 Troubleshooting Intelligent Collection of Power Consumption Information.....	310
8.2 Troubleshooting Serial Port Access Services.....	314
8.2.1 Troubleshooting Intelligent Collection of Power Consumption Information.....	314

9 Troubleshooting the FTTO Service.....318

9.1 Troubleshooting the Internet Access Service.....	318
9.1.1 Internet Access Failure.....	318
9.1.2 Internet Access Service Interruption.....	321
9.1.3 Low Internet Access Rate.....	326
9.1.4 PPPoE Dialup Failure.....	330
9.1.5 Failure to Obtain an IP Address in the DHCP Mode.....	339
9.2 IPTV Service Failure.....	347
9.2.1 Multicast User Fails to Go Online.....	348
9.2.2 Blank Screen After a Program Is Ordered.....	358
9.2.3 Pixelation in a Multicast Program.....	375
9.2.4 Abnormal Interruption of a Multicast Program.....	380
9.2.5 Long Program Switching Time.....	386
9.3 Troubleshooting Voice Service Faults.....	388
9.3.1 No Power Feed After Offhook.....	389
9.3.2 No Tone After Offhook.....	391
9.3.3 Busy Tone After Off-hook.....	393
9.3.4 One-Way Audio in a Voice Call.....	398
9.3.5 Noise in a Voice Call.....	400
9.3.6 Voice Interruptions in a Voice Call.....	403
9.3.7 Failure to Dial Certain Phone Numbers.....	405

10 Troubleshooting the FTTB and FTTC Service.....407

10.1 Internet Access Service Failure.....	407
10.1.1 Internet Access Service Fails.....	408
10.1.1.1 Symptoms.....	408

10.1.1.2 Fault Identification and Demarcation.....	408
10.1.1.3 User's PC Is Faulty.....	409
10.1.1.4 DNS Server Is Faulty.....	409
10.1.2 Internet Access Is Interrupted Frequently.....	410
10.1.2.1 Fault Identification and Demarcation.....	410
10.1.2.2 User's PC Is Faulty.....	411
10.1.2.3 User's Modem Is Faulty.....	411
10.1.2.4 Line from the User Terminal to the MDU Has Serious Packet Loss.....	411
10.1.2.5 MDU Port Is Faulty.....	413
10.1.2.6 MDU Has MAC Address Duplication.....	413
10.1.2.7 BRAS MAC Address Duplication.....	414
10.1.3 Internet Access Rate Is Low.....	414
10.1.3.1 Fault Identification and Demarcation.....	414
10.1.3.2 NIC of the User's PC Is Faulty.....	415
10.1.3.3 User's Modem Is Faulty.....	416
10.1.3.4 Line from the User Terminal to the MDU Has Serious Packet Loss.....	416
10.1.3.5 Unknown Traffic Occupies User Bandwidth.....	417
10.1.3.6 MDU Has MAC Address Duplication.....	418
10.1.3.7 BRAS MAC Address Duplication.....	419
10.1.4 IP Address Fails to Be Obtained Through PPPoE Dialup.....	420
10.1.4.1 Fault Identification and Demarcation.....	420
10.1.4.2 NIC of the User's PC Is Faulty or Is Disabled.....	421
10.1.4.3 User's Modem Is Faulty.....	421
10.1.4.4 MDU Port Is Faulty.....	421
10.1.4.5 PTP Configuration Is Incorrect.....	423
10.1.4.6 ACL That Restricts PPPoE Packets Is Configured.....	423
10.1.4.7 MDU Has MAC Address Duplication.....	424
10.1.4.8 BRAS MAC Address Duplication.....	424
10.1.4.9 User's Account Is Restricted on the BRAS.....	425
10.1.5 IP Address Fails to Be Obtained Through DHCP Dialup.....	425
10.1.5.1 Fault Identification and Demarcation.....	425
10.1.5.2 NIC of the User's PC Is Faulty or Is Disabled.....	426
10.1.5.3 User's Modem Is Faulty.....	427
10.1.5.4 MDU Port Is Faulty.....	427
10.1.5.5 MDU Has MAC Address Duplication.....	428
10.1.5.6 Link from the MDU to DHCP Server Fails.....	429
10.1.5.7 DHCP Server Is Faulty.....	429
10.1.5.8 User's Account Is Restricted on the BRAS.....	429
10.2 IPTV Service Failure.....	429
10.2.1 Online Access Failures.....	430
10.2.1.1 Symptoms.....	430
10.2.1.2 Fault Identification and Demarcation.....	430

10.2.1.3 Multicast User Is Blocked.....	431
10.2.1.4 The User Fails to Pass Bandwidth CAC.....	432
10.2.1.5 Number of Specific Videos Ordered Has Reached the Upper Limit.....	433
10.2.1.6 Total Number of Ordered Videos Has Reached the Upper Limit.....	433
10.2.1.7 User Has No Rights to Watch a Video.....	434
10.2.1.8 Match Program Fail.....	435
10.2.1.9 IGMP Has Been Incorrectly Configured.....	437
10.2.1.10 Subscriber Line or Terminal Is Faulty.....	438
10.2.2 Blank Screens on the Multicast Service.....	439
10.2.2.1 Symptoms.....	439
10.2.2.2 Fault Identification and Demarcation.....	440
10.2.2.3 Host attribute of multicast video is incorrect.....	442
10.2.2.4 User Has No Rights to Watch a Video.....	443
10.2.2.5 The User Fails to Pass Bandwidth CAC.....	444
10.2.2.6 Number of Specific Videos Ordered Has Reached the Upper Limit.....	445
10.2.2.7 Total Number of Ordered Videos Has Reached the Upper Limit.....	446
10.2.2.8 Match Program Fail.....	446
10.2.2.9 Prejoined Videos Use an Excessively High Bandwidth.....	448
10.2.2.10 Maximum Downstream Bandwidth Allocated to a PON Port Is Excessively Low.....	449
10.2.2.11 Poor Video Source Quality.....	450
10.2.2.12 User Terminal Is Faulty.....	452
10.2.3 Multicast Video Artifacts and Intermittent Video Stops.....	453
10.2.3.1 Symptoms.....	453
10.2.3.2 Fault Identification and Demarcation.....	454
10.2.3.3 Poor Video Source Quality.....	456
10.2.3.4 Poor OLT's Upper-Layer Network Quality.....	458
10.2.3.5 Poor ODN Line Quality.....	459
10.2.3.6 User Bandwidth Is Insufficient.....	460
10.2.3.7 User Terminal Is Faulty.....	463
10.3 Troubleshooting the Voice Service.....	464
10.3.1 No Tone When Offhook.....	466
10.3.1.1 Fault Identification and Demarcation.....	466
10.3.1.2 Fault Occurs Between the Phone Set and the POTS Port.....	471
10.3.1.3 ONU Is Faulty.....	474
10.3.1.4 ODN Fiber Quality Is Poor.....	476
10.3.1.5 OLT's Upper-Layer Network Is Faulty.....	477
10.3.2 Busy Tone When Offhook.....	478
10.3.2.1 Fault Identification and Demarcation.....	478
10.3.2.2 Fault Occurs Between the Phone Set and the POTS Port.....	480
10.3.2.3 MG or SIP Interface Is Faulty.....	482
10.3.2.4 ODN Fiber Quality Is Poor.....	485
10.3.2.5 OLT's Upper-Layer Network Is Faulty.....	485

10.3.3 One-Way Audio During Communication.....	487
10.3.3.1 Symptoms.....	487
10.3.3.2 Fault Identification and Demarcation.....	488
10.3.3.3 ONU Configuration Is Incorrect.....	490
10.3.3.4 OLT ACL Configuration Is Incorrect.....	491
10.3.3.5 OLT's Upper-Layer Network Is Faulty.....	491
10.3.4 Noise Interference During Communication.....	492
10.3.4.1 Fault Identification and Demarcation.....	492
10.3.4.2 Fault Occurs Between the Phone Set and the POTS Port.....	494
10.3.4.3 ONU Is Faulty.....	496
10.3.4.4 ONU's Upper-Layer Network Is Faulty.....	497
10.3.5 Poor Voice Service During Communication.....	498
10.3.5.1 Fault Identification and Demarcation.....	498
10.3.5.2 Fault Occurs Between the Phone Set and the POTS Port.....	500
10.3.5.3 ONU QoS Configuration Is Incorrect.....	502
10.3.5.4 ODN Fiber Quality Is Poor.....	502
10.3.5.5 OLT's Upper-Layer Network Is Faulty.....	503
11 Troubleshooting the FTTM Services.....	505
11.1 Ethernet Access Services.....	505
11.2 Abnormal PoE Power Supply.....	507
12 Troubleshooting the D-CCAP Service.....	511
12.1 Service Troubleshooting.....	511
12.1.1 NMS Fails to Manage a Device.....	511
12.1.2 Unexpected Reset of the System.....	513
12.1.3 Failure to Automatically Discover a CMC in the Extended Subrack.....	515
12.1.4 Failure to Access the Internet.....	526
12.1.5 Troubleshooting a Low Internet Access Rate.....	529
12.1.6 Troubleshooting Frequent Interruptions in the Internet Access Service.....	531
12.1.7 Pixelated or Frozen Display of a Program.....	532
12.1.8 Failure to Make a Call.....	535
12.1.9 VoD Failure or Pixelated or Frozen Display of a VoD Program.....	536
12.1.10 CM Going Online and Offline Repeatedly.....	539
12.1.11 Failure to Go Online of a CM.....	541
12.1.12 Failure to Lock a Downstream Frequency of a CM.....	552
12.1.13 Failure to Lock an Upstream Frequency of a CM.....	554
12.1.14 CM Fails to Obtain an IP Address.....	555
12.1.15 CM Fails to Download a Configuration File.....	556
12.1.16 CM Fails to Register with the D-CCAP.....	557
12.1.17 CM Remains in the Reject State.....	557
12.1.18 Failure to Obtain an IP Address of a PC.....	558
12.1.19 Failure to Power on the CMC.....	559
12.1.20 Poor-quality CATV/DOCSIS Signal Output from the RF Port.....	561

12.1.21 Low-power-level CATV/DOCSIS Signal Output from the RF Port.....	562
12.1.22 Abnormal Optical Receiver.....	563
12.1.23 Abnormal Optical Transmitter.....	564
12.2 Fault Cases.....	565
12.2.1 Failure to Provision Services Due to a Bug in the ARP Packet Interaction Mechanism.....	565
12.2.2 Interrupted Program Playing Because IGMP Proxy Was Not Enabled.....	566
12.2.3 Failure to Upgrade a CMC Due to Incorrect TFTP Tool Configuration.....	566
12.2.4 Low Internet Access Rates Due to Excessively Low Output SNRs of CMs.....	566
12.2.5 Frequent CM Online and Offline Due to a CM Fault.....	567
13 Glossary.....	568

1

About This Document

Content Introduction

This document describes how to troubleshoot access network products service faults, including:

- Field Maintenance Guide
- Common Service Troubleshooting
- Commonly Used Methods of Fault Locating and Troubleshooting
- TechNotes

Intended Audience

The intended audience of this document is:

- System maintenance engineers
- Field maintenance engineers
- Network monitoring engineers
- Troubleshooting engineers

Symbol Conventions

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
 CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.

Symbol	Description
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
 NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Update History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Updates in Issue 03 (2021-08-10)

- Added: Troubleshooting the xPON power distribution service.
- Optimized the document structure.

Updates in Issue 02 (2020-04-03)

Optimized the document structure.

Updates in Issue 01 (2018-07-27)

This is the first release.

2 Compliance and Safety

[2.1 Regulatory Compliance Information](#)

This chapter describes Electromagnetic Compatibility (EMC) and other safety standards compliance and information about the MA5800.

[2.2 Safety Information](#)

This document describes only general safety requirements for Huawei products. In the case of any inconsistency, requirements in this document have a lower priority than those in the installation and maintenance documents of a specific product.

2.1 Regulatory Compliance Information

This chapter describes Electromagnetic Compatibility (EMC) and other safety standards compliance and information about the MA5800.

2.1.1 Regulatory Compliance Standards

Table 2-1 Regulatory compliance standards

Discipline	Standards
EMC	<ul style="list-style-type: none">● CISPR32● CISPR24● EN55032● EN50024● ETSI EN 300 386 Class A● ETSI ES 201 468 V1.4.1:2014● AS/NZS CISPR 22● GB9254 Class A● VCCI Class A● IEC 61000-3-2● IEC 61000-3-3● EN 61000-3-2● EN 61000-3-3● ITU-T K.20● ITU-T K.44● ETSI EN 300 132-2● ETSI EN 300 253
Safety	<ul style="list-style-type: none">● IEC 60950-1● EN 60950-1● GB4943
Environment protection	<ul style="list-style-type: none">● 2011/65/EU & (RoHS Directive)● EC NO. 1907/2006 (REACH)● 2012/19/EU (WEEE)
Grounding	<ul style="list-style-type: none">● ITU-T K.27● ETSI EN 300 253

2.1.2 European Directives Compliance

The MA5800 complies with the following European directives and regulations.

- 2014/30/EU (EMC)
- 2014/35/EU (low voltage)
- 2011/65/EU & (RoHS Directive)
- EC NO.1907/2006(REACH)
- 2012/19/EU(WEEE)

- 2004/12/EC&94/62/EC (Packaging)

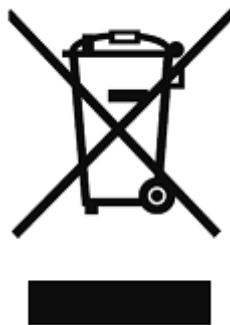
MA5800 complies with Directive 2011/65/EU and other similar regulations from the countries outside the European Union, on the RoHS in electrical and electronic equipment. The device does not contain lead, mercury, cadmium, and hexavalent chromium and brominated flame retardants (polybrominated biphenyls (PBB) or polybrominated Diphenyl ethers (PBDE)) except for those exempted applications allowed by RoHS directive for technical reasons.

MA5800 complies with Regulation EC NO. 1907/2006 (REACH) and other similar regulations from the countries outside the European Union. Huawei will notify to the European Chemical Agency (ECHA) or the customer when necessary and regulation requires.

MA5800 complies with Directive 2012/19/EU on waste electrical and electronic equipment (WEEE). Huawei is responsible for recycling its end-of-life devices, and contact Huawei local service center when recycling is required. Huawei strictly complies with the EU Waste Electrical and Electronic Equipment Directive (WEEE Directive) and electronic waste management regulations enacted by different countries worldwide. In addition, Huawei has established a system for recycling and reuse of electronic wastes, and it can provide service of dismantling and recycling for WEEE. By Huawei recycling system, the waste can be handled environmentally and the resource can be recycled and reused fully, which is also Huawei WEEE stratagem in the word. Most of the materials in product are recyclable, and our packaging is designed to be recycled and should be handled in accordance with your local recycling policies.

In accordance with Article 11(2) in Directive 2012/19/EU (WEEE), products were marked with the following symbol: a cross-out wheeled waste bin with a bar beneath as below:

Figure 2-1 A Cross-out Wheeled Waste Bin with A Bar Beneath



2.1.3 Japan Compliance

The MA5800 complies with VCCI Class A by Information Technology Equipment (ITE).

Figure 2-2 VCCI Class A by Information Technology Equipment (ITE)

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

 **NOTE**

This standard applies to only products delivered to the Japanese market.

2.1.4 CISPR 32 Compliance

The MA5800 complies with CISPR 32 for Class A by ITE.

Class A ITE is a category of all other ITE that satisfies only the Class A ITE regulations, and not the Class B ITE regulations. Such equipment should not be restricted in its sale but the following warning shall be included in the instructions for use:

 **CAUTION**

This is Class A Product. In a domestic environment this product may cause radio interference; therefore, the user is required to take appropriate measures.

EMC Class A declaration for China.

Applies to the systems that complies with the EMC Directive standard EN 55032 Class A.

2.1.5 India RoHS hazardous substance table

MA5800 described in this guide complies with the "e-waste (Management and Handling) Rules, 2011" of India which is also called India RoHS.

Part Descriptions	Restricted Substances in Product					
	Cd	Pb	Hg	Cr(VI)	PBBs	PBDEs
Cabinet/ Subrack	O	X	O	O	O	O
Power Adapter	O	X	O	O	O	O
PCBA	O	X	O	O	O	O
Cable	O	X	O	O	O	O
Auxiliary Equipments	O	X	O	O	O	O
Accessories	O	X	O	O	O	O

Part Descriptions	Restricted Substances in Product					
	Cd	Pb	Hg	Cr(VI)	PBBs	PBDEs
Battery	O	X	O	O	O	O
Label	O	O	O	O	O	O

O: indicates that the content of the toxic and hazardous substance in all the Homogeneous Materials of the part is below the concentration limit requirement as described in the e-waste (Management and Handling) Rules, 2011.

X: indicates that the content of the toxic and hazardous substance in at least one Homogeneous Material of the part exceeds the concentration limit requirement as described in S in the e-waste (Management and Handling) Rules, 2011.

2.1.6 Other Markets

For relevant compliance information/documentation for markets not mentioned above, contact Huawei representative.

2.2 Safety Information

This document describes only general safety requirements for Huawei products. In the case of any inconsistency, requirements in this document have a lower priority than those in the installation and maintenance documents of a specific product.

2.2.1 General Safety Precautions

- Read all safety information before installing, operating, and maintaining Huawei equipment.
- To minimize risk of personal injury and equipment damage, always follow all safety precautions marked on equipment and described in manuals.
- The **Caution**, **Warning** and **Danger** sections in the manual are only a supplement and do not represent all safety instructions.
- Use the equipment only where all design specifications are met. Otherwise, any resulting equipment failure and its negative consequences to equipment, parts, personnel, and property will not be covered by the warranty.

Definitions

- **Skilled personnel:**
Person with relevant education or experience to enable him or her to identify hazards and to take appropriate actions to reduce the risks of injury to themselves and others
- **Instructed person:**
Person instructed or supervised by a skilled person as to energy sources and who can responsibly use equipment safeguards and precautionary safeguards with respect to those energy sources.

- **Ordinary person:**

Person who is neither a skilled person nor an instructed person.

Symbol Conventions

- : Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
- : Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
- : Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
- indicates a part exposed to high voltage. This symbol warns operators that both direct and indirect contact with the power grid is fatal. Such areas include hazardous voltage points or protective power supply covers that may be removed during maintenance.
- Indicates overheating: Burned fingers when handling the parts, Wait one-half hour after switching off before handling parts.
- : High touch current warning labels: This identifier attached to the protection ground terminal nearby, Warn products have high touch current, Connect to earth before connecting to supply, To avoid danger of electric shock.
- : Multiple power sources warning labels: when the device is powered off, you must disconnect all power sources.
- indicates that microwave emission. The symbol is attached near the output socket of the transmitter power amplifier or antenna socket of the transmitter combiner to indicate RF radiation. Do not tamper with the transmitter output feeder or antenna feeder connector when the transmitter is on. Turn off the transmitter before disconnecting the feeder connector or working near the transmit antenna.
- or indicates protection earthing. This symbol is attached next to a protection ground terminal next to grounded equipment and an external ground system. An equipment ground cable is connected to an external ground bar through the protection ground terminal.
- indicates equipotential bonding. This symbol is found with equipotential terminals inside equipment.

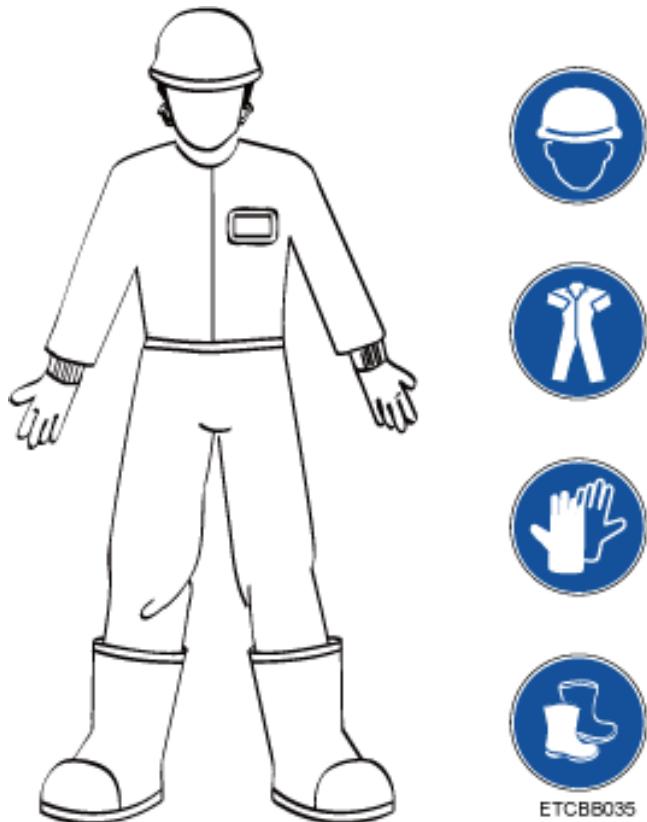
-  indicates electrostatic discharge. This symbol is used in all electrostatic sensitive areas. Before operating equipment in these areas, wear ESD gloves or an ESD wrist strap.
-  indicates that the equipment is safe to use in altitudes below 2000 m (6561.6 ft.).
-  indicates that the equipment is not safe to use in tropical climates.
-  Moving fan blade: Keep body parts away from fan blades.
-  : Prompts users to read the instruction manual.
-  : This label attached to products visible position, is used to indicate that equipment intended only for use in fixed installations and intended to be floor standing on a non-combustible surface need not be provided with a fire enclosure bottom.

Basic Precautions

- Trained personnel must be certified, understand all required safety regulations, and master correct operational methods before installing, operating and maintaining Huawei equipment.
- All work with equipment must comply with local laws and regulations. Safety information in the manual only serves as a supplement. In addition:
 - Only skilled and instructed person can install, operate, and maintain equipment.
 - Only skilled and instructed person can remove safety infrastructure and maintenance equipment.
 - Ordinary person must report faults or errors that may cause safety issues promptly.
 - All personnel working with equipment should have high-voltage operation, climbing, special equipment operation, and other operational qualifications required by the local country.
- If personal injury or equipment damage occurs during installation, stop operations immediately, report the situation to the project owner, and take effective protective measures.
- All work on outdoor equipment is strictly forbidden in lightning, rain, snow, wind and other adverse weather conditions. Such work includes but is not limited to outdoor equipment transportation, cabinet installation, power cable installation, and outdoor cable connection.
- Do not wear watches, jewelry, or other conductive objects when working with equipment.

- Dedicated insulation safety tools such as gloves, clothing, helmet, and shoes must be worn at all times, as shown in [Figure 2-3](#).

Figure 2-3 Safety personal protective equipment (PPE)



- Always follow the procedures in the Hardware Installation and Maintenance Guide, Configuration Guide, and Operation and Maintenance Guide while working.
- Use a voltmeter to measure the voltage at the contact point before touching any metal surface or terminal to prevent electric shocks.
- Ensure that all slots are filled with boards or filler panels. Avoid exposure to board hazardous voltage and heat by ensuring that ventilation channels are working normally, that electromagnetic interference is controlled, and that the backplane, motherboard, and boards are free from dust or foreign matter.
- After equipment installation, conduct routine checks and maintenance. Promptly replace faulty parts as required by the *Hardware Installation and Maintenance Guide* and *Operation and Maintenance Guide*.
- After equipment installation, clear the area of packaging materials such as the box, styrofoam, plastic, and cable ties.
- In case of fire, evacuate from the building or equipment area and activate the fire alarm or call the fire emergency number. Do not reenter the burning building under any circumstances.

2.2.2 Installation Environment

- Ensure that the installation environment complies with equipment specifications, including voltage, temperature, humidity, altitude, degree of pollution, overvoltage category, and waterproofing and dustproofing classification.
- Avoid flammable, explosive gas or smog environments.
- Keep the installation site free of acidic, alkaline or other corrosive gases.
- Keep the equipment away from sources of heat or fire, such as the electric heater, microwave oven, oven, water heater, fireplace, candle or other heat generators. Heat may cause the equipment to catch fire or its housing to melt.
- Do not obscure or cover running equipment with flammable materials such as paper or fabric. This hampers heat dissipation and can cause the equipment to catch fire or its housing to melt.
- Install and use the equipment and its system in a location with restricted access location.
- Do not block air vents when the equipment is running. Maintain air vents away from the wall or other objects as required in the *Hardware Installation and Maintenance Guide*. The minimum distance is 5 cm (1.97 in.) unless specified.
- This device is not suitable for places of use may occur in children.
- Do not use equipment that does not meet IP54 waterproof and dustproof standards in outdoor environments.

2.2.2.1 Indoor Installation

- Ensure that there is no water leakage or condensation from air conditioning failure in the equipment room on the top of the equipment. Introducing water into the equipment will cause it to fail.
- Install fixed equipment with a large hole at the bottom on concrete, tile or other non-combustible surfaces.
- Prevent rodent and pest infestations at the installation site.

Wall Installation

- Before drilling holes on the wall, ensure that there is no circuitry, water pipe, or gas pipeline in the wall area to be drilled to avoid bodily injury.
- Do not place any flammable or explosive objects above or under the equipment, and do not obstruct the equipment with foreign objects within a 1-meter (3.28 ft.) radius.
- Ensure that no holes are drilled that face upwards to prevent water ingress and equipment damage.
- Ensure that screws are securely installed. Otherwise, the equipment may fall due to tension after cable connection, causing equipment damage or even bodily injury.

Desktop Installation

- Ensure that the desk or workbench is in stable contact with the ground.
- Do not put other items on the equipment.
- Do not place cups with liquid on or next to the equipment. Spillage may enter the equipment and pose safety risks. If this happens, immediately stop the equipment, cut off the power supply, disconnect all cables, and contact after-sales personnel.
- Equipment with ventilation openings likely to be used on a soft support (like bedding, blankets and so on.), do not cover ventilation openings.

Cabinet Installation

- Before installing equipment in a cabinet, ensure that the cabinet is securely fastened with a balanced center of gravity. Otherwise, tipping or falling cabinets may cause bodily injury and equipment damage.
- Leave proper clearance around the equipment.
- Make sure an enclosed cabinet is adequately ventilated.

2.2.2.2 Outdoor Installation

Outdoor Installation Requirements

- Do not work on outdoor equipment and cables in lightning, rainy, snowy, windy (wind force > 6) and other adverse weather conditions.
- Ensure that the enclosure is class IP54 or higher.
- Comply with all related local regulations.
- Set up signs at the site to indicate a dangerous restricted area inaccessible to unauthorized personnel.
- The scaffolding, platforms, and workbench must pass safety checks to ensure structural integrity. Do not overload the scaffolding.
- Avoid simultaneous work at heights and on the ground. If such situations cannot be avoided, erect a special protective shed or other protective measures between the height and ground, and clear piles of tools and property from the area.
- Do not loiter in the work area.
- Any violations must be promptly pointed out by the site manager or safety supervisor and prompted for correction. If the problem persists, the personnel involved risks suspension that is regarded as absenteeism.

Operators are responsible for accidents resulting from violation of safety regulations or failure to make timely correction. Supervisors also bear responsibility.

Installation at Heights

- Work performed 2 m (6.56 ft.) above the ground is regarded as work at heights.
- Work at heights, comply with related local regulations.
- Only skilled and trained personnel are allowed to work at heights.

- Stop such work in any of the following conditions: adverse weather, wet steel tubes, and other risky situations. Resume work only after a Huawei safety director and related technical personnel have checked all the equipment.
- The ladder used in work at heights must be intact and skid-resistant to ensure safe climbing. The recommended angle between the ladder and the ground is 75°. When using a step ladder, the rope must be strong and the ladder must be supported.
- Place guardrails and warning signs around protrusions and holes to avoid accidents.

 DANGER

- Before proceeding, carefully check climbing and safety tools, such as the safety helmet, safety belt, ladder, springboard, scaffolding, and hoisting equipment. If any tool does not meet requirements, fix or replace it immediately, or postpone the work.
- Wear proper safety PPE and a helmet as well as a belt or waist rope secured to a robust support. Do not tie the belt or waist rope to an unstable object or metal with sharp edges. A fastener that detaches may cause a falling accident.
- Avoid dropping machinery and tools that may cause injury.
- Transport all objects from or to the ground level by a strong rope, basket, elevated vehicle, or crane instead of throwing them.
- Do not pile up scaffolding, materials, and other debris on the ground under the work area at heights that cause traffic obstructions.
- After completion, disassemble the scaffolding layer by layer from top to bottom. Do not disassemble top and bottom layers at the same time. When disassembling a part, prevent the collapse of other parts.

2.2.3 Electrical Safety

2.2.3.1 Grounding

- Ensure that the protection ground is reliably grounded in accordance with local building distribution specifications.
- For equipment requiring grounding, always connect the protection ground first and disconnect it last when installing the equipment.
- For the equipment using a socket with an earthing terminal, ensure that the earthing terminal is correctly grounded.

2.2.3.2 AC/DC Operation

 DANGER

- Do not contact the power system supply directly or indirectly through damp material. The hazardous voltage may cause electric shock.
- Improper operation may cause accidents such as fire and electric shock.

- This device relies on the building's installed overcurrent protection from short circuits. Ensure that a proper overcurrent protection mechanism has been deployed on the upper-level device. Protection specifications are suggested as follows:
 - For the MA5800-X17, each channel: 60 A
 - For the MA5800-X15, each channel: 60 A
 - For the MA5800-X7, each channel: 40 A
 - For the MA5800-X2, each DC channel: 20 A; each AC channel: 8 ACheck that all specifications are compatible before equipment installation, and ensure that the circuit breaker trip value of the upper-level device is greater than or equal to the rated value on the device nameplate.
- If the power input of the equipment is permanent, ensure that an easy-to-access disconnection device is installed on the exterior of the equipment.
- Use AC-supplied models for TN, TT power systems.
- For DC-supplied models, use reinforced insulation or double insulation to isolate the DC source from the AC mains supply.
- Before connecting equipment, disconnect the corresponding external-equipment circuit breaker.
- Before connecting the load (electrical equipment) or battery cable, verify that the input voltage is within the rated voltage range of the equipment.
- Before connecting the load (electrical equipment) or battery cable, check the cable and terminal polarities to avoid reverse connection.
- Before powering on, verify that equipment electrical connections are correct.
- If the device has more than one power supply, disconnect all of them when powering off the device.

2.2.3.3 Cabling Requirements

- Only cut the insulation layer at the wiring part when preparing the power cable at the site. Doing so prevents accidents and fire from short circuit.
- High-temperature environments may cause wear and tear on the insulation layer. Leave sufficient clearance between the cable and power busbar, current shunt, fuse, heat sink and other heating devices.
- Bind the signal cable and the strong current or high-voltage cable separately.
- Cables provided by the customer must comply with local cable regulations.
- Do not route any cable through the air exhaust vent in the cabinet.
- If cables have been stored in an ambient temperature below 0 °C (32 °F), move the cables to a room-temperature environment at least 24 hours before installation.

2.2.3.4 TNV Circuits

- To avoid electric shocks, do not connect the safety extra-low voltage (SELV) circuit to the telecommunication network voltage (TNV) circuit.
- Do not tamper with the cable connected to the outdoor signal port in adverse weather conditions.
- To reduce the risk of fire, use only a No. 26 AWG or larger telecommunication line cord.

2.2.3.5 ESD Requirements

- To avoid component damage caused by electrostatic buildup, wear ESD gloves or an ESD wrist strap and properly ground the other end of the ESD wrist strap before touching a circuit board.
- Hold the board by its component-free edge and do not touch chips with your hands.
- Place removed boards in ESD packaging for storage or transportation.

2.2.4 Battery Safety

The safety information in this document is a reminder and for reference only. Read the detailed safety information in the manufacturer instructions before battery installation, operation, and maintenance.

 DANGER

Before installing batteries, ensure that you understand the safety requirements and correct connection procedures.

2.2.4.1 Basic Requirements

- Do not expose batteries to high temperatures or heat sources such as sunlight, heaters, microwave ovens, ovens and water heaters. Overheating batteries may explode.
- Do not disassemble or refit batteries, insert foreign objects, or submerge into water or other liquid. Leakage, overheating, fire, or explosion may occur.
- Wear goggles, rubber gloves, and protective clothing during installation and maintenance to avoid injury caused by electrolyte spillage. Avoid contact with eyes and skin in case of battery leakage. Rinse any accidentally exposed area with water and seek immediate medical treatment.
- Transport batteries in their specified positions. Do not tilt or turn them upside down.
- Disconnect the circuit before battery installation and maintenance.
- Use the same or equivalent type of battery to replace faulty ones. Incorrectly replaced batteries may explode.
- Do not connect metallic conductors to battery terminals or contact battery endpoints. Battery short circuit or overheating may occur and cause injury.
- Follow local regulations for battery disposal. Do not dispose of batteries as domestic waste. Incorrectly disposed batteries may explode.
- Do not drop, squeeze or puncture batteries. Avoid strong external pressure that may cause internal short circuit and overheating.
- Do not use damaged batteries.
- Equipment containing one or more lithium coin / button cell batteries; Caution: "Do not ingest battery, Chemical Burn Hazard".

2.2.4.2 Requirements for Rechargeable Batteries

- If discoloration, deformation, overheating, or any other abnormality occurs, replace the batteries before continuing with usage, charging or storage.
- Tighten battery cables or copper bars using the torque specified in the battery documentation. Insecure connection of battery bolts may cause excessive voltage drop or even overcurrent leading to battery overheating.

Short Circuit Protection

 DANGER

Battery short circuit will produce a strong spike in current and release a large amount of heat energy that may cause bodily injury and property damage.

Disconnect running batteries before other operations whenever possible.

Flammable Gas Protection

 CAUTION

- Do not use unsealed lead-acid batteries.
- Lead-acid batteries should be positioned and secured horizontally for normal hydrogen discharge to avoid combustion or equipment corrosion.

Improper usage of lead-acid batteries will cause the release of flammable gas. Ensure that batteries are kept in a well-ventilated area and take preventive measures against fire.

Leakage Protection

 CAUTION

Battery overheating causes deformation, damage, and electrolyte spillage.

-
- If the battery temperature exceeds 60 °C (140 °F), check for and promptly handle any leakage.

 DANGER

Use a neutralizing liquid to absorb any electrolyte spillage. Exercise caution when handling the leaking battery because the electrolyte can cause injury.

-
- When removing or moving the battery with spilled electrolyte, be careful with the electrolyte that can bring potential injury. If any electrolyte spills, use NaHCO₃ or Na₂CO₃ to neutralize and absorb it.

Battery Discharge Protection

After batteries are installed, ensure that the fuse or circuit breaker is disconnected before powering on the system. This avoids battery damage caused by power discharge in case of long-term power-off.

2.2.4.3 Requirements for Non-Rechargeable Batteries

- If discoloration, deformation, overheating, or any other abnormality occurs, replace the batteries before continuing with usage, charging or storage.
- Do not attempt to replace non-removable, built-in batteries. Doing so may damage the batteries or the equipment. Batteries must be replaced by an authorized service center.
- Do not throw batteries into fire.

2.2.5 Radiation Safety

2.2.5.1 Electromagnetic Field Exposure



Strong electromagnetic signals harm human health.

- Equipment like radio transmitter or associated products must be handled with consideration of exposure to radio electromagnetic fields (electromagnetic radiation).
- Working with high-voltage equipment or facilities risks exposure to high-frequency electromagnetic fields.
- Radio service carriers and other users must comply with local laws and regulations when deploying wireless base station transceivers, or other equipment or facilities.
- Re-evaluate the risk of electromagnetic field exposure prior to equipment structure or antenna modification.
- Re-evaluate the risk of electromagnetic field exposure prior to modification of radio frequency (RF) output specifications or parameters.
- Re-evaluate the risk of electromagnetic field exposure prior to modification of the site environment where equipment or facilities are located.

Restricted Areas

An area with excessive electromagnetic field exposure is considered hazardous and must be at a specified distance away from the equipment or facility as stipulated by related exposure control limits. This distance controls exposure to the electromagnetic field by personnel or the public. Maintain this distance with measures including but not limited to:

- Plan to situate the equipment or facility in an area inaccessible and undisclosed to the public.

- Allow only authorized and trained personnel to access the site.
- Before entering the restricted area, personnel should be aware that it is restricted and shut down the transmitter.
- Set clear signs at the site to remind personnel that the area is restricted.
- Conduct regular post-installation monitoring and checks.
- Set effective physical shields and warning signs in all areas with excessive electromagnetic field exposure.
- Install an isolating device around the equipment structure.
- Comply with local regulations during operation.

Installation and Usage of a Wireless Base Station Transceiver

- A base transceiver station (BTS) is designed to emit less RF electromagnetic radiation than the maximum standard hazardous limit. A normal working BTS is therefore not harmful to the public and operating personnel. Defective antenna cables or other defects may however result in the emission of excessive RF electromagnetic radiation.
- Personnel must abide by the following rules during BTS installation and operation:
- Read through all safety recommendations and comply with local regulations before proceeding.
- Before installing or maintaining an antenna close to the tower or mast with a BTS and its antenna, contact related personnel to switch off the antenna transmitter.
- Personnel at the site should carry a radiation monitoring and alarm instrument.
- To shield the public from electromagnetic field exposure, abide by the following guiding principles during BTS antenna site installation:
 - Install rooftop antennas out of reach of human activity.
 - Install rooftop transmission antennas away from areas with high traffic, such as the rooftop access point, telephony service point, and HVAC equipment.
 - Install rooftop directional antennas on the periphery and facing away from buildings.
 - Choose the most suitable antenna size by balancing better signal coverage with less visual impact.
 - Install antennas as far away as possible without compromising local area requirements.
 - Exercise caution when constructing a common installation site for antennas from different manufacturers, especially high-power broadcasting (FM/TV) antennas. Installing antennas in one site increases safety risks.
 - Take special preventive measures at antenna sites next to hospitals or schools.

Usage of Other Wireless Equipment

- Apply the safe distance from electromagnetic field exposure specified by any related equipment manual.
- Such distance is not specified for equipment with low RF transmit power that meets electromagnetic field exposure requirements.

- Such distance is not specified for specially-designed equipment that meets electromagnetic field exposure requirements for working in close proximity.

Usage of High-voltage Equipment or Facilities

- Since only high voltages (such as over 100 kV) generate harmful electromagnetic fields, the usage of such equipment or facilities must be evaluated according to requirements.

2.2.5.2 Laser Radiation

DANGER

When handling optical fibers, do not stand close to or look into the optical fiber outlet directly without eye protection.

CAUTION

Use of controls or adjustment or performance of procedures other than those specified herein may result in hazardous radiation exposure.

- A laser transceiver is used in optical transmission system and related test tools. The laser transmitted through unterminated optical fibers or connectors has very high power density and is invisible to human eyes. A beam of light can cause damage to the retina.
- Looking into the end of an exposed optical fiber or broken optical fiber without eye protection from a distance of more than 150 mm (5.91 in.) will not cause eye injury. However, eyes may be damaged if an optical tool such as a microscope, magnifying glass, or eye loupe is used to view a bare optical fiber end.
- Observe the following precautions to avoid laser radiation hazards:
 - Only trained personnel are authorized to operate the laser.
 - Wear protective goggles during laser or optical fiber operation.
 - Disconnect the light source before disconnecting optical fiber connectors.
 - Use optical fiber caps to protect the disconnected optical fiber connectors.
 - Use an optical power meter to measure optical power and verify that the light source is disconnected.
 - Do not look into an exposed optical fiber or connector terminal until the light source is off. Immediately install dust-proof caps onto exposed optical fiber connectors.
 - Ensure that the optical fibers and light source are disconnected before fiber cutting or splicing.
 - Ensure that there is no laser radiation before opening the front door of the optical transmission system.
 - Do not view optical fiber terminals or connectors with a microscope, magnifying glass, or eye loupe.

2.2.6 Mechanical Safety

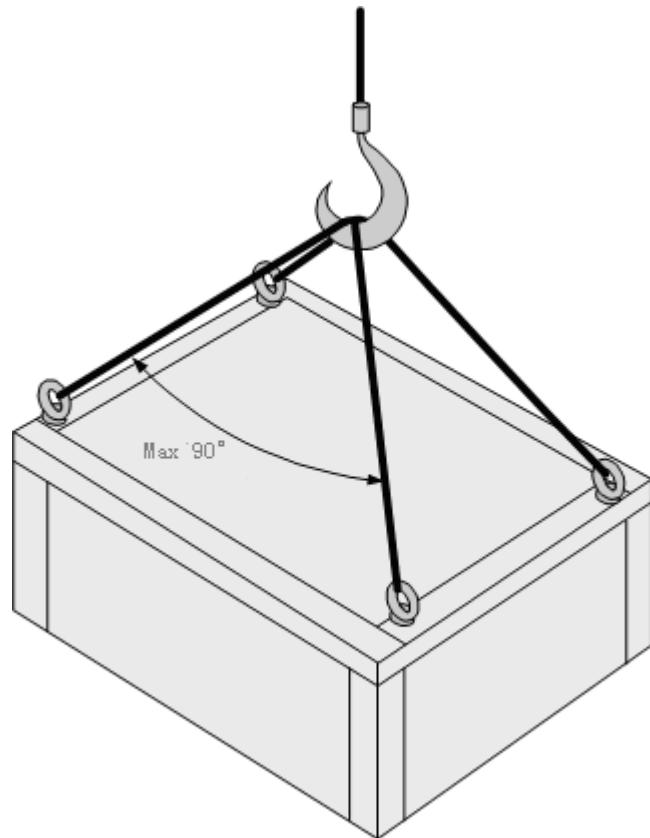
Hoisting Heavy Objects

 DANGER

Avoid walking areas under heavy objects being hoisted.

- Hoisting operators must be trained and qualified.
- Hoisting tools must be checked and complete.
- Before hoisting, fasten all tools to fixed load-bearing objects or walls.
- During hoisting, ensure that angles between lifting straps are under 90°, as shown in [Figure 2-4](#).

Figure 2-4 Hoisting heavy objects

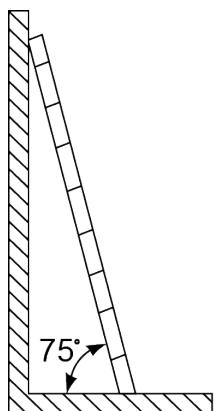


Ladder Usage

- Before using a ladder,
 - Check that it is intact and confirm its load bearing capacity. Do not overload it.

- A gradient of 75° is recommended between the ladder and the ground as measured with a right angle shown in [Figure 2-5](#). Place the wider feet at the bottom or take protective measures to avoid skidding. Place the ladder on a stable surface.

Figure 2-5 Ladder tilt angle

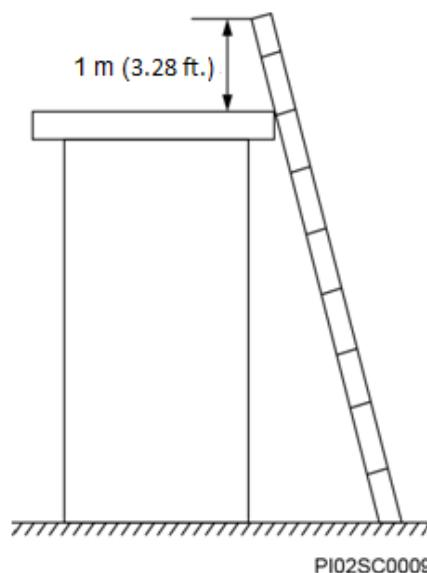


PI02SC0008

- When climbing a ladder:
 - Maintain your center of gravity within the ladder edges.
 - Keep your body balanced when climbing.
 - Do not climb higher than the fourth rung from the top.

To climb to a rooftop, ensure that the ladder has at least 1 m (3.28 ft.) extra height above the rooftop, as shown in [Figure 2-6](#).

Figure 2-6 1 m (3.28 ft.) excess height of the ladder above the rooftop



PI02SC0009

Drilling Holes

Pay attention to the following safety precautions when drilling holes on the wall or ground.

 CAUTION

Do not drill unauthorized holes on cabinets. Incorrectly drilled holes will damage cabinet electromagnetic shielding and internal cables. Metal scraps generated in drilling may also short circuit the cabinet boards.

- Wear protective goggles and gloves when drilling.
- Cover equipment before drilling to prevent metal scraps from entering the equipment interior. Remove these scraps immediately after drilling.

Transporting Heavy Objects

- Adopt a load bearing posture before moving heavy objects to avoid sprains or other injuries. When transporting a cabinet, keep your back straight and avoid sudden movement.
- When transporting equipment by hand, wear gloves to protect against sharp edges.
- When moving or lifting a shelf, hold it by its handles or bottom edge instead of the handles of installed cabinet modules such as power modules, fan modules and boards.

2.2.7 Maintenance Safety

- Wear an ESD wrist strap when replacing accessories or parts. Ensure that one end is grounded and the other end properly contacts the skin.
- When replacing parts, account for all parts, bolts, and tools and prevent them from dropping into fans and causing damage to equipment.
- When replacing cabinet shelves or parts, exercise caution when pulling them out to prevent injury resulting from falling objects.

Fuse Replacement

 DANGER

- Replace fuses with the same type and rating.
 - Disconnect the equipment power supply before replacement to prevent electric shock and injury.
-
- Install replaceable fuses on the panel next to the AC/DC power input or output ports.
 - Refer to the specifications of backup or panel fuses to select the fuse type for replacement. Using fuses of different specifications may cause equipment damage, bodily injury, and financial loss.

Fuse Welding

- If the fuse rating is silkscreened on the board, Huawei authorized personnel will replace fuses with the specified rating.
- If the fuse rating is not silkscreened on the board, do not maintain board fuses on site. Return them to the depot for repair. Huawei authorized personnel replace fuses using the supplier model and rating in the bill of materials (BOM).

Power Distribution Box and Board Replacement

- Wear insulation gloves and ensure that the external-equipment circuit breaker is disconnected before proceeding.
- When replacing a board, do not touch its components to avoid damage.
- Install filler panels in all vacant slots.

Fan Replacement

Pull out a part of the fan module by its handles, wait until the fan completely stops rotating, and then remove the fan module from the subrack. Keep fingers away from fan blades.

Battery Replacement

For details, see section "[2.2.4 Battery Safety](#)."

2.2.8 Safety Signs

Laser Class

Laser class sign: Class 1



Laser class sign: Class 1M



Laser class sign: HAZARD LEVEL 1M





- These signs warn you not to approach optical fibers without eye protection or look directly into optical fiber connectors.
- For detailed requirements, see standard IEC/EN60825-1, 60825-2 laser marking parts.

Equipment Weight



The replaceable/pluggable part or equipment is over 18 kg (40 lbs) and requires two people to transport it.

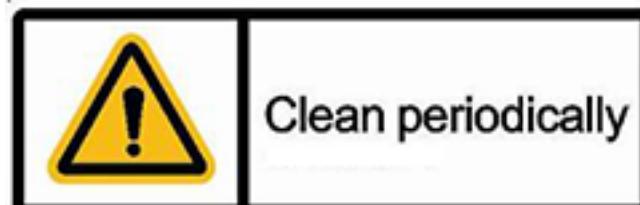


The replaceable/pluggable part or equipment is over 32 kg (70 lbs) and requires three people to transport it.



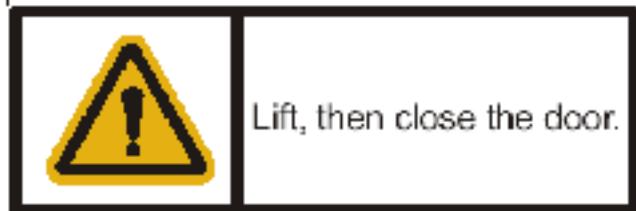
The part or equipment is over 55 kg (121 lbs) and requires a pallet truck or four people to transport it.

Dust Filter Maintenance



This sign reminds you to regularly clean and replace dust filters.

Interlocking Kit Warning



After the door to outdoor equipment is opened, keep it open with a secure metal rod to prevent accidental closing. Remove the rod to close the door.

This sign prompts you to lift the rod before closing the door.

High-voltage Cover Removal



This sign reminds you to read the safety manual to understand all precautions before removing the cover.

3 Maintenance Engineers' Must-Read

Maintenance engineers for troubleshooting are required to have more than one year's experience in engineering or equipment maintenance. After reading the must-read, maintenance engineers can know about the skills, procedures, and methods required to troubleshoot faults in the device.

NOTE

For fast fault locating and troubleshooting, you may use broadband protocol fault diagnosis, or mirroring during operations.

- Broadband protocol fault diagnosis may involve obtaining the personal information, such as the IP address and MAC address.
- Mirroring may involve obtaining the personal data of users and the content of users' communications (the product does not save, parse, or process such information).

Huawei alone is unable to collect or save the personal data of users and the content of users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the personal data of users and the content of users' communications are fully protected when the personal data and the content are being used and saved.

[3.1 Skill Requirements](#)

[3.2 Troubleshooting Precautions](#)

Before locating and troubleshooting faults, carefully read and strictly abide by the following precautions.

[3.3 Troubleshooting Procedure](#)

[3.4 Frequently Used Methods for Troubleshooting](#)

[3.5 How to Obtain Technical Support from Huawei](#)

3.1 Skill Requirements

Maintenance engineers need to possess troubleshooting skills so that they can troubleshoot faults successfully.

Maintenance engineers need to master the following:

1. Basics of communications technologies

- Computer network technologies, such as Ethernet and TCP/IP
 - X digital subscriber line (xDSL) access technology
 - passive optical network (PON) access technology
 - Principles of the multicast service
2. Networking, services, and functions of the devices
- Actual networking conditions
 - Hardware structure and performance specifications of the devices.
 - Functions of boards and slots for boards on the devices.
 - Working principles of services and functions of the devices.
 - Service configurations of the devices.
 - Connections between the devices and the other devices over the network
 - Protocols used between the devices and the other devices over the network
3. Common operations for locating faults in the devices, in addition to:
- Which operations may completely or partially interrupt the service
 - Which operations may result in customer complaints
 - Which emergency or backup measures are available
 - Which operations may damage the equipment
4. Use of common test tools and instruments, including:
- Multimeter
 - Line tester
 - Optical power meter
 - Optical attenuator
5. Methods of determining and handling emergencies in the devices (these methods can be mastered through practice and before practice, and the relevant standards and requirements of carriers need to be known about)
6. Collecting and saving onsite data
- Collecting and saving onsite data includes periodical data collection during normal running of the equipment and data collection when a fault occurs on the equipment. Before processing a fault, maintenance personnel need to collect and save onsite data first.
7. How to seek help in case of a fault, including but not limited to referring to the troubleshooting documents or contacting Huawei for assistance

3.2 Troubleshooting Precautions

Before locating and troubleshooting faults, carefully read and strictly abide by the following precautions.

For maintenance engineers, they should:

- Strictly follow the regulations on operations and industry safety to prevent personal injury and equipment damage.
- When replacing and maintaining parts of equipment, take antistatic measures (for example, wear the ESD wrist strap).

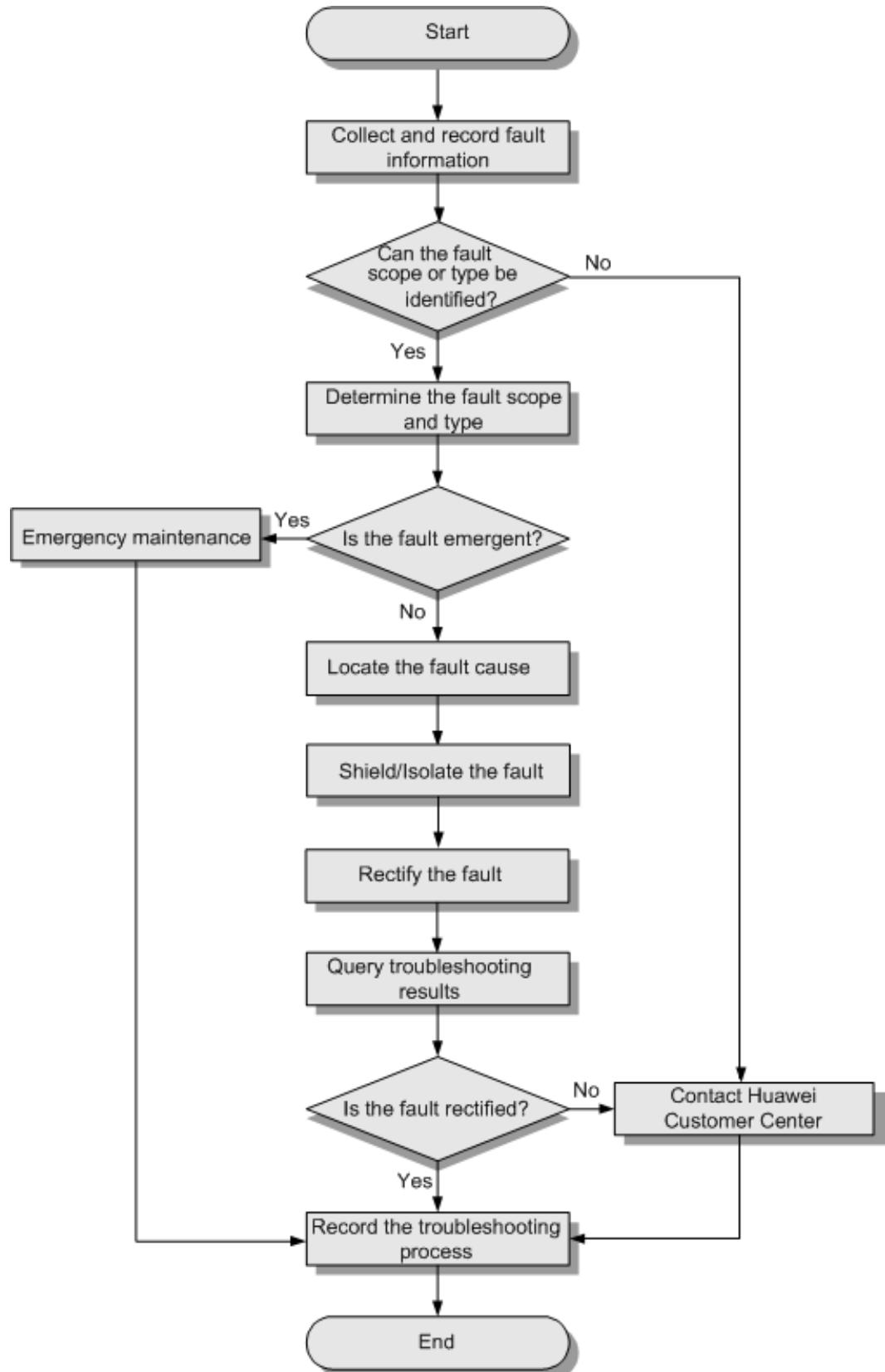
- When any problem occurs during the troubleshooting, record the original information in detail.
- Make a record when performing significant operations (for example, restarting the device or erasing the database). Before such significant operations are performed by qualified engineers, check whether these operations are feasible and at the same time carry out the backup and work out contingency and security measures.
- To improve troubleshooting efficiency, make the following preparations before a fault occurs on the device:
 - Get ready the information about physical connections of the on-site devices.
 - Make a table containing information (including VLAN, IP address, interconnected port ID, and firewall configurations) about the communications, interconnection, and rights of parts and devices.
 - Make on-site part/device archives where the software and hardware configurations, the software and hardware versions, and the change information are recorded.
 - Periodically maintain the backup device to ensure that its hardware configuration, software version, and parameters are the same as the working device running over the existing network. In this way, when the working device is faulty in an emergency, the faulty device can be replaced with the backup device quickly.

3.3 Troubleshooting Procedure

This topic describes the universal procedure for troubleshooting the common faults.

[Figure 3-1](#) shows the flowchart for troubleshooting the common faults.

Figure 3-1 Flowchart for troubleshooting the common faults



3.4 Frequently Used Methods for Troubleshooting

There are various methods for fault location. In fault location, different methods are used together. Therefore, mastering and using these methods are important for improving the efficiency of troubleshooting.

To improve fault location efficiency, follow the principles of from external to internal and from large to small. Specifically, check whether the connection of external cables is reliable and whether the indicators are normal, check the running status of the system through the console, and check the running status of each module.

Table 1 lists the frequently used methods for locating a fault.

Table 3-1 Table 1 Troubleshooting procedure

Troubleshooting Procedure	Frequently Used Methods	Other Methods
Troubleshoot an external device fault	<ul style="list-style-type: none">• Comparison analysis• Interchange analysis• Meter test• Protocol analysis	<ul style="list-style-type: none">• Alarm analysis• Performance analysis
Locate a fault to a specified device	<ul style="list-style-type: none">• Exclusive method• Configuration data analysis	<ul style="list-style-type: none">• Alarm analysis• Performance analysis
Locate a fault to a board	<ul style="list-style-type: none">• Exclusive method• Interchange analysis• Meter test	Protocol analysis

Configuration Data Analysis

Incorrect re-configurations and expansion configurations, and outstanding problems of existing configurations are possible causes of a fault. Therefore, when locating and troubleshooting a fault, analyze the configuration data. Maintenance engineers need to master configuration methods and implementation principles of different services and functions to check the configuration data for different faults and to improve troubleshooting efficiency.

Alarm Analysis

Causes of certain faults can be found by analyzing alarms, or a fault can be located using alarm analysis together with other methods.

An alarm is an important message when a fault or an event occurs. The alarm information includes the detailed description and the possible cause of a fault or an abnormality, and the troubleshooting advice. The information also involves aspects such as the hardware, link, service, and CPU usage. The volume of the

alarm information is large and complete, which is the important basis for fault analysis and location.

When a fault occurs in the system, check whether an alarm is generated in the system. If an alarm is generated, analyze the alarm associated with the fault, and clear the alarm to rectify the fault by referring to Alarm Reference.

Comparison Analysis

Comparison analysis compares the faulty components or symptoms with the normal components or symptoms, and find out differences, to locate the fault. For example, compare line parameters of faulty services with line parameters of normal services, or compare devices at the same network layer. Comparison analysis applies to faults that are caused by a single factor.

Interchange Analysis

When a fault cannot be located after the faulty parts are replaced, maintenance engineers can locate and troubleshoot the fault using the interchange analysis.

Interchange is to interchange the parts that may be faulty with normal parts (such as boards and cables), and compare the running conditions to locate the faults.

Before interchange parts, ensure that the versions of the parts are the same or compatible. It is recommended that you interchange the parts of the same type and version.

NOTE

The interchange operation is risky to certain extent. For example, when users install the short-circuited board in a normal running subrack, the subrack is damaged. Therefore, to prevent another fault from occurring, exercise caution when using the interchange analysis.

Exclusive Method

When a fault is complicated and involves multiple stages, maintenance engineers can locate the fault using the exclusive method to exclude the normal stages.

To use the exclusive method, maintenance engineers must know stages where the fault may occur, and use applicable methods (such as loopback and configuration data analysis) to locate the fault. Therefore, maintenance engineers must be familiar with the following information:

- System structure and working principles of the device
- Stages where the fault may occur
- Fault diagnosis operations, such as loopback and configuration data analysis
- Usage of testers

NOTE

The exclusive method involves all the stages on the entire network. It is recommended that maintenance engineers exclude normal stages in the following principle: remote end first and local end, major cause first and the minor cause, simpleness first and then complication. This reduces troubleshooting cost and improves troubleshooting efficiency.

Protocol Analysis

Protocol analysis locates and troubleshoots a fault when the device is improperly interconnected with the upper layer device.

Protocol analysis indicates the method for analyzing a fault by tracing the signaling and capturing the packets. To use the protocol analysis method, maintenance engineers must be familiar with the related protocols and the exchange process for packets so that they can locate the fault based on the obtained packets.

For example, a user fails to order multicast programs. After the packets are captured and analyzed, it is found that the BRAS discards the Internet Group Management Protocol (IGMP) packets sent from the user.

Meter Test

Meter test method locates and troubleshoots a fault by comparing the actual values of performance parameters tested by various instruments and meters with the correct values. Instruments and meters directly indicate the running status of the device through visual and quantitative data.

The following instruments and meters are frequently used for troubleshooting:

- Multimeter
- Line tester
- Optical power meter
- Optical attenuator

Performance Analysis

Performance analysis uses the performance statistics provided by the device to analyze the performance indexes of the faulty service to locate the fault.

Maintenance engineers must query different performance statistics to locate different faults and therefore they must be familiar with the following information:

- System structure and operation mechanism
- Statistics provided by the system
- Method of querying and analyzing the statistics

For example, run the **display port statistics** command in Ethernet port mode to query the statistics on Ethernet ports. Based on the statistics, maintenance engineers can check whether the system is running properly.

- If the number of cyclic redundancy check (CRC) error frames increases quickly, the links between the devices may be unavailable, port negotiation may be incorrect, or that a physical fault has occurred on the port.
- If a large number of frames are discarded, the traffic transmitted from the interconnected device exceeds the receive capability of the local port.

3.5 How to Obtain Technical Support from Huawei

During the equipment operation and maintenance, if a fault occurs and is difficult to locate or rectify, contact Huawei for assistance.

For enterprise customer:

- Log in to **Global Service Hotline** to obtain the Huawei global service hotline or Email address.

- Visit Huawei technical support website <http://support.huawei.com/enterprise> to search for troubleshooting cases or post your questions on BBS.

For carrier customer:

- Log in to [Global TAC Information](#) to obtain the Huawei global service hotline or Email address.
- Visit Huawei technical support website <http://support.huawei.com> to search for troubleshooting cases or post your questions on BBS.

4 Field Maintenance Guide

This topic describes the tasks of maintaining the hardware of the device, and the reference standard, operation guide, exception handling, and command reference of the tasks.

4.1 Basic Principles of the Maintenance

This topic describes the basic principles of the maintenance, including the remote maintenance guide, field maintenance guide, principles of parts replacement, and troubleshooting principles.

4.2 Maintenance Recommendations for the Third-Party Device

To ensure the performance of Huawei devices, you must periodically check and maintain the third-party device, which is not provided by Huawei, according to the recommendations for maintaining the third-party device.

4.3 Checking the Grounding of the Device

It is recommended that you check whether the ground cable is properly installed and whether the ground resistance complies with the relevant standard once every three months. This operation ensures the reliable running of the device and avoids the potential security risks that may exist in the system.

4.4 Checking the Hardware Status of Fans

It is recommended that you check the hardware status of fans once every three months. This operation ensures that the system can work under proper temperature.

4.5 Checking the Cabinet Appearance of the Cabinet

It is recommended that you should check the cabinet Appearance once every year. This operation ensures that the cabinet can work normally and stably.

4.6 Checking the Battery

It is recommended that you check the status of the battery once every year. This operation ensures that the power supply system can automatically switch to the battery in the case that the AC power supply is cut off. In this manner, the running of services is not affected.

4.7 Cleaning the Air Filter of the Cabinet

It is recommended that you clean the air filters of the cabinet once every year. This operation ensures that the heat dissipation system works properly.

4.1 Basic Principles of the Maintenance

This topic describes the basic principles of the maintenance, including the remote maintenance guide, field maintenance guide, principles of parts replacement, and troubleshooting principles.

Remote Maintenance Guide

When performing the remote maintenance, comply with the following principles:

- Do not install any software that is not relevant to device maintenance on the maintenance terminal.
- Perform the routine maintenance on the device according to the remote maintenance guide, and fill in the remote maintenance table.
- In the case of an emergency during the routine maintenance, such as a device fault, handle the fault according to the troubleshooting procedure, and keep related records. If the fault cannot be rectified, contact the local representative office of Huawei for technical support.
- Back up the data before data modification, and keep related records.

Field Maintenance Guide

When performing the field maintenance, comply with the following principles:

- Keep the telecommunications room neat and tidy, and prevent rodents or other insects from entering the device.
- Ensure that the device is properly grounded according to the grounding requirements.
- Do not insert, remove, reset, or load a board randomly.
- Do not insert a faulty board in the cabinet; otherwise, another fault may be caused.
- Use the ESD wrist strap or ESD gloves to protect the device from ESD damage.
- Place all the spare parts in ESD bags.
- Take ESD measures to protect the port on the board. When performing an operation on a port, wear the ESD wrist strap or ESD gloves. Make appropriate preparations for discharge, that is, prepare the external cables and protective jackets of ports.

NOTE

It is recommended that you reserve some installation materials for boards in the telecommunications room, such as the vacuum-formed box and the ESD bag.

- After the field maintenance operation on a device is complete, close the door of the cabinet properly to prevent accidents.
- Perform the routine maintenance on the device according to the field maintenance guide, and fill in the field maintenance table.
- In the case of an emergency during the routine maintenance, such as a device fault, handle the fault according to the troubleshooting procedure, and keep

related records. If the fault cannot be rectified, contact the local representative office of Huawei for technical support.

Principles of Parts Replacement

When replacing parts, comply with the following principles:

- Make sure that operations are feasible.
 - Check whether spare parts for the part to be replaced are available in the storehouse. If not, contact the local representative office of Huawei for technical support.
 - Make sure that parts replacement is performed only by qualified maintenance engineers who are acquired the following knowledge:
 - Functions of the parts.
 - Basic flow of parts replacement.
 - Basic skills of parts replacement.
 - Make sure that the risks of the replacement are controllable. Parts replacement is an operation subject to potential risks. Before replacing a part, estimate whether the risks can be controlled by technical protective measures without powering off a device. If yes, replace the part. If not, contact the local representative office of Huawei for technical support.
- Check the compatibility of spare parts before replacing faulty parts or upgrading parts.
- Use ESD bags and ESD boxes to contain and transport spare parts.
- Arrange, record, and return faulty parts in the routine maintenance for obtaining available spare parts in time, especially some important parts, such as boards.

Troubleshooting Principles

When rectifying a fault, comply with the following principles:

- Actively collect the fault information. When a fault occurs, learn the related information about the fault, and then make a plan for further actions. Do not handle the fault before collecting the details of the fault.
- During troubleshooting, keep detailed records of each operation and the related result. The details of the troubleshooting process serve as a ground for applying for Huawei technical support, which shortens the troubleshooting time.
- If you try to rectify the fault but fail, contact the Customer Service Center of Huawei. In addition, when you report the problem to Huawei engineers, provide the following information:
 - Full name of the office where the fault occurs
 - Name and telephone number of the contact person
 - Time when the fault occurs
 - Details of the fault
 - The software version

- Measures taken after detecting the fault and the related results
- Fault level and the expected time for resolution

4.2 Maintenance Recommendations for the Third-Party Device

To ensure the performance of Huawei devices, you must periodically check and maintain the third-party device, which is not provided by Huawei, according to the recommendations for maintaining the third-party device.

Maintenance Recommendations

The third-party device needs to be checked and maintained periodically according to the recommendations for maintaining the third-party device. In addition, the maintenance engineers need to perform the following:

- Periodically check the temperature and humidity of the telecommunications room to ensure the normal operating environment of the third-party device.
- Periodically check the power supply of the third-party device to prevent the interruption of power supply.
- Periodically check the alarms and known defects of the third-party device. Take effective measures in time to rectify the fault and ensure the normal operation of the third-party device, and reduce the fault ratio of the third-party device.
- Periodically check the link status or the connection status when the third-party device is running. Take effective measures in time to rectify the fault and ensure the normal operation of the third-party device.
- Periodically perform checking, backup, testing, and cleaning operations to detect the defects, such as normal aging, function invalidity, and performance deterioration. Take effective measures in time to rectify the fault and prevent accidents.
- Record the check results and the detected problems in the routine maintenance table as a reference for checking the running status and analyzing the fault cause in the future.

4.3 Checking the Grounding of the Device

It is recommended that you check whether the ground cable is properly installed and whether the ground resistance complies with the relevant standard once every three months. This operation ensures the reliable running of the device and avoids the potential security risks that may exist in the system.

Context

- The proper installation of the ground cable ensures the secure grounding of the device.
- If the ground resistance exceeds the limit, the functions of surge protection and grounding of the device and the telecommunications room are affected, which may lead to the security risks in the environment where the device is running.

Tools, Instruments, and Materials

- Multimeter
- Ground resistance tester

Reference Standard

- Check whether the ground cable meets the following requirements:
 - Each connection point is secure and reliable without corrosion or oxidation.
 - The ground cable is not deteriorating and its jacket is not damaged.
 - The ground bar is not corroded or oxidized, and proper anti-corrosion measures are taken for it.
- Check whether the ground resistance meets the following requirements:
 - The lap resistance between the ground cable of the device and the ground bar or the ground body is smaller than 0.1 ohm.
 - The ground resistance between the ground bar or the ground body and the earth is smaller than 10 ohms.

Precautions

NOTICE

Take appropriate measures to protect the device against lightning during the monsoon. This prevents damage to the device and personal injury.

Procedure

Step 1 Verify that the ground cable is connected properly.

- When a lightning-proof ground bar is installed at the bottom of the workbench, verify that the ground bar of the surge protector, the ground posts (PGND and BGND) of the cabinet, and the ground bar of the telecommunications room are connected properly.
- When no lightning-proof ground bar is installed at the bottom of the workbench, verify that the PDU and the ground cables (PGND and BGND) are connected properly.

Step 2 Check whether the ground resistance complies with the relevant standard.

1. Connect one end of the multimeter to the ground cable and the other end to the ground bar or the ground body to check whether the ground cable is installed reliably.
2. Check the resistance between the ground bar or the ground body and the earth by using a ground resistance tester.

Step 3 If the installation of ground cables is abnormal, handle the fault according to "Exception Handling" until the fault is rectified.

----End

Exception Handling

1. If a ground cable is aged or its jacket is damaged, replace the ground cable.
2. If a connection point is corroded or aged, replace the ground cable or the lightning-proof ground bar as required.
3. If the lap resistance between the ground cable of the device and the ground bar or the ground body is greater than 0.1 ohm, route the ground cable again.
4. If the ground resistance between the ground bar or the ground body and the earth is greater than 10 ohms, take one of the following measures to reduce the ground resistance:
 - Bury the ground body or the ground network deeper.
 - Increase the ground body (area or number of ground bodies) or the ground network.
 - Reduce the resistance of the earth.
5. If the fault persists, contact Huawei technical support engineers.

4.4 Checking the Hardware Status of Fans

It is recommended that you check the hardware status of fans once every three months. This operation ensures that the system can work under proper temperature.

Context

The normal status of fans ensures that the boards and the other parts of the device work in the normal state. Check fans carefully, especially before summer, and ensure that each fan works in the normal state.

Tools, Instruments, and Materials

- ESD wrist strip or ESD gloves
- Phillips screwdriver

Reference Standard

- Every fan in the fan tray works in the normal state and does not generate any abnormal noise.
- The STATUS indicator of the fan tray is green and is on for 1s and off for 1s repeatedly.

Procedure

Step 1 Check the running status of fans in the fan tray.

Step 2 If a fan is abnormal, handle the fault according to "Exception Handling" until the fault is rectified.

----End

Exception Handling

1. If the STATUS indicator of the fan tray is abnormal, do as follows:
 - If the STATUS indicator is yellow and blinks quickly, it indicates that the fan tray is not registered or is being loaded. In this case, you need not take any measures.
 - If the STATUS indicator is yellow and is on for 1s and off for 1s repeatedly, it indicates that a minor alarm is generated but does not affect services. In this case, solve this alarm accordingly.
 - If the STATUS indicator is always yellow, it indicates that the fan monitoring communication is interrupted. In this case, check the status of the communication between the fan tray and the device.
 - If the STATUS indicator is red and blinks quickly, it indicates that the fan is faulty or the over-temperature alarm is generated in the system. In this case, replace the faulty fan or increase the fan speed to lower the temperature.
2. If a fan generates abnormal noise, it indicates that some objects may block the fan or the fan blades may be loose. In this case, remove the objects that block the fan or replace the faulty fan tray accordingly.

NOTICE

If a fan tray needs to be removed for maintenance, it is recommended that you bring a spare fan tray to the site and replace the original fan tray with the spare fan tray. After maintenance is complete, install the original fan tray back onto the device. The replacement must be completed within 2 minutes. Otherwise, the heat dissipation capability of the subrack may be insufficient, and the device may be powered off due to high temperature.

3. If a fan is damaged, replace the faulty fan tray.

NOTICE

- Replace the entire fan tray instead of an individual fan.
- The duration of replacing the fan tray should be strictly controlled. It is recommended that you restrict the replacement to less than two minutes.
- Take ESD measures before the replacement.
- During the replacement of the fan tray, do not touch the fans when they are rotating.
- During the replacement of the fan tray, make sure that you comply with the electrical and mechanical safety precautions.
- Remove and install the fan tray carefully to prevent the fan tray from colliding with the other components in the device.
- During the replacement, prevent any metallic objects from causing short circuits. For example, tools that are placed improperly or screws that fall into the shelf accidentally can cause short circuits.

4. If the fault persists, contact Huawei technical support engineers.

4.5 Checking the Cabinet Appearance of the Cabinet

It is recommended that you should check the cabinet Appearance once every year. This operation ensures that the cabinet can work normally and stably.

Tools, Instruments, and Materials

- An anti-static wrist strip or gloves
- A phillips screwdriver

Reference Standard

The components of the cabinets are intact, the cabinet door can be opened and closed properly, and the door lock can be locked and unlocked properly.

Procedure

- Step 1** Check whether the paint of the cabinet has flaked off and whether the cabinet is damaged due to collision.
- Step 2** Check whether there are any corrosion marks, dents, or cracks on the cabinet.
- Step 3** Check whether the cabinet door can be opened and closed properly, and whether the door lock can be locked and unlocked properly. Then, close the cabinet door.

NOTICE

Make sure the cabinet door can be closed properly so that the accidents can be avoided.

- Step 4** If the cabinet door is damaged, handle the fault according to "Exception Handling" until the fault is rectified.

----End

Exception Handling

- If the paint on the cabinet surface has flaked-off, or the cabinet has been damaged due to collision, repaint and clean the cabinet.
- If the cabinet door or the door lock is faulty, contact Huawei technical support engineers.

4.6 Checking the Battery

It is recommended that you check the status of the battery once every year. This operation ensures that the power supply system can automatically switch to the battery in the case that the AC power supply is cut off. In this manner, the running of services is not affected.

Tools, Instruments, and Materials

- An adjustable wrench: Used to fasten screws.
- Screwdriver: Is used to unscrew the battery covering piece.

Reference Standard

- The shell of the battery is clean and intact.
- The shell of the battery is intact and free of leakage or distortion. There is no acid fume around the terminals or the safety valve.
- The joints between batteries are firm and free of corrosion.
- The proper spacing between batteries should be at least 10 mm.
- The terminals are not distorted or damaged. Damaged terminals will cause high contact resistance or cause cracks in the battery shell.
- The working temperature of the battery ranges from -20°C to 50°C.
- After the mains supply is disconnected, the cabinet switches to the battery and the power supply is normal.

Procedure

- Step 1** Check whether the cleanliness of the battery shell, spacing between batteries, connection between the battery terminal and the battery, and ambient temperature meet the requirement in "Reference Standard".
- Step 2** If the batteries are faulty, handle the fault according to "Exception Handling" until the fault is rectified.

----End

Exception Handling

- If the shell of the battery is dirty, clean the shell immediately.
- If the shell of the battery leaks or is distorted, replace the battery immediately.
- If the terminal of the battery is distorted or damaged, replace the battery immediately.
- If the spacing between batteries is less than 10 mm, adjust it to a proper spacing.
- If the joints between batteries turn loose or are corroded, fasten or replace the joints according to actual situations.
- If the working temperature of the battery is not within the range of -20°C-50°C, locate the cause that results in the over-temperature of the battery. Then, rectify the fault.

NOTE

The ambient temperature is critical to the service life of the battery. Research indicates that the service life of the battery is reduced to half each time the temperature increases by 10°C when the ambient temperature is beyond the temperature range of the battery.

- If the floating charging voltage of the battery is abnormal, it is recommended that you replace the faulty battery.

- If the fault persists, contact Huawei technical support engineers.

4.7 Cleaning the Air Filter of the Cabinet

It is recommended that you clean the air filters of the cabinet once every year. This operation ensures that the heat dissipation system works properly.

Tools, Instruments, and Materials

- Vacuum cleaner
- Cotton cloth

Reference Standard

The heat dissipation system works properly.

Precautions

- Huawei recommends that you should clean the air filter once every year. You can adjust the frequency according to the condition of the equipment room.
- Exercise caution when cleaning the air filter and prevent sharp objects from damaging it.
- When removing the air filter, apply proper force. Otherwise, the air filter may be distorted.
- Do not install a wet air filter in the cabinet. Otherwise, the cabinet absorbs moisture and a short-circuit may be caused, damaging the device.
- The air filter must be attached to the sticking bar firmly to prevent the air filter from coming off. If the sticking bar is faulty, replace it.

Procedure

- Step 1** Check whether the air filters of the cabinet are covered by the dust. If the air filters are covered by the dust, the ventilation of the heat dissipation system is affected. Perform the following steps to clean the air filters. The air filters of the cabinet are shown in [Figure 4-1](#).

Figure 4-1 Air filters of the cabinet



Step 2 Clean the air filter of the cabinet

1. Press down the two buckles of the air filter and lift up the air filter slightly, and then pull it out.
2. Flap dust on the air filter off, and clean it with a vacuum cleaner; or clean the air filter with water and dry it at a well-ventilated place.
3. Place the air filter at the bottom of the cabinet.
4. Adjust the position of the air filter and align the buckles. Press down the buckles to fix the air filter.

Step 3 Clean the air filter on the cabinet door

1. Open the door of the cabinet, and remove the black air filter from the sticking bar that is fixed on the inner side of the door.
2. Flap dust on the air filter off, and clean it with a vacuum cleaner; or clean the air filter with water and dry it at a well-ventilated place.
3. Use a clean and dry cotton cloth to clean the metal inner side of the cabinet.

4. Install the clean and dry air filter on the inner side of the cabinet door. Ensure that the air filter is attached to the sticking bar firmly.

Step 4 If the air filter is faulty, handle the fault according to "Exception Handling" until the fault is rectified.

----End

Exception Handling

If the air filter is damaged or wears out, replace it with a new air filter.

5 Commonly Used Methods of Fault Locating and Troubleshooting

This topic describes commonly used methods of fault locating and troubleshooting for functional modules, including OM methods of the equipment and methods of using common fault locating tools.

5.1 Service Emulation Test

This chapter describes service emulation test for locating service faults.

5.2 Common Methods of Locating Voice Service Faults

This chapter describes common tools and methods for locating voice service faults.

5.3 Common Methods for Locating DSL Faults

This chapter provides common methods for locating digital subscriber line (DSL) faults.

5.4 Common Fault Location and Rectification Methods for E1 Lines

This topic describes how to identify and rectify a fault when an E1 line is faulty.

5.5 Diagnosing Broadband Protocol Related Faults

This topic describes how to diagnose broadband protocol related faults.

5.6 Methods of Locating and Troubleshooting Common ODN Faults

This topic describes the location methods, related alarms, and common operations in locating and troubleshooting common ODN faults.

5.7 Locating and Troubleshooting ONT Faults

This topic describes ONT-related alarms and how to locate and troubleshoot ONT faults.

5.8 Traffic Burst Detection

Traffic burst detection is a feature of identifying traffic burst points by deploying detection points on the network and detecting the traffic at the detection points to obtain traffic information.

5.9 Packet Loss Query

This topic describes how to locate service faults for PON users using the packet loss query commands. The MA5800 is applicable to many other networking scenarios, such as P2P networking, Ethernet convergence networking, and Ethernet cascading networking. In these scenarios, you can use relevant packet loss query commands to locate faults by referring to this topic.

5.10 PPPoE Echo Packet Monitoring on the Upstream Port

PPPoE echo packet monitoring on the upstream port is mainly used to sense network faults and report corresponding events when PPPoE connections are online so that network faults can be quickly located.

5.1 Service Emulation Test

This chapter describes service emulation test for locating service faults.

5.1.1 DHCP Emulation

In a DHCP Emulation test, an access node simulates the DHCP client to implement remote acceptance for services that obtain IP addresses in DHCP mode (such as IPTV, IPoE, and VoIP services) and to locate faults.

5.1.1.1 DHCP Emulation Overview

In a DHCP emulation test, an access node emulates a DHCP client to apply for an IP address from a DHCP server. By doing so, the access node can test the connectivity between the access node and DHCP server and therefore the validity of DHCP configurations on the DHCP relay agent, DHCP agent, and DHCP server. In addition, the access node can ping a remote server to test the connectivity between them.

NOTE

- During DHCP simulation, certain DHCP simulation packets can be sent in a specified mode. Improper use of some simulation fields (such as source MAC address) may cause service abnormality. Therefore, use this feature only when you understand the impact of the simulation packets.
- The access node can be an OLT, MDU, or ONT.
- The remote server is an upstream network device, for example, an IPTV server or softswitch.
- The difference between a DHCP emulation test and the actual DHCP process is the initiator. In a DHCP emulation test, the access node functions as the initiator; in the actual DHCP process, the user terminal (for example, a PC, STB, or VoIP service terminal) functions as the initiator.

Mainly used for deployment acceptance and fault locating, a DHCP emulation test resolves the known issues in the traditional method. For details, see [Table 5-1](#).

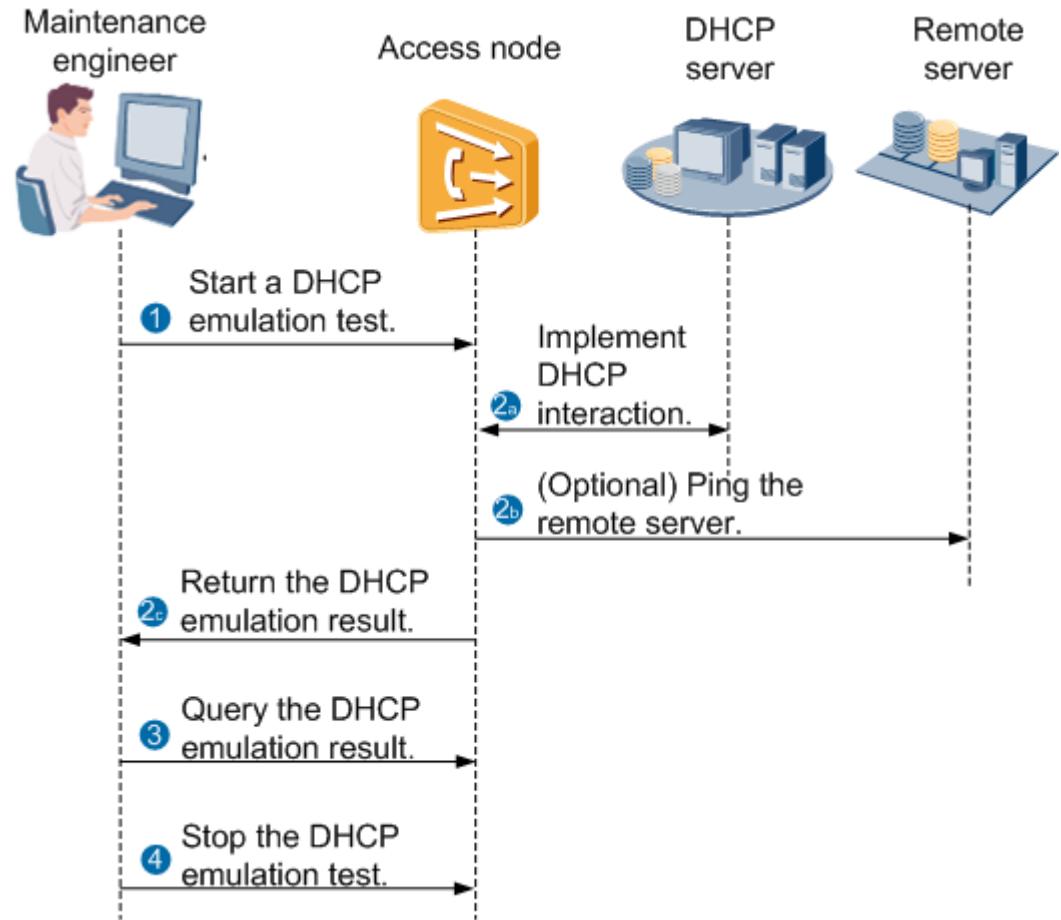
Table 5-1 Comparison between the traditional method and DHCP emulation test

Application Scenario	Traditional Method	DHCP Emulation Test
Deployment acceptance	At the device installation site, a test instrument is connected to the device and the process of users going online in batches is emulated. Alternatively, a laptop is connected to the device to test services on each port. The O&M costs are high.	A remote node implements an acceptance test for services, which does not require site visits and reduces the O&M costs.
Fault locating	When a user reports a fault, the maintenance engineer cannot remotely locate the specific network segment in a timely manner. The maintenance engineer needs to ask for the user's cooperation or go to the user's house to locate the fault, bringing about inconvenience to the user and incurring high O&M costs.	Faults can be remotely located and the specific network segment can be quickly located. Then a work order is assigned to the corresponding maintenance engineer. In this way, the efficiency is improved and the O&M costs are reduced.

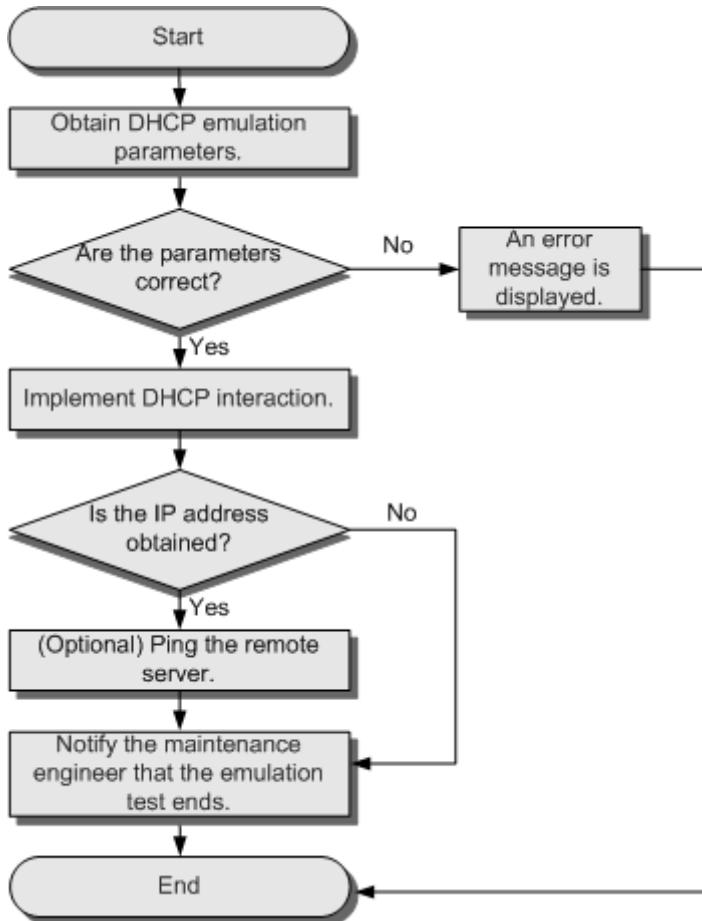
5.1.1.2 DHCP Emulation Principles

The principles of DHCP emulation.

Figure 5-1 Principles of DHCP emulation



1. The maintenance engineer remotely logs in to the access node and starts a DHCP emulation test.
2. The DHCP emulation process starts. **Figure 5-2** shows the DHCP emulation process.
 - a. DHCP interaction is implemented between the access node and DHCP server, which tests the link connectivity between them.
 - b. After obtaining an IP address, the access node pings the remote server if **hostip** (a DHCP emulation parameter indicating the IP address of the remote server) is set. This tests the link connectivity between the access node and remote server.
 - c. The DHCP emulation is completed and the DHCP emulation result is returned.

Figure 5-2 DHCP emulation flow

3. The maintenance engineer queries the DHCP emulation result.
4. The maintenance engineer manually stops the DHCP emulation test to release system resources in a timely manner.

NOTE

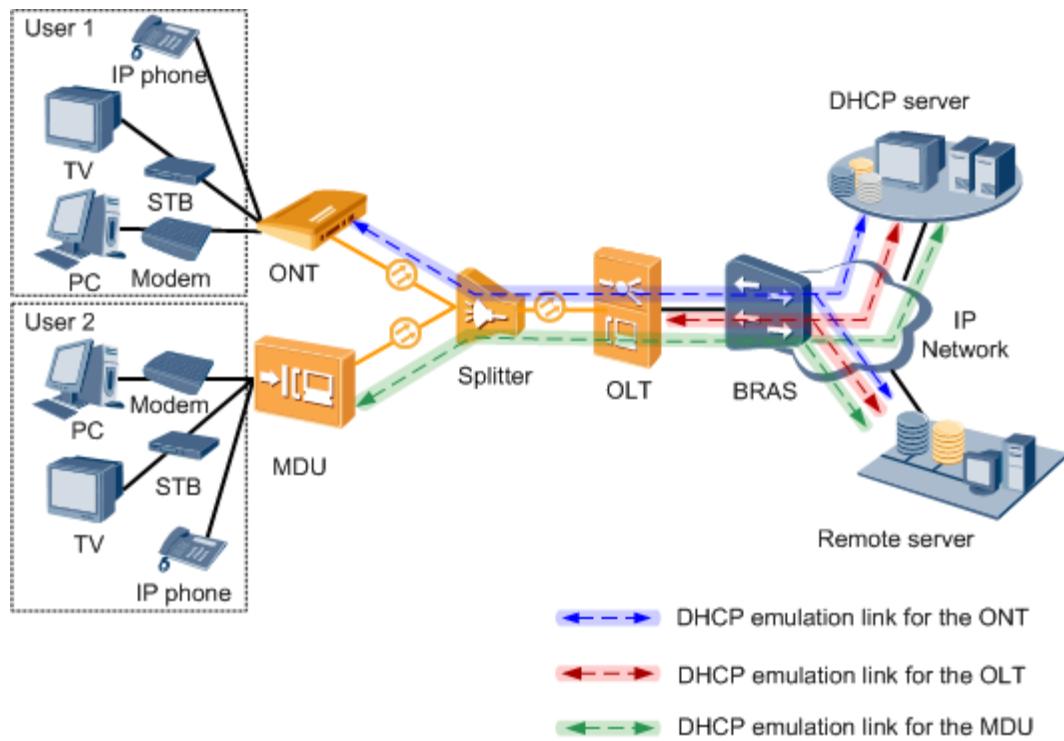
A DHCP emulation test automatically stops when the default timeout interval (210s) elapses and the emulation result will be deleted.

5.1.1.3 DHCP Emulation Usage Scenario

On an FTTx or D-CCAP network, access nodes are close to user terminals and are widely deployed. In a DHCP emulation test, an access node emulates the DHCP client to implement remote acceptance for services that obtain IP addresses in DHCP mode (such as IPTV, IPoE, and VoIP services) and locate faults, which reduces the O&M costs.

FTTx Network Application Scenarios

Figure 5-3 shows typical application scenarios of DHCP emulation on an FTTx network.

Figure 5-3 Typical application scenarios of DHCP emulation on an FTTx network**NOTE****In Figure 5-3:**

- Users 1 and 2 receive IP services (such as IPTV, IPoE, and VoIP services) and are authenticated through the BRAS.
- User 1, an FTTH user, receives IP services through the ONT; user 2, an FTTB/FTTC user, receives IP services through the MDU.

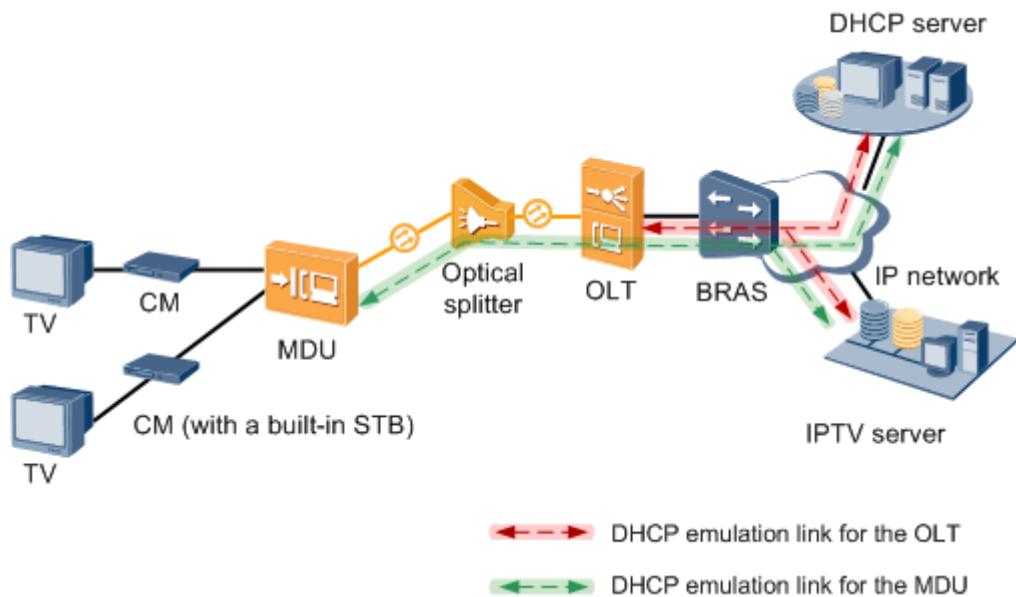
When a user receives IPTV, IPoE, or VoIP services and implements deployment acceptance or fault locating through a DHCP emulation test, only the user terminals and remote servers differ and the operation methods are the same. The following uses receiving IPTV services as an example.

When IPTV services are undergoing deployment acceptance or faulty:

- If the STB cannot obtain an IP address, network connectivity between the STB and DHCP server is abnormal. Perform a DHCP emulation test on the access node device to test the connectivity of each network segment.
- If the STB obtains an IP address successfully, network connectivity between the STB and DHCP server is normal. If users 1 and 2 still cannot watch IPTV programs, ping the remote server (for example, an IPTV server) to test the connectivity between the STB and remote server.

D-CCAP Network Application Scenarios

Figure 5-4 shows typical application scenarios of DHCP simulation on a D-CCAP network.

Figure 5-4 Typical application scenarios of DHCP simulation on a D-CCAP network

When engineers accept an IPTV service deployment or locate a fault,

- If the CM cannot obtain an IP address, the network between the CM and DHCP server is faulty. Perform a DHCP dialup simulation test on the MDU or OLT to test the connectivity of each network segment.
- If the CM can obtain an IP address, the network between the CM and DHCP server is available. If users cannot watch a program, enable the device to ping the IP address of the IPTV server using the CM's IP address to test the connectivity between the CM and the IPTV server.

Fault Locating

Locate the fault based on the obtained DHCP emulation result, as shown in [Table 5-2](#).

Table 5-2 Mapping between the emulation result and fault range

emulation Result	Description	Fault Scope
send packet fail	The access node failed to send packets to the DHCP server.	The access node is faulty.
DHCP server not found	After sending DHCP Discover packets, the access node did not receive response packets from the DHCP server.	The network segment between the access node and DHCP server is faulty.

emulation Result	Description	Fault Scope
DHCP server refuse request	The DHCP server rejected the DHCP request from the access node.	The DHCP server is faulty.
get IP overtime	After sending a DHCP request, the access node did not receive confirmation packets from the DHCP server.	The network segment between the access node and DHCP server is faulty.
get IP successful	The access node obtained an IP address from the DHCP server, indicating that the DHCP interaction was successful.	The possible fault scopes are as follows: <ul style="list-style-type: none">• The network segment between the user terminal and access node is faulty.• The network segment between the BRAS and remote server is faulty.
all ping succeed	The access node succeeded in pinging all the specified remote servers.	The network segment between the user terminal and access node is faulty.
partial ping succeed	The access node succeeded in pinging some of the specified remote servers.	The network segment between the BRAS and remote server that failed to be pinged is faulty.
all ping fail	The access node failed to ping all the specified remote servers.	Network segments between the BRAS and all remote servers are faulty.
system resource not enough	On the access node, resources for DHCP emulation are insufficient.	On the access node, resources for DHCP emulation are insufficient.
unknown	-	-

5.1.1.4 Configuring DHCP Emulation

Context

Maintenance engineers can log in to the access node and perform DHCP emulation configurations through the CLI or NMS. The following uses operations through the CLI as an example.

- For FTTB or FTTC scenario, a DHCP emulation test can be directly performed on the OLT or MDU.
- For FTTH scenario, a DHCP emulation test can be started on the ONT through the OLT.

Procedure

Step 1 Run the **simulate dhcp start** command to start a DHCP emulation test.

Step 2 Run the **display simulation dhcp** command to query the specified DHCP emulation result.



When the default timeout interval (210s) for the DHCP emulation test elapses or the DHCP emulation test is manually stopped, the DHCP emulation result will be deleted. Therefore, after the DHCP emulation test is completed, query the DHCP emulation result in a timely manner.

Locate the fault based on the obtained DHCP emulation result, as shown in [Table 5-2](#).

Step 3 Run the **simulate dhcp stop** command to stop the DHCP emulation test.

----End

Example

In the FTTB or FTTC scenario: Log in to the OLT or MDU and start a DHCP emulation test on it.

- ID of the service port: 0
- MAC address of the simulated server: 00e0-fc00-0001
- Option 60: HW
- Option 61 type corresponding to the option 61 field: 1; client ID: 00e0-fc00-0002
- IP address of the to-be-pinged remote server: 192.168.3.99

1. Start a DHCP emulation test.

```
huawei(config)#simulate dhcp start service-port
{ service-portid<U><0,131071> }:0
{ mac-address<P><H-H-H> }:00e0-fc00-0001
{ <cr>|host-ip1<K>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K>|option60<K>|option61<K>|user-vlan<K> }:option60
{ option60<S><Length 1-64> }:HW
{ <cr>|host-ip1<K>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K>|option61<K> }:option61
{ mac-addr<K>|string<K> }:mac-addr
{ mac-clientid<P><XXXX-XXXX-XXXX> }:00e0-fc00-0002
{ <cr>|host-ip1<K>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K> }:host-ip1
{ ipaddr1<I><X.X.X.X> }:192.168.3.99
{ <cr>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K>|overtime<K> }:
```

Command:

```
simulate dhcp start service-port 0 00e0-fc00-0001 option60 HW
option61 mac-addr 00e0-fc00-0002 host-ip1 192.168.3.99
```

Please check whether the input flow ID and MAC address are correct. Incorrect parameters may affect the services of normal users.

You are suggested to use the MAC address of the actual user.

Are you sure to continue?(y/n)[n]:y

2. Query the DHCP emulation result.

```
huawei(config)#display simulation dhcp
{ <cr>|service-port<K>||<K>|<K>|><K> }:service-port
{ service-portid<U><0,131071> }:0
{ mac-address<P><XXXX-XXXX-XXXX> }:00e0-fc00-0001

Command:
    display simulation dhcp service-port 0 00e0-fc00-0001
Total : 1
-----
----- common info -----
FlowID      : 0
User MAC    : 00e0-fc00-0001
User VLAN   : 10
Optin60     : HW
Option61 type : 1
Option61 client : 00e0-fc00-0002
Simulate status : finished
Simulate result : all ping succeed
Simulate start time : 2019-01-17 16:51:59+08:00
User IP      : 192.168.3.100/24
DHCP server IP : 192.168.3.8
Primary DNS server IP : -
Secondary DNS server IP : -
Relay gateway : 0.0.0.0
Default gateway : 192.168.3.201
-----
----- route info -----
Route:1 Destination IP : 192.168.5.0/24    Next hop IP : 192.168.3.66
      Next hop MAC : -          Local interface : -
Route:2 Destination IP : 192.168.4.0/24    Next hop IP : 192.168.3.88
      Next hop MAC : 00e0-fc00-dbba  Local interface : Y
Route:3 Dstination IP : -           Next hop IP : -
      Next hop MAC : -          Local interface : -
-----
----- ping info -----
Host:1 IP : 192.168.3.99    Total count : 3    Succeed count : 3
Host:2 IP : -           Total count : 0    Succeed count : 0
Host:3 IP : -           Total count : 0    Succeed count : 0
Host:4 IP : -           Total count : 0    Succeed count : 0
Host:5 IP : -           Total count : 0    Succeed count : 0
```

3. Stop the DHCP emulation test.

```
huawei(config)#simulate dhcp stop service-port 0 00e0-fc00-0001
```

In the FTTH scenario, log in to the OLT and start a DHCP emulation test on the ONT.



During the DHCP emulation, the IP address obtained can be used for multicast emulation.

- ID of the subrack/slot/port of the OLT connected to the ONT: 0/2/0
- ID of the ONT enabled with DHCP emulation: 1
- VLAN ID in the VLAN tag in packets: 10
- Option 61 type corresponding to the option 61 field: 0; client ID: user
- IP address of the to-be-pinged remote server: 192.168.3.99
- IP address of the multicast program: 224.1.1.1

1. Issue commands on the OLT to start a DHCP emulation test on the ONT.

```
huawei(config)#simulate dhcp start ont
{ frameid/slotid/portid<S>|Length 5-18> }:0/2/0
{ ontid<U><0,255> }:1
{ eth<K>|outer-vlan<K>|untag<K>|vlan<K> }:vlan
{ vlanid<U><1,4095> }:10
{ <cr>|host-ip1<K>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K>|option60<K>|option61<K>|priority1<U><0,7>|usermac<K> }:option61
```

```
{ mac-addr<K>|string<K> }:string
{ string_clientid<S><Length 1-64> }:user
{ <cr>|host-ip1<K>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K> }:host-ip1
{ ipaddr1<I><X.X.X.X> }:192.168.3.99
{ <cr>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K>|groupid<K> }:groupid
{ ip-addr<I><X.X.X.X>|<cr> }:224.1.1.1
{ igmp-version<K> }:igmp-version
{ v2<K>|v3<K> }:v2

Command:
simulate dhcp start ont 0/2/0 1 vlan 10 option61 string user host-ip1
192.168.3.99 groupid 224.1.1.1 igmp-version v2
```

2. Query the ONT DHCP emulation result.

```
huawei#display simulation dhcp
{ <cr>|ont<K>|service-port<K>||<K>|><K>|><K> }:ont
{ <cr>|frameid|slotid|portid<S><Length 5-18> }:0/2/0
{ ontid<U><0,255> } 1
```

Command:
display simulation dhcp ont 0/2/0 1

```
----- common info -----
simulation instance : F/S/P: 0/2/0 ONTId:1 ONTPort WAN
simulation VLAN tag num : 1
simulation outer VLANID : 10
simulation inner VLANID : -
Option60 : -
Option61 type : 0
Option61 client : user
Simulate status : finished
Simulate result : succeed
Simulate start time : 2013-01-17 15:49:20+09:00
User IP : 192.168.3.100/24
DHCP server IP : 192.168.3.99
Primary DNS server IP : 10.72.55.81
Secondary DNS server IP : 10.72.255.100
Relay gateway : 192.168.3.99
Default gateway : 192.168.3.99
----- route info -----
Route:1 Destination IP : 192.168.5.0/24 Next hop IP : 192.168.3.66
    Next hop MAC : - Local interface : -
Route:2 Destination IP : 192.168.4.0/24 Next hop IP : 192.168.3.88
    Next hop MAC : 00e0-fc00-dbba Local interface : Y
Route:3 Destination IP : - Next hop IP : -
    Next hop MAC : - Local interface : -
----- ping info -----
Host:1 IP : 192.168.3.99 Total count : 3 Succeed count : 3
Host:2 IP : - Total count : 0 Succeed count : 0
Host:3 IP : - Total count : 0 Succeed count : 0
Host:4 IP : - Total count : 0 Succeed count : 0
Host:5 IP : - Total count : 0 Succeed count : 0
----- multicast info -----
Multicast group IP : 224.1.1.1
Multicast source IP : -
Multicast version : IGMPv2
Data rate(kbps) : 1500
```

3. Stop the ONT DHCP emulation test.

```
huawei(config)#simulate dhcp stop ont 0/2/0 1
```

In the D-CCAP scenario: Log in to the OLT or MDU and start a DHCP emulation test on the CM.

- MAC address of the CM: 00e0-fc00-0001
- Option 60: docsis

- Option 61 type corresponding to the option 61 field: 1; client ID: 00e0-fc00-0002
 - IP address of the to-be-pinged remote server: 192.168.3.99
1. Issue commands on the OLT or MDU to start a DHCP emulation test on the CM.

```
huawei(config)#simulate dhcp start
{ cm<K>|ont<K>|service-port<K> }:cm
{ mac-address<P><XXXX-XXXX-XXXX> }:00e0-fc00-0001
{ <cr>|host-ip1<K>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K>|option60<K>|option61<K>|user-vlan<K> }:option60
{ option60<S><Length 1-64> }:docsis
{ <cr>|host-ip1<K>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K>|option61<K> }:option61
{ mac-addr<K>|string<K> }:mac-addr
{ mac-clientid<P><XXXX-XXXX-XXXX> }:00e0-fc00-0002
{ <cr>|host-ip1<K>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K> }:host-ip1
{ ipaddr1<I><X.X.X.X> }:192.168.3.99
{ <cr>|host-ip2<K>|host-ip3<K>|host-ip4<K>|host-ip5<K> }:

Command:
    simulate dhcp start cm 00e0-fc00-0001 option60 docsis option61 mac-addr
00e0-fc00-0002 host-ip1 192.168.3.99
Please check whether the input CM MAC address is correct. Incorrect parameters may
affect the services of normal users.
You are suggested to use the MAC address of the actual user.
Are you sure to continue?(y/n)[n]:y

Info: DHCP simulation instance is complete (FlowID=1, MAC=00e0-fc00-0001)
```

2. Query the CM DHCP emulation result.

```
huawei#display simulation dhcp
{ <cr>|cm<K> }:cm
{ mac_addr<P><XXXX-XXXX-XXXX> }:00e0-fc00-0001

Command:
    display simulation dhcp cm 00e0-fc00-0001
Total : 1
-----
----- common info -----
FlowID      : 0
User MAC    : 00e0-fc00-0001
User VLAN   : -
Option60     : docsis
Option61 type : 1
Option61 client : 00e0-fc00-0002
Simulate status : finished          /*Simulate status
Simulate result  : get IP successful /*Simulate result
Simulate start time : 2012-06-30 16:51:59+08:00
User IP      : 192.168.3.100/24
DHCP server IP : 192.168.3.8
Primary DNS server IP : -
Secondary DNS server IP : -
Relay gateway : -
Default gateway : 192.168.3.201
Tftp server Name : huawei
Bootfile name  : bootfile
Time server IP : 192.168.100.100
-----
----- route info -----
Route:1 Destination IP : 192.168.5.0/24    Next hop IP : 192.168.3.66
      Next hop MAC : -           Local interface : -
Route:2 Destination IP : 192.168.4.0/24    Next hop IP : 192.168.3.88
      Next hop MAC : 00e0-fc00-dbba Local interface : Y
Route:3 Destination IP : -                  Next hop IP : -
      Next hop MAC : -           Local interface : -
-----
----- ping info -----
Host:1 IP : 192.168.3.99  Total count : 3  Succeed count : 3
Host:2 IP : 192.168.4.99  Total count : 3  Succeed count : 0
```

Host:3 IP : 192.168.5.99	Total count : 3	Succeed count : 0
Host:4 IP : 192.168.3.77	Total count : 3	Succeed count : 0
Host:5 IP : 192.168.6.99	Total count : 3	Succeed count : 0

3. Stop the CM DHCP emulation test.

```
huawei(config)#simulate dhcp stop cm 00e0-fc00-0001
```

5.1.1.5 DHCP Emulation Reference Standards and Protocols

- IETF RFC 2131: Dynamic Host Configuration Protocol
- IETF RFC 1533: DHCP Options and BOOTP Vendor Extensions

5.1.2 PPPoE Dialup Emulation

5.1.2.1 PPPoE Dialup Emulation Introduction

In PPPoE dialup emulation, an access device emulates an end user and initiates PPPoE dialup. According to the PPPoE dialup emulation result (successful or failed), users can determine the network connectivity between the access device and the broadband remote access server (BRAS). If a fault has occurred in the network, PPPoE dialup emulation helps users quickly identify whether the fault is on the network side or user side.

 **NOTE**

During PPPoE simulation, certain PPPoE simulation packets can be sent in a specified mode. Improper use of some simulation fields (such as source MAC address) may cause service abnormality. Therefore, use this feature only when you understand the impact of the simulation packets.

PPPoE dialup emulation is used for remote fault location and acceptance tests.

Table 5-3 lists the comparison between the method of performing a PPPoE dialup emulation test and the method of performing a traditional PPPoE dialup test.

Table 5-3 Comparison between the method of performing a PPPoE dialup emulation test and the method of performing a traditional PPPoE dialup test

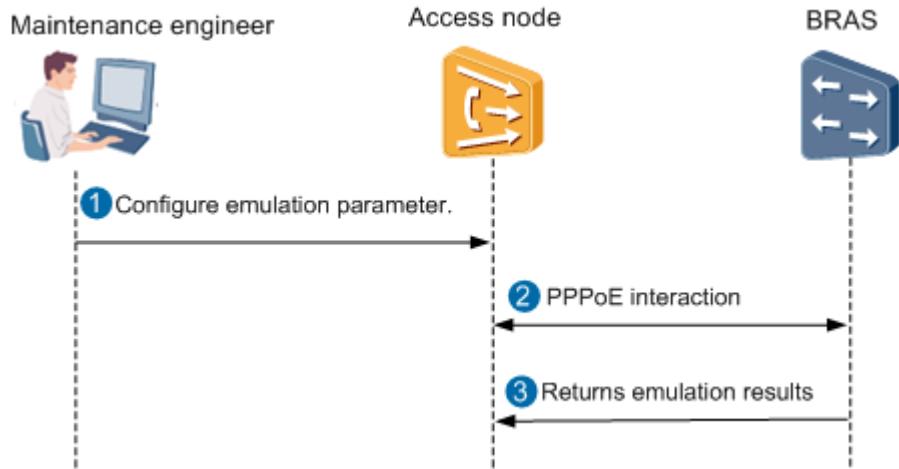
Scenario	Task	Method of Performing a Traditional PPPoE Dialup Test	Method of Performing a PPPoE Dialup Emulation Test
Acceptance test	After an access device is installed, a test engineer needs to check whether the PPPoE dialup service on the access device has been provisioned properly.	The test engineer visits the site where the access device is installed and uses an external tester or a portable computer to perform a PPPoE dialup test for each port.	The test engineer remotely logs in to the access device to perform a PPPoE dialup emulation test and determines the service status based on the test result. NOTE A PPPoE dialup emulation test cannot check the status of the line between an end user and an access device.
Fault location	A maintenance engineer needs to locate a fault on an access network that covers a large area and contains geographically dispersed network devices.	The maintenance engineer visits all sites where the access devices are installed and performs a PPPoE dialup test.	The maintenance engineer preliminarily determines the network segment where the fault occurs and remotely logs in to the access devices to perform a PPPoE dialup emulation test. Based on the test result, the maintenance engineer determines the fault cause and rectifies the fault.

5.1.2.2 PPPoE Dialup Emulation Principles

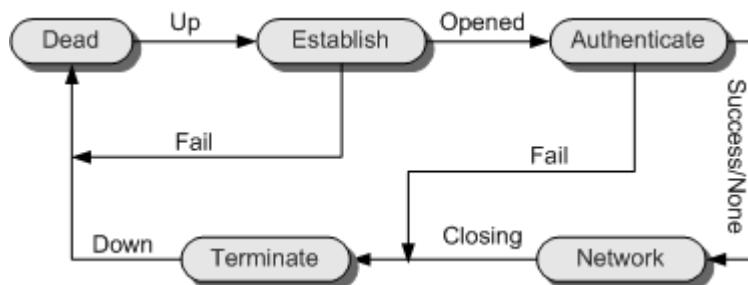
PPPoE dialup emulation differs from PPPoE dialup in the following aspects:

- The PPPoE dialup emulation process is initiated by an access device, while the PPPoE dialup is initiated by a PC, modem, or home gateway.
- The MAC address carried in the packet in PPPoE dialup emulation is the bridge MAC of an access device, while the MAC address carried in the packet in the PPPoE dialup is that of a PC, modem, or home gateway.

The principles of PPPoE dialup emulation.

Figure 5-5 Principles of PPPoE dialup emulation

1. A maintenance engineer can start a PPPoE dialup emulation on an access node, the access node emulates an end user and initiates PPPoE dialup.
Enter parameters required for the PPPoE dialup emulation, including service flow ID (identifying the user), MAC address, user name, password, authentication mode, and timeout time.
2. Access node interacts with the BRAS.
The emulated PPPoE dialup includes two phases:
 - a. PPPoE discovery phase.
The source host discovers the MAC address of the destination host (in this case, the BRAS), and a point-to-point PPP session is set up.
 - b. PPPoE session phase.
A point-to-point connection has been set up and carries PPP packets for link negotiation, as shown in [Figure 5-6](#).

Figure 5-6 PPPoE session flow

3. The maintenance engineer can stop a PPPoE dialup emulation on an access node.

5.1.2.3 PPPoE Dialup Emulation Usage Scenario

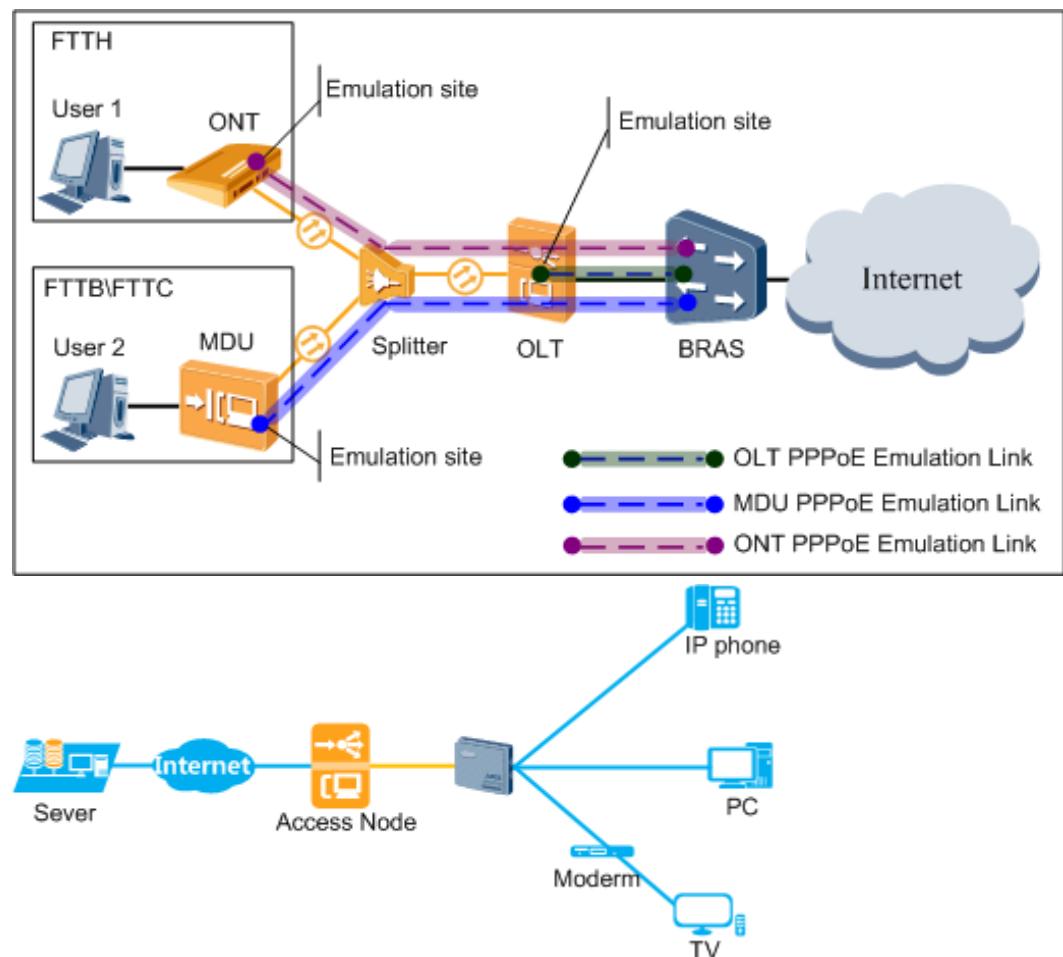
Context

On networks, access devices are closer to terminals and widely distributed. If a PPPoE dialup fault occurs, PPPoE dialup tests performed onsite increase fault location costs. To resolve this issue, PPPoE dialup emulation tests can be performed remotely.

Scenario

Figure 5-7 shows the typical networking.

Figure 5-7 Typical networking



In the preceding figure, users use the PPPoE dialup service and they are authenticated in PPPoE mode through the broadband remote access server (BRAS).

- For ONT user, perform the PPPoE dialup emulation on the ONT.
- For MDU user, perform the PPPoE dialup emulation on the MDU.
- For OLT user, perform the PPPoE dialup emulation on the OLT.

Fault Location

The troubleshooting roadmap based on the test result is as follows:

Table 5-4 PPPoE dialup emulation results

Emulation Result	Corresponding Windows Error Code	Description	Handling Guide
Success	-	<ul style="list-style-type: none">• The link between the access node and the BRAS is functional.• The service configuration of the PPPoE user is correct.• Parameters such as the user name, password, and authentication mode of the PPPoE user are correct.	-
Parameter negotiation fail	732 Your computer and the remote computer could not agree on PPP control protocols.	PPPoE dialup emulation has entered the link setup phase of the PPP session, but parameter negotiation fails, causing the link failure.	Check whether the Policy Information Transfer Protocol (PITP) configuration is correct.
Link unnormal	638 The remote server is not responding in a timely fashion.	PPPoE dialup emulation has entered the link setup phase of the PPP session, but the creation of the LCP link is abnormal.	Check whether an access control list (ACL) that does not allow transmission of PPPoE packets is configured on the access node.

Emulation Result	Corresponding Windows Error Code	Description	Handling Guide
Authentication fail	691 The connection was denied because the username or password you specified is not valid or because the selected authentication protocol is not permitted on the remote server.	PPPoE dialup emulation has entered the user authentication phase of the PPP session, but user name or password mismatch occurs between the client and server.	<ul style="list-style-type: none">The user's account is configured on the access node is not correct.The user's account is configured on the BRAS is not correct.
Time out	721 The remote computer is not responding.	PPPoE dialup emulation exceeds the preset emulation timeout time.	<ul style="list-style-type: none">The present emulation time out time is too short.The link between access node and BRAS is abnormal, transmission delay is too large.
Peer down request	668 The connection was terminated.	The server forcibly terminates the PPPoE dialup emulation.	The user's account is restricted on the BRAS.
Other error	635 There was an unknown error.	Unknown errors.	-

5.1.2.4 Configuring PPPoE Dialup Emulation

Context

If a PPPoE dialup fault occurs, a PPPoE dialup emulation test can be performed on the ONT or MDU to check the connection between the ONT or MDU and the BRAS and locate the fault according to the test result.

Procedure

- Step 1** Run the **simulate pppoe start** command to perform a PPPoE dialup emulation.
- Step 2** Run the **display simulation pppoe** command to query the status of the PPPoE dialup emulation.

 NOTE

Query the status of the PPPoE dialup emulation only after the test is started. The status cannot be queried if the emulation is stopped.

Step 3 Run the **simulate pppoe stop** command to stop PPPoE dialup emulation.

 NOTE

Another PPPoE dialup emulation can be performed only after the current PPPoE dialup emulation is stopped.

----End

Example

In FTTB or FTTC scenario, remotely log in to the access node device and perform PPPoE dialup emulation on it.

- Service port ID: 0
- MAC address of the emulation user: 00e0-fc00-1111
- 1. Start PPPoE dialup emulation.

```
huawei(config)#simulate pppoe start
Service-port(index<0-1999>):0
Mac-address<P><XXXX-XXXX-XXXX>[default 5623-5987-dead]:00e0-fc00-1111
User Name(length<1,65>):user-0
User Password(length<0,16>):*****
Authentication Mode:
1. Chap 2. Pap [default 1]:1
Overtime Time(5-60s)[default 5]:10
```

- 2. Query the status of PPPoE dialup emulation.

```
huawei(config)#display simulation pppoe
PPPoE simulate information is:
```

```
-----
Service-port: 0
Mac-address: 00e0-fc00-1111
User name: user-0
Current phase: -
Result: Success
Start time: 2019-03-06 08:20:23+08:00
End time: 2019-03-06 08:23:36+08:00
Session ID: 591
User IP: 192.168.1.172
Gateway IP: 192.168.1.1
-----
```

- 3. Stop PPPoE dialup emulation.

```
huawei(config)#simulate pppoe stop
```

In FTTH scenario, remotely log in to the OLT and perform PPPoE dialup emulation on the ONT.

 NOTE

During the PPPoE dialup emulation, the IP address obtained can be used for multicast emulation.

- Port to which the ONT connects: 0/2/0
- ONT ID: 0
- Ethernet port: 1
- VLAN ID: 100

- IP address of the multicast program: 225.0.0.1
 - IP address of the multicast source: 10.2.3.4
1. Start PPPoE dialup emulation.

```
huawei(config-if-gpon-0/2)#pppoe simulate start
{ portid<U><0,3>}:0
{ ontid<U><0,63>}:0
{ eth<K>|untagged<K>|vds1<K>|vlanid<U><0,4095> }:eth
{ ont-portid<U><1,24>}:1
{ untagged<K>|vlanid<K> }:100
{ priority<U><0,7>|user-name<K> }:2
{ user-name<K> }:user-name
{ user-name<S><Length 1-64> }:pppoe
{ user-password<K> }:user-password
{ password<S><Length 1-64> }:password
{ authentication-mode<K> }:authentication-mode
{ protocol<U><chap,pap> }:chap
{ <cr>|group-ip-address<K> }:group-ip-address
{ group-ip-address<I><X.X..X> }:225.0.0.1
{ <cr>|igmp-version<K> }:igmp-version
{ v2<K>|v3<K>}:v3
{ <cr>|source-ip-address<K> }:source-ip-address
{ source-ip-address<I><X.X..X> }:10.2.3.4
```

Command:

```
pppoe simulate start 0 0 eth 1 100 2 user-name pppoe user-password password authentication-
mode chap groupip 225.0.0.1 igmp-version v3 source-ip-address 10.2.3.4
```

ONT PPPoE Test Result

```
F/S/P      : 0/2/0
ONT-ID     : 0
ONT ETH Port ID   : 1
ONT Vlan ID      : 100
Vlan Priority    : 2
Multicast group IP : 225.0.0.1
Multicast source IP : 10.2.3.4
Multicast version  : v2
Multicast traffic(kbps) : 1500
Emulator result   : Multicast test fail
Session ID       : 0
User IP          : 192.168.1.1
Gateway IP       : 255.255.255.0
```

2. Query ONT PPPoE dialup emulation results of port 0/2/0.

```
huawei(config-if-gpon-0/2)#display pppoe simulate 0
{<cr>|ontid<U><0,127>}
```

Command:

```
display pppoe simulate 0
```

```
F/S/P      : 0/2/0
ONT-ID     : 0
ONT ETH Port ID   : 1
ONT Vlan ID      : 100
Vlan Priority    : 2
Multicast group IP : 225.0.0.1
Multicast source IP : 10.2.3.4
Multicast version  : v2
Multicast Data rate(kbps): 1500
Emulator result   : Multicast test fail
Session ID       : 0
User IP          : 192.168.1.1
Gateway IP       : 255.255.255.0
```

3. Run the **simulate pppoe stop** command to stop PPPoE dialup emulation.

```
huawei(config)#simulate pppoe stop
```

5.1.2.5 PPPoE Dialup Emulation Reference Standards and Protocols

IETF RFC 2516: A Method for Transmitting PPP Over Ethernet (PPPoE)

IETF RFC 1661: The Point-to-Point Protocol (PPP)

5.1.3 Multicast Emulation

A multicast emulation test remotely emulates an end user going online, and engineers query the real-time traffic of the multicast program to determine whether the multicast function is running properly.

5.1.3.1 Introduction

In multicast emulation, an access device remotely emulates an end user going online. Engineers query the real-time traffic of the multicast program to determine whether the multicast function is running properly.

Multicast emulation is used in acceptance tests or fault location. The following table lists the comparison between the multicast emulation test and traditional tests.

Table 5-5 Comparison between the multicast emulation test and traditional tests

Scenario	Task	Traditional Test	Multicast Emulation
Acceptance test	After an access device is installed and configured with data, a test engineer needs to check whether the multicast service has been provisioned to the access device successfully.	The test engineer visits the site where the access device is installed and uses an external tester or a portable computer to perform a multicast test on each port of the device.	The test engineer remotely logs in to the access device to perform a multicast emulation test and determines the service status based on the test results.

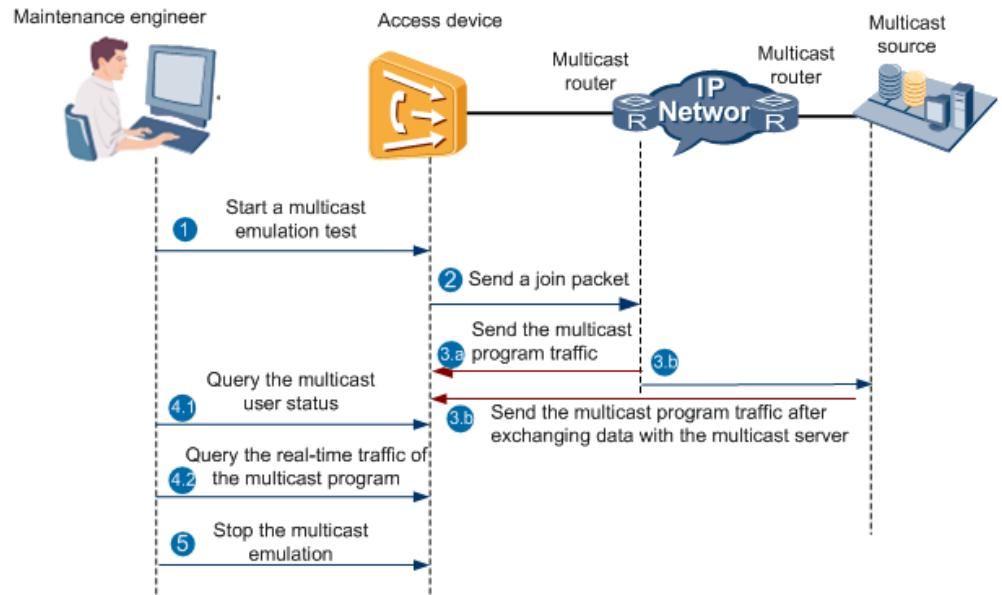
Scenario	Task	Traditional Test	Multicast Emulation
Fault location	The multicast service is abnormal, and a maintenance engineer needs to quickly locate the network segment of the fault to facilitate subsequent troubleshooting.	The maintenance engineer visits all sites where the access devices are installed and performs tests.	The maintenance engineer remotely logs in to an access device and performs a multicast emulation test to preliminarily determine the network segment of the fault. Based on the test results, the engineer diagnoses the fault cause and rectifies the fault. NOTE A multicast emulation test cannot check the status of the line between an end user and an access device.

5.1.3.2 Reference Standards and Protocols

- RFC-2236: Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997
- RFC 3376: B. Cain., "Internet Group Management Protocol, Version 3", RFC 3376, October 2002
- RFC 4607: H. Holbrook, "Source-Specific Multicast for IP", RFC 4607, August 2006

5.1.3.3 Principles

[Figure 5-8](#) shows the principles of multicast emulation.

Figure 5-8 Principles of multicast emulation

1. A maintenance engineer remotely logs in to an access device and starts a multicast emulation test on a user port.
The engineer sets parameters, such as the user information, program IP address, and multicast VLAN ID.
2. The access network device constructs a join packet and sends the packet to the multicast router for joining a multicast group.
3. The multicast router checks whether the multicast program traffic exists.
 - If the multicast program traffic exists, the multicast router sends the multicast program traffic to the access device.
 - If the multicast program traffic does not exist, the multicast source sends the multicast program traffic to the access device after exchanging data with the multicast router.
4. The maintenance engineer queries the status of the emulation user and the real-time traffic of the multicast program.
 - Checks whether the multicast emulation user is online to determine whether the user successfully orders the program.
 - Checks the real-time traffic of the multicast program to determine whether the communication between the access device and the multicast source is normal.
5. After the multicast emulation is complete, the maintenance engineer stops the emulation manually using the CLI to release resources.

5.1.3.4 Usage Scenario

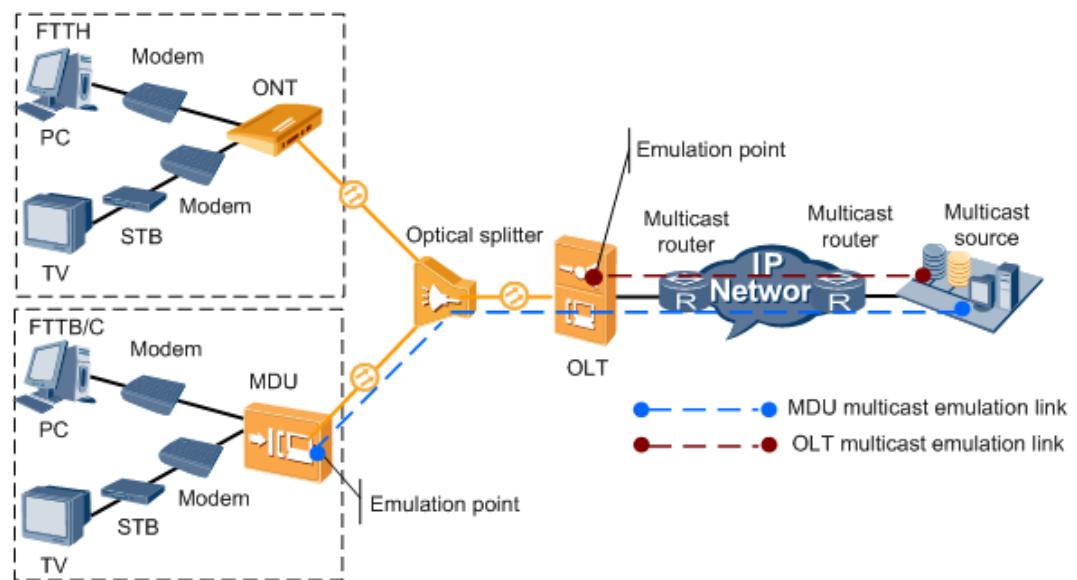
Context

On fiber to the x (FTTx) networks, access devices are located closer to user terminals and widely distributed. In a multicast emulation test, an access node emulates the multicast user to implement remote acceptance for services and locate faults, which reduces the O&M costs.

Scenario

[Figure 5-9](#) shows the multicast emulation on a typical FTTx network.

Figure 5-9 Multicast emulation on a typical FTTx network



NOTE

In [Figure 5-9](#), the MDU and ONT can provide the video on demand (VoD) service for a user through the PC. The MDU and ONT can also provide the BTV service using a set top box (STB).

In IPTV service acceptance or fault location:

- For MDU multicast users, multicast emulation can be performed on the MDU in service acceptance.
- For ONT multicast users, multicast emulation can be performed on the OLT.

NOTE

ONTs do not support multicast emulation. To emulate an ONT multicast user, perform an emulation test on the PON board of the OLT.

Fault Location

After the multicast emulation, you can query the user status and multicast program's real-time traffic through the CLI. The following table lists troubleshooting suggestions based on the query results.

 **NOTE**

Data configurations are seldom changed in daily operation and maintenance. Therefore, multicast faults are usually caused by hardware problems. Hardware must be checked prior to data configuration during fault location.

Table 5-6 Multicast emulation results and troubleshooting suggestions

Command	Results	Description	Troubleshooting Suggestions
display igmp user	The user status parameter State is online .	The multicast user can go online successfully.	<ul style="list-style-type: none">● If the user can go online and the access device can communicate with the multicast source, the fault may be caused by a communication failure between the access device and the set-top box (STB). The reasons are as follows:<ul style="list-style-type: none">- The hardware of the port on the access device is faulty.- The physical line between the access device and the modem is faulty.- The modem is faulty.- The STB is faulty.● If the user can go online but the traffic on the access device's uplink port is abnormal, the fault may be that the hardware connection between the access device and the upper-layer device (multicast router or multicast server) is incorrect, or the software configuration is incorrect. The common software configuration faults are as follows:<ul style="list-style-type: none">- The remaining multicast bandwidth of the user is lower than the required

Command	Results	Description	Troubleshooting Suggestions
			<p>bandwidth of the ordered program.</p> <ul style="list-style-type: none">- The number of programs watched by the multicast user reaches the upper limit so that the user cannot order a new program.- The multicast user does not have the permission to watch the program.- The program ordered is not in the MVLAN to which the multicast user belongs.- The multicast user does not have the permission to order certain types of programs (such as HDTV).- The number of programs at a level watched by the multicast user reaches the upper limit so that the user cannot order a new program at this level.- The rate configured in the traffic profile bound to the traffic stream is far lower than the bandwidth of the multicast program.- There are too many prejoined static programs, occupying too many bandwidths.

Command	Results	Description	Troubleshooting Suggestions
			<p>The common software configuration problems of the upper layer device are as follows:</p> <ul style="list-style-type: none">- The program is not configured on the multicast server.- The TTL value set on the multicast server for the multicast stream is very small.

Command	Results	Description	Troubleshooting Suggestions
	The user status parameter State is offline .	The multicast user fails to go online and therefore fails to order a program in the emulation.	<p>The case is more complicated than the scenario in which the user is online. Handling suggestions are as follows: Enable the multicast debugging function and start the multicast emulation again to check whether the access device receives the report packet from the user for ordering a program. Run the following commands to enable the multicast debugging function:</p> <pre>huawei(config)#terminal debugging huawei(config)#terminal monitor huawei(config)#debugging igmp service-port index</pre> <p>NOTE index is the ID of the multicast user's service port.</p> <ul style="list-style-type: none">• If the access device receives the report packet, the multicast link is normal but the access device fails to create a corresponding multicast entry. This is generally caused by incorrect multicast configurations on the access device.• If the access device does not receive the report packet, the multicast link fails. This is mainly caused by incorrect access device data configurations, faulty physical link between the access device and the modem, or

Command	Results	Description	Troubleshooting Suggestions
			hardware faults of terminals.
	The user status parameter State is block .	The multicast user is locked and therefore fails to order a program.	Run the undo igmp user block command to unblock the user.
display multicast flow-statistic	The multicast program's real-time traffic parameter Multicast flow statistic result is a small value or zero.	The program's traffic on the uplink port is small or zero.	The hardware connection between the access device and the upper-layer device (multicast router or multicast server) is incorrect, or the software configuration is incorrect. troubleshoot the fault based on the suggestions provided when the user can go online but the traffic on the access device's uplink port is abnormal.

Command	Results	Description	Troubleshooting Suggestions
	The multicast program's real-time traffic parameter Multicast flow statistic result is close to the program's bandwidth.	The device uplink port can communicate with the multicast source.	<ul style="list-style-type: none">● If the user can go online and the access device can communicate with the multicast source, the fault may be caused by a communication failure between the access device and the STB. The reasons are as follows:<ul style="list-style-type: none">- The hardware of the port on the access device is faulty.- The physical line between the access device and the modem is faulty.- The modem is faulty.- The STB is faulty.● If the access device can communicate with the multicast source but the user cannot go online, troubleshoot the fault based on the suggestions provided when the user status parameter State is offline.

5.1.3.5 Configuration

Context

- The configuration of the multicast port is correct.
- The multicast user for whom the multicast emulation test is performed has the rights to watch the configured multicast programs.

Procedure

Step 1 Run the **igmp static-join** command to perform the multicast emulation test for the multicast user.

```
huawei(config)#btv
huawei(config-btv)#igmp static-join service-port 500
{ ip<K>|ipv6<K> }:ip
{ ip-addr<I><X.X.X.X> }:224.1.1.1
{ vlan<K> }:vlan
{ vlanid<U><1,4093> }:4002
```

Step 2 Run the **display igmp user** command to query the status of the multicast user.

- If the multicast user is in **offline** state, the multicast user fails to request for programs.
- If the multicast user is in **online** state, the multicast user requests for programs successfully.
- If the multicast user is in **block** state, the multicast user is blocked. In this case, run the **undo igmp user block** command to unblock the user.

```
huawei(config)#display igmp user service-port 500
User           : 0/1/0
State: online // The multicast user is online.
Authentication   : auth
Quick leave      : MAC-based
IGMP flow ID     : 500
Video flow ID    : 500
Log switch       : enable
Bind profiles    : 2
IGMP version     : IGMP v3
Current version   : IGMP v3
.....
```

Step 3 Run the **display multicast flow-statistic** command to query the real-time traffic of the programs that the multicast user requests for in the multicast emulation test.

- If the real-time traffic of the multicast programs is a smaller value or 0, the multicast source does not deliver multicast programs or the multicast service stream does not arrive at the device. That is, the communication between the device and the multicast source is abnormal.
- If the real-time traffic of the multicast programs approaches the bandwidth of the multicast programs, the multicast source delivers the multicast programs to the device. That is, the communication between the device and the multicast source is normal.

```
huawei(config)#btv
huawei(config-btv)#display multicast flow-statistic vlan 4002 ip 224.1.1.1
Command is being executed, please wait...
Multicast flow statistic result: 29600(kbps) //The real-time traffic of multicast program 224.1.1.1 is
29600 kbit/s. This indicates that the multicast source issues multicast traffic.
```

Step 4 Run the **undo igmp static-join** command to stop multicast emulation.

```
huawei(config)#btv
huawei(config-btv)#undo igmp static-join service-port 500
{ ip<K>|ipv6<K> }:ip
{ ip-addr<I><X.X.X.X> }:224.1.1.1
{ vlan<K> }:vlan
{ vlanid<U><1,4093> }:4002
```

----End

5.1.4 Call Emulation Test

A call emulation test emulates call functions to verify data configuration for the voice service. The call emulation test can also be used to locate voice service faults.

5.1.4.1 Introduction to the Call Emulation Test

Definition

In a call emulation test, the device emulates the call function of a voice user. It is used to test the services on the POTS user port. A call emulation test includes:

- **Calling party emulation test:** The POTS user port on the device functions as the calling party. In this test, a test engineer acting as a called party is required.
- **Called party emulation test:** The POTS user port on the device functions as the called party. In this test, a test engineer acting as a calling party is required.
- **Calling and called party emulation test:** Two POTS user ports function as the calling and called parties. The test does not require manual operations. Specifically, the device automatically performs the process from calling party off-hook to called party off-hook to set up a call between the two parties and stops the test after the call hold time expires.

Application Scenarios

A call emulation test can be used in the following scenarios:

- Acceptance test during a new deployment: The software and hardware functions, including service configurations, of the device need to be verified after the device is installed. The verification ensures follow-up service provisioning.
Traditionally, the engineer goes to the device installation site, makes cables, connects a test phone set to the ONT, uses the test phone set as a caller or callee, and verifies basic voice services.
- Fault locating in the OAM phase: After the device enters the OAM phase, it is usually necessary to test basic voice services in order to locate a fault. In the access network, however, a large number of devices are installed in complicated environment, geographically dispersed, and remotely located. It is inconvenient and costly either to test a newly installed device or locate faults.

Call emulation tests can be conducted remotely. In a call emulation test, the test engineer does not need to prepare cables on the device installation site, connect test terminals to the device, or perform dialup tests on site. Instead, the test engineer enables the call emulation function in the maintenance center through the command line interface (CLI) or network management system (NMS) and uses a test phone set in the central office (CO) to make calls to the emulation port on the device. In this way, the test engineer can verify the data configurations and basic service functions.

Benefits

- The call emulation feature can be used to remotely verify and accept services and locate faults, which greatly reduces the operating expense (OPEX) for carriers.
- The call emulation feature shortens fault location time, which significantly improves the fault locating efficiency.

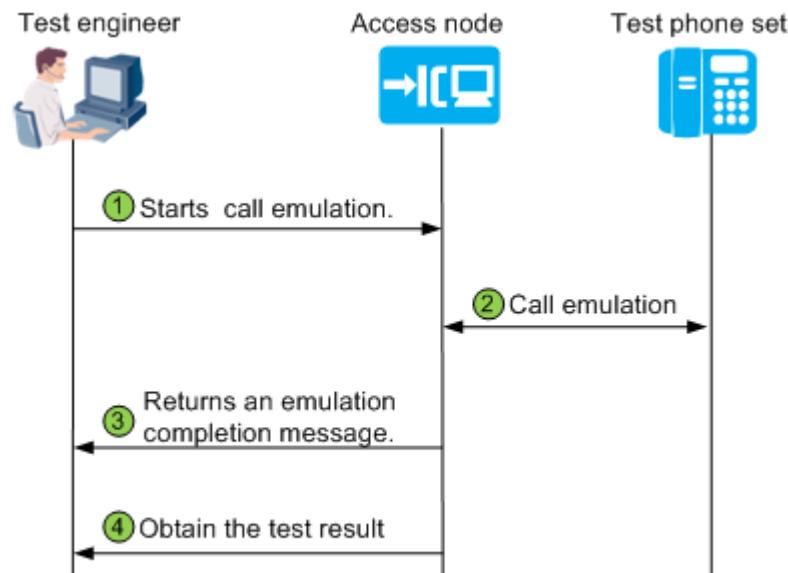
5.1.4.2 Principles of the Call Emulation Test

In a call emulation test, the system emulates the actions of a user port to achieve the emulation of the calling party and called party. The actions of a user port include off-hook, on-hook, number dialing, and ringing detection. [Figure 5-10](#) shows the principles of a call emulation test. The test phone set, placed at the central office (CO), is used to perform a call emulation test with a configured port on the access node. This test method remotely checks whether the voice service on the device is functional.

 **NOTE**

For a calling and called party emulation test, no phone set is required. Both the calling and called parties are emulated by the POTS ports on the access node.

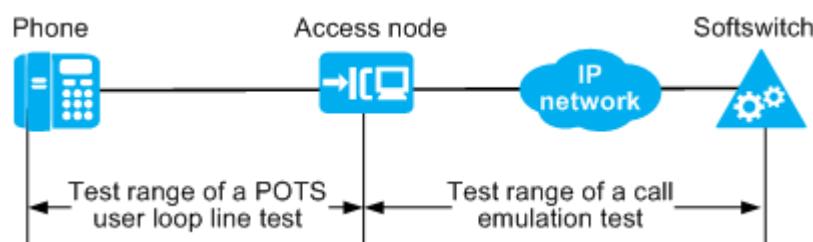
Figure 5-10 Principles of a call emulation test



Networking Application

[Figure 5-11](#) shows the example network of a call emulation test.

Figure 5-11 Example network of a call emulation test



A call emulation test checks whether the voice service is functional only on the network side of the device.

- If a conversation channel cannot be established during a call emulation test, check whether the network data configurations are correct.
- If the conversation channel is established but the voice is not clear during a call emulation test, check whether the cables are connected properly.

If test engineers need to check whether the voice service is functional on the user side, they can:

- Perform a POTS user loop line test to check whether the line between the device and the user phone set is functional. For details, see [POTS User Loop Line Test](#).
- Perform a POTS user circuit test to check whether the POTS board on the device is functional. For details, see [POTS User Circuit Test](#).

Calling Party Emulation Test

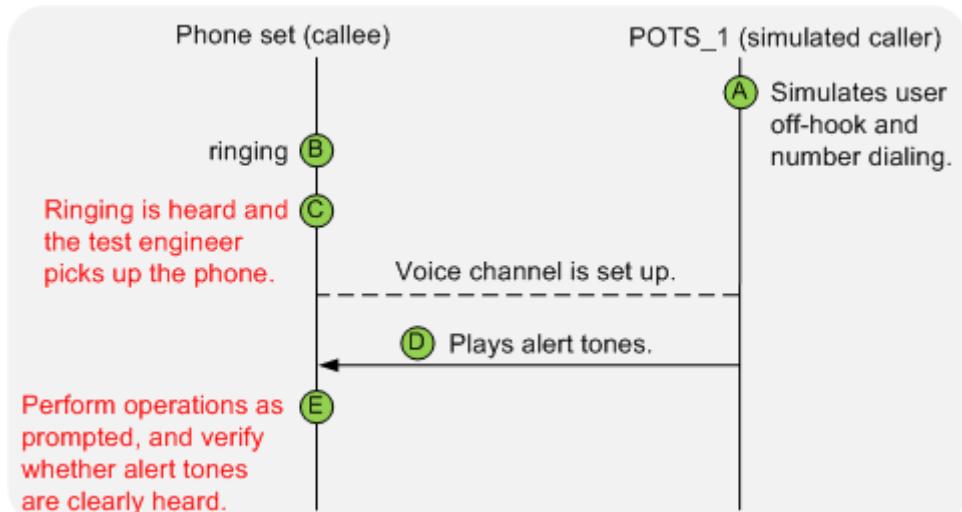
In a calling party emulation test, the device port emulates user off-hook, number dialing, communication, and on-hook.

1. Start a calling party emulation test.

On the access node, the test engineer sets the POTS_1 port as the calling party emulation port, configures the phone number to be dialed, and starts the calling party emulation test. If the function of playing alert tones upon the test beginning is enabled, alert tones are played after the test is started.

2. Initiate the calling party emulation test.

Figure 5-12 Interaction between the POTS_1 port and phone set during a calling party emulation test



NOTE

The information marked red in the following figure indicates the operations that need to be performed by the test engineer on the test phone set at the CO.

- a. The calling party emulation test is started on the access node and the calling party emulation port automatically emulates user off-hook. After detecting the dial tone, the port emulates number dialing.

- b. The called party (whose number is automatically dialed by the calling party emulation port) waits for the phone to ring. If the phone rings, the signaling channel is functional and the configured data is correct. If the phone does not ring, the test engineer needs to check service data (such as route, VLAN, and core-network data), troubleshoot the voice fault if any, and perform the test again.
- c. The called party picks up the phone. The call is set up.
- d. The calling party emulation port plays announcements for the called party.
- e. The test engineer checks whether the announcements are clearly heard. After hearing the announcements, the test engineer presses the specified verification number (a matched DTMF number, the asterisk key (*) by default), indicating that the media channel is functional. The test result is "Test Succeed."

 NOTE

If the function of playing alert tones based on the DTMF matching result is enabled, the system plays the alert tones after the test engineer presses the DTMF number. The alert tones include the DTMF number matching success alert tone and DTMF number matching failure alert tone.

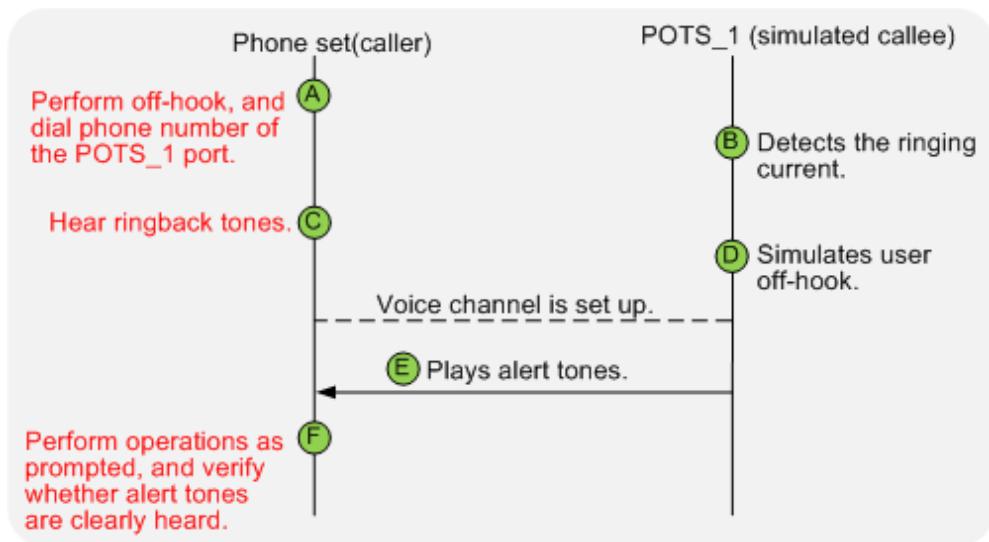
3. Obtain the test result. If the test fails, the system outputs the failure causes, with which the test engineer can identify the possible cause of the fault.

Table 5-7 lists the test results.

Called Party Emulation Test

In a called party emulation test, the POTS port on the access node emulates a called party. The called party emulation port automatically emulates user off-hook after detecting the ringing current.

1. Start a called party emulation test.
On the access node, the test engineer sets the POTS_1 port as the called party emulation port and starts the called party emulation test. If the function of playing alert tones upon the test beginning is enabled, alert tones are played after the test is started.
2. Initiate the called party emulation test.

Figure 5-13 Interaction between the POTS_1 port and phone set during a called party emulation test**NOTE**

The information marked red in the following figure indicates the operations that need to be performed by the test engineer on the test phone set at the CO.

- The test engineer picks up the phone, hears the dial tone, and dials the number of the POTS_1 port.
- If the called party emulation port of the device detects the ringing current, the configured user data is correct. If the called party emulation port does not detect the ringing current, the test engineer needs to check service data (such as route, VLAN, and core-network data), troubleshoot the voice fault if any, and perform the test again.
- If the calling party hears ringback tones before the called party picks up the phone (in this test, off-hook is automatically emulated by the called party emulation port), the signaling channel is functional. Otherwise, the test engineer needs to verify the configured service data and perform the test again.
- The called party emulation port emulates off-hook. The call is set up.
- The called party emulation port plays announcements for the calling party.
- The test engineer checks whether the announcements are clearly heard. After hearing the announcements, the test engineer presses the specified verification number (a matched DTMF number, the asterisk key (*) by default), indicating that the media channel is functional. The test result is "Test Succeed."

NOTE

If the function of playing alert tones based on the DTMF matching result is enabled, the system plays the alert tones after the test engineer presses the DTMF number. The alert tones include the DTMF number matching success alert tone and DTMF number matching failure alert tone.

3. Obtain the test result. If the test fails, the system outputs the failure causes, with which the test engineer can identify the possible cause of the fault.

Table 5-8 lists the test results.

Calling and Called Party Emulation Test

In a calling and called party emulation test, two POTS ports emulate the calling party and called party respectively. The calling party emulation port emulates the actions of the calling party, while the called party emulation port emulates the actions of the called party. These two ports automatically emulate calling party off-hook, number dialing, called party off-hook (after detecting the ringing current), mutual DTMF number sending for media channel verification, and on-hook after the verification.

NOTE

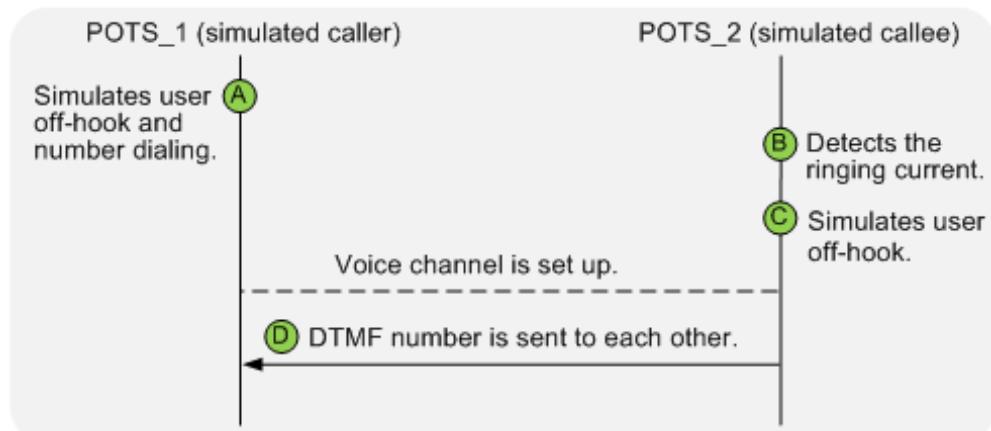
A calling and called party emulation test does not require any manual operation, which greatly improves the test efficiency. In this test, the device automatically verifies whether the media channel is functional. However, the device's sensitivity to media streams may vary from the human ears' sensitivity to media streams. Therefore, the call quality cannot be verified.

1. Start a calling and called party emulation test.

On the access node, the test engineer sets the POTS_1 port as the calling party emulation port and the POTS_2 port as the called party emulation port, configures the phone number to be dialed, and starts the calling and called party emulation test.

2. Initiate a calling and called party emulation test.

Figure 5-14 Interaction between the POTS_1 and POTS_2 ports during a calling and called party emulation test



- a. The calling and called party emulation test is started on the access node and the POTS_1 port automatically emulates user off-hook. After detecting the dial tone, the port emulates number dialing.
- b. The POTS_2 port (whose number is automatically dialed by the POTS_1 port) waits and checks whether the ringing current can be detected. If the POTS_2 port detects the ringing current, the signaling channel is

- functional and the configured user data is correct. If the POTS_2 port does not detect the ringing current, the test engineer needs to check service data (such as route, VLAN, and core-network data), troubleshoot the voice fault if any, and perform the test again.
- c. POTS_2 simulates a user to pick up the phone and sets up a communication channel with POTS_1.
 - d. The POTS_1 and POTS_2 ports send the DTMF number to each other to verify whether the media channel is functional. If the DTMF numbers sent by POTS_1 and POTS_2 ports are correct, the media channel is functional. The test result is "Test Succeed."
3. Obtain the test result. If the test fails, the system outputs the failure causes, with which the test engineer can identify the possible cause of the fault.

Table 5-7 and **Table 5-8** list the test results.

Test Results

Table 5-7 Results of a calling party emulation test

Test Result	Description
Test Succeed	The test is successful. The media channel of the test port is functional.
Test Failed: No dialing tone is played when the calling party dials a number	The calling party emulation port does not detect the dial tone. Possible causes are as follows: <ul style="list-style-type: none">• The calling party emulation port does not detect the off-hook signal.• The off-hook signal is not reported.• No dial tone is issued after the off-hook signal is reported.
Test Failed: Busy tone is played after the calling party picks up the phone off the hook	The calling party emulation port detects the busy tone. Possible causes: The calling party emulation port does not subscribe to the POTS services or the digital signal processor (DSP) is faulty.
Test Failed: Busy tone is played when the calling party dials a number	The calling party emulation port detects the busy tone during number dialing. Possible cause: The number that the calling party emulation port dials does not match the digitmap.
Test Failed: The calling party does not dial a number	The calling party emulation port does not automatically emulate number dialing after detecting the dial tone. Possible cause: The internal processing mechanism of the system encounters an error.

Test Result	Description
Test Failed: Busy tone is played after the calling party dials a number	The calling party emulation port detects the busy tone after number dialing. Possible causes: The dialed number is busy or the dialed number is incorrect.
Test Failed: The calling party does not communicate with the called party after dialing a number	The call is not set up. Possible cause: The called party does not pick up the phone.
Test Failed: Release before pick-up of the calling party	The call is released before the calling party and called party enter a conversation. Possible cause: The signaling processing mechanism encounters an error.
Test Failed: The number matching of the calling party is not complete	The calling party emulation port fails to match the DTMF number sent by the called party after entering the conversation. Possible causes: The called party does not press the DTMF number or the DTMF number is lost during the transmission.
Test Failed: The number sending of the calling party is not complete	The called party does not complete the sending of the DTMF number to the calling party emulation port after entering the conversation. Possible cause: The called party hangs up the phone before the sending of the DTMF number is completed.
Test Failed: The number matching of the calling party fails	The DTMF number sent from the called party is incorrect.
Test Failed: The calling port is abnormal	The calling party emulation port is faulty. Possible causes are as follows: <ul style="list-style-type: none">● The board is faulty.● The board is removed.● The calling party emulation port is faulty.

Table 5-8 Results of a called party emulation test

Test Result	Description
Test Failed: The phone of the called party does not ring	The called party emulation port does not receive any call. Possible causes: The calling party dials the wrong number or the signaling transmission encounters an error.
Test Failed: The called party does not pick up the phone off the hook	The called party emulation port does not automatically emulate off-hook after detecting the ringing current. Possible cause: The internal processing mechanism of the system encounters an error.
Test Failed: Busy tone is played after the called party picks up the phone off the hook	The called party emulation port detects the busy tone after off-hook. Possible cause: The calling party hangs up the phone.
Test Failed: The called party does not communicate with the calling party	The called party emulation port cannot enter the conversation after off-hook. Possible cause: The called party emulation port emulates off-hook so slowly that the calling party has hung up the phone.
Test Failed: Release before pick-up of the called party	The call is released before the calling party and called party enter a conversation. Possible cause: The signaling processing mechanism encounters an error.
Test Failed: The number matching of the called party is not complete	The called party emulation port fails to match the DTMF number sent by the calling party after entering the conversation. Possible causes: The calling party does not press the DTMF number or the DTMF number is lost during the transmission.
Test Failed: The number sending of the called party is not complete	The calling party does not complete the sending of the DTMF number to the called party emulation port after entering the conversation. Possible cause: The calling party hangs up the phone before the sending of DTMF number is completed.
Test Failed: The number matching of the called party fails	The DTMF number sent from the calling party is incorrect.

Test Result	Description
Test Failed: The called port is abnormal	The called party emulation port is faulty. Possible causes are as follows: <ul style="list-style-type: none">• The board is faulty.• The board is removed.• The called party emulation port is faulty.

5.1.4.3 Configuring the Call Emulation Test

Prerequisites

- The voice service must be configured.
- A normal phone must be provided.

Procedure

Step 1 Run the **simulate call parameter** command to configure the parameters for the call emulation test.

The type of the call emulation alert tone and DTMF number must be set before the automatic call emulation test is performed on the port.

By default, the type of the call emulation alert tone is voice announcement.

Step 2 Run the **display simulation call parameter** command to query the parameters configured for the current call emulation test.

Step 3 Start a call emulation test. You can start a calling party emulation test, a called party emulation test, or a calling and called party emulation test based on actual requirements.

- To start a calling party emulation test, run the **simulate call start caller** command.
- To start a called party emulation test, run the **simulate call start callee** command.
- To start a calling and called party emulation test, run the **simulate call start call** command.

----End

Result

After completing the call emulation test, the device directly outputs the test result. The test result is used to check whether the call is normal.

5.2 Common Methods of Locating Voice Service Faults

This chapter describes common tools and methods for locating voice service faults.

5.2.1 POTS User Circuit Test

A POTS user circuit test is used to check whether the chip of a POTS board functions normally. If the POTS services are faulty and the loop line works normally, POTS user circuit tests can be used to test the functions (such as the ringing and power feeding) and some parameters (such as the feeding voltage and ringing voltage) of the board circuit to check whether the circuit works normally.

Feature Dependency and Limitation

- The to-be-tested POTS port must not be faulty.
- Only one circuit test can be started on a POTS board at a time.

Test Procedure

1. Maintenance engineers start a circuit test by using the NMS or running the **pots circuit-test** command.

If users are making calls during a circuit test, maintenance engineers can cancel, forcibly perform, or delay the test based on actual conditions. If maintenance engineers forcibly perform the test, services on the port are interrupted and users' telephone services are affected. Therefore, exercise caution when performing this operation.



If maintenance engineers forcibly perform the test, services on the port are interrupted and users' telephone services are affected. Therefore, exercise caution when performing this operation.

2. Maintenance engineers check whether the circuit is faulty based on the test results. The results of a circuit test include: Normal, Abnormal, and Not supported. **Table 5-9** lists the specific test items and exception description of a circuit test.

Table 5-9 Test items and exception description of a circuit test

Test Item	Exception Description
Digital voltage	Indicates the digital voltage. Users cannot make calls if this item is abnormal.
Low power supply voltage (negative)	Indicates the low-voltage power supply (negative) to the POTS chip. The power consumption of the board increases if this item is abnormal.
High power supply voltage (negative)	Indicates the high-voltage power supply (negative) to the POTS chip. Users cannot make calls or the ringing tone is irregular if this item is abnormal.

Test Item	Exception Description
Positive power supply voltage	Indicates the high-voltage power supply (positive) to the POTS chip. The ringing tone is irregular if this item is abnormal.
A->B feeder voltage	
A->ground feeder voltage	
B->ground feeder voltage	
A->B antipole voltage	
Loop current	Indicates the output current of the POTS chip. The call quality may be impaired if the output current is lower than 18 mA.
Vertical current between A and B	Indicates the output voltage of the POTS chip. The call quality may be impaired if this item is abnormal.
Ringing current voltage	Indicates the output ringing voltage of the POTS chip. The ringing tone is excessively low if this item is abnormal.
Ringing current frequency	Indicates the output ringing frequency of the POTS chip. The ringing tone is irregular if this item is abnormal.
SLIC temperature	Indicates the temperature of the SLIC. The SLIC will be locked and the call will be interrupted if the SLIC temperature is abnormal.
Stop ringing	Indicates the ringing stopping frequency of the POTS chip. Users can hear the ringing tone, but cannot communicate with the peer party after picking up the phone if this item is abnormal.
Off hook detective	Indicates the off-hook detection function of the POTS chip. Users cannot make calls if this item is abnormal.
On hook detective	Indicates the on-hook detection function of the POTS chip. Users cannot make calls if this item is abnormal.

5.2.2 POTS User Loop Line Test

A POTS user loop line test is used to test the electrical indicators of the line from the test device (an access node) to a phone. When users' POTS services are faulty, POTS user loop line tests can be performed to test the performance and electrical indicators of the loop line to diagnose whether the loop line is faulty.

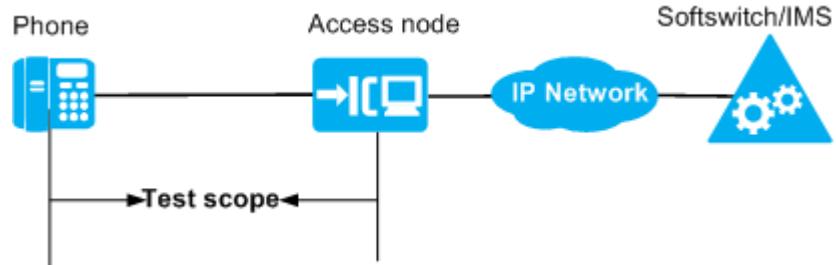
NOTE

The to-be-tested POTS port must not be faulty.

Networking Application

Figure 5-15 shows the example network of a POTS user loop line test. A POTS user loop line test is used to locate faults on the line from an access node to a phone.

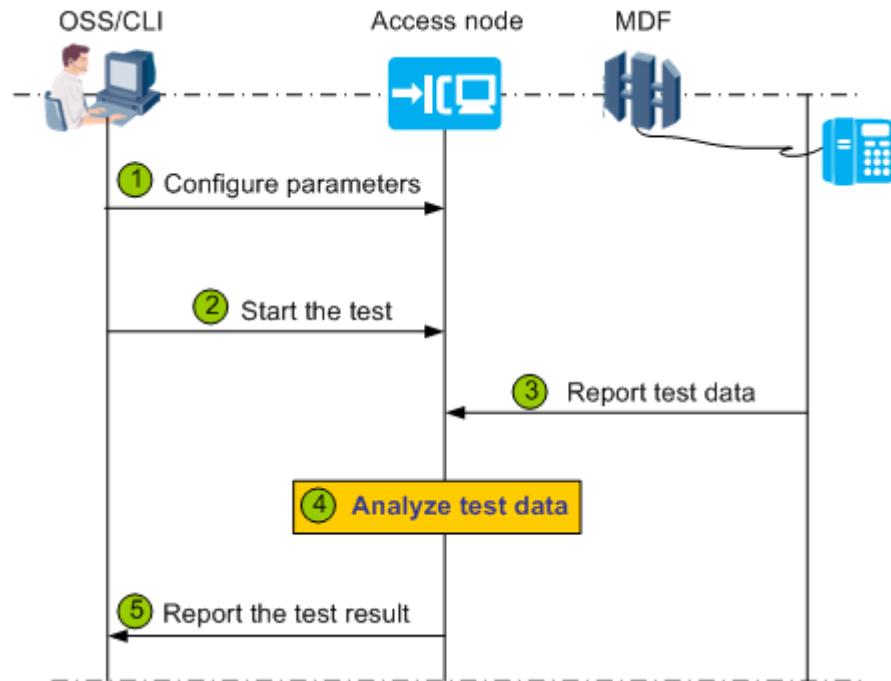
Figure 5-15 Example network of a POTS user loop line test



Test Procedure

Figure 5-16 shows the test procedure of a POTS user loop line test.

Figure 5-16 Test procedure of a POTS user loop line test



1. (Optional) Maintenance engineers set the parameters for the access node on the NMS or remotely log in to the access node from a management PC to set the parameters.

 **NOTE**

Generally, the default parameter values are used, and maintenance engineers do not need to set them.

- In test mode, run the **pots test-para** command to set the physical layer parameters.

During a loop line test, to avoid affecting the services and functions of the live network, it is necessary to set the physical layer parameters to control the electrical indicators, such as the maximum and minimum voltages supported by the test.

- In test mode, run the **pots loop-line-threshold** command to set thresholds of the test.

The access node uses these thresholds as the criteria to check whether the line is faulty when analyzing the test data.

2. Maintenance engineers start a loop line test by using the NMS or running the **pots loop-line-test** command.

If users (connected to the access node) are making calls during a loop line test, maintenance engineers can cancel, forcibly perform, or delay the test based on actual conditions.

 **NOTE**

If maintenance engineers forcibly perform the test, services on the port are interrupted and users' telephone services are affected. Therefore, exercise caution when performing this operation.

3. The access node collects the data of the test items. **Table 5-10** lists the loop line test items.

Table 5-10 Loop line test items

Test Item	Specific Test Item
Voltage	A->G DC voltage
	B->G DC voltage
	A->B DC voltage
	A->G AC voltage
	B->G AC voltage
	A->B AC voltage
	A->G AC frequency
	B->G AC frequency
	A->B AC frequency
Resistance	A->ground insulation resistance

Test Item	Specific Test Item
	B->ground insulation resistance
	A->B insulation resistance (low)
	B->A insulation resistance (low)
	A->B insulation resistance (high)
	B->A insulation resistance (high)
Capacitance	A->ground capacitance
	B->ground capacitance
	A->B capacitance (low)
	A->B capacitance (high)
Conductance	A->ground conductance
	B->ground conductance
	A->B conductance (low)
	A->B conductance (high)
Susceptance	A->ground susceptance
	B->ground susceptance
	A->B susceptance (low)
	A->B susceptance (high)
Current	A->ground DC current
	B->ground DC current
	A->B DC current
	B->A DC current
	A->ground AC current
	B->ground AC current
	A->B AC current
	B->A AC current

4. The access node analyzes the collected data according to the algorithm, and outputs the test conclusion.
5. The access node reports the test conclusion, and maintenance engineers diagnose whether the tested line is faulty based on the test conclusion.

Test Conclusion

Table 5-11 lists the loop line test conclusions.

Table 5-11 MG loop line test conclusions

Item	Conclusion
Line state	Normal
	A->ground AC voltage is hazardous to persons
	B->ground AC voltage is hazardous to persons
	AB->ground AC voltage is hazardous to persons
	AC voltage between A line and B line is hazardous to persons
	A->ground EMF AC voltage exists
	B->ground EMF AC voltage exists
	AB->ground EMF AC voltage exists
	A->ground abnormal AC voltage exists
	B->ground abnormal AC voltage exists
	AB->ground abnormal AC voltage exists
	A->ground DC voltage is hazardous to persons
	B->ground DC voltage is hazardous to persons
	AB->ground DC voltage is hazardous to persons
	DC voltage between A line and B line is hazardous to persons
	A->ground EMF DC voltage exists
	B->ground EMF DC voltage exists
	AB->ground EMF DC voltage exists
	A->ground abnormal DC voltage exists
	B->ground abnormal DC voltage exists
	AB->ground abnormal DC voltage exists
	A line grounding
	B line grounding
	AB line grounding
	A->ground resistance fault
	B->ground resistance fault

Item	Conclusion
	AB->ground resistance fault
	A->ground resistance leak
	B->ground resistance leak
	AB->ground resistance leak
	AB->ground poor insulation
	AB->ground capacitance leak
	A->ground capacitance leak
	B->ground capacitance leak
	Double line break or no terminal
	A break off
	B break off
	Cut off in MDF (that is, a line cut occurs between the main distribution frame and the device)
	Cut off out MDF (that is, a line cut occurs between the main distribution frame and the user side)
	Unknown
PPA test result NOTE A passive test termination (PPA) is similar to a test reference point. It is used to detect whether a fault occurs on the loop line between a point and the PPA so that maintenance engineers can locate faults section by section.	PPA not detected A->B PPA detected B->A PPA detected A->B 2 PPA detected B->A 2 PPA detected
Terminal status	Off hook ETSI Signature or Elec ring circuit A-B short R-C network (on hook or modem exist) Other terminal

Item	Conclusion
	Self mixed in MDF (shorted wires within the same twisted pair, occurring between the main distribution frame and the device) Self mixed out MDF (shorted wires within the same twisted pair, occurring between the main distribution frame and the user side)

References

Reference standard and protocol: ITU-T G.996.2 Single-ended line testing for digital subscriber lines (DSL)

5.2.3 POTS Port Loop Test

A POTS port loop test is used to test the hardware and configurations related to POTS services during device installation or before POTS service provisioning. It helps reduce the number of site visits and minimize maintenance costs.

Overview

Maintenance engineers can locally start a POTS port loop test on the device, or remotely log in to the device and then start the test. A POTS port loop test consists of two parts:

- Device hardware test: This test targets at access nodes that are not yet provisioned with the voice service. When an access node is newly deployed, the hardware of the voice module needs to be tested to evaluate the hardware capabilities in supporting future voice services.
- Device service test: This test targets at access nodes that are already provisioned with the voice service. Before voice services are provisioned from the access node to a user, a device service test is performed to determine whether the voice service capabilities are supported by the access node.

NOTE

- Do not pick up the phone during a loop test. Otherwise, the test results will be incorrect.
- If the dialup mode of a POTS port is set to **DTMF-only**, no loop test can be started.

Device Hardware Test

The device hardware test involves the following items:

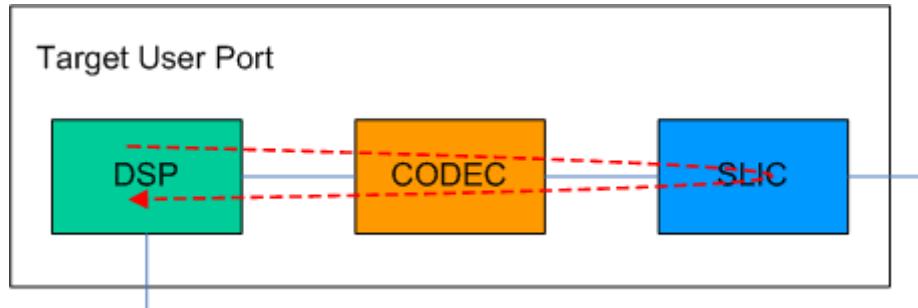
- Off-hook detection
- On-hook detection
- Ringing and ringing stopping detection on a service port
- Speech path detection

For the first 3 test items, a POTS board emulates off-hook, on-hook, ringing, and ringing stopping, while the control board of the device performs the loop test on the POTS board. The last test item (speech path detection) is used to verify the

service processing capability of the chip through service loopbacks. A speech path detection involves 3 loopback tests: SLIC loopback test, CODEC loopback test, and DSP loopback test.

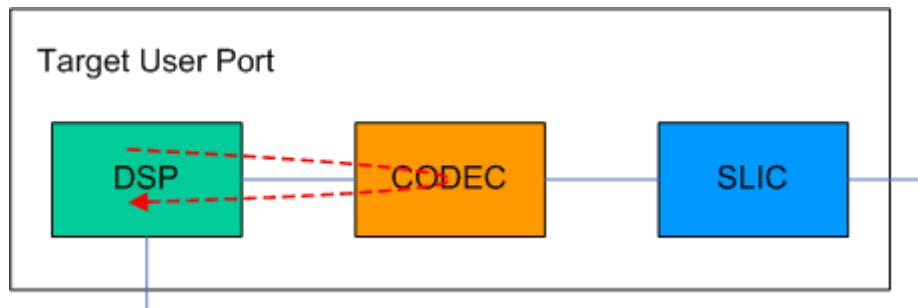
- In a SLIC loopback test, a POTS port is connected to a DSP channel, and the DSP chip generates the DTMF authentication code, which is sent to the TDM side. The DSP chip then detects the DTMF returned from the TDM side to check whether the channel between the DSP, CODEC, and SLIC is normal, as shown in [Figure 5-17](#).

Figure 5-17 Working principles of a SLIC loopback test

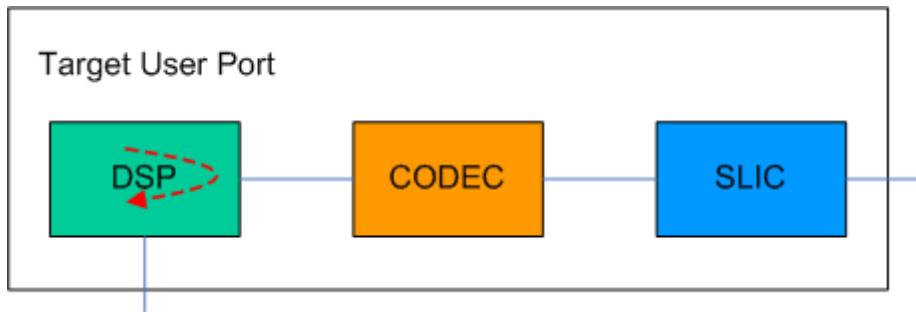


- In a CODEC loopback test, the CODEC loopback is set to the network side (remote loopback), and the DSP chip generates the DTMF authentication code, which is sent to the TDM side. The DSP chip then detects the DTMF returned from the TDM side to check whether the channel between the DSP and the CODEC is normal, as shown in [Figure 5-18](#).

Figure 5-18 Working principles of a CODEC loopback test



- In a DSP loopback test on the TDM side, a DSP channel is looped back from the TDM side to the IP side, and the DSP chip generates the DTMF authentication code, which is sent to the TDM side. The DSP chip then detects the DTMF returned from the TDM side to verify the transmit and receive functions of the TDM side, as shown in [Figure 5-19](#).

Figure 5-19 Working principles of a DSP loopback test on the TDM side**NOTE**

In test mode, run the **pots path-test frameid/slotid port portid type hardware** command to start a device hardware test. The test results will be displayed after the test is completed. Engineers diagnose whether the system functions normally based on the test results.

Device Service Test

The principles of a device service test are similar to those of a call emulation test. In a device service test, the device acts as both the calling party and called party (that is, the dest port on the device calls another assistant port on the same device), and the system checks whether the configurations are correct. User ports do not enter the conversation state during a POTS port loop test. When the called port detects the ringing, the calling port emulates user on-hook, and therefore, no charge record is generated. A device service test checks:

- Device interface data, including the signaling data (such as MG interface data, protocol parameters, and call server parameters)
- User port data, including the media gateway (MG) IDs and terminal IDs (TIDs) of H.248 users and user accounts and service rights of SIP users

NOTE

In test mode, run the **pots path-test frameid/slotid port portid type business** command to start a device service test. The test results will be displayed after the test is completed. Engineers diagnose whether the system functions normally based on the test results.

5.2.4 Search Tone Test

In a search tone test, the test module sends voice signals with the specific frequency and amplitude to a line, and then maintenance engineers use a receiver or a dedicated device to detect the signals on the line. A search tone test is a simple line fault locating function intended for maintenance engineers. In addition, search tone tests can help maintenance engineers pinpoint the specific line among multiple user lines.

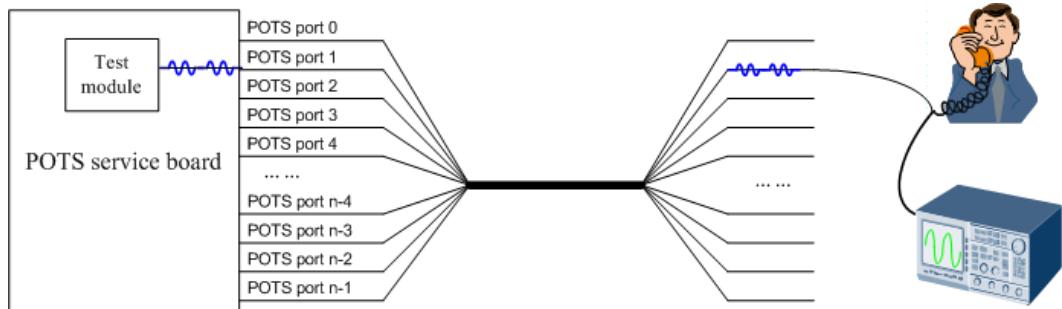
NOTE

- A search tone test can be performed even when a port is powered off.
- A search tone test cannot be performed when another test task (such as a POTS user circuit test, POTS user loop line test, call emulation test, signal tone test, or POTS port loop test) is in progress.
- A search tone test cannot be performed when a port is in the prohibit state.

Test Procedure

Figure 5-20 shows the principles of a search tone test.

Figure 5-20 Principles of a search tone test



1. The test module sends voice signals with the specific frequency and amplitude (as underlined by blue wave lines in **Figure 5-20**) to a line after a search tone test is started.

In test mode, run the **pots search-tone-test frameid/slotid/portid test-flag enable** command to start a search tone test. If users are making calls during a search tone test, maintenance engineers can cancel or forcibly perform the test based on actual conditions.

NOTE

If maintenance engineers forcibly perform the test, services on the port are interrupted and users' telephone services are affected. Therefore, exercise caution when performing this operation.

2. Maintenance engineers use a receiver or a dedicated device connected to the other end of the line to detect whether the voice signals can be received. If the voice signals can be received, the line works normally.
3. (Optional) Stop a search tone test.

Run the **pots search-tone-test frameid/slotid/portid test-flag disable** command to stop a search tone test.

NOTE

In a search tone test, the duration of playing the search tone needs to be set based on actual requirements.

- If the preset duration does not expire, maintenance engineers can run this command to manually stop the test.
- If the preset duration has expired, the system automatically stops the test.

5.2.5 Signal Tone Test

In a signal tone test, the system sends the signal tone signals to a specific port of a POTS board and makes the port loop back the signals, and then checks whether the loopback signals can be detected. This test function helps maintenance engineers check whether the system can normally process the detection of the user off-hook and signal tone and locate hardware faults related to the user off-hook and signal tone playing.

A signal tone test includes the following types, as listed in the following table.

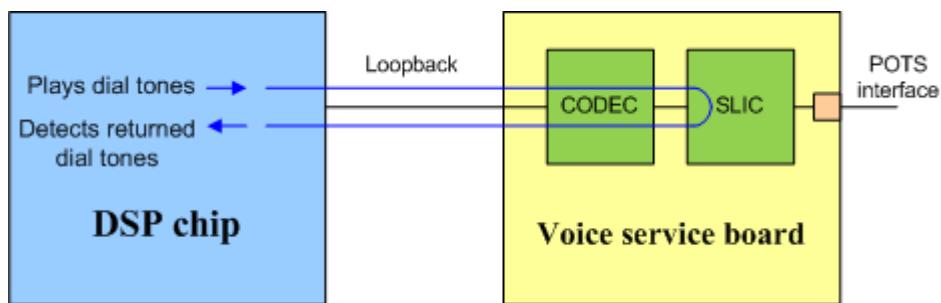
Test Type	Requiring Coordination of Upper-Layer Device?
Busy tone test	The coordination of the upper-layer device is not required.
Ringback tone test	
Dial tone test	The dial tone test and special dial tone test include the following modes. <ul style="list-style-type: none">● out-of-service: In this mode, the test is performed on the device, which is independent of the upper-layer device. If the device is not connected to the upper-layer device, use this mode.● in-service: In this mode, the device coordinates with the upper-layer device to perform the test. The upper-layer device controls the playing of the dial tone or special dial tone.
Special dial tone test (that is, the dial tone test started by the device based on different service requirements, such as call forwarding-unconditional)	

NOTE

- The POTS port supports local loopbacks.
- The POTS port must be in the on-hook state during a signal tone test.
- A signal tone test cannot be performed if the port is in the **prohibit** or **loopback** state.
- A signal tone test cannot be performed when another test task (such as a POTS user circuit test, POTS user loop line test, call emulation test, search tone test, or POTS port loop test) is in progress.

Test Procedure

[Figure 5-21](#) shows the test procedure of a signal tone test. As shown in [Figure 5-21](#), the subscriber line interface circuit (SLIC) supplies feeding current to the telephone, sends voice frequency, generates ringing, detects off-hook signals and on-hook signals, and processes analog signals. The CODEC performs the conversion between analog signals and digital signals.

Figure 5-21 Test procedure of a signal tone test

1. Maintenance engineers start a signal tone test on a POTS user port by using the CLI or NMS.
 - In test mode, run the **pots signal-tone-test frameid/slotid/portid signal-tone busy-tone** command to start a busy tone test.
 - In test mode, run the **pots signal-tone-test frameid/slotid/portid signal-tone ringback-tone** command to start a ringback tone test.
 - In test mode, run the **pots signal-tone-test frameid/slotid/portid signal-tone dial-tone** command to start a dial tone test.
 - In test mode, run the **pots signal-tone-test frameid/slotid/portid signal-tone special-dial-tone** command to start a special dial tone test.
2. The DSP chip plays the signal tone.
 - For the busy tone test or ringback tone test, the device requests the DSP chip to issue the busy tone or ringback tone to the POTS port after the test is started.
 - For the dial tone test or special dial tone test:
 - If the test is started in **out-of-service** mode, the POTS port emulates the user off-hook. After the device detects the off-hook signal, it requests the DSP chip to issue the dial tone or special dial tone to the POTS port.
 - If the test is started in **in-service** mode, the POTS port emulates the user off-hook. After the device detects the off-hook signal, it reports the signal to the softswitch/IMS, and the softswitch/IMS requests the DSP chip to issue the dial tone or special dial tone to the POTS port.
3. The POTS board loops back the signal tone signals (as shown by the blue lines in **Figure 5-21**).
4. If the DSP chip can detect the loopback signals, the system runs normally. If any exception occurs during the test, the following methods can be used for troubleshooting.

NOTE

You can start the test in **in-service** mode only after you have configured the users.

Exception	Troubleshooting Method
No looped back signal is detected.	<ul style="list-style-type: none">Run the display ptn state command to query the port status to check whether the port is faulty.Run the display ptn state command to query the port status to check whether the port is busy.Run the display dsp state command to query the DSP channel status to check whether the DSP resources are sufficient.
The delay of the signal tone is too long.	<ul style="list-style-type: none">Run the display cpu command to query the CPU usage to check whether the system is overloaded.If the test is started in in-service mode, check whether the interaction between the device and the softswitch/IMS is delayed.

5. (Optional) Stop a signal tone test.

Run the **pots signal-tone-test frameid/slotid/portid test-flag disable** command to stop a signal tone test.

 **NOTE**

In a signal tone test, the duration of playing the signal tone needs to be set based on actual requirements.

- If the preset duration does not expire, maintenance engineers can run this command to manually stop the test.
- If the preset duration has expired, the system automatically stops the test.

5.2.6 Line Matching Test

A line matching test is used to check wiring connectivity between the subscriber line and the main distribution frame (MDF), and check wiring sequence.

 **NOTE**

- A line matching test may cause service interruption. Therefore, exercise caution when starting this test.
- During a line matching test, do not perform any service operations on the board to be tested. If a service operation is needed for such a board, reset the board after the test completes so that services can be restored.

Value

Previously, a line matching test was implemented for a single line under the cooperation between 2 deployment or maintenance engineers using a multimeter.

This process is of low efficiency and high labor costs. Furthermore, subscriber lines are removed and inserted multiple times during the test, which harms the board and line connectors.

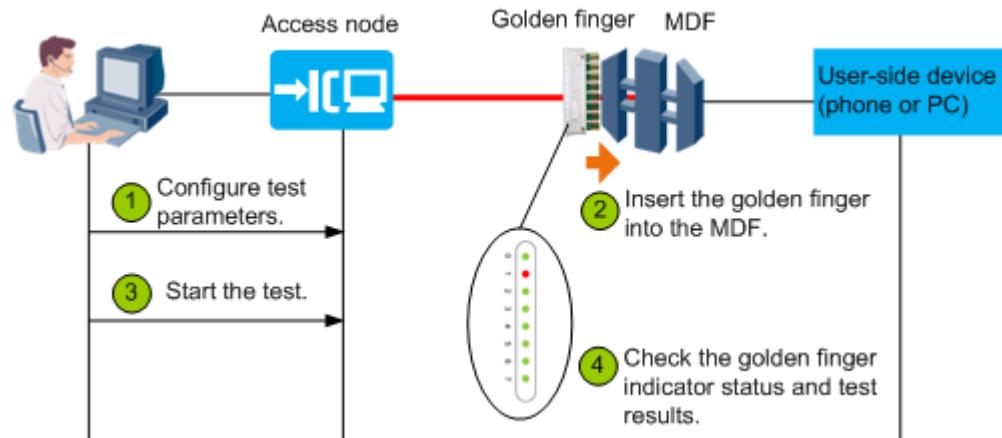
Now, a line matching test can be implemented by using the test tool CLT-Match and golden finger indicator board by only one engineer. Also, lines can be tested by groups. This process dramatically improves test efficiency and correctness. However, damages caused by subscriber line removal and insertion are unavoidable.

In an actual test, the software can substitute for the CLT-Match. Specifically, the software triggers a line matching test. Then, using together with the golden finger indicator board, subscriber lines do not need to be removed or inserted. This process improves test efficiency and protects the board and subscriber lines.

Procedure

As shown in [Figure 5-22](#), the red line indicates the route from the subscribe line to the MDF, which is tested in a line matching test for its wiring connectivity and sequence.

Figure 5-22 Procedure



1. The deployment or maintenance engineer logs in to the device and runs the **line-match-config** command to configure parameters for a line matching test. In the configuration, the number of line matching test cycles, the blinking rate of the line matching test indicator, and the line matching test mode can be specified.
2. The deployment or maintenance engineer inserts the golden finger indicator board into the equipment-side MDF module of the corresponding wiring module.
3. The deployment or maintenance engineer runs the **line-match-test** command to start a line matching test. Only one board can be tested at a time.
4. The deployment or maintenance engineer observes the indicator blinking status on the MDF side to determine whether wiring is correct.
 - If the indicator blinks green, the line connectivity is normal.
 - If the indicator blinks red, the line connectivity is abnormal and a manual check is required.

- If the one-by-one test mode is set and indicators blink in the sequence of ports, wiring sequence is correct.
- If the one-by-one test mode is set and indicators do not blink in the sequence of ports, wiring sequence is incorrect. This may be caused by shorted wires and a manual check is required.

5.3 Common Methods for Locating DSL Faults

This chapter provides common methods for locating digital subscriber line (DSL) faults.

5.3.1 Common DSL Faults

This section provides the methods for identifying and addressing common digital subscriber line (DSL) faults.

Table 5-12 lists common DSL faults as well as methods for identifying and resolving these faults.

Table 5-12 Common DSL faults

Fault	Fault Identification	Fault Resolution
The line is old or is not properly connected to the main distribution frame (MDF).	<ul style="list-style-type: none">• Check whether insulation has worn away and the line is exposed.• Check whether the line connector is rusted or the line is not properly connected to the MDF.• Check whether a cyclic redundancy check (CRC) packet loss occurs on the line.	Replace the line or reconnect it to the MDF.
The line is connected incorrectly to the associated devices.	<p>If a user has a splitter to split voice and data services, common line connection faults are:</p> <ul style="list-style-type: none">• The phone and the modem are not connected to the output ports on the splitter. Instead, they are connected directly to the drop-in twisted pair.• The phone or the modem is connected to the input port on the splitter.	<p>Reconnect the line as follows:</p> <ul style="list-style-type: none">• Connect the drop-in twisted pair to the input port on the splitter.• Connect the phone and the modem to the output ports on the splitter.

Fault	Fault Identification	Fault Resolution
Subscriber lines form a loop.	Check whether two asymmetric digital subscriber line (ADSL) lines are connected directly to each other.	Reconnect the subscriber lines to disconnect the loop.
An interference source exists around the subscriber lines.	Check whether a strong interference source, such as a wireless base station or a high-frequency switch power system, exists around the subscriber lines.	Remove the interference source or re-route the subscriber lines.

5.3.2 MELT Test

Metallic line testing (MELT) is an integrated digital multimeter (DMM) test solution provided by a DSLAM device. The MELT function is integrated in a board. It can test the physical characteristics of the copper line for each service port.

5.3.2.1 Introduction

Metallic line testing (MELT) detects faults on the copper twisted pair from a service board to an xDSL user terminal. These faults include grounded subscriber lines, shorted wires within the same twisted pair, wires touching a high-voltage power line. MELT tests facilitate fast fault locating and minimize customers' operating expense (OPEX).

- Test electrical parameters, such as the compound capacitance, pure capacitance, voltage, resistance, and current of xDSL lines.
- Detect the potential physical faults on xDSL lines.
- Identify the fault range (such as intra-office faults or inter-office faults) and maintenance owner,

The N2510 can be used for analyzing the test results and locating the fault.

Two applications are included.

- Testing the electrical parameters of the line (that is, electrical parameter test)
- Testing the voice signal receiving capability of the line (that is, search tone test)

Electrical Parameter Test

In a MELT test, the MELT test chip sends test signals to the target port to test related electrical parameters, and then the chip calculates the major physical parameters of the line. (The MELT test chip can be regarded as a multimeter that can test the voltage, resistance, and capacitance.)

 NOTE

During the MELT test, service running is not affected.

Search Tone Test

A search tone test helps users pinpoint the subscriber line connected to a specific port. The device plays the search tone on a specific port. Connect a phone (or a headset) to a line. Pick up the phone (or headset). If you can hear the search tone on the line through the phone (or headset), the line is connected to the specific port.

When the search tone test is started at the 600-ohm load, the search tone shall be applied symmetrically between wires A and B. The frequency of the search tone shall be 800 Hz. The voltage of the search tone at xDSL ports is within 120 mV and 330 mV.

 NOTE

During the search tone test, SHDSL services are affected.

5.3.2.2 Electrical Parameter Test

Procedure

- Step 1** (Optional) In test mode, run the **xdsl melt polarity** command to set the mode of a twisted pair.

During the metallic line testing (MELT), the device applies a voltage between wires A and B to perform the test. If there is a passive test termination (PPA) model integrated into the phone socket, the line is not reachable. After the mode of the twisted pair is set, the device can apply a reverse voltage between wires A and B. By default, the polarity of a twisted pair is set to normal, which means the polarity of wire A is negative and the polarity of wire B is positive.

- Step 2** Run the **xdsl melt frameid/slotid/portid** command in test mode to start the electrical parameter test.

 NOTE

During a MELT test, if the discharge function is enabled, residual voltage on the cable will be automatically discharged. The discharge function is disabled by default.

- Step 3** Wait until the electrical parameter test is completed and the test result is reported. Then, run the **display xdsl melt data frameid/slotid/portid** command to query the test result.

Currently, the system saves only the last MELT data.

- Step 4** Determine the line condition based on the test result.

----End

Result

The following is an example test result of an electrical parameter test.

```
huawei(config-test)#display xDSL melt data  
frameid/slotid/portid<s><Length 1-15> }:0/2/0
```

Command: display xdsl melt data 0/2/0		
Tested port: 0/2/0 Start time of the test: 2010-08-19 15:54:20+08:00 End time of the test: 2010-08-19 15:54:40+08:00 I--Invalid V--Valid		
<hr/>		
Test Item	Flag	Result
<hr/>		
Conclusion:		
Does PPA exist?	I no	
Does signature exist?	V no	
Does hazardous voltage (AC) exist?	V no	
Does hazardous voltage (DC) exist?	V no	
Line open	V yes	
Line short	V no	
Is the phone in the off-hook state?	V no	
Significant terminal device capacitance detected?	V no	
Main measurement results:		
a->ground AC voltage(V)	V 0.010	
b->ground AC voltage(V)	V 0.013	
a->b AC voltage(V)	V 0.012	
Frequency of a->ground foreign AC voltage(Hz)	I 0	
Frequency of b->ground foreign AC voltage(Hz)	I 0	
Frequency of a->b foreign AC voltage(Hz)	I 0	
a->ground DC voltage(V)	V -0.191	
b->ground DC voltage(V)	V -0.141	
a->b DC voltage(V)	V -0.051	
a->ground resistance(Ohm)	V 10000000	
b->ground resistance(Ohm)	V 10000000	
a->b resistance(Ohm)	V 10000000	
b->a resistance(Ohm)	V 10000000	
a->ground capacitance(nF)	V 0	
b->ground capacitance(nF)	V 0	
a->b capacitance(nF)	V 1	
Capacitance of signature or ringer(nF)	I 0	
Resistance of signature or ringer(Ohm)	I 0	
Vzener(V)	I -31.144	
Rzener(Ohm)	I 10000000	
Rbat_a(Ohm)	I 10000000	
Rbat_b(Ohm)	I 10000000	
Measurement results for reference:		
Aggregate a->ground conductance(uS)	V 0.0	
Aggregate a->ground susceptance(uS)	V 0.0	
Aggregate b->ground conductance(uS)	V 0.0	
Aggregate b->ground susceptance(uS)	V 0.0	
Aggregate a->b conductance(uS)	V 0.0	
Aggregate a->b susceptance(uS)	V 0.0	
AC foreign current on a wire(uA)	V 0	
AC foreign current on b wire(uA)	V 1	
DC foreign current on a wire(uA)	V -8	
DC foreign current on b wire(uA)	V -6	
Aggregate a->b capacitance under low voltage ramps(nF)	V 28	
Aggregate a->b capacitance under high voltage ramps(nF)	V 31	
Aggregate a->b capacitance under low AC signal(nF)	V 27	
Resistance in series with a->ground capacitance(Ohm)	V 5010911	
Resistance in series with b->ground capacitance(Ohm)	V 0	
Resistance in series with a->b capacitance(Ohm)	V 0	
Applied measurement parameters:		
AC measurement frequency(Hz)	275	
a->ground highest measurement DC voltage(V)	V -3.622	
a->ground lowest measurement DC voltage(V)	V -53.032	
b->ground highest measurement DC voltage(V)	V -3.680	
b->ground lowest measurement DC voltage(V)	V -53.718	
a->b measurement DC voltage(V)	V 46.790	
b->a measurement DC voltage(V)	V -46.626	
Current mapping the a-wire highest voltage for test(uA)	V -49	

Current mapping the a-wire lowest voltage for test(uA)	V	-83
Current mapping the b-wire highest voltage for test(uA)	V	80
Current mapping the b-wire lowest voltage for test(uA)	V	116
Current mapping the a->b voltage for test(uA)	I	32
Current mapping the b->a voltage for test(uA)	I	0
Amplitude of AC voltage for a->ground test(V)	V	7
Amplitude of AC voltage for b->ground test(V)	V	7
Amplitude of AC voltage for a->b test(V)		

System Response

Parameter	Description
Tested port	Indicates the ID of the test port.

Parameter	Description
Test Item	<p>Indicate the test item. Currently, the test items include the following:</p> <ul style="list-style-type: none">• Does PPA exist?: indicates whether the PPA circuit exists.• Does signature exist?: indicates whether the signature circuit can be detected.• Does hazardous voltage (AC) exist?: indicates whether the AC voltage exceeds the threshold .• Does hazardous voltage (DC) exist?: indicates whether the DC voltage exceeds the threshold.• Line open: indicates that the circuit line is in the open circuit state.• Line short: indicates that the line is short-circuited.• Is the phone in the off-hook state?: indicates whether the phone is in the off-hook state.• Significant terminal device capacitance detected?: indicates whether the significant terminal device capacitance is detected.• a->ground AC voltage(V): indicates the wire A-to-ground (A-G) AC voltage (V).• b->ground AC voltage(V): indicates the wire B-to-ground (B-G) AC voltage (V).• a->b AC voltage(V): indicates the AC voltage (V) between wires A and B.• Frequency of a->ground foreign AC voltage(Hz): indicates the frequency (Hz) of the external AC voltage coupled to wire A and ground.• Frequency of b->ground foreign AC voltage(Hz): indicates the frequency (Hz) of the external AC voltage coupled to wire B and ground.• Frequency of a->b foreign AC voltage(Hz): indicates the frequency (Hz) of the external AC voltage coupled to wires A and B.• a->ground DC voltage(V): indicates the A-G DC voltage (V).• b->ground DC voltage(V): indicates the B-G DC voltage (V).• a->b DC voltage(V): indicates the DC voltage (V) between wires A and B.• a->ground resistance(Ohm): indicates the A-G resistance (Ohm).• b->ground resistance(Ohm): indicates the B-G resistance (Ohm).• a->b resistance(Ohm): indicates the wire A-to-wire B (A-B) resistance (Ohm)• b->a resistance(Ohm): indicates the wire B-to-wire A (B-A) resistance (Ohm)

Parameter	Description
	<ul style="list-style-type: none">• a->ground capacitance(nF): indicates the A-G capacitance (nF).• b->ground capacitance(nF): indicates the B-G capacitance (nF).• a->b capacitance(nF): indicates the capacitance (nF) between wires A and B.• Capacitance of signature or ringer(nF): indicates the capacitance (nF) in a signature or ringer circuit.• Resistance of signature or ringer(Ohm): indicates the resistance (ohm) in a signature or ringer circuit.• Vzener(V): indicates the Zener diode breakdown threshold (V) in the case of an off-hook phone.• Rzener(Ohm): indicates the DC resistance (ohm) between wires A and B in the case of an off-hook phone.• Rbat_a(Ohm): indicates the equivalent coupling resistance (ohm) of wire A in the case of external voltage.• Rbat_b(Ohm): indicates the equivalent coupling resistance (ohm) of wire B in the case of external voltage.• Aggregate a->ground conductance(uS): indicates the A-G conductance (μS).• Aggregate a->ground susceptance(uS): indicates the A-G susceptance (μS).• Aggregate b->ground conductance(uS): indicates the B-G conductance (μS).• Aggregate b->ground susceptance(uS): indicates the B-G susceptance (μS).• Aggregate a->b conductance(uS): indicates the conductance (μS) between wires A and B.• Aggregate a->b susceptance(uS): indicates the susceptance (μS) between wires A and B.• AC foreign current on a wire(uA): indicates the A-G AC current (μA).• AC foreign current on b wire(uA): indicates the B-G AC current (μA).• DC foreign current on a wire(uA): indicates the A-G DC current (μA).• DC foreign current on b wire(uA): indicates the B-G DC current (μA).• Aggregate a->b capacitance under low voltage ramps(nF): indicates the aggregate capacitance between wire A and wire B under the low voltage test (nF).• Aggregate a->b capacitance under high voltage ramps(nF): indicates the aggregate capacitance between wire A and wire B under the high voltage test (nF).

Parameter	Description
	<ul style="list-style-type: none">Aggregate a->b capacitance under low AC signal(nF): indicates the capacitance between wire A and wire B under the low AC voltage signal test (nF).Resistance in series with a->ground capacitance (Ohm): indicates the resistance in series with the A-G capacitance (ohm).Resistance in series with b->ground capacitance(Ohm): indicates the resistance in series with the A-B capacitance (ohm).Resistance in series with a->b capacitance(Ohm): indicates the resistance in series with the A-B capacitance (ohm)AC measurement frequency(Hz): indicates the signal frequency (Hz) used in the complex impedance test.a->ground highest measurement DC voltage(V): indicates the A-G upper measurement DC voltage (V).a->ground lowest measurement DC voltage(V): indicates the A-G lower measurement DC voltage (V).b->ground highest measurement DC voltage(V): indicates the B-G upper measurement DC voltage (V).b->ground lowest measurement DC voltage(V): indicates the B-G lower measurement DC voltage (V).a->b measurement DC voltage(V): indicates the (A-B) measurement DC voltage (V).b->a measurement DC voltage(V): indicates the (B-A) measurement DC voltage (V).Current mapping the a-wire highest voltage for test(uA): indicates the current (μA) generated to the A-G upper measurement DC voltage.Current mapping the a-wire lowest voltage for test(uA): indicates the current (μA) generated to the A-G lower measurement DC voltage.Current mapping the b-wire highest voltage for test(uA): indicates the current (μA) generated to the B-G upper measurement DC voltage.Current mapping the b-wire lowest voltage for test(uA): indicates the current (μA) generated to the B-G lower measurement DC voltage.Current mapping the a->b voltage for test(uA): indicates the current (μA) generated to the A-B measurement DC voltage.Current mapping the b->a voltage for test(uA): indicates the current (μA) generated to the B-A measurement DC voltage.Amplitude of AC voltage for a->ground test(V): indicates the amplitude of AC voltage (V) generated for the A-G measurement.

Parameter	Description
	<ul style="list-style-type: none">Amplitude of AC voltage for b->ground test(V): indicates the amplitude of AC voltage (V) generated for the B-G measurement.Amplitude of AC voltage for a->b test(V): indicates the amplitude of AC voltage (V) generated for the A-B measurement.
Flag	Indicates the valid flag. It can be set to I (invalid) or V (valid).
Result	Indicates the test result of the corresponding test item.

5.3.2.3 Search Tone Test

Procedure

- Step 1** Run the **xdsl melt searching-tone** command in test mode to start the search tone test.
- Step 2** Check whether the search tone is normal at the other end of the line using a headset or a receiver.

----End

Result

The system does not display any message after the command is executed successfully. You can use a headset or receiver to check whether the search tone is normal based on the configured search tone parameters.

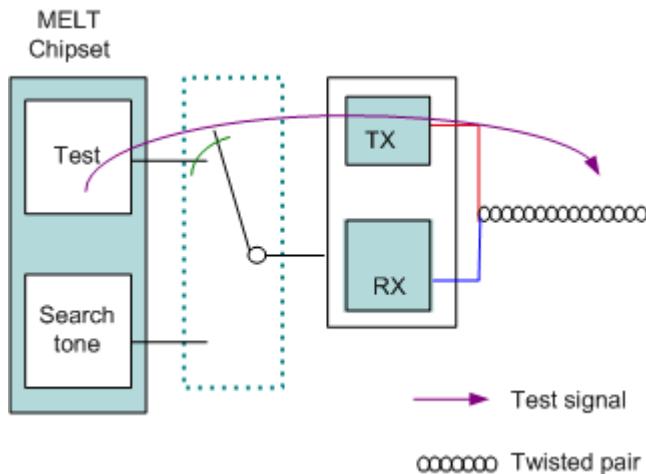
5.3.2.4 Reference Standards and Protocols

The following lists the reference standard of this feature:

- RFC1155, RFC1157, and RFC1213 SNMP V1 series standards
- RFC1905, RFC1906, RFC1907, and RFC1908 SNMP V2 series standards
- RFC2571, RFC2572, RFC2573, RFC2574, RFC2576, RFC2578, and RFC2579 SNMP V3 series standards
- RFC959 FTP standard
- ITU-T Recommendation G.996.2

5.3.2.5 Principles

Figure 5-23 shows the principles of the metallic loop test (MELT). MELT tests involve two aspects of tests: testing the electrical parameters of a line and testing the voice signal receive capabilities of a line. The electrical parameter tests cannot be performed at the same time as the search tone tests.

Figure 5-23 MELT test principle

Electrical Parameter Test

In the electrical parameter test, the MELT test chip sends test signals to the target port for testing related electrical parameters. The chip then calculates the major physical parameters of the line. In some usage scenarios, the MELT test chip can be regarded as a multimeter that can test the voltage, resistance, and capacitance.

Table 5-13 lists the MELT test items.

Table 5-13 MELT test items

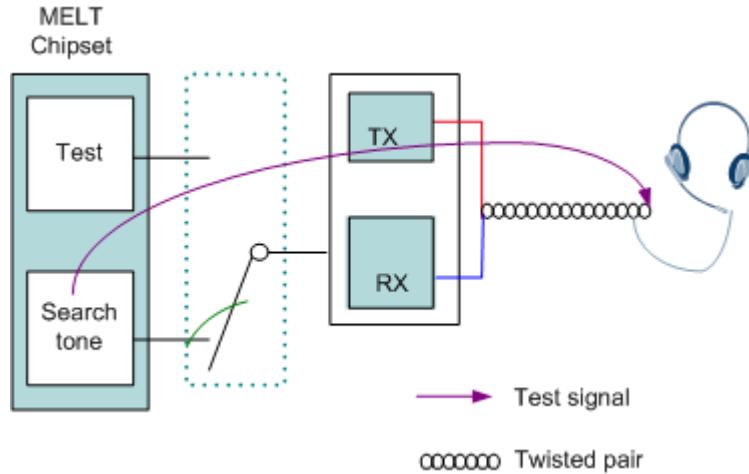
Test Item	Description
AC voltage	AC voltage of line A to the ground, AC voltage of line B to the ground, and AC voltage between line A and line B
DC voltage	DC voltage of line A to the ground, DC voltage of line B to the ground, and DC voltage between line A and line B
Full resistance	Resistance of line A to the ground, resistance of line B to the ground, and resistance between line A and line B
Full capacitance	Capacitance of line A to the ground, capacitance of line B to the ground, and capacitance between line A and line B

Search Tone Test

Figure 5-24 shows the principles of a search tone test. In a search tone test, the test device sends 120 mV voices signals at a frequency of 800 Hz to an x digital subscriber line (xDSL). Users can use an earphone or a receiver to receive the

signals at the other side of the line to determine whether the voice signals are normal.

Figure 5-24 Search tone test principles



5.3.3 Loopback on a VDSL2 Port

This section describes how to perform a loopback on a very-high-speed digital subscriber line 2 (VDSL2) port to locate a VDSL2 service fault. A loopback on a VDSL2 port can be performed to determine whether the service board housing the VDSL2 port is communicating with the backplane properly.

Prerequisites

- The VDSL2 port is deactivated.
- The VDSL2 service ran properly before the fault occurred. (This confirms that a downstream service flow exists between the control board and the VDSL2 service board).

Impact on the System

- When a VDSL2 port is executing loopback operations, the port cannot forward packets properly, and all services carried on the port are interrupted.
- When a VDSL2 port is executing loopback operations, if ports are not isolated at Layer 2, services of other ports may be affected. By default, ports are isolated at Layer 2 except that Layer 2 user bridging is configured. For details about how to enable or disable Layer 2 user bridging, see "Layer 2 User Bridging" in *Feature Guide*.

You must, therefore, set a loopback duration before starting the loopback, or run the **undo loopback** command to cancel the loopback immediately after it is complete.

Procedure

Step 1 Run the **loopback** command in VDSL mode to start a loopback on a VDSL2 port.

NOTE

Port loopback is classified as local loopback and remote loopback. For details about local loopback and remote loopback, see section *Reference* in the following section. VDSL2 ports support only local loopback.

For example, run the following command to start a local loopback on port 0/1/0:

```
huawei(config-if-vdsl-0/1)#loopback 0 local
```

Step 2 If the VDSL board is working in asynchronous transfer mode (ATM), run the **atm-ping** command in VDSL mode to check the connectivity of the loopback channel. If the VDSL board is working in packet transfer mode (PTM), use an external testing device, such as the SmartBits, to check the connectivity of the loopback channel by sending packets to the service board.

If, for example, the virtual path identifier (VPI) and virtual channel identifier (VCI) of the tested service flow on port 0/1/0 is 0/35, and the port is working in ATM mode, run the following command to check the connectivity of the loopback channel set up in Step 1:

```
huawei(config-if-vdsl-0/1)#atm-ping 0 0 35
```

NOTE

- If the ping operation is successful and no packets are lost, the loopback channel is connected.
- If the ping operation fails, the channel is broken.
- If the ping operation is successful but some packets are lost, the channel is faulty.

Step 3 Run the **undo loopback** command to cancel the loopback after the loopback operation is complete.

For example, run the following command to cancel a local loopback on port 0/1/0:

```
huawei(config-if-vdsl-0/1)#undo loopback 0
```

NOTE

A port on which a loopback is being performed cannot be activated.

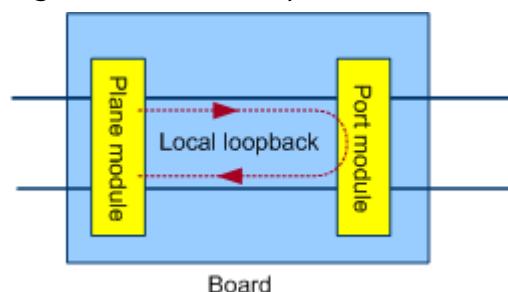
----End

Reference

Introduction to local loopback

Local loopback, also called inloop, near-end loopback, or central office (CO) loopback, is a loopback performed from the port processing module of a service board to the backplane. In this loopback, signals are sent from the backplane to the port processing module, and then be sent back to the backplane. The following figure shows a local loopback.

Figure 5-25 Local loopback

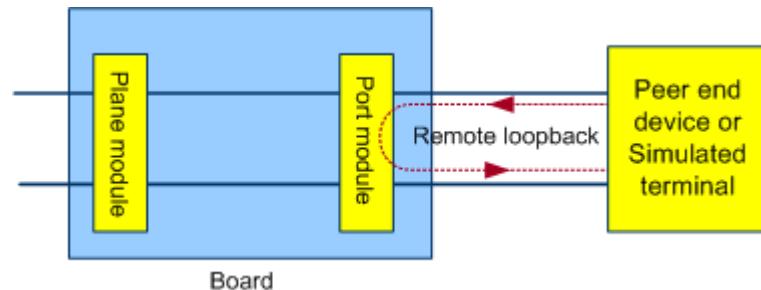


A local loopback checks whether the service channel between the control board and the service board is working properly. When a service failure occurs, this operation can be used to locate faults that occur on the control board or on the logic chip or board chipset of a service board.

Remote Loopback

Remote loopback, also called outloop, refers to the loopback from the port processing module inside the board to the subscriber line. In remote loopback, the signals between the user-side device (such as the modem) and the port signal receiving module directly return to the user-side device through the port signal sending module over the subscriber line. The test aims to check whether the upstream service between the customer premises equipment (CPE) and the board is through, and whether packet loss exists. When the service failure occurs, the fault is located on the CPE or the board chip set. The following figure shows the remote loopback.

Figure 5-26 Remote loopback



5.3.4 Loopback on a G.fast Port

This section describes how to perform a loopback on a G.fast port to locate a G.fast service fault. A loopback on a G.fast port can be performed to determine whether the service board housing the G.fast port is communicating with the backplane properly.

Prerequisites

- The G.fast port is deactivated.
- The G.fast service ran properly before the fault occurred. (This determines that a downstream service flow is available between the control board and the G.fast service board).

Impact on the System

- When a G.fast port is executing loopback operations, the port cannot forward packets properly, and all services carried on the port are interrupted.
- When a G.fast port is executing loopback operations, if ports are not isolated at Layer 2, services of other ports may be affected. By default, ports are isolated at Layer 2 except that Layer 2 user bridging is configured. For details about how to enable or disable Layer 2 user bridging, see "Layer 2 User Bridging" in *Feature Guide*.

Procedure

Step 1 Run the **loopback** command in G.fast mode to start a loopback on a G.fast port.

 **NOTE**

Port loopback is classified as local loopback and remote loopback. For details about local loopback and remote loopback, see section *Reference* in the following section. G.fast ports support only local loopback.

For example, run the following command to start a local loopback on port 0/1/0:

```
huawei(config-if-gfast-0/1)#loopback 0 local
```

Step 2 G.fast boards work in PTM mode. In this case, use an external testing device, such as the SmartBits, to check the connectivity of the loopback channel by sending packets to the service board.

Step 3 Run the **undo loopback** command to cancel the loopback after the loopback operation is complete.

For example, run the following command to cancel a local loopback on port 0/1/0:

```
huawei(config-if-gfast-0/1)#undo loopback 0
```

 **NOTE**

A port on which a loopback is being performed cannot be activated.

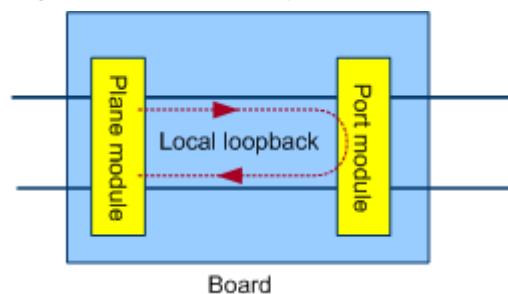
----End

Reference

Introduction to local loopback

Local loopback, also called inloop, near-end loopback, or central office (CO) loopback, is a loopback performed from the port processing module of a service board to the backplane. In this loopback, signals are sent from the backplane to the port processing module, and then be sent back to the backplane. The following figure shows a local loopback.

Figure 5-27 Local loopback



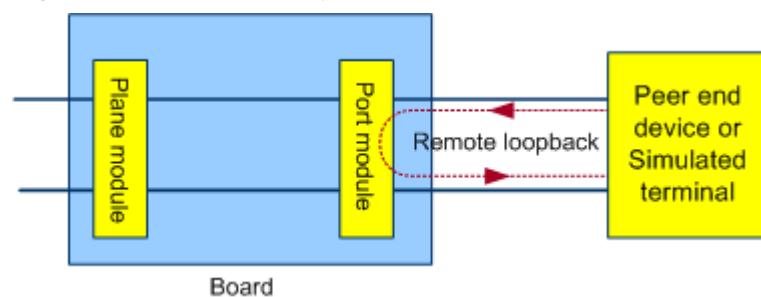
A local loopback checks whether the service channel between the control board and the service board is working properly. When a service failure occurs, this operation can be used to locate faults that occur on the control board or on the logic chip or board chipset of a service board.

Introduction to remote loopback

Remote loopback, also called outloop, refers to the loopback from the port processing module inside the board to the subscriber line. In remote loopback, the

signals between the user-side device (such as the modem) and the port signal receiving module directly return to the user-side device through the port signal sending module over the subscriber line. The test aims to check whether the upstream service between the customer premises equipment (CPE) and the board is through, and whether packet loss exists. When the service failure occurs, the fault is located on the CPE or the board chip set. The following figure shows the remote loopback.

Figure 5-28 Remote loopback



5.3.5 Changing the Line Profile (Template) Configured on a DSL Port

This section describes how to change the line profile or line template configured on a digital subscriber line (DSL) port when the profile or template cannot meet service requirements.

Impact on the System

The DSL port must be deactivated before you change the line profile or line template configured on the port. If the port is deactivated, services carried on the port are interrupted.

Context

Use the line template to activate a DSL port when the port is working in the following modes:

- Asymmetric digital subscriber line (ADSL) ports: RFC4706 mode
- Very-high-speed digital subscriber line (VDSL) ports: TR129 mode

Use the line profile to activate a DSL port when the port is working in the following modes:

- ADSL ports: RFC2662 mode
- Single-line high speed digital subscriber line (SHDSL): none

Procedure

- To change the line template configured on an ADSL2+ port that works in RFC4706 mode, perform the following steps:
 - a. Run the **interface adsl** command to navigate to ADSL mode.
 - b. Run the **deactivate** command to deactivate the ADSL2+ port whose line template needs to be changed.

- c. Run the **activate** command to activate the ADSL2+ port and bind a proper line template to the port.

 **NOTE**

A line template includes a line profile and a channel profile. The commands for adding a set of ADSL line templates are as follows:

1. Run the **adsl line-profile add** command to add a line profile.
 2. Run the **adsl channel-profile add** command to add a channel profile.
 3. Run the **adsl line-template add** command to add a line template.
- d. Run the **display adsl line-template** command to check the line template reconfigured on the ADSL2+ port.
- To change the line profile configured on an ADSL2+ port that works in RFC2662 mode, perform the following steps:
 - a. Run the **interface adsl** command to navigate to ADSL mode.
 - b. Run the **deactivate** command to deactivate the ADSL2+ port whose line profile needs to be changed.
 - c. Run the **activate** command to activate the ADSL2+ port and bind a proper line profile to the port.

 **NOTE**

The **adsl line-profile add** command can be used to add an ADSL line profile to an ADSL2+ port.

- d. Run the **display adsl line-profile** command to check the line profile reconfigured on the ADSL2+ port.
- To change the line template configured on a VDSL2 port that works in TR129 mode, perform the following steps:
 - a. Run the **interface vdsl** command to navigate to VDSL mode.
 - b. Run the **deactivate** command to deactivate the VDSL2 port whose line template needs to be changed.
 - c. Run the **activate** command to activate the VDSL2 port and bind a proper line template to the port.

 **NOTE**

A line template includes a line profile and a channel profile. The commands for adding a set of VDSL line templates are as follows:

1. Run the **vdsl line-profile add** command to add a line profile.
 2. Run the **vdsl channel-profile add** command to add a channel profile.
 3. Run the **vdsl line-template add** command to add a line template.
- d. Run the **display vdsl line-template** command to check the line template reconfigured on the VDSL2 port.
- To change the line profile configured on an SHDSL port, perform the following steps:
 - a. Run the **interface sh1** command to navigate to SHDSL mode.
 - b. Run the **deactivate** command to deactivate the SHDSL port whose line profile needs to be changed.
 - c. Run the **activate** command to activate the SHDSL port and bind a proper line profile to the port.

 NOTE

The **shdsl line-profile add** command can be used to add an SHDSL line profile to an SHDSL port.

- d. Run the **display shdsl line-profile** command to check the line profile reconfigured on the SHDSL port.

----End

5.3.6 Changing the Traffic Profile of a DSL Port

This topic describes how to change the traffic profile when the traffic profile bound to the DSL port cannot meet the requirements.

Impact on the System

The service port needs to be deleted before the profile change. As a result, the service of the user corresponding to the service port is interrupted.

Procedure

- Step 1** Run the **display traffic table ip** command to check whether a traffic profile that meets the requirement exists in the system.
- If a traffic profile that meets the requirement exists in the system, proceed to [Step 2](#).
 - If no traffic profile that meets the requirement exists in the system, run the **traffic table ip** command to create a traffic profile and then proceed to [Step 2](#).

- Step 2** Run the **undo service-port** command to delete the original service port.

 NOTICE

The service port cannot be deleted in the following conditions:

- The service port is configured with a multicast user. In this case, if you need to delete the service port, run the **igmp user delete** command to delete the multicast user first. You can run the **display igmp user** command to query the information about a multicast user.
- The service port is bound with an IP address. In this case, if you need to delete the service port, run the **undo bind** command to unbind the IP address first. You can run the **display bind** command to query the binding relationship between the IP address and the port.
- The service port is configured with a static MAC address. In this case, if you need to delete the service port, run the **mac-address static** command to delete the static MAC address first. You can run the **display mac-address port** command to query the MAC address of a service port.
- The service port is bound with 802.1x authentication. In this case, if you need to delete the service port, run the **undo dot1x service-port** command to unbind the 802.1x authentication first. You can run the **display dot1x service-port** command to check whether the 802.1X authentication is enabled on a service port.

Step 3 Run the **service-port** command to re-configure the service port and bind the service port with a new traffic profile.

----End

5.3.7 Locating and Troubleshooting of a Vectoring Activation Failure

After vectoring is enabled globally, ports in a vectoring group are activated in common mode. When vectoring is invalid on the port, see this topic to locate and rectify the fault.

Context

After vectoring is enabled globally, run the **display line operation** command to query the port activation mode of the vectoring group. If **Standard in port training** in command output is **G.993.5**, vectoring takes effect on ports. If it is not **G.993.5**, vectoring does not take effect on ports.

The possible causes are:

- Vectoring is disabled.
- The CPE does not support G.993.5.
- Upstream and downstream crosstalk cancellations are not enabled.
- Band plan division encounters a compatibility problem.
- The synchronization status between the vectoring processing board and vectoring service boards is abnormal.

Procedure

Step 1 Run the **display xdsl vectoring config** command to check whether vectoring is enabled globally. Ports can be activated in vectoring mode only after vectoring is enabled globally. If vectoring is not enabled globally, run the **xDSL vectoring** command to enable it globally.

Step 2 Run the **display inventory cpe** command to check whether the transmission mode capability set of the CPE supports G.993.5. Ports can be activated in vectoring mode only when the transmission mode capability set of the CPE supports G.993.5.

For example:

```
-----  
G.994.1 vendor ID      : 0xB5004244434D0000  
G.994.1 country code   : 0xB500  
G.994.1 provider code  : BDCM  
G.994.1 vendor info    : 0x0000  
System vendor ID       : 0xB5004244434D0000  
System country code    : 0xB500  
System provider code   : BDCM  
System vendor info     : 0x0000  
Version number         : A2pv6C037g  
Version number(octet string) : 0x41327076364330337670000000000000  
Vendor serial number   : -  
Self-test result        : PASS  
Transmission mode capability :  
G.992.1(Annex A)      : G.992.3(Annex A)  
G.992.5(Annex A)      : G.993.2(Annex A/B/C)
```

G.993.5

Full G.993.5 friendly

//Supports G.993.5 mode//

- Step 3** Run the **display xdsl vectoring-profile** command to check whether upstream and downstream crosstalk cancellation is enabled. If they are disabled, run the **xDSL vectoring-profile modify** command to enable them.
- Step 4** Run the **display xDSL vectoring line-info** command to check whether bandplan configured on the profile bound to the port is compatible with that configured globally. If **BandPlan Compatible** in the command output is **Y**, the band plans are compatible. If it is **N**, the band plans are not compatible. Run the **xDSL vectoring bandplan-type** command to select the band plan configured globally that is compatible with that on the profile bound to the port, and activate the port again.
- Step 5** Run the **display xDSL vectoring state** command in diagnose mode to query interface and synchronization status between the vectoring processing board and vectoring service boards. If **Sync state** in the command output is **Synchronized**, the synchronization status is normal. If it is **Unsynchronized**, the synchronization status is abnormal. Please collect the log information.

For example:

F/S	VP vectoring interface state	VDSL vectoring interface state	Sync state
0/x	Up	Up	Synchronized

- Step 6** Connect Huawei for technical support.

----End

5.4 Common Fault Location and Rectification Methods for E1 Lines

This topic describes how to identify and rectify a fault when an E1 line is faulty.

5.4.1 Common E1 Line Faults

This topic describes how to identify and rectify a common E1 line fault.

When an E1 line is faulty, rectify the fault by referring to [Table 5-14](#).

Table 5-14 Common E1 line faults

Fault	Identification Method	Rectification Method
An E1 line deteriorates or a connector is not securely installed (for example, wire seating is not firm on the distribution frame).	<ul style="list-style-type: none">Check whether the line is exposed.Check whether the connector is rusted or wire seating is not firm.	Replace the line or perform wire seating again.
An E1 line is improperly connected.	<ul style="list-style-type: none">Check whether the transmit and receive ends of the line are correctly connected.Check whether the 75 ohm E1 trunk cable is grounded.	<ul style="list-style-type: none">Correctly connect the transmit and receive ends of the line.Ground the shield layer of the 75 ohm E1 trunk cable. The 120 ohm E1 trunk cable does not need to be grounded.
A loop occurs on E1 lines.	Check whether the two wires of an E1 line are directly connected.	Disconnect the loop and properly connect the lines.
Interference occurs on an E1 line.	Check whether a strong interference source is around the line.	Remove the interference source or reroute the line.
An E1 line is incorrectly configured.	<ul style="list-style-type: none">Check whether clock configurations are consistent on the two ends of the line.Check whether port mode, signaling mode, and CRC4 attribute are consistent on the two ends of the line. CRC is the acronym for cyclic redundancy check.	Configure port attributes on the two ends of the line according to data plan.

5.4.2 Performing a Loopback on an E1 Port

When the services carried on an E1 port are abnormal, you can perform a loopback on the E1 port to locate a fault. When the result of the **Performing a Loopback on an E1 Line** is abnormal, you can perform this operation to further locate the fault.

Prerequisites

None

Tools, Meters, and Materials

Emulation terminal (such as the E10 meter)

 NOTE

The emulation terminal is optional. When you perform a remote loopback if no service stream is carried on the tested link, you can use the emulation terminal to emulate the peer device to send packets. In addition, you can determine the link status according to the indication on the meter. When you perform a local loopback, the emulation terminal is not needed, but you can still determine the link status according to the indication on the meter.

Impact on the System

- After the port loopback is configured, the port cannot forward data packets correctly, and all the services carried on the port are interrupted. Therefore, backup the service data before performing the loopback, or perform the operation when the port carries the minimum traffic.
- After the port loopback is configured, the broadcast storm may occur if the E1 port is not isolated. Therefore, it is recommended that you run the **undo loopback** command to cancel the loopback in time after the loopback test is complete.

Precautions

The loopback cannot be configured if the E1 port is in any of the following states:

- Idle
- Blocked

The loopback of each E1 port is configured independently and only one type of loopback can be configured each time. That is, if you need to configure another loopback after configuring a loopback, you need to cancel the existing loopback and then configure another loopback.

Procedure

- Configure a remote loopback on the E1 port.
 - a. (Optional; perform this operation when using the emulation terminal.) Connect the transmit and receive ends of the E1 line on the tested E1 port to the corresponding ports on the emulation terminal, and ensure that they are in good contact.
 - b. Start the remote loopback on the E1 port.
For example, run the **loopback** command in TDM mode to start the remote loopback on port 0/1/0.

```
huawei(config-if-tdm-0/1)#loopback 0 remote
```
 - c. Verify the loopback result.

By checking whether the peer device receives the signal sent by itself (for example, if the remote loopback is started on a port, the user of the peer

device should hear the voice of himself/herself when making calls), you can determine whether the tested link is accessible. If an emulation terminal such as the E10 meter is used, you can determine the result according to the indication on the meter.

- Configure a local loopback on the E1 port.
 - a. (Optional; perform this operation when using the emulation terminal.) Connect the transmit and receive ends of the E1 line on the tested E1 port to the corresponding ports on the emulation terminal, and ensure that they are in good contact.
 - b. Start the local loopback on the E1 port.
For example, run the **loopback** command in TDM mode to start the local loopback on port 0/1/0.

```
huawei(config-if-tdm-0/1)#loopback 0 local
```
 - c. Verify the loopback result. By checking whether the local device receives the signal sent by itself (for example, if the local loopback is started on the port, the user of the peer device should hear the voice of himself/herself when making calls), you can determine whether the tested link is accessible. If an emulation terminal such as the E10 meter is used, you can determine the result according to the indication on the meter.

----End

References

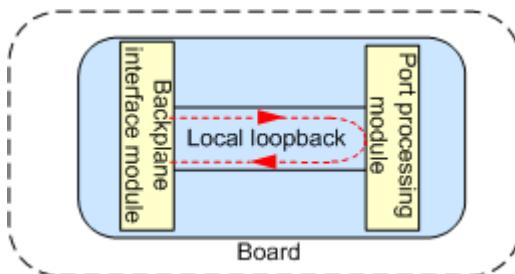
The E1 port on the device supports two types of loopbacks.

- Local loopback
- Remote loopback

Local loopback on the E1 port

Local loopback, also called inloop, is the loopback from the port processing module of the board to the backplane. In the local loopback, the signals that are transmitted from the backplane to the E1 port are directly sent back to the backplane to check whether the board that houses the E1 port can communicate with the backplane normally. [Figure 5-29](#) shows the local loopback on the E1 port.

[Figure 5-29](#) Local loopback on the E1 port

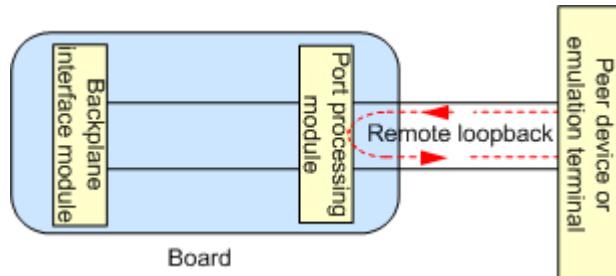


Remote loopback on the E1 port

Remote loopback, also called outloop, is the loopback from the port processing module of the board to the line. In the remote loopback, the signals that are

transmitted from the peer device to the port processing module are directly sent back to the peer device to check whether the board that houses the E1 port can communicate with the peer device normally. **Figure 5-30** shows the remote loopback on the E1 port.

Figure 5-30 Remote loopback on the E1 port



5.4.3 Performing a Loopback on an E1 Line

The E1 line loopback is also called the 2M link physical loopback. When the services carried on an E1 port are abnormal, you can perform a loopback on the E1 line to check whether the E1 port is normal and whether the internal communication of the system is normal.

Prerequisites

The services carried on the E1 port must run normally before a fault occurs. That is, the tested loop must carry service streams.

Tools, Meters, and Materials

- E1 self-loop line (When an accurate test for the signal quality is not required, use the E1 self-loop line to perform the loopback on the E1 line.)
- Bit error meter (When an accurate test for the signal quality is required, use the bit error meter to perform the loopback on the E1 line.)

Impact on the System

- Performing a loopback on the E1 line requires the disconnection of the E1 line. In this case, all the services carried on the E1 port are interrupted. Therefore, perform the loopback when the E1 line carries the minimum traffic.
- After the loopback is performed on the E1 line, the broadcast storm may occur if the E1 port is not isolated. Therefore, it is recommended that you cancel the loopback in time after the loopback test is complete.

Precautions

None

Procedure

- Step 1** Connect the transmit and receive ends of the tested E1 line to the E1 self-loop line or the corresponding ports on the bit error meter, and ensure that they are in good contact.

Step 2 Verify the loopback result.

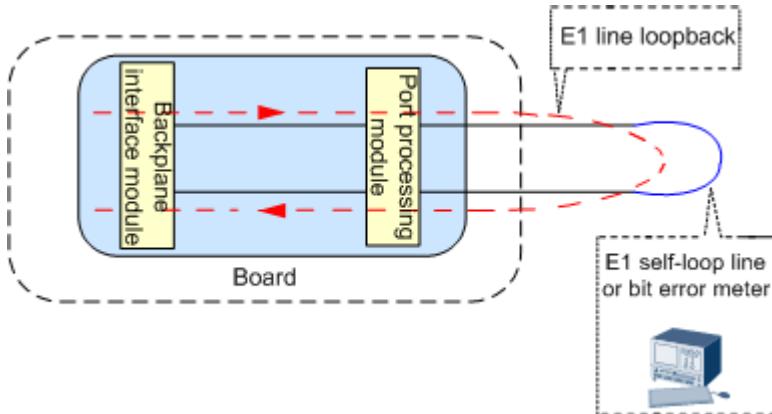
- When you use the E1 self-loop line to perform the loopback, run the **display port state** command to query the status of the port involved in the loopback. If the port is in the normal state, it indicates that the E1 port works in the normal state and the internal communication of the system is also normal.
- When you use the bit error meter to perform the loopback, you can determine whether the E1 port and the internal communication of the system are normal through the indication (whether there is a signal stream or not) on the bit error meter. In addition, you can determine the signal quality of the line according to the indication on the bit error meter.

----End

References

The E1 line loopback is also called the 2M link physical loopback. It is a type of hardware loopbacks, namely, the loopback on a manually created hardware loop. [Figure 5-31](#) shows the E1 line loopback.

Figure 5-31 E1 line loopback



5.5 Diagnosing Broadband Protocol Related Faults

This topic describes how to diagnose broadband protocol related faults.

5.5.1 Introduction

Context



Broadband protocol fault diagnosis may involve obtaining the personal information, such as the IP address, MAC address, the personal data of users and the content of users' communications (the product does not save, parse, or process such information). Huawei alone is unable to collect or save the personal data of users and the content of users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the personal data of users and the content of users' communications are fully protected when the personal data and the content are being used and saved.

Broadband protocol-related fault diagnosis is an important OAM method for a MA5800 running on a network. If a service failure occurs, such as a dialing failure, ping failure, or multicast pixelation, you can locate the fault by analyzing packets.

Broadband protocol-related fault diagnosis of the MA5800 frees OAM engineers from onsite fault locating, which shortens the fault locating duration.

Table 5-15 describes broadband protocol-related fault diagnosis methods.

Table 5-15 Broadband protocol-related fault diagnosis methods

Meth od	Advantage	Disadvantage	Typical Application Scenario
Diagn osis based on an ACL rule	A lot of packets can be captured continuously.	Packets must be uploaded to the file server, which cannot be viewed on the CLI directly.	<ul style="list-style-type: none">• The CPU usage is too high.• The terminal fails to ping the Layer 3 interface of the MA5800.• The NMS fails to manage the MA5800.• The NMS fails to issue configurations.
Diagn osis based on a service port	Packets with fine granularity, that is, packets on a service port can be captured.	<ul style="list-style-type: none">• Packets must be uploaded to the file server, which cannot be viewed on the CLI directly.• Packet loss occurs in a large traffic volume.	<ul style="list-style-type: none">• The ONU fails to ping the BRAS.• Dialup fails.

5.5.2 Diagnosis Based on an ACL Rule

Prerequisites

The TFTP/FTP/SFTP server is configured and can be pinged by the device.

NOTICE

FTP, TFTP are insecure protocols and has security risks. SFTP is recommended.

Context

Diagnosis based on an ACL rule filters protocol packets sent to the CPU by ACL rules, buffers the filtered packets, and uploads the packets as a file to the file server by TFTP/FTP/SFTP.

Limitation:

Only packets sent to the CPU can be captured.

Procedure

- Step 1** In Acl-basic or Acl6-basic mode, run the **rule** command to create an ACL rule to match the protocol packet to be captured.
- Step 2** In diagnose mode, run the **file-server auto-backup debug primary** command to set the information about the server for storing the automatically backed up file.

NOTE

In the command output, 10.11.1.20 is the IP address of the SFTP server. Ensure that the device can ping the SFTP server.

- Step 3** In diagnose mode, run the **capture item** command to configure the data associated with remote packet capture.

NOTE

When the downstream packets of the service board are captured, the packets can match only subrack/slot. Therefore, it is normal if the downstream protocol packets of an unspecified port are captured. When the upstream protocol packets of the service board are captured, the correct port ID needs to be configured. For example, the packets of port 0/1/0 need to match inbound port 0/1/0.

- Step 4** In diagnose mode, run the **capture start** command to start the remote packet capture function.
- Step 5** After packet capture, run the **capture stop** command in diagnose mode to stop the remote packet capture function. Then, the device uploads the packets as a file to the server.
- Step 6** Delete the corresponding configurations.

----End

Example

To capture IGMP packets, do as follows:

```
huawei(config)#acl 3000
huawei(config-acl-adv-3000)#
huawei(config-acl-adv-3000)#rule 1 permit 2
huawei(config-acl-adv-3000)#quit
huawei(config)#diagnose
huawei(diagnose)%file-server auto-backup debug primary 10.11.1.20 sftp
huawei(diagnose)%capture item 1 bidirection ip-group 3000 rule 1 port 0/1/0
huawei(diagnose)%capture start -c 10000 //10000 indicates the number of captured packets
huawei(diagnose)%capture stop
huawei(diagnose)%undo capture item 1
huawei(diagnose)%undo file-server auto-backup debug primary
huawei(diagnose)%config
huawei(config)#undo acl 3000 //Delete configurations.
```

5.5.3 Diagnosis Based on a Service Port

Prerequisites

The TFTP/FTP/SFTP server is configured and can be pinged by the device.

NOTICE

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

Context

Diagnosis based on a service port captures packets by service ports and uploads the packets as a file to the file server by TFTP/FTP/SFTP.

NOTE

For data packets, only the packet header is captured. For protocol packets, the entire packet is captured.

Procedure

- Step 1** In diagnose mode, run the **file-server auto-backup board-info primary** command to set the information about the server for storing the automatically backed up file.
- Step 2** In diagnose mode, run the **capture service-port** command to start the remote packet capture function for a service port. The number of packets to be captured or capture duration can be specified. By default, packets are captured for 300s or 10000 packets are captured.
- Step 3** After packet capture, run the **undo capture service-port** command in diagnose mode to stop the remote packet capture function for a service port.
- Step 4** In diagnose mode, run the **undo file-server auto-backup board-info primary** command to delete the information about the server for storing the automatically backed up file.

----End

Example

To capture about 500 packets on service port 1 for 600s, do as follows:

```
huawei(diagnose)%%file-server auto-backup board-info primary 192.168.1.20 sftp
huawei(diagnose)%%capture service-port 1 capture-time 600 capture-count 500
huawei(diagnose)%%undo capture service-port
Huawei(diagnose)%%undo file-server auto-backup board-info primary
```

5.5.4 Diagnosis by ACL-matched Traffic Mirroring on the Upstream Port

Prerequisites

ACL rules are configured.

Context

The system sends all packets matching the ACL rule of a port to the destination port.



If an aggregation port is configured, **traffic-mirror** must be configured on every source port of the member ports in the aggregation group.

Procedure

- Step 1** In diagnose mode, run the **traffic-mirror** command to mirror the packets that match an ACL rule on an upstream port.
- Step 2** In diagnose mode, run the **undo traffic-mirror** command to cancel mirroring the packets that match an ACL rule on an upstream port.

----End

Example

To mirror the received packets filtered by ACL 2001 on port 0/3/1 to destination port 0/19/0 for capturing, do as follows:

```
huawei(config)#traffic-mirror inbound ip-group 2001 port 0/3/1 to port 0/19/0
huawei(config)#undo traffic-mirror inbound ip-group 2001 port 0/3/1
```

5.5.5 Diagnosis by Mirroring on the Upstream Port

Context

All packets are mirrored from the source port to the target port by configuring the port mirroring command and LSW chip parameters.

Limitation:

Only intra-board packet mirroring is supported (inter-board packet mirroring is not supported).

Procedure

- Step 1** Run the **mirror port** command to configure mirroring on an upstream port.
- Step 2** After packet capture, run the **undo mirror port** command to cancel mirroring on an upstream port.

----End

Example

To mirror the received packets on Ethernet port 0/19/0 to Ethernet port 0/19/1 for capturing, do as follows:

```
huawei(config)#interface eth 0/19
huawei(config-if-eth-0/19)#mirror port 0 1 ingress
huawei(config-if-eth-0/19)#undo mirror port
```

5.5.6 Remote Diagnosis on TCP Traffic

Context

Based on configured packet capture rules, TCP packets can be captured, encapsulated into UDP packets, and then sent to a destination server. Packets can be captured based on access control list (ACL) rules or packet contents.

Limitations:

Only IPoE and IPoPPPoE IPv4 TCP packets are supported.

Procedure

- Step 1** Run the **capture traffic-mirror server-config** command to configure encapsulation parameters of TCP packets and the IP address of the destination server that receives packets.
- Step 2** Configure filtering rules for TCP packets.
 - Capture packets based on ACL rules.
 1. Run the **acl** and **rule** commands to configure ACL rules.
 2. Run the **capture traffic-mirror** command to configure the rules to capture TCP packets.
 - Remotely capture packets based on packet contents.
 1. Run the **capture traffic-mirror** command to configure the rules to capture TCP packets.
- Step 3** After packets are captured, run the **undo capture traffic-mirror** command to delete relevant configurations.

----End

Example

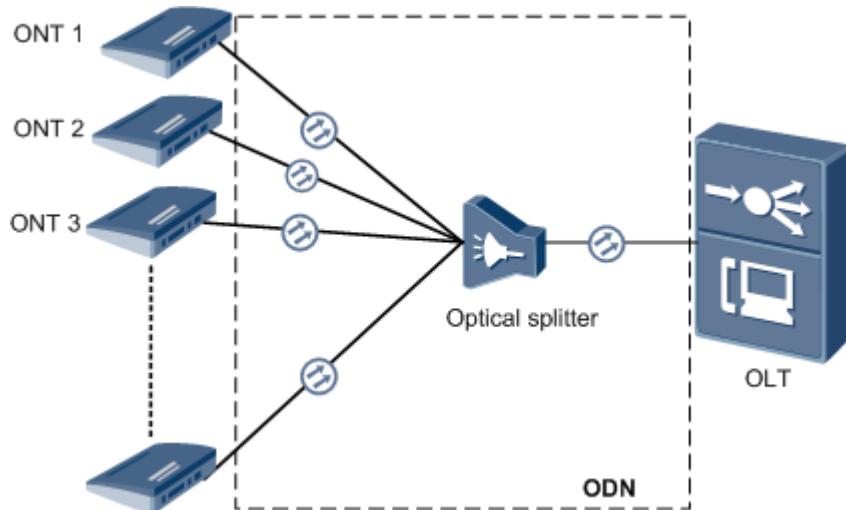
Example: Run the following commands to capture TCP packets received by port 0/3/1 (MAC address of the TCP packets: 00e0-fc00-0001; mask: 00e0-fc00-0000; packet capture duration: 100 minutes; IP address of the destination server that receives the captured packets: 10.63.141.206):

```
huawei(diagnose)#capture traffic-mirror server-config server-ip 10.63.141.206 time 100
huawei(config)#acl 4000
huawei(config-acl-link-4000)#rule 1 permit destination 00e0-fc00-0001 00e0-fc00-0000
huawei(config-acl-link-4000)#quit
huawei(diagnose)#capture traffic-mirror inbound link-group 4000 rule 1 port 0/3/1
huawei(diagnose)#undo capture traffic-mirror all
huawei(config)#undo acl 4000 //Delete relevant configurations.
```

5.6 Methods of Locating and Troubleshooting Common ODN Faults

This topic describes the location methods, related alarms, and common operations in locating and troubleshooting common ODN faults.

The ODN contains all lines and devices between the optical line terminal (OLT) and optical network unit (ONU), such as backbone fibers, optical splitters, and branch fibers. The ODN assigns power of optical signals and provides physical channels for transmitting optical signals between the OLT and ONU, as shown in the following figure.



5.6.1 Common ODN Faults

This topic describes how to locate and troubleshoot common ODN faults.

You can determine the fault point according to the judgment criteria and then troubleshoot the fault.

Table 5-16 Locating and troubleshooting common ODN faults

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The connector endface of an optical fiber is unclean, scratched, or indented.</p> <p>NOTE An unclean, scratched, or indented optical fiber connector will cause excessive attenuation and abnormal reflection.</p>	<p>The connector endface of an optical fiber is unclean, scratched, or indented if one of the following situations occurs:</p> <ul style="list-style-type: none">• The attenuation (calculated using the optical power on both sides of the optical fiber connector tested by the optical power meter) of the optical fiber connector is larger than the theoretical attenuation. For details about how to check the optical power, see 5.6.3 Checking the Optical Power.• The reflection and return loss of the backbone fiber and branch fiber are abnormal as tested by the OTDR. For details about how to use the OTDR, see 5.6.4 Using the OTDR to Locate Abnormal Attenuation Points on the Optical Line.• The optical fiber endface check finds that the connector endface of the optical fiber is unclean, scratched, or indented.	<ul style="list-style-type: none">• Clean the connector endface if it is not clean. For details about how to clean the connector, see 5.6.6 Cleaning the Connector of an Optical Fiber.• Replace the optical fiber if its connector endface is scratched or indented.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The optical fiber connector is too tight or loose.</p> <p>NOTE An over tightly or loosely connected optical fiber will cause excessively large attenuation and reflection.</p>	<p>The connector of the optical fiber is too tight or loose if one of the following situations occurs:</p> <ul style="list-style-type: none">• The attenuation (calculated using the optical power on both sides of the optical fiber connector tested by the optical power meter) of the optical fiber connector is larger than the theoretical attenuation. For details about how to check the optical power, see 5.6.3 Checking the Optical Power.• Points with abnormal return loss exist on the backbone fiber and branch fiber as tested by the OTDR. For details about how to use the OTDR, see 5.6.4 Using the OTDR to Locate Abnormal Attenuation Points on the Optical Line.• The optical fiber connector checked onsite is too tight or loose.	<p>Connect the optical fiber again to ensure that the optical fiber is properly connected.</p> <p>NOTE FC/PC connectors are generally difficult to fasten properly. SC/PC connectors are recommended. When an SC/PC connector is properly connected, you will hear a click.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>Optical fiber connectors of different types are connected.</p> <p>NOTE If different types of optical fiber connectors are connected, the attenuation and reflection will be excessively large.</p>	<p>Optical fiber connectors of different types are connected if one of the following situations occurs:</p> <ul style="list-style-type: none">• The attenuation (calculated using the optical power on both sides of the optical fiber connector tested by the optical power meter) of the optical fiber connector is larger than the theoretical attenuation. For details about how to check the optical power, see 5.6.3 Checking the Optical Power.• Points with abnormal return loss exist on the backbone fiber and branch fiber as tested by the OTDR. For details about how to use the OTDR, see 5.6.4 Using the OTDR to Locate Abnormal Attenuation Points on the Optical Line.• The PC connector (blue) is connected to the APC connector (green) onsite.	<p>Replace the incompatible connector with a compatible one or replace relevant devices.</p> <p>NOTE In the CATV service scenario, it is recommended that you use APC connectors (green) only.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The optical fiber is excessively bent.</p> <p>NOTE Optical signals attenuate seriously on an optical fiber with an excessively small bending radius.</p>	<p>The optical fiber is excessively bent if one of the following situations occurs:</p> <ul style="list-style-type: none">Points with abnormal return loss exist on the backbone fiber and branch fiber as tested by the OTDR. For details about how to use the OTDR, see 5.6.4 Using the OTDR to Locate Abnormal Attenuation Points on the Optical Line.The optical fiber has red light leaking as tested by a red pointer in a short distance (within 1000 m). For details about how to use the red pointer, see 5.6.5 Checking Whether the Optical Fiber Is Damaged Using the Red Pointer.The optical fiber is excessively bent onsite. <p>NOTE The bending radius of the optical fiber should be more than 20 times the cable radius. In general, the bending radius of the optical fiber is more than or equal to 40 mm.</p>	Replace the optical fiber.

Possible Cause	Judgment Criterion	Troubleshooting Method
The optical fiber is damaged.	<p>The optical fiber is damage if either of the following situations occurs:</p> <ul style="list-style-type: none">Points with abnormal return loss exist on the backbone fiber and branch fiber as tested by the OTDR. For details about how to use the OTDR, see 5.6.4 Using the OTDR to Locate Abnormal Attenuation Points on the Optical Line.The optical fiber has red light leaking as tested by a red pointer in a short distance (within 1000 m). For details about how to use the red pointer, see 5.6.5 Checking Whether the Optical Fiber Is Damaged Using the Red Pointer.	<ul style="list-style-type: none">Replace the optical fiber if it is damaged.Splice the optical fiber again if air bubbles exist at the splicing point. <p>NOTICE Only specially trained and qualified personnel are allowed to splice optical fibers.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The multi-mode optical fiber is used.</p> <p>NOTE Only single-mode optical fibers can be used on the ODN lines. If the multi-mode optical fiber is used, the optical signal attenuates quickly and the return loss increases.</p>	<p>The multi-mode optical fiber is used if one of the following situations occurs:</p> <ul style="list-style-type: none">• The attenuation (calculated using the optical power of the backbone fiber and branch fiber tested by the optical power meter) of the backbone fiber and branch fiber is larger than the theoretical attenuation. For details about how to check the optical power, see 5.6.3 Checking the Optical Power.• Optical signals of the backbone fiber and branch fiber attenuate seriously as tested by the OTDR. For details about how to use the OTDR, see 5.6.4 Using the OTDR to Locate Abnormal Attenuation Points on the Optical Line.• The multi-mode optical fiber is used onsite. <p>NOTE The single-mode optical fiber is yellow and the multi-mode optical fiber is orange.</p>	Replace the multi-mode optical fiber with a single-mode optical fiber.

Possible Cause	Judgment Criterion	Troubleshooting Method
The optical splitter is faulty or the fiber adapter for the optical splitter is not clean.	<p>The optical splitter is faulty or the fiber adapter for the optical splitter is not clean if either of the following situations occurs:</p> <ul style="list-style-type: none">• The attenuation (calculated using the optical power on both sides of the optical splitter tested by the optical power meter) of the optical splitter is larger than the theoretical attenuation. For details about how to check the optical power, see 5.6.3 Checking the Optical Power.• The attenuation of the optical splitter is excessively large as tested by the OTDR. For details about how to use the OTDR, see 5.6.4 Using the OTDR to Locate Abnormal Attenuation Points on the Optical Line. <p>NOTE The common OTDR cannot test attenuation of the optical splitter in the penetration manner. Therefore, the attenuation of an optical splitter can be tested only by the OTDR that can penetrate the optical splitter.</p>	<ul style="list-style-type: none">• Replace the optical splitter if it is faulty.• Clean the fiber adapter for the optical splitter if it is not clean. For details about how to clean the fiber adapter, see 5.6.6 Cleaning the Connector of an Optical Fiber.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The optical attenuation of the optical line is excessively small.</p> <p>NOTE</p> <ul style="list-style-type: none">• If the optical attenuation of the optical line is excessively small, the optical power received by the ONU will exceed the overload optical power of the ONU.• Such a situation usually occurs in labs, where the OLT and ONU may be directly connected to each other by using a short optical fiber.	<p>The optical attenuation of the optical line is excessively small if either of the following situations occurs:</p> <ul style="list-style-type: none">• The actual receive optical power of the ONU is larger than -8 dBm as tested by the optical power meter.• The optical attenuation of the optical line between the OLT and ONU is excessively small. The normal attenuation range is 15-25 dB.	Add an optical attenuator on the optical line between the OLT and ONU.
<p>The ODN is not properly planned.</p> <p>NOTE</p> <ul style="list-style-type: none">• The split ratio of the ODN link is not determined by the number of ONTs connected but by the split ratio of optical splitters. When an optical splitter is connected to the ODN, attenuation occurs and the split ratio of the optical splitter needs to be calculated.• The differences between the OLT-received optical power from the two adjacent ONUs must be smaller than or equal to 15 dB.	<p>The ODN does not meet the requirements of the ODN link plan or GPON Class B+.</p> <ul style="list-style-type: none">• Three-level splitting exists in the ODN.• The network coverage of the ODN far exceeds 20 km.• The split ratio exceeds the specification. For example, a board supports a maximum split ratio of 1:64. If the first-level split ratio is 1:8, the second level is 1:16, the actual split ratio is 1:128. This exceeds the specification (1:64).• The optical attenuation difference of two optical lines exceeds 15 dB.	Optimize the ODN to meet Huawei's ODN planning requirements and protocol requirements.

5.6.2 ODN-Related Alarms

This topic describes ODN-related alarms on OLT.

[Table 5-17](#) describes GPON ODN faults and corresponding alarms.

Table 5-17 GPON ODN alarms on OLT

Fault	Related Alarms
<ul style="list-style-type: none">The split ratio is excessively large.The optical fiber is excessively long.The branch fiber deteriorates or is bent.The branch fiber connector is loose or contaminated.	0x2e112002 The loss of GEM channel delineation (LCDGi) occurs 0x2e112003 The signal degrade of ONTi (SDi) occurs 0x2e112004 The signal fail of ONTi (SFi) occurs 0x2e112006 The loss of frame of ONTi (LOFi) occurs 0x2e112007 The distribute fiber is broken or the OLT cannot receive expected optical signals from the ONT(LOSi/LOBi) 0x2e11a00a The loss of acknowledgement PLOAM message with ONTi (LOAi) occurs 0x2e11a00c The loss of PLOAM of ONTi occurs(LOAMi/LOPCi)
<ul style="list-style-type: none">The backbone fiber is broken or disconnected.The optical module of the OLT PON port is faulty or removed.	0x2e11a001 The feeder fiber is broken or the OLT cannot receive any expected optical signals(LOS)
The optical module of the ONU PON port is faulty or removed.	0x2e112007 The distribute fiber is broken or the OLT cannot receive expected optical signals from the ONT(LOSi/LOBi)

5.6.3 Checking the Optical Power

Checking the optical power is a common method for ODN troubleshooting. By checking and analyzing upstream and downstream optical power, you can determine whether the optical line quality is good.

5.6.3.1 Analyzing the Optical Power

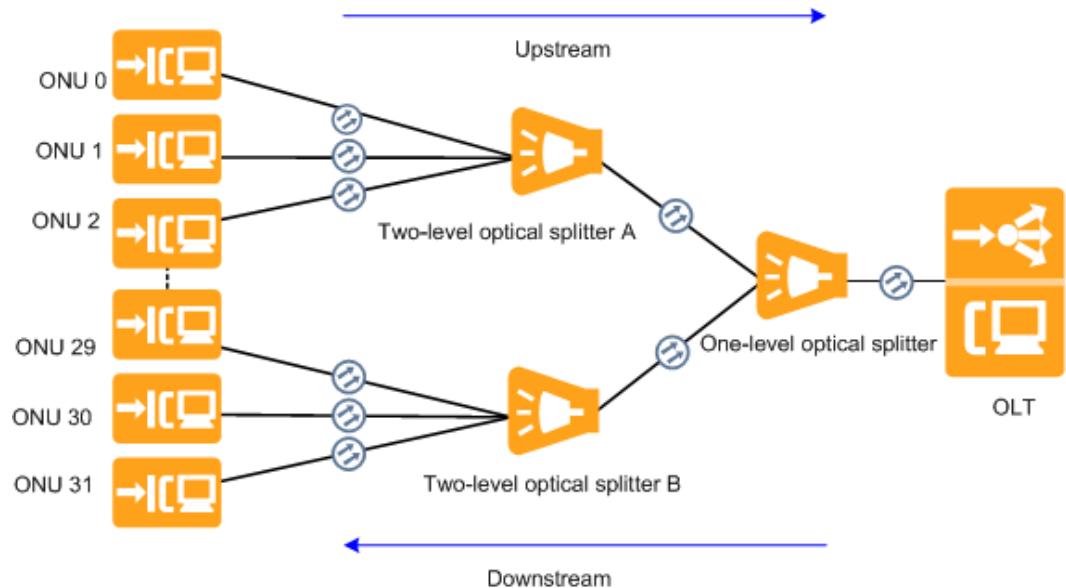
In optical power analysis, the actual optical attenuation is compared with the theoretical value to determine the quality of the optical line and locate the abnormal attenuation point in the optical line.

The optical power attenuates after being transmitted through the optical components or optical fibers. Normally, the actual attenuation is close to the

theoretical value. If the actual attenuation is much larger than the theoretical value, abnormal attenuation point exists in the optical line.

Figure 5-32 shows the ODN optical line

Figure 5-32 ODN optical line



Actual optical attenuation = Upstream optical power on one side of the test point - Upstream optical power on the other side of the test point. Alternatively, Actual optical attenuation = Downstream optical power on one side of the test point - Downstream optical power on the other side of the test point. These two calculated values are the same. For details about how to measure the optical power, see [5.6.3.3 Measuring the Upstream Optical Power Using the Optical Power Meter](#) and [5.6.3.4 Measuring the Downstream Optical Power Using the Optical Power Meter](#).

For example, to calculate the actual optical attenuation of two-level optical splitter A in **Figure 5-32**, do as follows:

- Method 1: Actual optical attenuation of two-level optical splitter A = Upstream optical power of the IN port on two-level optical splitter A - Upstream optical power of the OUT port on two-level optical splitter A
- Method 2: Actual optical attenuation of two-level optical splitter A = Downstream optical power of the OUT port on two-level optical splitter A - Downstream optical power of the IN port on two-level optical splitter A

 NOTE

- If the upstream optical power is used for calculating the optical attenuation of an optical splitter, only the ONU to be tested is powered on. That is, other ONUs connected to the same optical splitter are powered off. This ensures accurate optical power.

In the preceding example, only ONU 0, ONU 1, or ONU 2 is powered on and the other two ONUs are powered off.

- It is recommended that you use the downstream optical power for calculating the optical attenuation because the downstream optical is easy to measure.
- You can run commands to query the optical power if it cannot be measured onsite. However, the optical power of an optical splitter cannot be queried using the CLI. For details, see [5.6.3.2 Querying the Optical Power Using the CLI](#). When the CLI is used for querying the optical power, the query result is accurate and stable if a great volume of data is transmitted; the query result has a maximum difference of 2 dB from the actual optical power if a small volume of data is transmitted. Therefore, it is not recommended that you run commands to query the optical power.

Table 5-18 lists theoretical optical attenuation.

Table 5-18 Theoretical optical attenuation

Component	Type	Average Loss (dB)
Connection point	Fusion splicing	≤ 0.1
	Active connector (fiber adapter)	≤ 0.3
	Mechanical splicing or quick connector	≤ 0.5
Optical splitter	1:64	≤ 20.5
	1:32	≤ 17.5
	1:16	≤ 13.8
	1:8	≤ 10.6
	1:4	≤ 7.5
	1:2	≤ 3.8
Optical fiber	1490 nm / 1577 nm (1 km)	≤ 0.23
	1310 nm / 1270 nm (1 km)	≤ 0.35

Table 5-19 describes possible faults and causes if the actual optical attenuation is much larger than the theoretical value.

Table 5-19 Possible faults and causes

Fault	Possible Cause
Connection point (such as mechanical splicing point, fusion splicing point, active connector, and quick connector)	<ul style="list-style-type: none">Cores at the two ends of an optical fiber of the mechanical splicing point or the fusion splicing point are not aligned.The fusion splicing point has air bubbles.The active connector or the quick connector is faulty or not clean.
Optical splitter	The optical splitter is faulty or the fiber adapter for the optical splitter is not clean.
Optical fiber	<ul style="list-style-type: none">The connector endface of an optical fiber is unclean, scratched, or indented.The optical fiber connector is too tight or loose.Optical fiber connectors of different types are connected.The optical fiber is excessively bent.The optical fiber is damaged.The multi-mode optical fiber is used.

5.6.3.2 Querying the Optical Power Using the CLI

If the optical power cannot be measured onsite, you can query the Tx and Rx optical power of the device using the CLI. It is not recommended that you use the CLI to query the optical power because there is a difference between the query result and actual value.

Context



When the CLI is used for querying the optical power, the query result is accurate and stable if a great volume of data is transmitted; the query result has a maximum difference of 2 dB from the actual optical power if a small volume of data is transmitted. Therefore, it is recommended that you use the optical power meter to measure the optical power onsite.

Table 5-20 OLT commands for querying the optical power

Item	Command
Rx optical power of the OLT	display ont optical-info
Tx optical power of the OLT	display port state
Rx optical power of the ONU	display ont optical-info
Tx optical power of the ONU	display ont optical-info

5.6.3.3 Measuring the Upstream Optical Power Using the Optical Power Meter

This topic describes how to measure the upstream optical power using the optical power meter.

Prerequisites

- The OLT and the ONU are powered on.
- The PON port is enabled.

Tools and Materials

- A new SC/PC single-mode patch cord not longer than 1 m is recommended.
- Burst optical power meter: Measures the upstream and downstream optical power without disconnecting a working optical line. This power meter is usually used in external tests. It generally measures the optical power at the ingress for optical signals and displays the result on its screen. Optical signals attenuate from their entry into the optical power to their departure from the optical power, which affects the measurement result. However, this attenuation is not considered in actual external tests.

Impact on the System

Services carried on the optical line will be interrupted.

Precautions

NOTICE

Never look into the optical port or the connector of an optical fiber without eye protection. Never put the optical port towards the flammables.

Clean the connector of an optical fiber after testing the optical power by referring to [5.6.6 Cleaning the Connector of an Optical Fiber](#). This is because if a contaminated optical fiber is connected to a functional optical fiber connector, the connector will be contaminated, which leads to abnormal attenuation and reflection and therefore affects the quality of the optical line.

Procedure

Step 1 Configure the measurement parameters of the burst optical power meter.

- Optical power unit: dBm
- Wavelength (nm): 1310

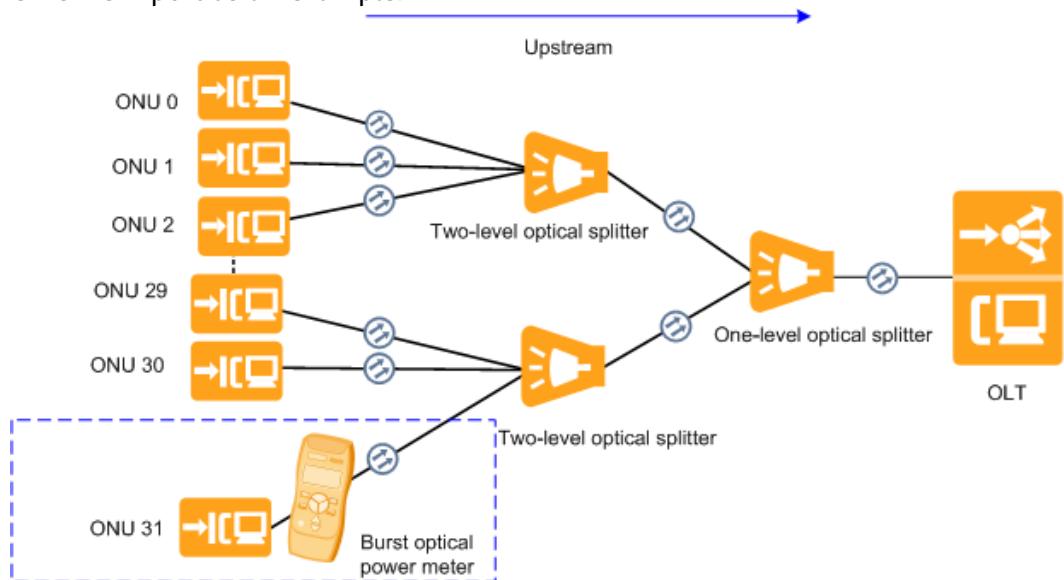
NOTE

A functional ONU does not proactively send optical signals. An ordinary optical power meter measures only the upstream optical power or downstream optical power at one time and the optical line is disconnected in measuring. Therefore, a burst optical power meter is required in measuring the upstream optical power.

Step 2 Use the patch cord to connect the burst optical power meter to the measurement point in an ODN link to measure the optical power.

Points for measuring the upstream optical power are connection points (such as mechanical splicing points, fusion splicing points, active connector, and quick connector) in an ODN link, IN and OUT ports of an optical splitter, OLT PON ports, and ONU PON ports.

The following figure shows measurement of the upstream optical power using an ONU PON port as an example.



Step 3 View and record the optical power read from the burst optical power meter.

NOTE

- If the value on the optical power meter changes within a range of 0.2 dBm, take the average value.
- If the value on the optical power meter changes in a range wider than 0.2 dBm, there is a possibility that the optical fiber is not properly connected, the optical fiber is excessively bent, or the optical fiber connector is unclean.
- Do not bend the optical fiber. A bent optical fiber may affect the test result.

Step 4 Remove the burst optical power meter after measurement and reconnect the optical line.

Step 5 Analyze the quality of the optical line. For details, see [5.6.3.1 Analyzing the Optical Power](#).

----End

5.6.3.4 Measuring the Downstream Optical Power Using the Optical Power Meter

This topic describes how to measure the downstream optical power using the optical power meter.

Prerequisites

- The OLT and the ONU are powered on.
- The PON port is enabled.

Tools and Materials

- A new SC/PC single-mode patch cord not longer than 1 m is recommended.
- Burst optical power meter or common optical power meter
 - Burst optical power meter: Measures the upstream and downstream optical power without disconnecting a working optical line. This power meter is usually used in external tests. It generally measures the optical power at the optical signal ingress and displays the result on its screen. Optical signals attenuate from their entry into the optical power to their departure from the optical power, which affects the measurement result. However, this attenuation is not considered in actual external tests.
 - Ordinary optical power meter: Measures only the upstream or downstream optical power at one time and the optical line is disconnected in measuring.

NOTE

When measuring the downstream optical power, disconnect the optical line and connect the optical power meter to the measurement point. That is, you do not need to connect the optical power meter to the optical line. The optical power meter can be the burst optical power meter or ordinary optical power meter.

Impact on the System

Services carried on the optical line will be interrupted.

Precautions

NOTICE

Never look into the optical port or the connector of an optical fiber without eye protection. Never put the optical port towards the flammables.

Clean the connector of an optical fiber after testing the optical power by referring to [5.6.6 Cleaning the Connector of an Optical Fiber](#). This is because if a contaminated optical fiber is connected to a functional optical fiber connector, the connector will be contaminated, which leads to abnormal attenuation and reflection and therefore affects the quality of the optical line.

Procedure

Step 1 Configure the measuring parameters of the optical power meter.

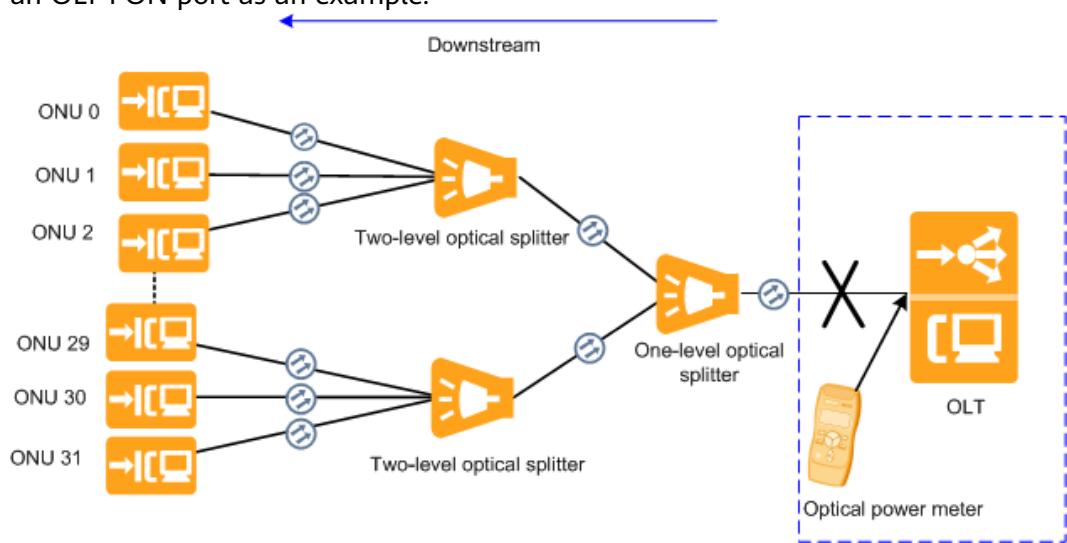
- Optical power unit: dBm
- Wavelength (nm): 1490

Step 2 Connect the optical power meter to the measurement point.

Points for measuring the downstream optical power are connection points (such as mechanical splicing points, fusion splicing points, active connector, and quick connector) in an ODN link, IN and OUT ports of an optical splitter, OLT PON ports, and ONU PON ports.

- If the measurement point is the IN port of an optical component (such as the IN port of an optical splitter or the ONU PON port), remove the optical fiber of the measurement point and connect the optical fiber to the optical power meter.
- If the measurement point is the OUT port of an optical component (such as the OUT port of an optical splitter or the OLT PON port), remove the optical fiber of the measurement point and use the patch cord to connect the optical power meter to the measurement point.

The following figure shows measurement of the downstream optical power using an OLT PON port as an example.



Step 3 View and record the optical power read from the optical power meter.

NOTE

- If the values on the optical power meter change within a range of 0.2 dBm, use the average value.
- If the values on the optical power meter change in a range wider than 0.2 dBm, there is a possibility that the optical fiber is not properly connected, the optical fiber is excessively bent, or the optical fiber connector is unclean.
- Do not bend the optical fiber. A bent optical fiber may affect the test result.

Step 4 Remove the optical power meter after measurement and reconnect the optical line.

Step 5 Analyze the quality of the optical line. For details, see [5.6.3.1 Analyzing the Optical Power](#).

----End

5.6.4 Using the OTDR to Locate Abnormal Attenuation Points on the Optical Line

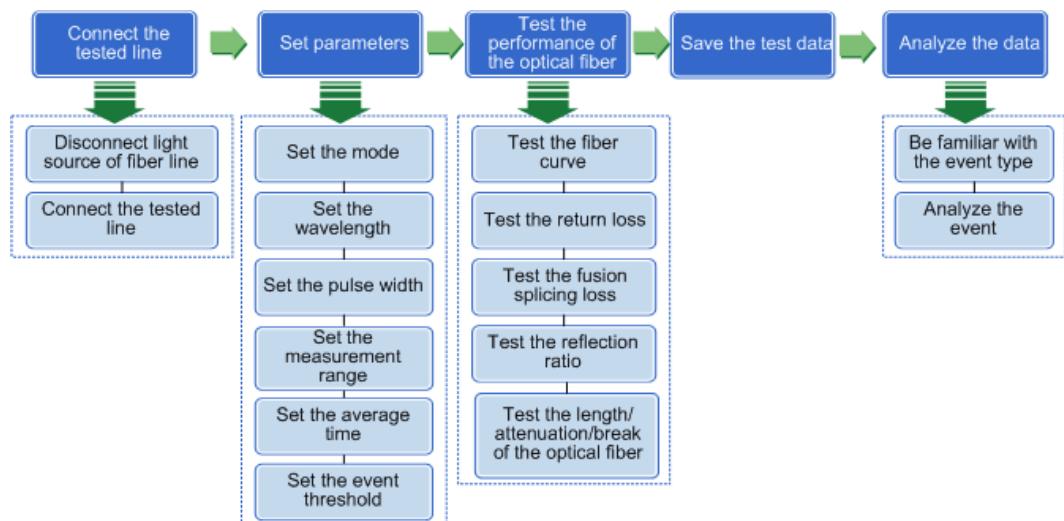
The optical time domain reflectometer (OTDR) is usually used for locating abnormal attenuation points on the optical line.

Concept

The OTDR is used to test parameters such as the optical fiber curve, return loss, fusion splicing loss, reflection ratio, and length/attenuation/break of the optical fiber on the cable line. The OTDR issues a laser pulse signal to the tested optical fiber, and receives the reflected optical signal on the optical port in certain intervals. Based on the optical power of the Rayleigh scattering and Fresnel reflection, the OTDR shows the signal trail of the whole optical fiber. In this way, the loss of different parts on the optical fiber and the fiber end position can be determined based on the test result.

Figure 5-33 shows the procedure for testing the performance (such as the loss) of the fiber line by using the OTDR.

Figure 5-33 OTDR test procedure



Rayleigh scattering

When the optical fiber is heated during manufacturing, thermal agitation causes uneven atom compression, which leads to uneven material density, and further leads to uneven refraction ratio. When the optical fiber is cooled, the unevenness is fixed and it arises optical scattering, which is called Rayleigh scattering. The Rayleigh scattering is an inherent feature of the optical fiber. Points that can generate Rayleigh scattering exist on the entire optical fiber and they are continuous.

Fresnel reflection

The Fresnel reflection generally occurs on discrete interfaces such as the connector and adapter. It is caused by air gap, misalignment or refraction mismatch. The Fresnel reflection is a discrete reflection and it is generated on some discrete points of the fiber. The reflection points generally include the fiber connector (at the gap between the glass and the air), smooth mirror cross section that blocks the optical fiber, and the fiber end.

OTDR dynamic range

The OTDR dynamic range is a physical quantity used to test the maximum capacity of events on the fiber line. It determines the longest fiber distance that the OTDR can measure. If the OTDR dynamic range is small and the tested optical fiber is with high loss, the remote end may be displayed as noise in the OTDR curve.

Deadzone

A deadzone is two events that are close to each other but still can be measured, namely, the resolution of two events. The deadzone of the OTDR is a certain range within which the OTDR curve cannot reflect the fiber line status due to the impact of Fresnel reflection. Attenuation deadzone is the part of OTDR trail whose measured data is covered by a strong reflection. Event deadzone is the minimum distance between two reflection events when they can still be distinguished. In this case, the distance between two events can be measured, but the loss of each of them cannot be measured.

Event

An event on the optical fiber is anything (apart from normal scattering of the optical material itself) that causes loss or reflection. The event includes all kinds of connections and damages (such as bends, cracks or breaks). An event can be reflective or non-reflective. A reflective event occurs when some pulse energy is reflected (for example on a connector), and it generates a peak signal on the trail. A non-reflective event occurs on the optical fiber at the part where some loss is generated but no reflection occurs, and it generates an angle on the trail.

Optical attenuation

The attenuation of the optical fiber is the power loss occurred when optical signals travel along the optical fiber. The unit of the attenuation (A) is dB, and the attenuation can be calculated using the following formula: $A = 10 \times \lg P_1/P_2$. In the formula, A is the attenuation, P₁ is the optical power of the input end, and P₂ is the optical power of the output end.

Impact on the System

Services carried on the optical line will be interrupted.

Precautions

- Select the OTDR whose test wavelength is the same as communication wavelength of the tested system.
- Select test instruments that are of good performance.
- Select the OTDR with a relatively large memory.

- Select the OTDR with USB port or network cable to facilitate data reading.
- Select the OTDR that is with a relatively long power supply duration and then prepare for power supplying.
- Do not replace the test instruments during the test to prevent great change of the test value.
- Record the parameter settings and test results of the instrument in detail during the test. After the test, collect and save the record data for reference in subsequent maintenance.
- Before storing the instruments, fully charge their batteries to extend the life cycle of the batteries. If the instruments are idle for a long time, charge and discharge the batteries at least once every three months.
- Clean the connector of an optical fiber after testing the optical power by referring to [5.6.6 Cleaning the Connector of an Optical Fiber](#). This is because if a contaminated optical fiber is connected to a functional optical fiber connector, the connector will be contaminated, which leads to abnormal attenuation and reflection and therefore affects the quality of the optical line.

NOTICE

Never look into the optical port or the connector of an optical fiber without eye protection. Never put the optical port towards the flammables.

Procedure

Step 1 Connect the tested line.

1. Disconnect the light source of the tested fiber line.
2. If the OTDR optical port does not match the connector of the tested optical fiber, prepare a 300-2000 m transitional patch cord, with one end matching the OTDR optical port and the other end matching the connector of the tested optical fiber.

 **NOTE**

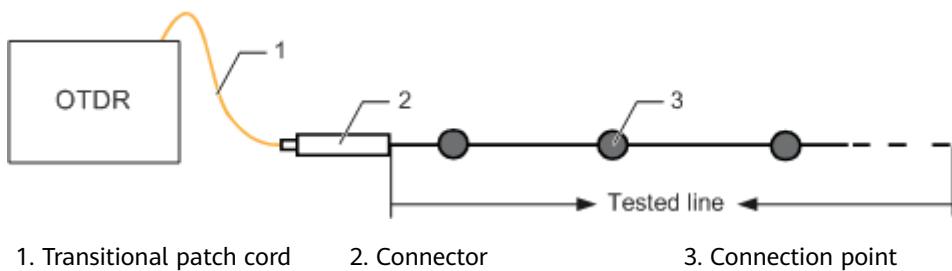
If the OTDR optical port matches the connector of the tested optical fiber, an additional 300-2000 m optical fiber can be used to process the deadzone and to test the insertion loss of the terminal connector. The additional optical fiber includes the following two types: the transmitting optical fiber and receiving optical fiber. The transmitting optical fiber is connected between the OTDR optical port and the connector of the tested optical fiber. It is used to cover the front deadzone so that the front part of the tested optical fiber is in the linear stable zone of the OTDR curve, and to measure the insertion loss of the front connector. The receiving optical fiber is connected to the end of the tested optical fiber. It is used to prevent the Fresnel reflection peak from affecting the measurement of the event that occurs close to the end of the tested optical fiber, and to measure the insertion loss of the rear connector.

3. Clean the OTDR optical port and the fiber connector by using alcohol.

 **NOTE**

Avoid other detergents or refractive index matching liquid that dissolve the adhesive in the fiber connector.

4. Connect the tested line, as shown in [Figure 5-34](#).

Figure 5-34 Connecting the tested line**Step 2** Set parameters.

1. Set the mode.

The following modes can be used as required: automatic, manual and fault locating.

NOTE

- The automatic mode is used in common tests.
- The manual mode is used in the following situations:
 1. The event point is determined and located incorrectly in a short-distance (within tens of meters) or ultra-long-distance test.
 2. Test results of the same optical fiber are different in different tests.
- The fault locating mode is used to fast locate obvious fault positions.

2. Set the wavelength.

Generally, the test wavelength is the same as the communication wavelength of the tested system. For example, if the system opens a wavelength of 1550 nm, the test wavelength must also be 1550 nm.

3. Set the pulse width.

The pulse width varies with the distance of the tested optical fiber. The shorter the distance, the smaller the pulse width. **Figure 5-35** shows reference values for setting the pulse width.

Figure 5-35 Reference values for setting the pulse width

	3 ns	30 ns	100 ns	300 ns	1 us	3 us	10 us	20 us
5 km								
10 km								
20 km								
40 km								
80 km								
140 km								
260 km								
380 km								

4. Set the measurement range.

The best measurement range is between 1.5 times and twice the length of the tested optical fiber.

NOTE

- In actual tests, perform the automatic test that is of the maximum measurement range first to locate the faulty section, and then select a proper measurement range that is larger than and closest to the tested distance. In this way, the accuracy of the OTDR is utilized sufficiently.
- Keep the measurement range twice the length of the tested optical fiber to prevent second reflection at the fiber end.
- If the measurement range is shorter than twice the length of the tested optical fiber, second reflection peak of the fiber end may occur on the even test curve, hence causing the ghost, which leads to a faint that the optical fiber line is faulty.

5. Set the average time.

Generally, the average time is around 30s. The recommended average time is 20s or 30s.

6. Set fiber parameters.

The refraction ratio n and backscattering coefficient η can be set based on the ratio and coefficient provided by the manufacturer. If the provided values cannot be obtained, use the default values of the instrument.

NOTE

- If different sections of optical fibers are of different refraction ratios, set the refraction ratio by section to reduce test errors caused by inaccurate settings.
- If the refraction ratio error is 0.001, the measured distance error can be 0.7 m/km.

7. Set the event threshold.

The setting of the event threshold depends on your interested events. **Table 5-21** lists reference values for setting the event threshold.

Table 5-21 Reference values for setting the event threshold

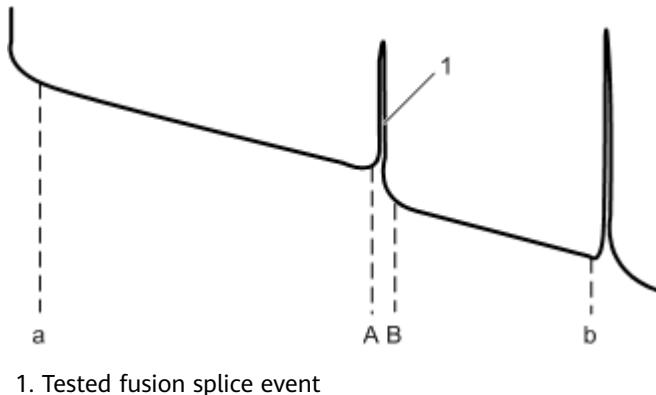
Threshold	Minimum Value (Unit: dB)	Default Value (Unit: dB)	Maximum Value (Unit: dB)
Fusion splicing point	0.01	All	1.99
Reflection	-98.00	All	-11.00
Fiber end	3.00	Automatic detection	20.00

Step 3 Test the performance of the optical fiber.

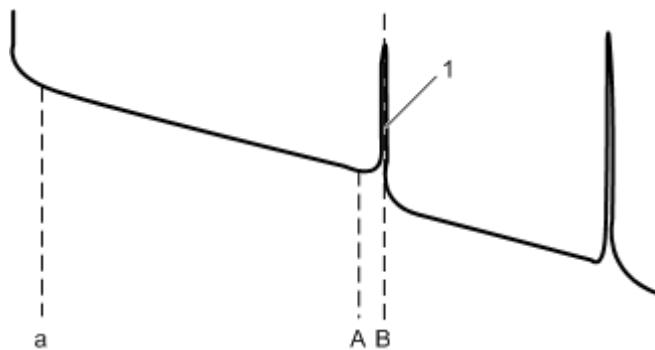
- Test the fiber curve.
 - a. Select **Start** to perform the test.
 - b. The test result is the fiber curve.
- Test the return loss.

- a. Enter the test interface after testing the fiber curve.
- b. Select **Return Loss**. Then two marking lines A and B are displayed on the interface.
- c. Move the marking lines A and B to delimit the area for testing the return loss.
- d. Select **Return Loss Test** to obtain the return loss of area A-B.
- Test the fusion splicing loss.
 - a. Enter the test interface after testing the fiber curve.
 - b. Select **4-pt SPL**. Then four marking lines a, A, B and b are displayed on the fiber curve.
 - c. Move marking lines a and A to the start point and end point of the linear area before the tested event respectively, and move marking lines B and b to the start point and end point of the linear area after the tested event respectively, as shown in [Figure 5-36](#).

[Figure 5-36](#) Setting the marking lines for a fusion splice event



- d. Select **Fusion Splicing Loss** and perform the test. The test result is the loss value of the fusion splice event.
- Test the reflection ratio.
 - a. Enter the test interface after testing the fiber curve.
 - b. Select **4-pt SPL**. Then three marking lines a, A and B are displayed on the fiber curve.
 - c. Move marking lines a and A to the start point and end point of the linear area before the tested event respectively, and move marking line B at the peek of the tested event, as shown in [Figure 5-37](#).

Figure 5-37 Setting the marking lines for a reflection event

- d. Select **Reflection Coefficient** and perform the test. The test result is the reflection ratio of the reflection event.
- Test the length/attenuation/break of the optical fiber.
 - a. Enter the interface of the event list after testing the fiber curve.
 - b. Check the length of the optical fiber displayed in the event list.
 - c. Check whether the fiber curve is consecutive. If the curve is consecutive, the optical fiber is not broken. Otherwise, the optical fiber is broken.
 - d. Check the attenuation of the optical fiber between two points by reading the vertical level difference between them directly from the fiber curve.

Step 4 Save the test data.

- Common saving mode of the test data includes the OTDR curve mode and figure mode.
- To save the test data using a USB disk, insert the USB disk directly into the USB port on the OTDR and then export the files.
- To save the test data using a network cable, connect the computer to the OTDR by using the network cable and then export the files.

Step 5 Analyze the data.

1. Check the trail whose vertical axis displays the optical power and horizontal axis displays the distance. The test trail shows the optical power of the return signal relative to the distance.

NOTE

- Normally, the slopes of each section (such as single or multiple spools of optical cables) on the entire curve are basically the same in an OTDR test.
- A greater slope in a section indicates a greater attenuation in it.
- If the entire curve is anomalous with large change of slopes or is bent or bracket-shaped, the quality of the optical fiber degrades severely.

2. Analyze the event.

[Figure 5-38](#) shows common events.

Figure 5-38 Common events

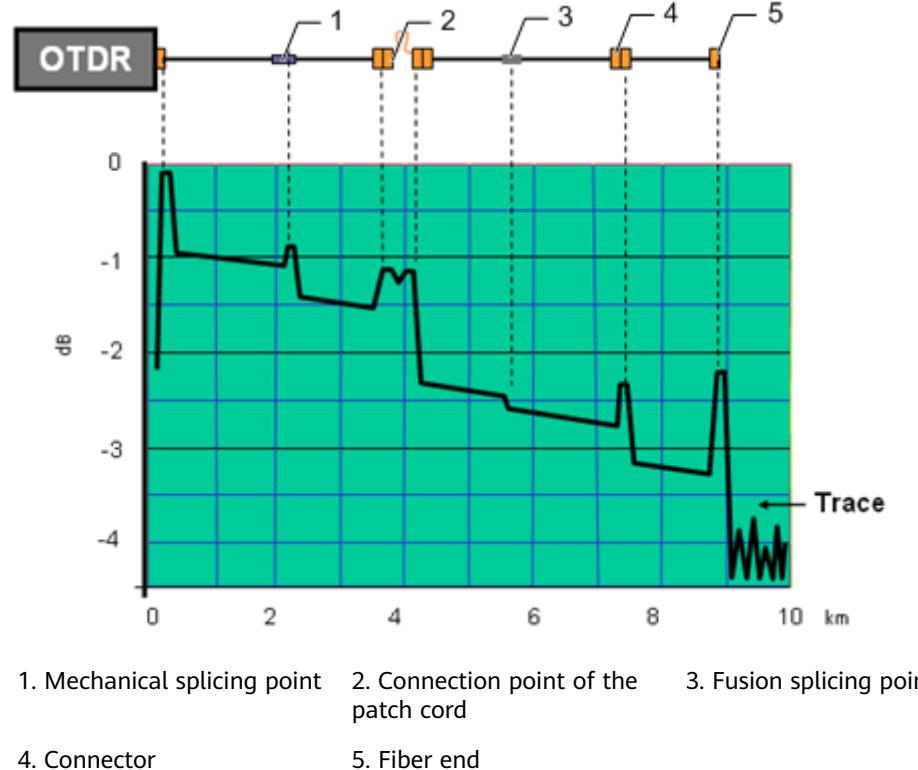
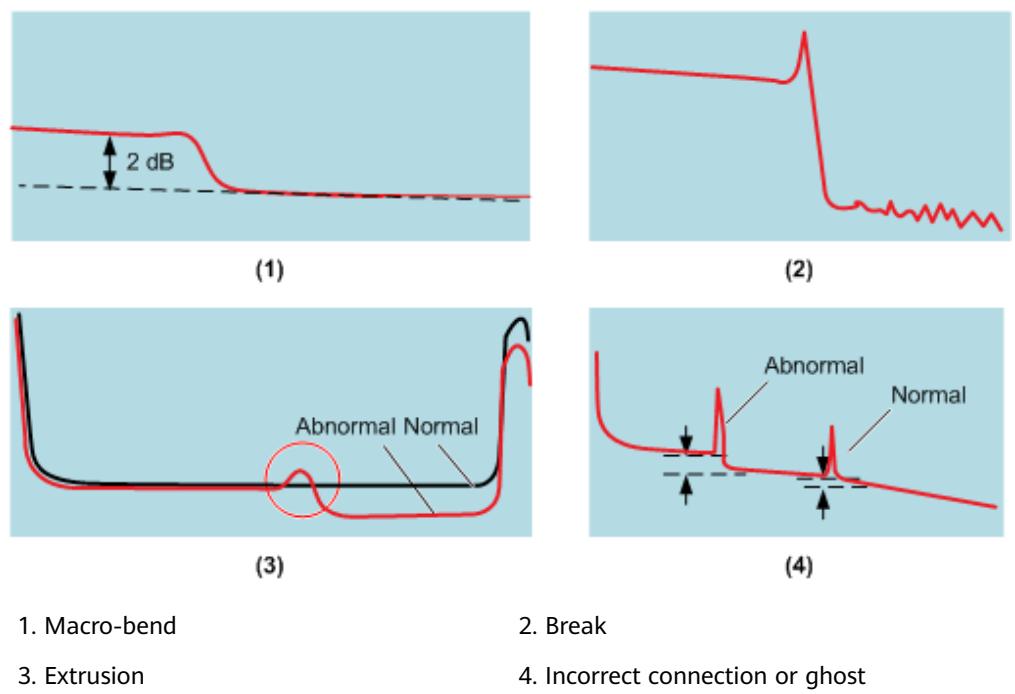


Figure 5-39 shows common curves of fiber faults.

Figure 5-39 Common curves of fiber faults



 NOTE

- **Ghost:** The position of the ghost is generally an integer multiple of the distance from a strong-reflection event to the instrument, and no loss occurs at the position. The ghost can be cleared by selecting a short pulse width or adding attenuation to the front part (such as the OTDR output end) of the strong-reflection even. If the event causing ghost occurs at the fiber end, make a small bending to increase the attenuation for the optical signal that reflects back to the start part.
- **Positive gain:** Some connectors are displayed as amplifiers, and the power level seems to be increased by certain gain. Positive gain is caused by the situation that more backscattering optical signals are reflected in the optical fiber after the fusion splicing point than the fiber before the fusion splicing point. Actually, the fusion splicing loss occurs at the fusion splicing point of the optical fiber. The actual loss can be obtained as follows: Perform multiple measurements from the other end opposite to the end where amplifiers are displayed to obtain the measured loss values of the fusion splicing point, and then calculate the average loss; the difference between the gain and the average loss is the actual loss of the fusion splicing point.
- **Fiber connection:** Main factors that affect cable safety are mechanical damages. An excessively large connection loss does not affect the connection intensity. Therefore, in the cases that some connecting loss values are excessively large with about 1% of them exceeding the standard value, and the values do not decrease after multiple re-connecting, the fiber connection can still be determined as qualified.

----End

5.6.5 Checking Whether the Optical Fiber Is Damaged Using the Red Pointer

The red pointer, also called visual fault locating meter or visual fault detector, sends red light to check whether the optical fiber has red light leak to locate the damage point of an optical fiber.

Context

You can directly see the position with red light leak by using the red pointer. For onsite observation, it can only be used for locating the damage point of an optical fiber in a short distance.

An optical fiber is generally damaged on the bare fiber, coiled fiber or fusion splicing point.

Precautions

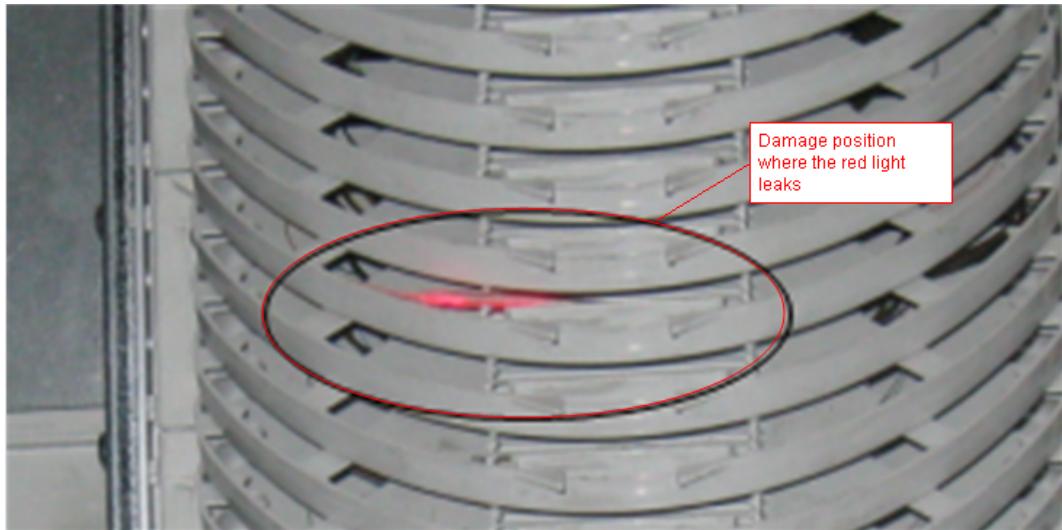
 DANGER

Never look directly into the optical fiber connector or the laser transmit port on the optical port board without eye protection. Never put the optical port towards the flammables.

Procedure

Step 1 Place the red pointer on the endface of an optical fiber and send red light.

Step 2 Check whether the optical fiber has red light leak. If the red light leaks, the fiber is damaged.



Step 3 Replace or re-splice the optical fiber that has red light leak.

- Replace the optical fiber if its bending is excessively large.

NOTE

The bending diameter of an optical fiber must be longer than 6 cm.

- Splice the optical fiber again if air bubbles exist at the splicing point.

----End

5.6.6 Cleaning the Connector of an Optical Fiber

This topic describes how to clean the connector of an optical fiber. Frequent insertion and removal or not taking dustproof treatment for a long time causes the connector to be unclean and deteriorated, which compromises the quality of the line. Therefore, you need to take measures to prevent dust and periodically clean optical fiber connectors, including the connector endface of an optical fiber, optical port of an optical module, and fiber adapter.

Prerequisites

Prepare the cleaning tools before cleaning, and follow the instructions in "Precautions".

Context

A large number of optical fiber connectors are used in optical transmission, which are easy to be contaminated in OM. The dust particles that can be seen by a microscope affect the quality of optical signals. As a result, the system performance deteriorates and network stability is affected. For two connected optical components, dust particles may damage the surface of the optical fiber. If the cladding or edge of an optical fiber has dust particles, the cores of two

connected optical fibers may not be exactly aligned. As a result, the quality of optical signals is affected.

A 1 μm dust particle on a single-mode optical fiber blocks 1% optical signals and therefore leads to 0.05 dB attenuation loss. A 9 μm dust particle is hard to be seen without a microscope but it completely blocks the core of an optical fiber. Therefore, even an extremely small contaminant that can only be found by an instrument such as a microscope may block the connector of an optical fiber. Besides dust particles, the following contaminants need to be cleaned away:

- Grease (usually brought by hands)
- Condensation residues
- Powder (evaporation residues of water or solvent)

Such contaminants will also damage optical components and are more difficult to clean away than dust particles. To clean optical components, you must follow the corresponding steps.

Tools and Materials

The following lists commonly used cleaning tools and materials:

- Optical power meter: used for testing whether the laser on the connector of an optical fiber is disabled.
- Lint-free wipe: a piece of long silk cotton specially used for cleaning the connector endfaces of an optical fiber.
- Lint-free swab: used for cleaning the optical port of an optical module, and a fiber adapter. It has two specifications: $\phi 2.5$ mm and $\phi 1.25$ mm. You can select one according to the port type (use the lint-free swab with $\phi 2.5$ mm for the ports of SC and FC types, and use that with $\phi 1.25$ mm for the ports of LC and MTRJ types).
- Protective cap: used on the connector of an optical fiber, optical port of an optical module, and fiber adapter.
- Cleaning tool box: used for placing lint-free wipes and protective caps. Place lint-free wipes and protective caps separately from other tools.
- Cleaning reagent (alcohol): used for cleaning the connector of an optical fiber. It is flammable and therefore must be safely stored and kept clean.
- Optical fiber endface magnifier: a microscope (400 \times) used for checking whether the connector endface of an optical fiber is clean and smooth.

Impact on the System

An optical module must be powered off before its port is cleaned. In this case, services carried on the optical port will be interrupted.

Precautions

DANGER

- Never look into the optical port or the connector of an optical fiber without eye protection. Never put an optical port towards the flammables.
 - Never clean an optical fiber connector when the laser is on.
 - ESD discharge damages the equipment. To remove or insert a pluggable optical module before or after cleaning, wear an ESD wrist strap or ESD gloves.
-
- Put a protective cap into the cleaning tool box immediately after taking it off. Place unused protective caps in the cleaning tool box, or in the ESD bag for sealed storage. Clean protective caps quarterly (it is recommended to clean them by using an ultrasonic cleaner).
 - Keep your hands clean and dry before cutting a lint-free wipe, and place unused lint-free wipes in the clean ESD bag or the cleaning tool box for sealed storage.
 - After the cleaning, cover the connector of the optical fiber, optical module, and fiber adapter that will not be immediately used with protective caps.

Procedure

- Clean the connector endface of an optical fiber.
 - a. Power off the laser of the connector before cleaning. Disconnect the optical fiber (at both ends) to be cleaned.
 - b. Use the optical power meter to test the optical power and ensure that no optical signals are sent from the connector of the optical fiber.
 - c. Clip a piece of lint-free wipe into 32 small pieces of the same size.
 - d. Use a dry lint-free wipe (two-layer) to wipe the connector endface of the optical fiber along one direction once. For a seriously contaminated connector, use a lint-free wipe (two-layer) dipped with a little cleaning reagent to wipe the connector endface of the optical fiber along one direction once, and then use a dry lint-free wipe (two-layer) to wipe it along one direction once again for ensuring that the connector endface is dry
-  NOTE
- A lint-free wipe can be used only once. Use the portion of the lint-free wipe that is not touched by your hands.
 - You can use the optical fiber end magnifier to check the cleaning and abrasion condition of an optical fiber connector.
- e. After the cleaning, do not touch the connector. Connect the optical fiber (at both ends) immediately. Cover the optical connectors that will not be immediately used with protective caps.
 - f. Power on the laser.
- Clean the optical port of an optical module.
 - a. Power off the laser of the optical module before cleaning. Disconnect the optical fiber (at both ends) from the optical module.

- b. Use the optical power meter to test the optical power and ensure that no optical signals are sent from the port of the optical module.
- c. Wear an ESD wrist strap or ESD gloves to remove a pluggable optical module.
- d. Select lint-free swabs with a suitable diameter according to the type of the optical port. Dip a swab with the cleaning reagent, insert the swab into the inside of the optical port, and then clean it by rotating the swab 360 degrees in one direction along the inner wall of the optical port.

 **NOTE**

The lint-free swab with $\phi 2.5$ mm is used for the ports of SC and FC types and that with $\phi 1.25$ mm is used for the ports of LC and MTRJ types.

- e. Insert a dry swab of the same type into the inside of the optical port and clean it by rotating the swab 360 degrees in one direction along the inner wall of the optical port.
 - f. After the cleaning, connect the optical fiber (at both ends). Cover the ports of the optical modules that will not be immediately used with protective caps. Wear an ESD wrist strap or ESD gloves to insert a pluggable optical module.
 - g. Power on the laser.
- Clean a fiber adapter.
 - a. Power off the laser of the optical port before cleaning. Disconnect the optical fiber (at both ends) from the fiber adapter.
 - b. Use the optical power meter to test the optical power and ensure that no optical signals are sent from the connector of the fiber adapter.
 - c. Select lint-free swabs with a suitable diameter according to the type of the fiber adapter. Dip a swab with the cleaning reagent, insert the swab into the socket inside the fiber adapter, and then clean it by rotating the swab 360 degrees in one direction along the inner wall of the fiber adapter.

 **NOTE**

The lint-free swab with $\phi 2.5$ mm is used for the ports of SC and FC types and that with $\phi 1.25$ mm is used for the ports of LC and MTRJ types.

- d. Insert a dry swab of the same type into the socket inside the fiber adapter and clean it by rotating the swab 360 degrees in one direction along the inner wall of the fiber adapter.

 **NOTE**

Use an ultrasonic cleaner to clean fiber adapters when there are a large quantity of them.

- e. After the cleaning, connect the optical fiber (at both ends). Cover the fiber adapters that will not be immediately used with protective caps.
- f. Power on the laser.

----End

5.7 Locating and Troubleshooting ONT Faults

This topic describes ONT-related alarms and how to locate and troubleshoot ONT faults.

5.7.1 ONT-Related Alarms

This topic describes ONT-related alarms.

Table 5-22 GPON ONT alarms

Fault	Related Alarms
The ONT is powered off.	0x2e11a00b The dying-gasp of GPON ONTi (DGi) is generated 0x2e11a001 The feeder fiber is broken or OLT can not receive any expected optical signals(LOS) 0x2e112007 The distribute fiber is broken or the OLT cannot receive expected optical signals from the ONT(LOSi/LOBi)
The ONT hardware is faulty.	0x2e112002 The loss of GEM channel delineation (LCDGi) occurs 0x2e112003 The signal degrade of ONTi (SDi) occurs 0x2e112004 The signal fail of ONTi (SFi) occurs 0x2e11a00c The loss of PLOAM of ONTi occurs(LOAMI/LOPCi) 0x2e11a00f The physical equipment error of ONTi (PEEi) occurs 0x2e112007 The distribute fiber is broken or the OLT cannot receive expected optical signals from the ONT(LOSi/LOBi) 0x2e11a107 The status of ONT's E1/T1 port is abnormal 0x2e313015 The hardware of the ONT is faulty
The ONT software is faulty.	0x2e21a102 The GPON ONT configuration recovery fails 0x2e11a00c The loss of PLOAM of ONTi occurs(LOAMI/LOPCi)

Fault	Related Alarms
The ONT internal interface is faulty.	0x2e313015 The hardware of the ONT is faulty
The ONT hardware self-check fails.	0x2e313015 The hardware of the ONT is faulty
The device connected to the E1/T1 port is faulty or the line between the device and the E1/T1 port is not connected properly.	0x2e11a107 The status of ONT's E1/T1 port is abnormal
The line of the ONT E1/T1 port is not connected properly.	0x2e11a107 The status of ONT's E1/T1 port is abnormal
The ONT software upgrade fails.	0x2e30a10e Fail to load the GPON ONT file
The mains supply of the ONT is unavailable.	0x2e313016 The ONT switches to the standby battery
The backup battery of the ONT is lost or is faulty.	0x2e313017 The standby battery of the ONT is lost
The backup battery of the ONT cannot be charged.	0x2e313018 The standby battery of the ONT cannot be charged
The voltage of the backup battery of the ONT is over low.	0x2e313019 The voltage of the standby battery of the ONT is too low
The ONT enclosure is open.	0x2e31301a The shell of the ONT is opened
There is a rogue ONT.	0x2e314021 There are illegal incursionary rogue ONTs under the port

5.7.2 Querying ONT Information

You can query ONT information such as the ONT status and traffic by running commands on the OLT, which helps locate an ONT fault remotely.

Table 5-23 Commands for querying information about a GPON ONT

Information	Command
Version	display ont version
Status and configurations	display ont info
Capability	display ont capability

Information	Command
Optical module	display ont optical-info
Real-time traffic of an Ethernet port	display ont traffic
Registration status of the ONT on the MG interface (H.248 protocol)	display ont mg status
Information about the IP address of the ONT	display ont ipconfig
Information about the WAN port of the ONT	display ont wan-info

5.7.3 Collecting ONT Performance Statistics

You can run commands on the OLT to set and query ONT performance statistics.

Table 5-24 Commands for collecting GPON ONT performance statistics

Function	Command
This command is used to query the performance statistics of an online ONT.	display ont statistics performance
This command is used to clear the performance statistics of an online ONT.	reset statistics ont
This command is used to query the line quality statistics of an online ONT.	display statistics ont-line-quality
This command is used to clear the line quality statistics of an online ONT.	reset statistics ont-line-quality

Function	Command
This command is used to query the discarded byte alarm statistics in a priority queue when the buffer on the ONT is overflowed.	display statistics ont-priority-queue
This command is used to clear the discarded byte alarm statistics in a priority queue when the buffer on the ONT is overflowed.	reset statistics ont-priority-queue
This command is used to query the performance statistics of an ETH port on an online ONT.	display statistics ont-eth
This command is used to clear the performance statistics of an ETH port on an online ONT.	reset statistics ont-eth
This command is used to query the performance statistics of an online ONT.	display statistics ont
This command is used to query relevant parameters of the performance statistics of an online ONT.	display statistics ont-performance
This command is used to query the performance statistics of an IPHOST port on an online ONT.	display statistics ont-iphost

Function	Command
This command is used to clear the performance statistics of an IPHOST port on an online ONT.	reset statistics ont-iphost
This command is used to query the performance statistics of a TDM port on an online ONT.	display statistics ont-tdm
This command is used to query real-time transfer protocol (RTP) and call control statistics of the SIP user on an online ONT.	display statistics ont-pots call
This command is used to query SIP agent and SIP call initiation statistics of the SIP user on an online ONT.	display statistics ont-pots sip
This command is used to configure the ONT statistics probe.	ont statistics probe
This command is used to query the ONT statistics probe.	display ont statistics probe
This command is used to clear statistics of the ONT statistics probe.	reset statistics ont-probe
This command is used to query statistics of the ONT statistics probe.	display statistics ont-probe

Function	Command
This command is used to query the performance statistics of an VDSL port on the ONT.	display statistics ont-vdsl display statistics performance ont-vdsl
This command is used to clear the performance statistics of an online ONT VDSL port.	reset statistics ont-vdsl

5.7.4 ONT Call Emulation

An ONT call emulation test uses a test module on an ONT to simulate call functions to verify basic voice services.

5.7.4.1 Introduction to ONT Call Emulation

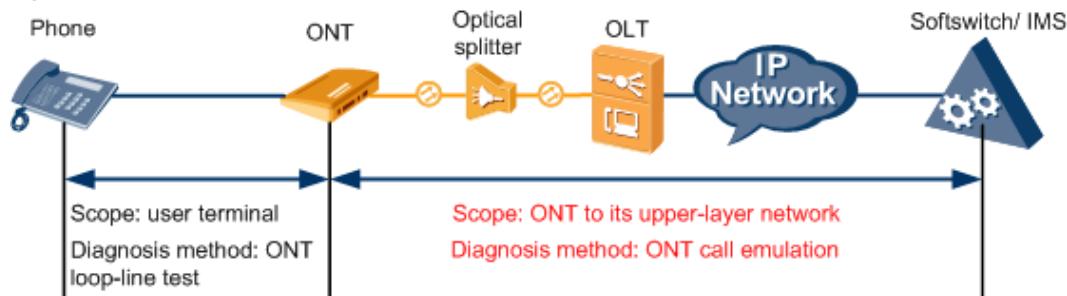
Benefits

ONT call emulation, also called ONT call emulation test, achieves the emulation of the caller and callee by simulating their actions on an ONT port. The actions on an ONT port include off-hook, on-hook, number dialing, ringing detection, and conversation. ONT call emulation is a method for testing the service functionality of POTS ports. Using ONT call emulation, the test personnel only need to start a call emulation test on the OLT CLI or the NMS at the maintenance center, and make calls using the test phone set at the maintenance center and the simulated terminal on the ONT to verify basic voice services.

ONT call emulation applies to acceptance tests during new deployments or fault diagnosis, which resolves the issues that would have been encountered if traditional methods are used. The following table lists these issues.

Application Scenario	Traditional Method	ONT Call Emulation
Acceptance tests during new deployments	A user submits an ONT service deployment application at a customer service center. If a fault occurs during service acceptance, fault diagnosis requires the user's cooperation or must be performed in the user's home, which brings high manpower costs and low acceptance efficiency.	Services are accepted remotely, reducing manpower costs and increasing acceptance efficiency.
Fault diagnosis	After receiving fault information reported from a user, the maintenance personnel cannot remotely and quickly determine the fault scope. Fault diagnosis requires the user's cooperation or must be performed in the user's home, which causes trouble for the user, brings high O&M costs, and decreases fault diagnosis efficiency. In addition, a large number of ONTs are geographically dispersed and remotely located. It is inconvenient to diagnose faults.	Faults are preliminarily diagnosed remotely, reducing O&M costs and increasing fault diagnosis efficiency.

When an ONT voice service fails, the [5.7.5 ONT Loop-Line Test](#) can be used together with ONT call emulation to diagnose faults, as shown in the following figure (the contents in red indicate ONT call emulation).



Function

ONT call emulation includes two emulation functions: caller emulation and callee emulation.

Function	Purpose
Caller emulation	Simulates the off-hook, number dialing, conversation, and on-hook of a caller on an ONT port.
Callee emulation	Simulates the off-hook, conversation, and on-hook of a callee on an ONT port. The ONT port automatically simulates off-hook after detecting ringing.

NOTE

The preceding table lists the ONT call emulation functions supported by the OLT. The NMS also supports automatic ONT call emulation. For the feature description and operations, see the delivered NMS manuals.

5.7.4.2 Principles of ONT Call Emulation

Caller Emulation

Caller emulation simulates the off-hook, number dialing, conversation, and on-hook of a caller on an ONT port. The following figure shows the flowchart for a caller emulation test.

Figure 5-40 Flowchart for a caller emulation test

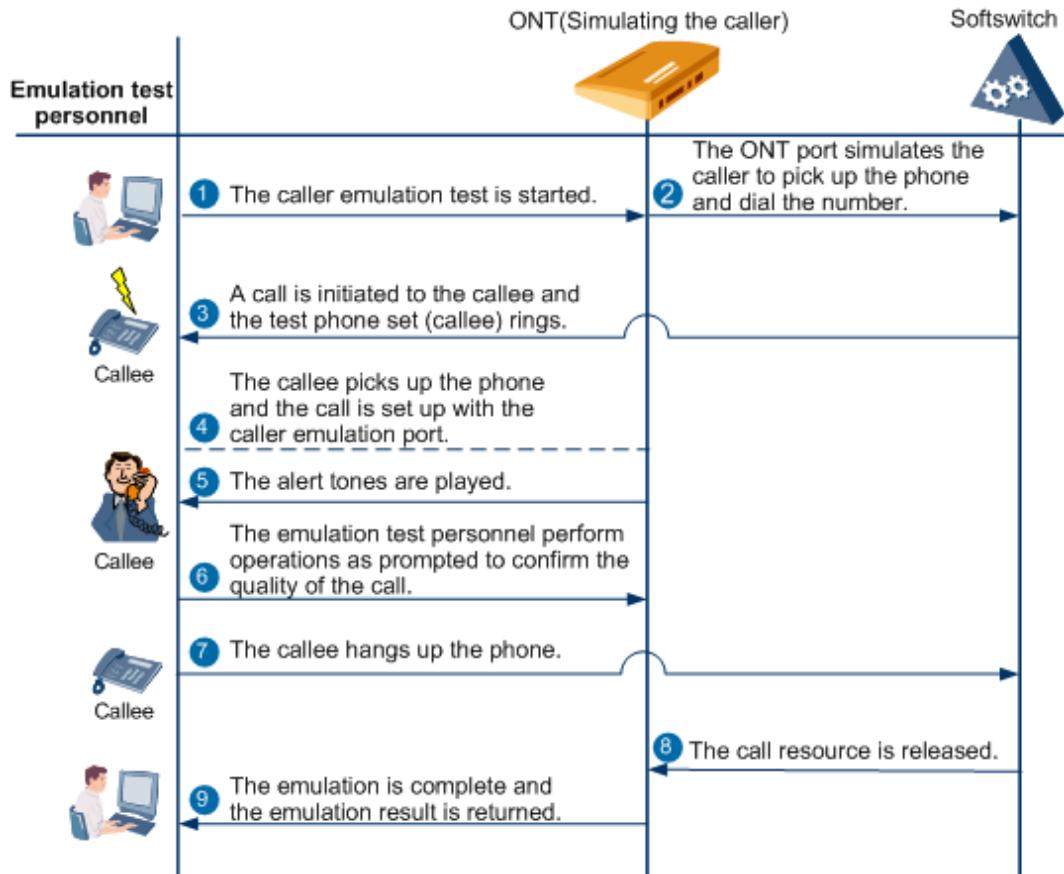


Table 5-25 Interactions in a caller emulation test

Step	Role	Description
1	Emulation test personnel	The emulation test personnel set an ONT POTS port as the caller emulation port on the OLT CLI or the NMS, configure the phone number to be dialed, and start a caller emulation test. It is recommended that the test phone set of the callee be located in the same place as the emulation test personnel.
2	ONT	The caller emulation port on the ONT is started, automatically simulates user off-hook, and dials the number of the callee.
3	Softswitch and test phone set of the callee	After receiving the message sent by the caller simulated on the ONT, the softswitch initiates a call and the test phone set of the callee rings. NOTE If the test phone set of the callee rings, the signaling channel is functioning and the user configuration data is correct. If the test phone set does not ring, the caller emulation fails. The emulation test personnel must check service data, such as route, VLAN, and core-network data, troubleshoot the voice fault if any, and perform the test again.
4	Emulation test personnel and ONT	The emulation test personnel pick up the phone. The call is set up.
5	ONT	The caller emulation port plays alert tones for the callee.
6	Emulation test personnel and ONT	After hearing the alert tones, the emulation test personnel dial the specified confirmation number, indicating that the media channel is functioning. Then the ONT matches the dialed number. (The confirmation number is a matched DTMF number, which is the pound key [#] by default. Retaining the default number is recommended.) NOTE If the emulation test personnel dial other numbers or do not dial any number after hearing the alert tones, the test result is "Voice channel is set up but the specified confirmation by key is not received."
7	Emulation test personnel	The callee hangs up the phone and an on-hook message is reported to the softswitch.
8	Softswitch	The softswitch releases the call resource.

Step	Role	Description
9	ONT, OLT/NMS	After the emulation is complete, the ONT reports the test result to the OLT. The OLT converts the test result into command lines, or into traps and reports the traps to the NMS.

Callee Emulation

Callee emulation simulates the off-hook, conversation, and on-hook of a callee on an ONT port. The ONT port automatically simulates off-hook after detecting ringing. The following figure shows the flowchart for a callee emulation test.

Figure 5-41 Flowchart for a callee emulation test

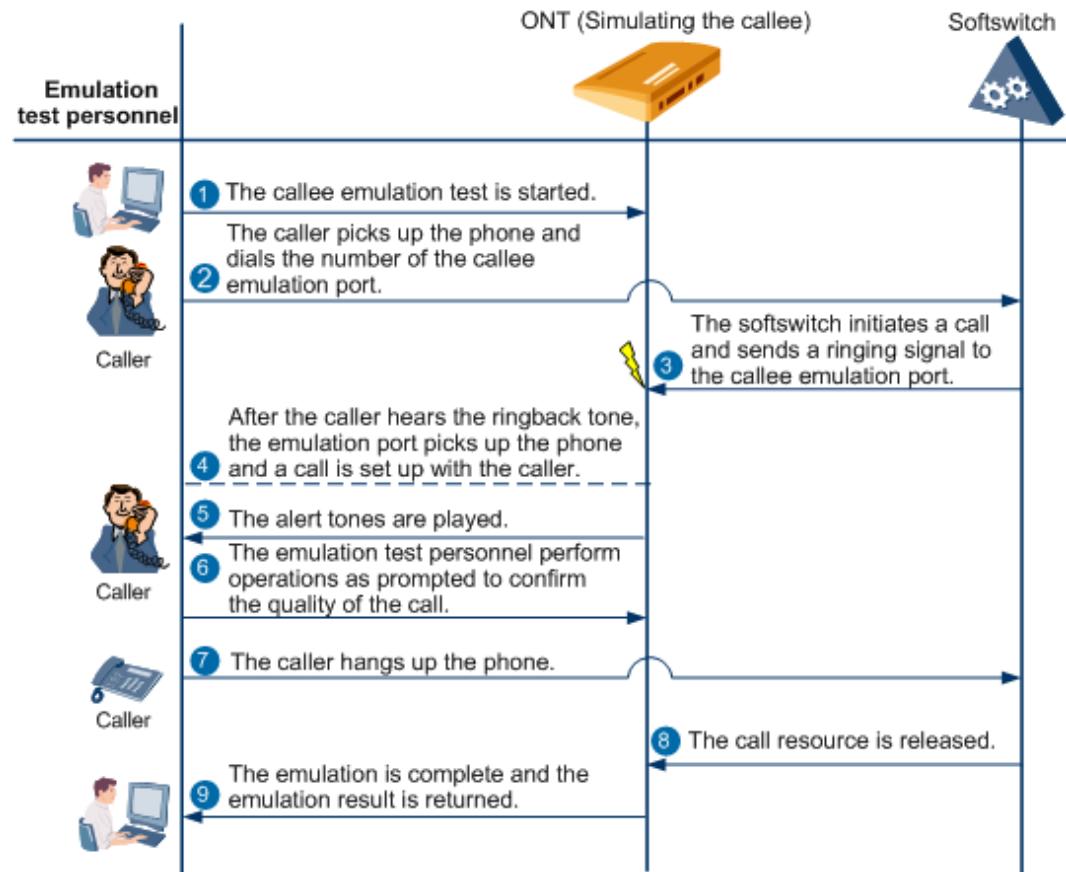


Table 5-26 Interactions in a callee emulation test

Step	Role	Description
1	Emulation test personnel	The emulation test personnel set an ONT POTS port as the callee emulation port on the OLT CLI or the NMS and start a callee emulation test.

Step	Role	Description
2	Emulation test personnel	The emulation test personnel pick up a phone and dial the number of the callee emulation port.
3	Softswitch	<p>After receiving the message sent by the caller, the softswitch initiates a call and sends a ringing signal to the callee emulation port.</p> <p>NOTE</p> <p>If the callee emulation port detects ringing current, the signaling channel is functioning and the user configuration data is correct. If the callee emulation port cannot detect ringing current, the callee emulation fails. The emulation test personnel must check service data, such as route, VLAN, and core-network data, troubleshoot the voice fault if any, and perform the test again.</p>
4	Emulation test personnel and ONT	<p>The callee emulation port simulates off-hook. The call is set up.</p> <p>NOTE</p> <p>If the caller hears ringback tones before the callee simulated on the callee emulation port picks up the phone, the signaling channel is functioning. If the caller cannot hear ringback tones, the callee emulation fails. The emulation test personnel must troubleshoot the signaling channel fault and perform the test again.</p>
5	ONT	The callee emulation port plays alert tones for the caller.
6	Emulation test personnel and ONT	<p>After hearing the alert tones, the emulation test personnel dial the specified confirmation number, indicating that the media channel is functioning. Then the ONT matches the dialed number. (The confirmation number is a matched DTMF number, which is the pound key [#] by default. Retaining the default number is recommended.)</p> <p>NOTE</p> <p>If the emulation test personnel dial other numbers or do not dial any number after hearing the alert tones, the test result is "Voice channel is set up but the specified confirmation by key is not received."</p>
7	Emulation test personnel	The caller hangs up the phone and an on-hook message is reported to the softswitch.
8	Softswitch	The softswitch releases the call resource.
9	ONT, OLT/NMS	After the emulation is complete, the ONT reports the test result to the OLT. The OLT converts the test result into command lines, or into traps and reports the traps to the NMS.

5.7.4.3 Configuring ONT Call Emulation

Prerequisites

- Only the OLTs and ONTs that support the protocols support ONT call emulation.
- Caller emulation and callee emulation require a test phone set. In default test mode, the quality of calls over media channels is determined through DTMF numbers. Therefore, it is recommended to use a test phone set that supports DTMF dialing.

Precaution

The phone set connected to an ONT call emulation port must be in the on-hook state or unconnected state during call emulation.

Impact on Services

- Caller and callee emulation:
 - A call emulation test simulates actual calls on the network, and billing records are generated for the simulated calls. There is no obvious difference between simulated calls and actual calls. Therefore, measures are required to avoid user misunderstanding. For example, filter the call detail records (CDRs) generated by emulation tests from the actual CDRs provided for users.
 - Services on a call emulation port are interrupted after a test is started on the port. Services will recover only after the test is finished on the port.
- Callee emulation:
 - On a port where a callee emulation test is started, the caller hears silence instead of the dial tone after picking up the phone.
 - After a callee emulation test is started on a port, the port will quit the callee emulation state 3 minutes later if no caller initiates a call to this port. When the port is in the callee emulation state, basic call services and other test services are interrupted on this port.

Procedure

- ONT caller emulation
 - a. The emulation test personnel run the **test** command to enter the test mode.
 - b. The emulation test personnel run the **ont emulational call** command to start an ONT caller emulation test.

```
huawei(config-test)#ont emulational call
{ callee-port<K>|caller-port<K> }:caller-port
{ frameid/slotid/portid<S><Length 5-15> }:0/2/0
{ ontid<U><0,1023> }:0
{ ont-potsid<U><1,255> }:1
{ telno<K> }:telno
{ telno-value<S><Length 1-16> }:12345603          //The number of the test phone set for
the callee is 12345603.
{ <cr>|caller-stop-time<K> }:caller-stop-time
{ caller-stop-time-value<U><60,300> }:60          //The caller emulation test duration is 60s.
```

Command:

ont emulational call caller-port 0/2/0 0 1 telno 12345603 caller-stop-time 60

 NOTE

- An ONT call emulation test is a special operation. After the test commands are executed, test results are returned only when the emulation test duration has elapsed. During the test, users can run the **display ont emulational call status** command to query the test status.
 - Generally, a call emulation test automatically terminates after the preset emulation test duration has elapsed. If you want to manually terminate a call emulation test before the preset duration elapses, run the **undo ont emulational call** command.
- c. The caller emulation port automatically dials the number of the callee's test phone set.
 - d. The callee picks up the phone after hearing ringing.
 - e. The callee hears alert tones and presses the pound key (#) for confirmation.
 - f. The OLT outputs the test result. The caller emulation test ends.

The following table lists the possible caller emulation test results.

Table 5-27 Caller emulation results

Emulation Result	Description
The test is successful.	<p>Basic voice services are running normally.</p> <ul style="list-style-type: none">● The service data, such as route, VLAN, and core-network data, is correct.● The link between the ONT and its upstream device is functioning normally.
Voice channel is set up but the specified confirmation by key is not received.	The signaling is normal, but the voice quality is poor or the emulation test personnel have not pressed the confirmation number after hearing alert tones.
Offhook message is reported but response is not received.	The caller's waiting for the off-hook response signaling has timed out. This result may occur only when H.248 is used. Check for: <ul style="list-style-type: none">● Incorrect service data, such as route, VLAN, and core-network data● Faults on the link between the ONT and its upstream device
Dial tone request is not received.	The caller's waiting for the dial tone signaling has timed out. This result may occur only when H.248 is used. Check for incorrect core-network data.
Reported number differs from dialed.	The digitmaps do not match. Check for incorrect digitmap configurations.

Emulation Result	Description
Ringback tone request is not received.	The caller's waiting for the ringback tone signaling has timed out. Check for: <ul style="list-style-type: none">Faults in the test phone set of the calleeIncorrect callee numberIncorrect core-network data
Callee no offhook.	The callee does not pick up the phone.
Voice channel is not set up or fails to be set up.	The voice channel is not correctly set up. Check for media channel faults.
Onhook message is reported but response is not received.	The call is not released properly. Check for core-network processing faults.

```
huawei(config-test)#
-----
F/S/P      : 0/2/0
ONT-ID     : 0
ONT-POTSID : 1
Test type   : caller emulational call test
Detected number : 12345603
Reported number : 12345603
Current status  : test end
Test Result    : success
-----
```

- ONT callee emulation
 - a. The emulation test personnel run the **test** command to enter the test mode.
 - b. The emulation test personnel run the **ont emulational call** command to start an ONT callee emulation test.

```
huawei(config-test)#ont emulational call
{ callee-port<K>|caller-port<K> }:callee-port
{ frameid/slotid/portid<S><Length 5-15> }:0/2/0
{ ontid<U><0,1023> }:0
{ ont-potsid<U><1,255> }:1
{ <cr>|callee-stop-time<K> }:callee-stop-time
{ callee-stop-time-value<U><60,300> }: 120          //The callee emulation test duration is 120s.

Command:
  ont emulational call callee-port 0/2/0 0 1 callee-stop-time 120
```

NOTE

- An ONT call emulation test is a special operation. After the test commands are executed, test results are returned only when the emulation test duration has elapsed. During the test, users can run the **display ont emulational call status** command to query the test status.
- Generally, a call emulation test automatically terminates after the preset emulation test duration has elapsed. If you want to manually terminate a call emulation test before the preset duration elapses, run the **undo ont emulational call** command.

- c. The caller uses the test phone set to dial the number of the callee emulation port.
- d. The callee emulation port automatically simulates off-hook after receiving ringing.
- e. The caller hears alert tones and presses the pound key (#) for confirmation.
- f. The OLT outputs the test result. The callee emulation test ends.

Table 5-28 Callee emulation results

Emulation Result	Description
The test is successful.	<p>Basic voice services are running normally.</p> <ul style="list-style-type: none">• The service data, such as route, VLAN, and core-network data, is correct.• The link between the ONT and its upstream device is functioning normally.
Voice channel is set up but the specified confirmation by key is not received.	The signaling is normal, but the voice quality is poor or the emulation test personnel have not pressed the confirmation number after hearing alert tones.
Offhook message is reported but response is not received.	The callee's waiting for the off-hook response signaling has timed out. This result may occur only when H.248 is used. Check for faults on the link between the ONT and its upstream device.
Ringing request is not received.	<p>The callee emulation port does not receive a call. Check for:</p> <ul style="list-style-type: none">• Abnormal caller voice service functions• Unreachability of the voice IP address of the callee• Abnormal signaling interactions
MG internal cause.	Check for an ONT port faults.

```
huawei(config-test)#
-----
F/S/P      : 0/2/0
ONT-ID     : 0
ONT-POTSID : 1
Test type   : callee emulational call test
Current status : test end
Test Result  : success
-----
```

----End

Follow-up Procedure

Determine whether basic ONT voice services are functioning based on the emulation test results. When an ONT voice service fails, the [5.7.5 ONT Loop-Line Test](#) can be used together with ONT call emulation to diagnose faults.

5.7.5 ONT Loop-Line Test

An ONT loop-line test checks the quality of the line between an ONT POTS port and a phone set. This test verifies whether the current, voltage, and phone connection of the line are normal.

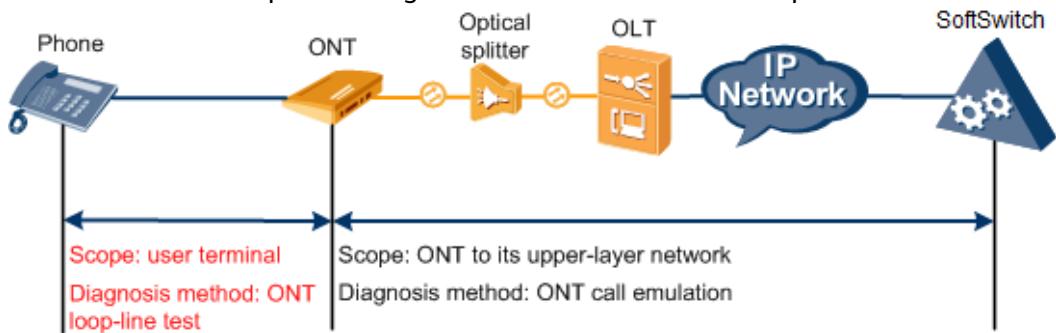
5.7.5.1 Introduction to ONT Loop Test

Line maintenance is important for voice services. When service quality issues or call failures occur before or after service provisioning, the subscriber line needs to be tested to determine whether a fault occurs on the subscriber line or the device.

In FTTH scenarios, a large number of ONTs are geographically dispersed and remotely located. It is inconvenient and inefficient to perform acceptance tests during new deployment or diagnose faults during O&M, which brings high manpower costs.

An ONT loop-line test addresses these issues. An engineer can remotely start an ONT loop-line test in the OLT CLI or the NMS at the maintenance center and view test results. This test helps quickly and accurately check the quality of the line between an ONT POTS port and a phone set by verifying whether the current, voltage, and phone connection of the line are normal.

When an ONT voice service fails, [5.7.4 ONT Call Emulation](#) is another means that can be used together with the ONT loop-line test to diagnose faults. The contents in red shows the scope and diagnosis method of the ONT loop-line test.

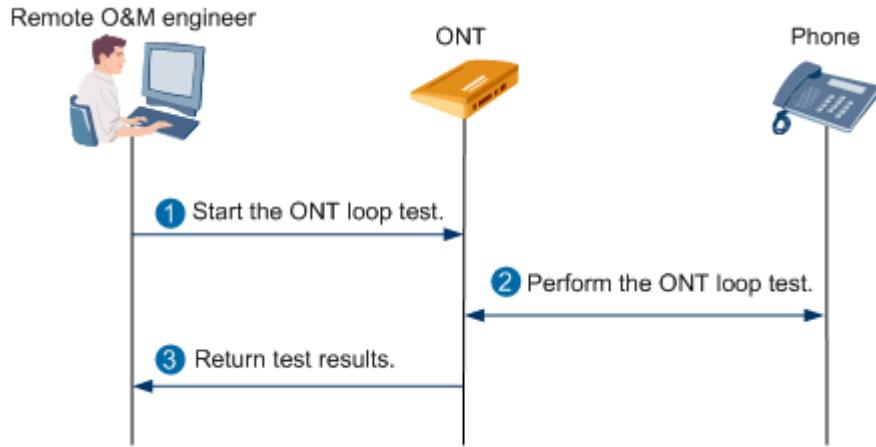


5.7.5.2 Principles of ONT Loop Test

An ONT loop-line test checks the quality of the line between an ONT POTS port and a phone set. This test verifies whether the current, voltage, and connected phone of the line are normal. In an ideal situation, lines are passive, inter-line insulation resistance is large, and inter-line capacitance is small. When the line conditions change (for example, water penetration) or the connecting point is faulty, the inter-line insulation resistance becomes small or the inter-line capacitance becomes large. Line quality deterioration finally leads to quality issues that users can be aware of. For example, a phone call fails or crosstalk or noise

exists in a call. The following figure shows how an ONT loop-line test is performed.

Figure 5-42 Process of performing an ONT loop-line test



1. A remote maintenance engineer sets a loop-line test for an ONT POTS port in the OLT CLI or the NMS.

 **NOTE**

The following two test options are available:

- **all-MLT**: indicates that the test covers all mechanized loop testing (MLT) items defined in the Optical Network Terminal Management and Control Interface (OMCI) protocol.
- **subscriber-line**: indicates the test covers loop-line test items in Huawei-defined OMCI extension protocol.

2. The ONT starts the loop-line test on the POTS port.
3. After the test is complete, the ONT reports the test results to the OLT. The OLT converts the test results into command output in the CLI, or into traps and reports the traps to the NMS.

5.7.5.3 Configuring ONT Loop Test

Prerequisites

The ONT subscriber-line test is supported by using the matched OLT and ONT. The ONT V100R003C00, V100R003C01, and later versions support ONT subscriber-line test.

Precaution

The phone set connected to an ONT loop test port must be in the on-hook state or unconnected state during call emulation.

Procedure

Step 1 Run the **test** command to enter the test mode.

Step 2 (Optional) Run the **ont pots-test-threshold set** command to set loop-line test thresholds for an ONT POTS port.

 **NOTE**

- It is recommended not to run this command but use the default values of the ONT.
- The **ont pots-test-threshold restore** command can be run to restore the loop-line test thresholds to the defaults for the ONT POTS port.
- The **display ont pots-test-threshold** command can be run to query the loop-line test thresholds of the ONT POTS port.

Step 3 Run the **ont pots-test** command to start the ONT loop-line test, and view the test results in the command output. The command output includes the test conclusion and the values of test items.

You can select the **all-MLT** or **subscriber-line** loop-line test based on site requirements. The following table lists test conclusions and test items of each type of test.

 **NOTE**

The loop-line test interrupts the services carried on the tested port.

Item	Description
Test Conclusion	<ul style="list-style-type: none">• Normal• AC current abnormal• DC current abnormal• Loop current abnormal• Loop resistance abnormal• Insulating resistance abnormal• Capacitance abnormal• Impedance abnormal• Insulating abnormal• Broken lines• Line mixing• Connected to ground• AB Line reversal• Line leaking• Phone offhook• Time out• Failed

Item	Description
All-MLT loop-line test items	<ul style="list-style-type: none">• A->ground DC voltage• B->ground DC voltage• A->ground AC voltage• B->ground AC voltage• A->ground insulation resistance• B->ground insulation resistance• A->B insulation resistance
Subscriber-line loop-line test items	<ul style="list-style-type: none">• A->ground DC voltage• B->ground DC voltage• A->B DC voltage• A->ground AC voltage• B->ground AC voltage• A->B AC voltage• A->ground insulation resistance• B->ground insulation resistance• A->B insulation resistance• A->ground capacitance• B->ground capacitance• A->B capacitance

----End

Example

To start a loop-line test on POTS port 1 of ONT 0 connected to OLT port 0/2/0 and cancel the test if the port is busy, run the following commands:

```
huawei(config)#test
huawei(config-test)#ont pots-test
{ frameid/slotid/portid<S><Length 5-15> }:0/2/0
{ ontid<U><0,127> }:0
{ ont-potsid<U><1,255> }:1
{ testitem<K> }:testitem
{ all-MLT<K>|custom<K>|dial-tone<K>|EMF<K>|high-voltage<K>|off-hook<K>|resistance<K>|ringer<K>|self-test<K>|subscriber-line<K> }:subscriber-line
{ <cr>|busy<K> }:busy
{ cancel<K>|force<K> }:cancel

Command:
    ont pots-test 0/2/0 0 1 testitem subscriber-line busy cancel
under testing, Please wait.....
```

huawei(config-test)#

F/S/P	:0/2/0
ONT-ID	:0
ONT-POTSID	:1
Subscriber line test	:Normal

Test Items	Value	Unit
A->ground DC voltage	0.000	V
B->ground DC voltage	0.000	V
A->B DC voltage	0.000	V
A->ground AC voltage	0.000	Vrms
B->ground AC voltage	0.000	Vrms
A->B AC voltage	0.000	Vrms
A->ground insulation resistance	214.748	megohm
B->ground insulation resistance	214.748	megohm
A->B insulation resistance	214.748	megohm
A->ground capacitance	29.000	nF
B->ground capacitance	28.000	nF
A->B capacitance	1.102	uF

Follow-up Procedure

Determine whether the line between the ONT POTS port and the phone set is faulty based on the test results. When an ONT voice service fails, use [5.7.4 ONT Call Emulation](#) together with the ONT loop-line test to diagnose faults.

5.7.5.4 Reference Documents of ONT Loop Test

ITU-T G.984.4: ONT management and control interface specification

5.7.6 Pinging from an ONT Remotely

You can determine whether an ONT under a PON port is interconnected with a device at the network layer by pinging the IP address of the device from the ONT.

Prerequisites

- You have the operator authority or higher.
- The ONT is in the online state.

Precautions

- For a same ONT, do not ping the IP address of a device repeatedly before an ongoing ping operation times out.
- In type C scenario, the ONT whose Role is Protect (queried by running the display protect-group command) does not support the remote ping operation.

Procedure

- In GPON access, ping a device from an ONT as follows:
 - a. Run the **interface gpon** command to enter the GPON mode.
 - b. Run the **ont remote-ping** command to ping the IP address of a device from the ONT under a PON port to check whether the ONT is interconnected with the device at the network layer.

----End

5.7.7 Restoring Factory Defaults

You can run commands on the OLT to restore factory defaults for an ONT to rectify the ONT service failure caused by unauthorized configurations.

Prerequisites

- You have the operator authority or higher to the OLT.
- The ONT is in the online state.

Context

Some ONTs support the following operations for restoring factory defaults:

- Holding down the reset button on the ONT panel.
- Logging in to the Web page of the ONT and restoring factory defaults on the Web page.

Impact on the System

All services of the ONT are interrupted.

Precautions

NOTICE

Restoring factory defaults resets an ONT and all services of the ONT are interrupted. Therefore, exercise caution when performing this operation.

Procedure

- In GPON access mode, run the following commands on the OLT to restore factory defaults for an ONT:
 - a. Run the **interface gpon** command to enter the GPON mode.
 - b. Run the **ont factory-setting-restore** command to restore factory defaults for an ONT.

NOTE

When receiving the restoration command issued by the OLT, the ONT resets. In the restoration process, the ONT running status is **offline**. You can run the **display ont info** command to query the ONT status.

----End

5.7.8 Resetting an ONT

You can remotely reset an ONT by running commands on the OLT to make ONT configurations take effect or to resolve certain unexpected faults that occur on the ONT.

Prerequisites

- You have the operator authority or higher to the OLT.
- The ONT is in the online state.

Context

Some ONTs support the following local reset operations:

- Pressing the reset button on the ONT panel for a short while.
- Logging in to the Web page of the ONT and resetting the ONT on the Web page.

Impact on the System

All services of the ONT are interrupted.

Precautions

NOTICE

Resetting an ONT directly interrupts all its services. Therefore, exercise caution when performing this operation.

Procedure

- In GPON access mode, reset an ONT as follows:
 - a. Run the **interface gpon** command to enter the GPON mode.
 - b. Run the **ont reset** command to reset an ONT.

NOTE

When receiving the reset command issued by the OLT, the ONT resets. In the resetting process, the ONT running status is **offline**. You can run the **display ont info** command to query the ONT status.

----End

5.7.9 Detecting a Rogue ONT

A rogue ONT affects communication of the other ONTs under the same OLT. This topic describes how to locate and isolate a rogue ONT.

Context

PON uses time division multiplexing. Using this mechanism, an ONT sends packets to the upstream direction according to the time stamp allocated by an OLT. If an ONT sends optical signals when it is not allocated a time stamp, its optical signals conflict with optical signals sent by other ONTs. Such an ONT is called a rogue ONT.

There are many types of rogue ONTs. Based on the time of optical signal transmission, rogue ONTs can be classified as:

- Continuous-mode rogue ONTs: ONTs transmitting optical signals continuously.
- Irregular-mode rogue ONTs: ONTs transmitting optical signals in a period other than specified, such as at a premature time or in a prolonged period.

A rogue ONT has the following impacts on the system:

- If a rogue ONT is online, one or all of the other ONTs connected to the same PON port on the OLT go offline or go online and offline frequently.
- If a rogue ONT is not configured, the other ONTs that are not configured will fail to be automatically discovered.

There are two methods to resolve the rogue ONT issue: detecting a rogue ONT on an OLT and self-detecting a rogue ONT on an ONT.

- Detecting a rogue ONT on an OLT: Detect, locate and isolate rogue ONTs on the OLT. This method is mainly used to diagnose continuous-mode rogue ONTs. For irregular-mode rogue ONTs, you need to manually diagnose them one by one.
- Self-detecting a rogue ONT on an ONT: The ONT monitors the optical signal transmission of its optical module. When the ONT detects abnormal communication in the downstream direction or uncontrollable optical signal transmission in the upstream direction, the ONT disables the power supply in the Tx direction of the optical module.

NOTE

For self-detecting a rogue ONT on an ONT, optical modules on the ONT are required to support rogue ONT detection, and the power supply of ONT optical modules can be cut off independently. Once an ONT self-detects a rogue ONT, the OLT receives an LoS alarm, the indicator on the ONT turns to the status indicating a rogue ONT, and other ONTs can go online normally. In this case, you only need to replace the ONT by referring to [5.7.10 Replacing an ONT](#). The following will introduce the method of detecting a rogue ONT on an OLT, while the method of self-detecting a rogue ONT on an ONT will not be described here.

The continuous-mode rogue ONT detection includes automatic detection and manual detection.

- Automatic detection: you can run the **anti-rogueont autodetect** command to enable the function of automatically detecting continuous-mode rogue ONTs. When this function is enabled, the OLT will automatically detect, locate, and isolate continuous-mode rogue ONTs. When this function is disabled, the OLT only detects continuous-mode rogue ONTs but will not locate or isolate them.

NOTICE

During the locating process, all services of ONTs under a PON port will be interrupted. Therefore, it is recommended that you disable automatic detection (system default configuration).

- Manual detection: you can run the **anti-rogueont manual-detect** command to detect, locate, and isolate continuous-mode rogue ONTs under a port.

The function of automatic detecting continuous-mode rogue ONTs has the following limitations:

- The ONT does not need to support extended PLOAM messages for detecting a continuous-mode rogue ONT on the PON line. The system, however, can only determine whether a continuous-mode rogue ONT exists but cannot locate it.
- All ONTs connected to a PON port on the OLT must support Huawei-defined extended PLOAM messages for detecting a continuous-mode rogue ONT. Furthermore, optical signal transmission of the ONT optical modules must be controllable.

Procedure

- Step 1** If an ONT goes online and other ONTs connected to the same PON port go offline or go online and offline frequently, or the 0x2e314021 There are illegal

incursionary rogue ONTs under the port alarm is reported to the OLT, a rogue ONT may exist in the system. In this case, locate the rogue ONT according to the following steps.

 NOTE

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

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

 NOTE

When you detect a rogue ONT, if a type B protection group is configured on the port that is connected to the ONT to be detected, you need to run the **force-switch** command to forcibly switch the protection group and then detect the rogue ONT to ensure that protection group switching does not occur during rogue ONT detection. You can forcibly switch services to the work side for rogue ONT detection if you are not sure which backbone fiber functions properly. If the rogue ONT is not detected, forcibly switch services to the protect side for rogue ONT detection. Then, run the **undo force-switch** command to cancel forced protection group switching.

- If the 0x2e314022 The ONT is rogue ONT or 0x2e314021 There are illegal incursionary rogue ONTs under the port alarm is generated, a continuous-mode rogue ONT may exist. In this case, go to **Step 3**.
- If the 0x2e314022 The ONT is rogue ONT or 0x2e314021 There are illegal incursionary rogue ONTs under the port alarm is not generated, an irregular-mode rogue ONT may exist. In this case, go to **Step 4**.

Step 3 Handle the ONT according to the generated alarm.

- If the 0x2e314022 The ONT is rogue ONT alarm is generated, replace the ONT by seeing [5.7.10 Replacing an ONT](#). Then, go to **Step 7**.
- If the 0x2e314021 There are illegal incursionary rogue ONTs under the port alarm is generated, go to **Step 4**.

 NOTE

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

Step 4 Run the **ont reset** command or the **ont deactivate** command to reset or deactivate ONTs under the PON port one by one. Then, check whether other ONTs that encounter the fault (going offline or going online and offline repeatedly) can go online.

- If other ONTs that encounter the fault can go online, the ONT is a rogue ONT. In this case, replace the ONT by referring to [5.7.10 Replacing an ONT](#). Go to **Step 7**.
- If other ONTs that encounter the fault cannot go online, the ONT optical module may be damaged so that the rogue ONT fails to be reset or deactivated by running the command. In this case, go to **Step 5**.

Step 5 Locate a rogue ONT manually: On the optical splitter, remove upstream optical fibers of the ONTs one by one and check whether other ONTs that encounter the fault (going offline or going online and offline repeatedly) can go online.

 **NOTE**

You can determine whether a rogue ONT exists in the system by measuring the Tx optical power of the ONT. For details, see "Reference Information".

- If other ONTs that encounter the fault can go online, the ONT is a rogue ONT. In this case, replace the ONT by referring to [5.7.10 Replacing an ONT](#). Then, go to [Step 7](#).
- If other ONTs that encounter the fault cannot go online, the optical module may be damaged so that the rogue ONT fails to be reset or deactivated. In this case, go to [Step 6](#).

Step 6 Connect Technical Support.

Step 7 The fault is rectified.

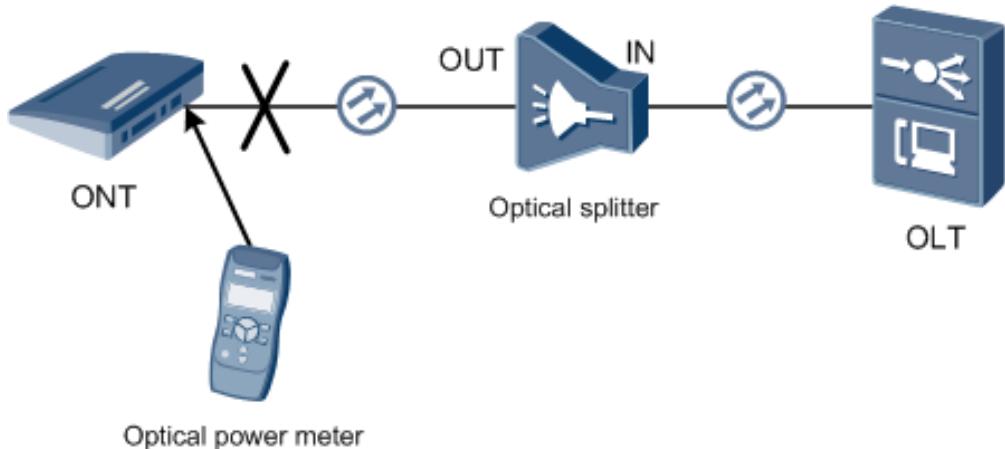
----End

Reference Information

To determine whether a rogue ONT exists in the system by measuring the Tx optical power of the ONT, perform the following operations:

1. Configure the measuring parameters of the optical power meter.
 - Optical power unit: dBm
 - Wavelength (nm): 1310
2. Record the status of the optical fiber connection.
3. Remove the optical fiber of the measurement point, and connect the optical power meter to the point to measure the optical power.
 - If the measurement point is the IN port of an optical component (such as the IN port of an optical splitter or a PON port of an ONT), remove the optical fiber of the measurement point and use a fiber patch cord to connect the optical power meter to the measurement point.
 - If the measurement point is the OUT port of an optical component (such as the OUT port of an optical splitter or a PON port of an OLT), remove the optical fiber of the measurement point and connect the optical fiber to the optical power meter.

The following figure describes how to measure the Tx optical power using an ONT PON port as a measure point.

Figure 5-43 Measuring the Tx optical power of an ONT PON port

4. Wait 10s and then read the value. Check the value on the optical power meter within 1 minute.
5. Insert the optical fiber removed in step 2 to restore the connection between the ONT and the OLT. Ensure that the connection status is the same as that recorded in step 2.
6. Check whether a rogue ONT exists according to the measurement result.
 - If no value is displayed on the optical power meter, no continuous-mode rogue ONT or irregular-mode rogue ONT exists at this measurement point.
 - If a value is displayed on the optical power meter, a continuous-mode rogue ONT exists at this measurement point.
 - If a value is displayed intermittently on the optical power meter, an irregular-mode rogue ONT exists at this measurement point.

5.7.10 Replacing an ONT

An ONT needs to be replaced if it is faulty or its hardware needs to be upgraded.

Prerequisites

The type of the ONT remains the same after the replacement.

Procedure

Step 1 Replace an ONT onsite.

1. Remove the optical fiber from the ONT and the cable from the port.
2. Replace the ONT. Then, connect the removed optical fiber and cable.
3. Log in to the ONT web page to configure the ONT information.
 - a. Modify the ONT authentication information.
 - If the ONT is authenticated by password, password+SN, LOID, or LOID+CHECKCODE, modify the password, LOID, or CHECKCODE of

the ONT and ensure that they are the same as those before the replacement.

- If the ONT is authenticated by SN, you do not need to modify its SN after the replacement.

 **NOTE**

Each ONU has unique SN, which is configured before factory delivery and cannot be changed.

- b. (Optional) Configure the ONT service data.

If the ONT service data such as the Wi-Fi authentication information is configured on the ONT web page, you need to configure such data again after the replacement.

 **NOTE**

If the NMS is used in the live network, you do not need to configure the service data again because the NMS will issue the original data.

Step 2 Log in to the OLT and modify the ONT authentication information.

Run the **ont modify (gpon)** command to change the SN so that the ONT authentication information configured on the OLT is the same as that on the ONT.

 **NOTE**

You can run the **display ont autofind** command to query the automatically discovered SN and then change the SN.

----End

5.8 Traffic Burst Detection

Traffic burst detection is a feature of identifying traffic burst points by deploying detection points on the network and detecting the traffic at the detection points to obtain traffic information.

5.8.1 Traffic Burst Detection Overview

In the high bandwidth era, traffic burst occurs irregularly in peak hours of network services, causing congestion or committed access rate (CAR)-triggered packet loss and affecting the performance of the end-to-end (E2E) network. Therefore, it is important to identify traffic burst points on the network.

Conventional detection methods are complex and time-consuming and do not apply to Gigabit Ethernet (GE)-level traffic burst.

Traffic burst detection enables you to easily monitor gigabit-level traffic burst on the E2E network and identify traffic burst points.

5.8.2 Traffic Burst Detection Principle

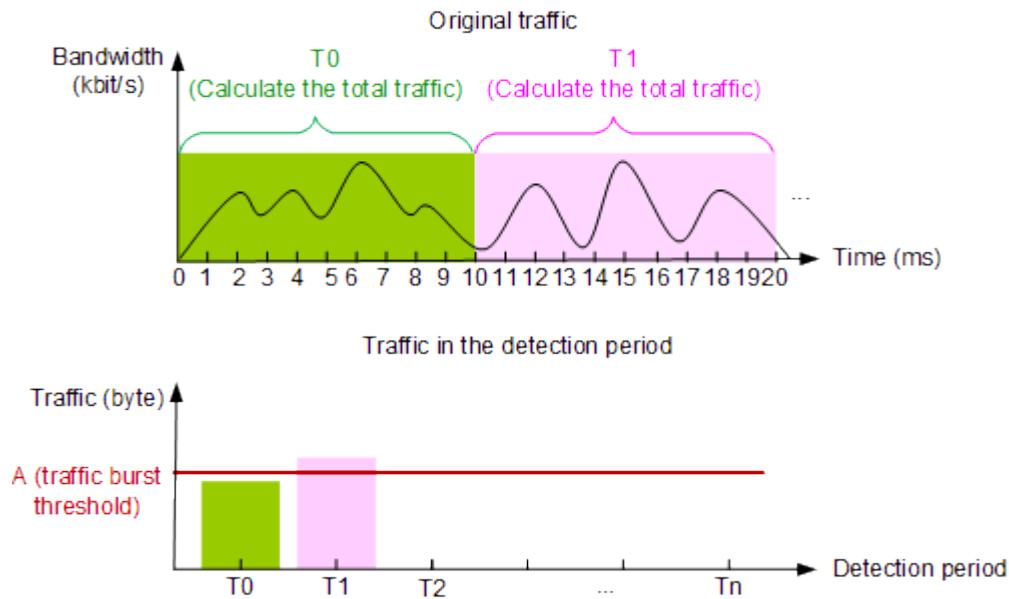
Traffic burst detection enables you to monitor traffic status in the detection period and determine whether traffic burst occurs in the detection period. Traffic burst detection can be performed based on either of the following factors:

- Periodic traffic
- Rate limitation threshold

Traffic Burst Detection Based on Periodic Traffic

Figure 1 shows the operating principle of traffic burst detection based on periodic traffic.

Figure 5-44 Operating principle of traffic burst detection based on periodic traffic



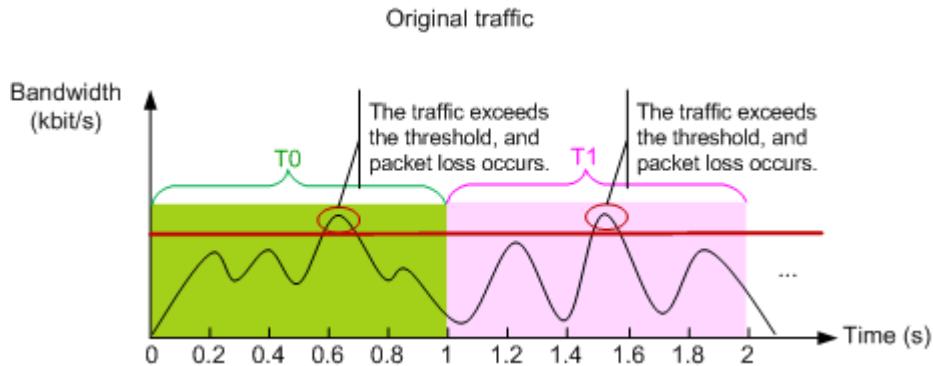
In this scenario, the traffic in each detection period (for example, $T = 10 \text{ ms}$) is calculated, and the system determines whether the traffic in each detection period exceeds the threshold.

- If the traffic in the detection period (for example, T_0) does not exceed the threshold, the system checks the traffic in the next detection period (for example, T_1).
- If the traffic in the detection period (for example, T_1) exceeds the threshold, the system generates a traffic burst record and checks the traffic in the next detection period (for example, T_2).

Traffic Burst Detection Based on the Rate Limitation Threshold

Figure 2 shows the operating principle of traffic burst detection based on the rate limitation threshold.

Figure 5-45 Operating principle of traffic burst detection based on the rate limitation threshold



In this scenario, a virtual rate limitation threshold (not actually taking effect) is set for the to-be-detected traffic. The system determines whether traffic burst occurs in each detection period (for example, $T = 1\text{s}$) based on whether virtual packet loss is identified.

- If no packet loss is identified, no traffic burst occurs, and the system checks the traffic in the next detection period.
- If packet loss is identified, traffic burst occurs, and the system generates a traffic burst record and checks the traffic in the next detection period.

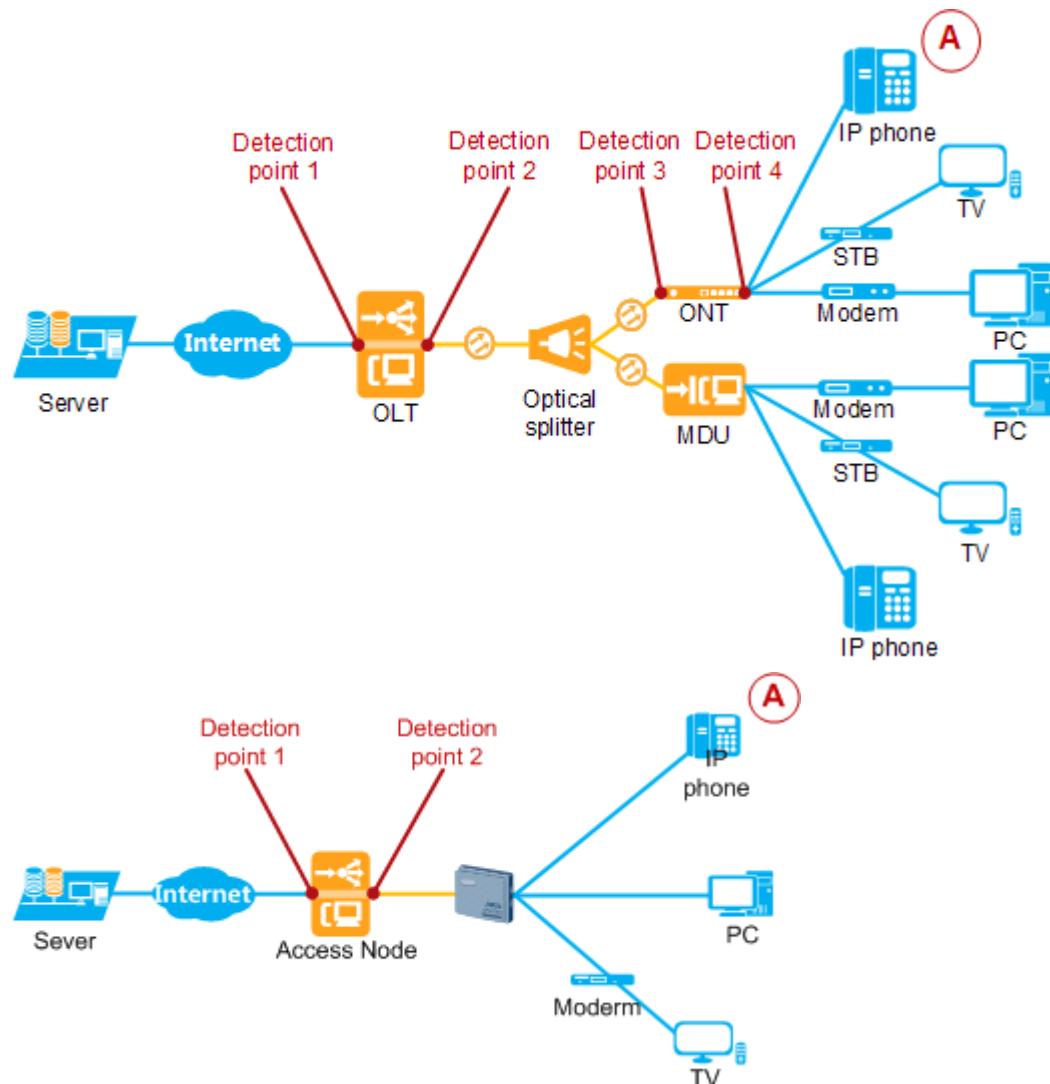
NOTE

In traffic burst detection based on the rate limitation threshold, the system determines only whether traffic burst occurs, but cannot identify the specific traffic burst value.

5.8.3 Traffic Burst Detection Application Scenario

Scenario Description

[Figure 1](#) shows the application scenario of traffic burst detection on the network.

Figure 5-46 Application scenario of traffic burst detection

Traffic burst detection is performed on different ports of the devices, to identify the traffic burst points on the network. **Table 1** describes the detection points and detection directions supported on the devices.

Table 5-29 Detection points and detection directions on different devices

Device	Detection Point	Detection Direction
OLT	Upstream port(Detection point 1)	Upstream and downstream
	User port(Detection point 2)	Upstream and downstream
ONT	WAN port (Detection point 3)	Upstream and downstream
	User port(Detection point 4)	Upstream and downstream

Table 5-30 Detection points and detection directions on different devices

Device	Detection Point	Detection Direction
Access Node	Upstream port(Detection point 1)	Upstream and downstream
	User port(Detection point 2)	Upstream and downstream

 NOTE

Traffic burst detection is not limited to specific structures of the upstream network of the optical line terminal (OLT) or the user network.

Detection Point Deployment

Scenario description: In the upstream direction, traffic burst occurs on an intermediate device, causing congestion- or committed access rate (CAR)-triggered packet loss on the device at point A.

Detection point deployment: Deploy detection points at the detection point 1 and detection point 2 and at the detection point 4, to identify the device where traffic burst occurs. Functions of the detection points are as follows:

- The detection point 1 is used to identify whether traffic burst occurs on the upstream network or occurs on the OLT and its downstream network.
- The detection point 2 is used to identify whether traffic burst occurs on the OLT and its upstream network or occurs on the ONT and its downstream network.
- The detection point 4 is used to identify whether traffic burst occurs on the ONT and its upstream network or occurs on the user network.

 NOTE

Traffic burst detection points in the egress direction of the ports do not cover queue scheduling. Traffic burst caused by queue scheduling in the egress direction can be identified only on the downstream device, instead of on this device.

5.8.4 Configure Traffic Burst Detection

Procedure

Step 1 Run the **traffic-burst-detect instance** command to configure traffic burst detection instances.

 NOTE

You can configure instances for the optical network terminal (ONT) after logging in to the optical line terminal (OLT).

- Step 2** Run the **traffic-burst-detect start** command to modify the start/end time of traffic burst detection instances.
- Step 3** During traffic burst detection, run the **traffic-burst-detect stop** command to stop the detection as required.
- Step 4** Query traffic burst detection instances.
- Run the **display traffic-burst-detect instance all** command to query all configured traffic burst detection instances in batches.
 - Run the **display traffic-burst-detect instance instance-id** command to query a single traffic burst detection instance.
- Step 5** Run the **display traffic-burst-detect result** command to query traffic burst detection records.
- Step 6** Run the **undo traffic-burst-detect** command to delete traffic burst detection instances.

 **NOTE**

In a service stream, delete the original traffic burst detection instance when you attempt to configure a new instance in the same direction at a port.

----End

Example

Provided that the service stream ID is 11 and a traffic burst detection instance needs to be configured at the downstream input port 0/9/0, detailed parameter settings are as follows:

- Access control list (ACL) rule ID of the service stream: 2000
 - ACL filtering rule ID of the service stream: 5
 - Traffic burst detection period (ms): 10
 - Traffic burst detection threshold (kbit/s): 1000
1. Configure the traffic burst detection instance.

```
huawei(config)#traffic-burst-detect instance 11
{ inbound<K>|outbound<K> }:inbound
{ ip-group<K>|ipv6<K>|link-group<K>|period<K>|user-group<K> }:ip-group
{ access-list-number2<U><2000,3999> }:2000
{ rule<K> }:rule
{ rule-id<U><0,4294967294> }:5
{ link-group<K>|period<K> }:period
{ period<U><1,100> }:1
{ threshold<K> }:threshold
{ threshold<U><64,10240000> }:1000
{ link-aggregation<K>|ont<K>|port<K>|protect-group<K> }:port
{ frameid/slotid/portid<S><Length 5-18> }:0/9/0
{ <cr>|detect-time<K>|from<K>|to<K> }:
```

Command:
traffic-burst-detect instance 11 inbound ip-group 2000 rule 5 period 10 threshold 1000 port 0/9/0
 2. Modify the start/end time of the traffic burst detection instance.

```
huawei(config)#traffic-burst-detect start instance 11
{<cr>|detect-time<K>|from<K>|to<K> }:from
{ time1<T><hh:mm:ss> }:10:03:10
{data1<D><yyyy-mm-dd> }: 2019-09-15
{<cr>|detect-time<K>|to<K> }:to
```

```
{ time2<T><hh:mm:ss>}:10:04:10
{data2<D><yyyy-mm-dd>}:2019-09-15
```

Command:
traffic-burst-detect start instance 11 from 10:03:10 2019-09-15 to 10:04:10 2019-09-15

3. Stop the traffic burst detection instance.

```
huawei(config)#traffic-burst-detect stop instance 11
```

4. Query traffic burst detection instances.

- Query all traffic burst detection instances.
huawei(config)#display traffic-burst-detect instance all

ID	Direction	F/S/P	ONT	ONT_PORT	Period	Threshold	state
					(ms)	(Kbps)	
11	inbound	0/9/0			--	10	1000 running

Note: The detection instance based on service-port.
The F/S/P contains the service flow ID.

- Query a single traffic burst detection instance.

```
huawei(config)#display traffic-burst-detect instance 11
```

```
Instance ID      : 11
Direction       : inbound
Position        : port 0/9/0
Period          : 10 ms
Threshold       : 1000 Kbit/s
State           : stopped
Start time      : 2019-09-15 10:03:10+08:00
End time        : 2019-09-15 10:04:10+08:00
ACL match information:
Matches: ACL 2000 rule 5
```

5. Query the traffic burst detection record.

```
huawei(config)#display traffic-burst-detect result instance 11
```

It will take some time, please wait...

```
Instance ID      : 11
Direction       : inbound
Position        : port 0/9/0
Period          : 10 ms
Threshold       : 1000 Kbit/s
State           : stopped
Start time      : 2019-09-15 10:03:10+08:00
End time        : 2019-09-15 10:04:10+08:00
ACL match information:
Matches: ACL 2000 rule 5
```

Total traffic burst records: 2

Time	Traffic BandWidth(Kbit/s)
2019-09-15 10:03:41.0 +08:00	-
2019-09-15 10:03:40.0 +08:00	-

6. Delete the traffic burst detection instance.

```
huawei(config)#undo traffic-burst-detect instance 11
```

5.9 Packet Loss Query

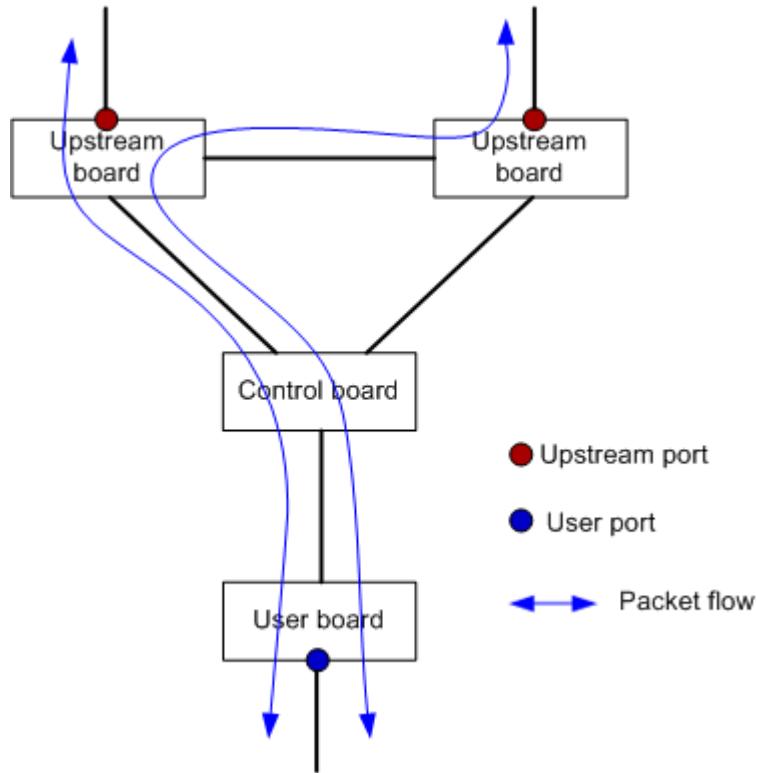
This topic describes how to locate service faults for PON users using the packet loss query commands. The MA5800 is applicable to many other networking scenarios, such as P2P networking, Ethernet convergence networking, and

Ethernet cascading networking. In these scenarios, you can use relevant packet loss query commands to locate faults by referring to this topic.

Context

For a PON user, the typical forwarding path involves the upstream boards, control board, and PON user boards as shown in [Figure 5-47](#).

Figure 5-47 Data forwarding structure for a PON user



Commands for querying packet loss vary with ports. A PON network involves the upstream ports and user ports as follows:

- Upstream ports on the MA5800 connect to upstream equipment, can be seen from outside, and are provided by the upstream boards or control board.
- User ports on the MA5800 connect to users, can be seen from outside, and are usually provided by user boards.

Procedure

Step 1 Collect the networking information.

Before locating a service fault for a PON user, make clear the networking and service configuration parameters of the user. Then, perform the packet loss query based on collected information.

- The networking information to be collected includes the type of the upstream port (uplink interface board port, or control board port), the type of user port (GPON or 10G GPON port).

- The configuration parameters to be collected include slot numbers of the upstream board, control board, and PON user board, upstream port number, PON port number, ONT ID, service port type, and service port ID related to the user.

Step 2 Query packet loss on an upstream port. Run the **display port statistics** command to query packet loss of the board providing the upstream port.

Upstream Port Type	Packet Loss Occurs or Not
<p>The upstream port is provided by the uplink interface board or control board.</p> <p>NOTE The uplink interface board does not support the forwarding function, which is provided by the control board in this case.</p>	<ul style="list-style-type: none">Yes. The packet loss occurs on the control board and the location ends.No. Go to the next step.

```
huawei(config-if-eth-0/19)#display port statistics
{ portid<U><0,7> }:0
{ <cr>||<K>|><K>|><K> }:

Command:
    display port statistics 0

Number of transmitted frames      : 0
Number of received frames        : 0
Total number of frames           : 0
Number of transmitted multicast frames : 0
Number of received multicast frames : 0
Total number of multicast frames  : 0
Number of transmitted broadcast frames : 0
Number of received broadcast frames : 0
Total number of broadcast frames  : 0
Number of transmitted unicast frames : 0
Number of received unicast frames : 0
Total number of unicast frames   : 0
Number of transmitted pause frames : 0
Number of received pause frames  : 0
Number of transmitted octets     : 0
Number of received octets       : 0
Total number of octets          : 0
Number of alignment error frames : 0
Number of discarded frames in the Tx direction : 0
Number of discarded frames in the Rx direction : 0
Total number of discarded frames : 0
Number of CRC error frames      : 0
Number of collision frames      : 0
Number of undersized frames     : 0
Number of oversized frames      : 0
Number of CRC error frames(less than 64 octets in length) : 0
Number of CRC error frames(oversized frames)   : 0
Number of frames(64 octets in length)  : 0
Number of frames(65~127 octets in length) : 0
Number of frames(128~255 octets in length) : 0
Number of frames(256~511 octets in length) : 0
Number of frames(512~1023 octets in length) : 0
Number of frames(1024~1518 octets in length) : 0
Number of frames(1519~2047 octets in length) : 0
Number of frames(2048~4095 octets in length) : 0
Number of frames(4096~9216 octets in length) : 0
Number of single collision frames : 0
//Packet loss statistics//
//Packet loss statistics//
//Packet loss statistics//
```

Number of multiple collision frames	: 0
Number of status change times	: 0
Number of transmitted green octets	: -
Number of transmitted green packets	: -
Number of discarded green packets due to congestion	: -
Number of transmitted yellow octets	: -
Number of transmitted yellow packets	: -
Number of discarded yellow packets due to congestion	: -
Number of transmitted CRC error frames	: 0
Number of received CRC error frames	: 0
Number of transmitted oversized frames	: 0
Number of received oversized frames	: 0
Number of transmitted undersized frames	: 0
Number of received undersized frames	: 0
Number of transmitted fragments	: 0
Number of received fragments	: 0
Number of transmitted jabbers	: 0
Number of received jabbers	: 0
Number of transmitted frames 64 octets	: 0
Number of received frames 64 octets	: 0
Number of transmitted frames 65 to 127 octets	: 0
Number of received frames 65 to 127 octets	: 0
Number of transmitted frames 128 to 255 octets	: 0
Number of received frames 128 to 255 octets	: 0
Number of transmitted frames 256 to 511 octets	: 0
Number of received frames 256 to 511 octets	: 0
Number of transmitted frames 512 to 1023 octets	: 0
Number of received frames 512 to 1023 octets	: 0
Number of transmitted frames 1024 to 1518 octets	: 0
Number of received frames 1024 to 1518 octets	: 0
Number of transmitted errors frames	: 0
Number of received errors frames	: 0

Step 3 Query packet loss on a PON port. Run the **display statistics gmac** command to query packet loss on the PON MAC chip, that is, the PON board.

```
huawei(diagnose)%%display statistics gmac 0/3 0
{ <cr>|ont<K>||<K>|><K> }:
  Command:
    display statistics gmac 0/3 0
  Received ETH frames      : -
  Received CRC error frames: -
  Received undersize frames: -
  Received oversize frames: -
  Received buffer overflow discarded frames: 0      //Packet loss statistics//
  Received TDM frames      : -
  Sent ETH frames          : 0
  Sent CRC error frames    : -
  Sent undersize frames    : -
  Sent oversize frames    : -
  Sent buffer overflow discarded frames: -      //Packet loss statistics//
  Sent TDM frames          : -
  -----
  PLOAM received notification count   : 19672
  PLOAM received CRC error count     : 476
  PLOAM sent inserted count         : 44394
  OMCI received frames              : -
  OMCI received discarded frames    : -      //Packet loss statistics//
  OMCI received notification count  : 234906
  OMCI sent frames                 : -
  OMCI sent inserted count         : 234722
  GEM received valid frames        : 234906
  GEM received invalid PORTID frames: 0
  GEM received HEC error count     : -
  GEM sent valid frames           : 234722
  -----
  ARB received ETH frames          : -
  ARB received discarded Ethernet frames: -      //Packet loss statistics//
  ARB received IDLE frames        : 3608290
  ARB sent ETH frames            : 0
```

HBUS received frames	: -
HBUS received bytes	: -
HBUS received frames length error count	: -
HBUS sent frames	: -
HBUS sent bytes	: -
HBUS sent discarded frames	: - //Packet loss statistics//
<hr/>	
PLOAM received SN count	: 9371
PLOAM received PEE count	: 0
PLOAM received PST count	: 0
PLOAM received REI count	: 0
PLOAM received ACK count	: 8379
PLOAM received password count	: 1920
PLOAM received dying gasp count	: 0
PLOAM received no message count	: 0
PLOAM received encryption key count	: 0
PLOAM received registration count	: -
PLOAM received sleep request count	: -
PLOAM sent upstream overhead count	: 3864
PLOAM sent assigned ONU-ID count	: 799
PLOAM sent ranging time count	: 799
PLOAM sent deactivate ONU-ID count	: 878
PLOAM sent disable SN count	: 5
PLOAM sent encrypted Port-ID count	: 946
PLOAM sent request password count	: 755
PLOAM sent assigned Alloc-ID count	: 294
PLOAM sent no message count	: 0
PLOAM sent POPUP count	: 0
PLOAM sent request key count	: 0
PLOAM sent configure Port-ID count	: 799
PLOAM sent PEE count	: 0
PLOAM sent PST count	: 0
PLOAM sent BER interval count	: 799
PLOAM sent key switching time count	: 0
PLOAM sent extended burst length count	: 3864
PLOAM sent change power level count	: 0
PLOAM sent profile count	: -
PLOAM sent request registration count	: -
PLOAM sent key control count	: -
PLOAM sent sleep allow count	: -
<hr/>	

Step 4 Connect Technical Support.

Step 5 The fault is rectified.

----End

Result

You can determine whether packet loss occurs on the current equipment using the previous steps. If packet loss occurs on the current equipment, you can locate the board where the packet loss occurs. However, the board where the packet loss occurs may be not faulty because packet loss may be caused by normal service processing. For example, if the downstream packets have CRC errors, the upstream board will discard them, which does not mean that the upstream board is faulty. In this case, the upstream equipment may be faulty. Another example, if the traffic of service packets sent upstream by a user exceeds bandwidth of the service port, logic chip of the PON board will discard excessive packets. In this case, the PON board is not faulty, but a fault may have occurred on the user side.

5.10 PPPoE Echo Packet Monitoring on the Upstream Port

PPPoE echo packet monitoring on the upstream port is mainly used to sense network faults and report corresponding events when PPPoE connections are online so that network faults can be quickly located.

Context

Originally, online PPPoE connections of the entire device can be monitored only after PITP is enabled and the online status can be obtained by querying UDM entries. Network faults cannot be sensed when PPPoE connections are online, which is difficult for fault locating.

Principle

In PPPoE echo packet monitoring on the upstream port, the number of PPPoE echo packets within the specified monitoring period are collected on the upstream port, the ratio of the statistics collected within this monitoring period to those collected in the last monitoring period is calculated, and then this calculated ratio is compared with the monitoring threshold. According to the compared result, the network status can be determined and the corresponding event is sent.

- If the compared result is smaller than the monitoring threshold, the system sends an event.
- If the compared result is greater than or equal to the monitoring threshold, the system does not perform any operations.

By default, PPPoE echo packet monitoring on the upstream port is disabled. To enable this function, the upstream port to be monitored, monitoring period, and monitoring threshold need to be specified.

The port adding for monitoring after this function is enabled will be monitored in the next monitoring period.

NOTE

This function can be used separately and does not need to be used together with PITP.

Procedure

- Step 1** Run the **monitor uplink-port pppoe enable** command to enable PPPoE echo packet monitoring on the upstream port.

```
huawei(config)#monitor uplink-port pppoe enable
```

- Step 2** Run the **monitor uplink-port pppoe port** command to add the upstream port for monitoring.

```
huawei(config)#monitor uplink-port pppoe port 0/18/0
```

- Step 3** Run the **monitor uplink-port pppoe period** command to configure the monitoring period.

```
huawei(config)#monitor uplink-port pppoe period 1
```

- Step 4** Run the **monitor uplink-port pppoe threshold** command to configure the monitoring threshold.

```
huawei(config)#monitor uplink-port pppoe threshold 60
```

- Step 5** Run the **display monitor uplink-port pppoe record** command to query monitoring records.

```
huawei#display monitor uplink-port pppoe record 0/9/0
{ all<K>|frameid/slotid/portid<S><Lenth 5-18>}:0/9/0
{ <cr>||<K>}:
```

Command:
display monitor uplink-port pppoe record 0/9/0

Port	Period	End Time	Echo Type	Last	Current
0/9/0	2018-01-20	12:01:01+08:00	Peak	-	660122
0/18/0	2018-01-20	11:56:01+08:00	Request	258475	0
			Reply	258475	0
		2018-01-20 10:40:00+08:00	Request	50053	0
			Reply	250269	0
		2018-01-20 10:39:01+08:00	Request	60009	50053
			Reply	300042	250269

- Step 6** Run the **monitor uplink-port pppoe disable** command to disable PPPoE echo packet monitoring on the upstream port.

```
huawei(config)#monitor uplink-port pppoe disable
```

----End

Result

If the number of PPPoE Request and Reply packets reduces in the preceding results, the network has faults.

6 GPON ONU Abnormal State

This topic describes how to troubleshoot common faults in ONU abnormal state, including ONU fail to go online, fail to recover ONU configurations, mismatch of ONU profile, fail to auto discover an ONU, and ONU frequently goes offline. ONU includes HG series ONT and MDU.

6.1 Failure to Go Online of a GPON ONU

A failure to go online is also called a registration failure. An ONU connected to a GPON port of an OLT fails to go online normally, but the queried **Run state** of the ONU is displayed as **offline** by running the **display ont info** command on the OLT.

6.2 Failure to Recover GPON ONU Configurations

An ONU connected to a GPON port of an OLT can go online successfully, but the queried **Config state** of the ONU is displayed as **failed** by running the **display ont info** command on the OLT.

6.3 GPON ONU Profile Match state is Mismatch

An ONU connected to a GPON port of an OLT can go online successfully, but the queried **Match state** of the ONU is displayed as **mismatch** by running the **display ont info** command on the OLT.

6.4 Failure to Auto Discover a GPON ONU

The ONU auto discovery failure is a fault in which an OLT fails to auto discover an ONU after the ONU is powered on.

6.5 GPON ONU Frequently Goes Online and Offline

ONUs connected to a GPON port frequently go online and offline and therefore the OLT reports a large number of ONU LOS alarms and relevant recovery alarms.

6.1 Failure to Go Online of a GPON ONU

A failure to go online is also called a registration failure. An ONU connected to a GPON port of an OLT fails to go online normally, but the queried **Run state** of the ONU is displayed as **offline** by running the **display ont info** command on the OLT.

6.1.1 Fault Identification and Demarcation

A failure to go online is also called a registration failure. An ONU connected to a GPON port of an OLT fails to go online normally, but the queried **Run state** of the ONU is displayed as **offline** by running the **display ont info** command on the OLT.

Context

Going online refers to a process that after being powered on, an ONU registers with an OLT and sets up a management channel with the OLT. An ONU can be managed by the OLT and be configured with services only after going online. You can check whether an ONU goes online by querying its **Run state** in the **display ont info** command output.

- **offline:** Indicates that the ONU is offline, which means that the ONU does not exist for the OLT.
- **online:** Indicates that the ONU is online.



You can also check whether an ONU goes online by observing its indicators. Indicator status varies with ONUs. For details, see the matched ONU manuals.

Location Method

When an ONU fails to go online, locate the fault based on the following fault symptoms and possible causes.

Fault Scope	Symptom	Possible Cause
OLT	A single ONU or some ONUs connected to an OLT fail to go online.	<ul style="list-style-type: none">• The SN or password configured on the OLT is different from the actual SN or password of the ONU; hence, the ONU fails to pass authentication and go online.• The actual distance between the ONU and OLT exceeds the ranging compensation distance configured on the OLT.• The OLT deactivates the ONU.
	All the ONUs connected to a PON port of an OLT fail to go online.	<ul style="list-style-type: none">• The laser on the PON port is disabled.• The pluggable optical module of the PON is faulty.• The PON port is faulty.
	All the ONUs connected to a board of an OLT fail to go online.	<ul style="list-style-type: none">• The board or the slot is faulty.

Fault Scope	Symptom	Possible Cause
ODN	The PON port reports alarms described in ODN-Related Alarms, including: <ul style="list-style-type: none">• 0x2e11a001 The feeder fiber is broken or OLT can not receive any expected optical signals(LOS)• 0x2e112007 The distribute fiber is broken or the OLT cannot receive expected optical signals from the ONT(LOSi/LOBi)	ODN failures are generally caused by large reflection and attenuation caused by improper optical components, design, or construction. For details, see Common ODN Faults . <ul style="list-style-type: none">• If a single ONU or multiple ONUs fail to go online, the branch fiber and the optical component may have faults.• If all ONUs fail to go online, the backbone fiber and the optical component may have faults.
ONU	A single ONU or some ONUs connected to an OLT fail to go online.	<ul style="list-style-type: none">• The ONU is not powered on.• The information (including SN and password) for ONU authentication conflicts; hence, the later power-on ONU fails to go online.• A rogue ONU exists on the network and affects other ONUs.• The ONU hardware is faulty.• The optical module of the ONU is faulty.• The patch cord of the ONU is broken or bent excessively.• The ONU is incorrectly connected to another PON port.

NOTICE

The parameters of the optical module in this topic comply with Class B+. Note that such parameters are slightly different from the parameters in Class C.

6.1.2 Alarming Handling

Procedure

Query the related alarms to locate the fault scope.

1. Run the **display alarm active alarmparameter frameid/slotid/portid** command to query OLT PON port alarms that are not cleared.
2. In GPON mode, run the **display ont alarm-state** command to query ONU alarms that are not cleared.
3. If an ONU can go online but fails to go online later, run the **display ont info** command to query its **Last down cause**.

If an ONU fails to go online, the following alarms may be generated:

Fault Scope	Alarms
ODN	<p>ODN-Related Alarms, including:</p> <ul style="list-style-type: none">• 0x2e11a001 The feeder fiber is broken or OLT can not receive any expected optical signals(LOS)• 0x2e112007 The distribute fiber is broken or the OLT cannot receive expected optical signals from the ONT(LOSi/LOBi)
ONU	<ul style="list-style-type: none">• 0x2e305015 The authentication information about the ONT is invalid• 0x2e314021 There are illegal incursionary rogue ONTs under the port• 0x2e314022 The ONT is rogue ONT• 0x2e11a00b The dying-gasp of GPON ONTi (DGi) is generated

6.1.3 OLT Fault

Procedure

Check for the possible causes on the OLT and troubleshoot the faults accordingly.

Possible Cause	Judgment Criterion	Troubleshooting Method
The SN configured on the OLT is different from the actual SN of the ONU; hence, the ONU fails to pass authentication and to go online.	Run the display ont info command to query the ONU information. It is found that the SN in the result is different from the actual ONU SN.	Run the ont modify command to modify the configured SN or password to be the correct one.

Possible Cause	Judgment Criterion	Troubleshooting Method
The actual distance between the ONU and OLT exceeds the ranging compensation distance configured on the OLT.	<p>Run the display port info command to query the minimum logical reach (Min distance) and maximum logical reach (Max distance) configured for the GPON port. It is found that the actual distance between the ONU and OLT exceeds the ranging compensation distance.</p> <p>For example, the actual length of the optical fiber between the ONU and OLT is about 25 km, which exceeds the ranging compensation distance of 0-20 km.</p>	<p>Run the port range command to adjust the minimum logical reach and maximum logical reach so that the actual distance between the ONU and OLT is within the ranging compensation distance.</p> <p>NOTE</p> <ul style="list-style-type: none"> • By default, the ranging compensation distance of a GPON port is from 0 km to 20 km. • According to Class B+, the maximum logical reach of a GPON port must not exceed 60 km, and the difference between the minimum logical reach and maximum logical reach must not exceed 20 km.
The OLT deactivates the ONU.	<p>Run the display ont info command to query the ONU information. It is found that Control flag is displayed as deactivated.</p>	<p>Run the ont activate command to activate an ONU.</p> <p>NOTE</p> <p>When an ONU is activated, its optical module only receives optical signals but does not transmit optical signals.</p>
The laser on the PON port is disabled.	<p>Run the display port info command to query the information about the PON port. It is found that Admin State is in the Off state.</p>	<p>Run the port laser-switch command to enable the laser on the PON port.</p> <p>NOTE</p> <p>By default, the laser on a GPON port is enabled.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
The PON port is faulty.	If either of the following two situations occurs, the PON port is faulty. <ul style="list-style-type: none"> Run the display port state command to query the status of the PON port. It is found that abnormal items exist in the query result. For example, the laser status (Laser state) is abnormal and the transmit optical power (TX power) exceeds the normal range (1.5-5.0 dBm). Migrate the service to another port. It is found that the ONU goes online normally. 	Replace the optical module of the PON port or replace the board.
The board or the slot is faulty.	All the ONUs connected to the board fail to go online.	Change the board to another slot. If the fault persist, replace the board.

6.1.4 ODN Fault

Procedure

Check for the possible causes on the ODN and troubleshoot the faults accordingly.

Possible Cause	Judgment Criterion	Troubleshooting Method
The optical fiber connector is not clean. NOTE An unclean optical fiber connector will cause excessive attenuation and abnormal reflection.	1. Test the backbone fiber and branch fiber by using the OTDR. It is found that the reflection and return loss are abnormal. 2. Check the optical fiber connector on site by using the optical fiber endface detector. It is found that the optical fiber connector is not clean.	Clean the optical fiber connector. For details about how to clean the connector, see Cleaning the Connector of an Optical Fiber .

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The optical fiber is bent excessively.</p> <p>NOTE Optical signals attenuate seriously on an optical fiber with an excessively small bending radius.</p>	<ol style="list-style-type: none"> Test the backbone fiber and branch fiber by using the OTDR. It is found that abnormal return loss points exist on the optical fiber. Check the optical fiber on site. It is found that the optical fiber is bent excessively. 	Route and bundle the optical fiber in a proper manner.
<p>The quality of optical fiber splicing is poor. For example, the splicing point has air bubbles.</p> <p>NOTE Poor optical fiber splicing leads to unstable transmission of optical signals. As a result, packet loss occurs.</p>	<ol style="list-style-type: none"> Test the backbone fiber and branch fiber by using the OTDR. It is found that abnormal return loss points exist on the optical fiber. Check the optical fiber splicing points by using the magnifying glass on site. It is found that the splicing points have quality problems, for example, air bubbles exist. 	Splice the optical fiber again.
<p>The optical fiber is not firmly connected or different types of optical fiber connectors are interconnected.</p> <p>NOTE If the optical fiber is not firmly connected or different types of optical fiber connectors are interconnected, the attenuation and reflection will be excessively large.</p>	<ol style="list-style-type: none"> Test the backbone fiber and branch fiber by using the OTDR. It is found that abnormal return loss points exist on the optical fiber. Check the optical fiber connectors on site. It is found that the optical fiber is not firmly connected or PC connector (blue) and APC connector (green) are interconnected. 	<ul style="list-style-type: none"> If the optical fiber is not firmly connected, reconnect the optical fiber firmly. If different types of optical fiber connectors are interconnected, replace the incompatible connector with a compatible one or replace relevant devices, such as the optical splitter. <p>NOTE In the scenario of the CATV service, it is recommended that you use APC connectors (green) only.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The multi-mode optical fiber is used as the backbone or branch optical fiber.</p> <p>NOTE If the multi-mode optical fiber is used as the backbone or branch optical fiber, the optical signal attenuates quickly and the return loss increases.</p>	<ol style="list-style-type: none"> Check the backbone fiber and branch fiber by using the OTDR. It is found that optical signals attenuate seriously. Check the optical path on site. It is found that the multi-mode optical fiber is used. The multi-mode optical fiber can be recognized by its physical features such as its color. 	Replace the multi-mode optical fiber with the single-mode optical fiber.
<p>The optical attenuation of the optical path is excessively small.</p> <p>NOTE</p> <ul style="list-style-type: none"> If the optical attenuation of the optical path is excessively small, the optical power received by the ONU will exceed the overload optical power of the ONU. Such a situation occurs usually in labs, where the OLT and ONU may be directly connected to each other through a short optical fiber. 	<p>If either of the following two situations occurs, the optical attenuation of the optical path is excessively small.</p> <ul style="list-style-type: none"> Measure the receive optical power of the ONU by using the optical power meter. It is found that the actual receive optical power of the ONU is greater than -8 dBm. Check the optical path between the OLT and ONU. It is found that the optical attenuation of the optical path is excessively small. The normal attenuation range is 10-25 dB. 	Add an optical attenuator on the optical path between the OLT and ONU.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The ODN is not properly planned.</p> <p>NOTE</p> <ul style="list-style-type: none"> • The split ratio of the ODN link is not determined by the number of ONTs connected but by the split ratio of optical splitters. When an optical splitter is connected to the ODN, attenuation occurs and the split ratio of the optical splitter needs to be calculated. • The differences between the OLT-received optical power from the two adjacent ONUs must be smaller than or equal to 15 dB. 	<p>The ODN does not meet the requirements of the ODN link plan or GPON Class B+.</p> <ul style="list-style-type: none"> • Three-level splitting exists in the ODN. • The network coverage of the ODN exceeds 20 km by far. • The split ratio exceeds the maximum split ratio that the board allows. Assuming that the maximum split ratio of a board is 1:64. If the first-level split ratio is 1:8 and the second-level split ratio is 1:16, the actual split ratio is 1:128, which exceeds the maximum split ratio of the board. • The optical attenuation difference of two optical paths exceeds 15 dB. 	Optimize the ODN to meet Huawei's ODN planning requirements and protocol requirements.
<p>The optical splitter is faulty or the connectors on the optical splitter are not clean.</p>	<p>Measure the input and output optical power of the optical splitter by using the optical power meter. It is found that the actual attenuation exceeds the theoretical attenuation.</p> <p>NOTE The faults in the optical splitter cannot be located by the OTDR because the OTDR cannot penetrate the optical splitter.</p>	Replace the faulty optical splitter or clean the connectors on the optical splitter.

Possible Cause	Judgment Criterion	Troubleshooting Method
A backbone fiber break occurs.	<ol style="list-style-type: none"> Check the backbone fiber by using the OTDR. It is found that a backbone fiber break occurs. Check the optical fiber on site. It is found that the optical fiber is broken or not connected. 	Reconnect the branch optical fiber.
A branch fiber break occurs.	<ol style="list-style-type: none"> Check the branch fiber by using the OTDR. It is found that a branch fiber break occurs. Check the optical fiber on site. It is found that the optical fiber is broken or not connected. 	Reconnect the branch optical fiber.

6.1.5 ONU Fault

Procedure

Check for the possible causes on the ONU and troubleshoot the faults accordingly.

Possible Cause	Judgment Criterion	Troubleshooting Method
The ONU is not powered on.	<p>If either of the following two situations occurs, the ONU is not powered on.</p> <ul style="list-style-type: none"> The 0x2e11a00b The dying-gasp of GPON ONTi (DGi) is generated alarm is generated on the OLT, but the corresponding recovery alarm is not generated. Check the power supply of the ONU. It is found that the power supply of the ONU fails or is turned off. 	Restore the power supply of the ONU.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>A rogue ONU exists on the network and affects other ONUs.</p> <p>NOTE If a rogue ONU exists, the ONU that fails to go online may be a normal one and the ONU that can go online may be a rogue one.</p>	<p>If either of the following two situations occurs, a rogue ONU exists.</p> <ul style="list-style-type: none"> • The 0xe314021 There are illegal incursionary rogue ONTs under the port alarm is generated on the OLT. • The 0xe314022 The ONT is rogue ONT alarm is generated on the OLT. • Remove the optical fiber from the OLT port and connect the optical fiber to the optical power meter for measurement. If a value can be read from the optical power meter, a continuous-mode ONU or irregular-mode ONU exists. <p>NOTICE Measuring the optical power interrupt services, Therefore, it is recommended that you measure the optical power when a PON port does not run any services, such as deployment.</p>	Replace the rogue ONU with a normal one.
<p>The information (SN) for ONU authentication conflicts; therefore, the power-on ONU fails to go online.</p>	<p>The 0xe10a10b The GPON ONT is discovered by the OLT alarm is generated on the OLT. The alarm cause is that the authentication information (such as the SN and password) about the newly connected ONU conflicts with that of the current ONU.</p>	Replace the ONU with conflicted SN.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The ONU is incorrectly connected to another PON port.</p> <p>NOTE After being configured on the OLT, the ONU can only be connected to the corresponding PON port. If being connected to another PON port, the ONU fails to go online.</p>	<p>The ONU is incorrectly connected to another PON port if either of the following symptoms occurs:</p> <ul style="list-style-type: none"> • The 0x2e10a10b The GPON ONT is discovered by the OLT event is generated on the OLT and the authentication information (such as the SN and password) about the ONU automatically discovered on the PON port is the same as that about the ONU connected to another PON port. • The 0x2e305015 The authentication information about the ONT is invalid event is generated on the OLT and the alarm cause is that the SN of the newly connected ONU is the same as that of the ONU configured. 	<p>Select one of the following two ways:</p> <ul style="list-style-type: none"> • Retain the connection between the ONU and the PON port. On the OLT, run the ont delete command to delete ONU configurations and then run the ont confirm command to confirm the ONU on the PON port that automatically discovers the ONU. • Retain the configurations. Connect the ONU to the PON port that is configured with the ONU.
The ONU hardware is faulty.	<p>If either of the following two situations occurs, the ONU hardware is faulty.</p> <ul style="list-style-type: none"> • The LEDs of the ONU are off when the ONU is powered on. • After the ONU is replaced with another ONU, the new ONU is auto discovered by the OLT. 	Replace the faulty ONU or the optical module of the ONU.

Possible Cause	Judgment Criterion	Troubleshooting Method
The optical module of the ONU is abnormal. For example, the transmit optical power of the optical module is excessively small or its receiver sensitivity is low.	Replace the faulty ONU with a normal one. It is found that the new ONU is auto discovered by the OLT. An alternative is to locate the fault as follows: <ul style="list-style-type: none">Set the optical module of the ONU to the continuous mode, and measure the transmit optical power by using the optical power meter. It is found that the actual transmit optical power is beyond the normal range (0.5 dBm to 5.0 dBm).Measure the receive optical power of the ONU by using the optical power meter. It is found that the actual receive optical power is within the normal range (-27 dBm to -8 dBm).	Replace the faulty ONU or the optical module of the ONU.
The patch cord of the ONU is broken or bent excessively.	Check the Patch cord of the ONU. It is found that the Patch cord is broken or bent excessively.	Replace the Patch cord of the ONU.

6.2 Failure to Recover GPON ONU Configurations

An ONU connected to a GPON port of an OLT can go online successfully, but the queried **Config state** of the ONU is displayed as **failed** by running the **display ont info** command on the OLT.

6.2.1 Fault Identification and Demarcation

An ONU connected to a GPON port of an OLT can go online successfully, but the queried **Config state** of the ONU is displayed as **failed** by running the **display ont info** command on the OLT.

Context

The ONU configuration status indicates whether the configuration restoration is enabled and whether the configuration restoration is complete. Configuration

recovery refers to a process in which, after an ONU goes online, the OLT issues configurations to the ONU and then the ONU adjusts its operating parameters based on the issued configurations.

The ONU configuration status has the following states: initial, normal, configuring (config), and configuration failure (failed). When an ONU goes online, the ONU is in the configuration restoration stage.

- The first status is initial. Soon the initial is complete and the ONU enters the config state.
- In the config state, the ONU capability and configuration data are restored. The duration of the config state is determined by the amount of the data configured on the ONU.
- If the configuration restoration is successful, the ONU transitions from the config state to the normal state.
- If the configuration restoration fails, the ONU transits from the config state to the failed state. Then the service is probably not carried forward.

Location Method

Fault Scope	Judgment Criterion	Possible Cause
OLT	ONUs of the same type fail to recover their configurations.	<ul style="list-style-type: none">• The configurations issued by the OLT mismatch the actual ONU capabilities.
ONU	A single ONU fails to recover its configurations.	<ul style="list-style-type: none">• The ONU functions improperly or is faulty.• The ONU has been configured at local and the configurations conflict with configurations issued by the OLT.

6.2.2 Alarming Handling

Procedure

When **Config state** of the ONU is displayed as **failed**, check whether the OLT generates the following alarm. If such an alarm is generated, clear it and check whether the fault is rectified.

0x2e21a102 The GPON ONT configuration recovery fails.

6.2.3 OLT Fault

Procedure

Check for the possible causes on the OLT and troubleshoot the faults accordingly.

Possible Cause	Judgment Criterion	Troubleshooting Method
The configurations issued by the OLT mismatch the actual ONU capabilities.	Check configurations issued to the ONU by the OLT. It is found that some configurations are not supported by the ONU. For example, the number of GEM ports exceeds the number supported by the ONU.	Modify OLT configurations based on actual ONU capabilities.

6.2.4 ONU Fault

Procedure

Check for the possible causes on the ONU and troubleshoot the faults accordingly.

Possible Cause	Judgment Criterion	Troubleshooting Method
The ONU has been configured at local and the configurations conflict with configurations issued by the OLT.	The management-related ONU configurations such as IP address and management mode are configured on the web page.	Delete the web page configurations and issue configurations to the ONU by the OLT.
The ONU functions improperly or is faulty.	Run the ont reset command to reset the ONU. It is found that the ONU fails to recover its configurations.	Replace the faulty ONU with a functional one.

6.3 GPON ONU Profile Match state is Mismatch

An ONU connected to a GPON port of an OLT can go online successfully, but the queried **Match state** of the ONU is displayed as **mismatch** by running the **display ont info** command on the OLT.

6.3.1 Fault Identification and Demarcation

An ONU connected to a GPON port of an OLT can go online successfully, but the queried **Match state** of the ONU is displayed as **mismatch** by running the **display ont info** command on the OLT.

Context

The ONU matching status indicates whether the actual ONU capability is the same as the service profile bound to the ONU. The status includes: initial, mismatch, and match. To some extent, the matching status is determined by the ONU running status and configuration status.

- The matching status of the ONU can be queried only when the ONU running status is online. The matching status is match when the actual hardware capability of ONU is the same as the ONU service profile bound with the ONU. Otherwise, the status is mismatch.
- In other configuration states, the matching status is initial.
- The ONU matching status does not affect the normal forwarding of the service flow, and only indicates whether the actual ONU capability is the same as the service profile bound to the ONU.

In practice, ONUs in the offline state are bulk pre-configured on the OLT to facilitate service provisioning. An ONU service profile and an ONU line profile are specified during such configurations. The ONU profiles together can be regarded as a virtual ONU. Subsequent services are configured based on this virtual ONU. Inconsistency between the capability set configured in the ONU profiles and the actual ONU capabilities involves the following two situations:

- The configured capability set outmatches the actual ONU capabilities. If the ONU is bound to such ONU profiles, ONU configurations will fail to match when the ONU goes online.
- The configured capability set undermatches the actual ONU capabilities. In this case, the ONU capabilities that are not covered by the ONU profiles will fail to be configured or applied.

Location Method

When the queried **Match state** of the ONU is displayed as **mismatch**, locate the fault according to the following procedure:

1. Check whether the capability set configured in the ONU service profile matches the actual ONU capabilities.

6.3.2 Fault of a Single ONU

Procedure

Run the **display ont capability** command to query the actual ONU capabilities. According to the data plan, modify the current ONU profiles, or bind matching ONU profiles to the ONU.

If this problem occurs on only one ONU, it is suggested to bind matching ONU profiles to the ONU.

- If the OLT works in the distributed mode:
 - a. Run the **display ont-profile** command to query the current ONU profiles that are configured on the OLT.
 - b. If the OLT does not have matching ONU profiles, run the **ont-profile add** command to add matching ONU profiles.

- c. Run the **ont modify** command to bind the ONU profiles to the ONU.
- If the OLT works in the profile mode:
 - a. Run the **display ont-srvprofile** command to query the information about the ONU service profile and run the **display ont-lineprofile** command to query the information about the ONU line profile.
 - b. If the OLT does not have matching ONU profiles, add matching ONU profiles by referring to **Configuring a GPON ONT Profile** in the *GPON Feature Guide*.
 - c. In the GPON mode of the OLT, run the **ont modify** command to bind the ONU profiles to the ONU.

6.3.3 Fault of All ONUs

Procedure

Run the **display ont capability** command to query the actual ONU capabilities. According to the data plan, modify the current ONU profiles, or bind matching ONU profiles to the ONU.

If this problem occurs on all the ONUs of the same type, the configurations of the ONU profiles may be incorrect.

- If the OLT works in the distributed mode, the profiles that are bound to the ONU cannot be modified or deleted. In this case, bind matching ONU profiles to the ONU.
- If the OLT works in the profile mode:
 - a. Run the **display ont-srvprofile** command to query the information about the ONU service profile and run the **display ont-lineprofile** command to query the information about the ONU line profile.
 - b. Modify the ONU profiles by referring to **Configuring a GPON ONT Profile** in the *GPON Feature Guide*.

6.4 Failure to Auto Discover a GPON ONU

The ONU auto discovery failure is a fault in which an OLT fails to auto discover an ONU after the ONU is powered on.

6.4.1 Fault Identification and Demarcation

The ONU auto discovery failure is a fault in which an OLT fails to auto discover an ONU after the ONU is powered on.

Location Method



The ONU auto discovery is a feature in which a pre-configured ONU automatically registers with an OLT after the ONU is powered on; if the OLT does not pre-configure the ONU, the ONU enters the auto discovery state and waits to be configured by the OLT.

When an OLT fails to auto discover an ONU, locate the fault based on the following fault symptoms and possible causes.

Fault Scope	Symptom	Possible Cause
OLT	A single ONU or some ONUs connected to an OLT fail to be auto discovered by the OLT.	The actual distance between the ONU and OLT exceeds the ranging compensation distance configured on the OLT.
	All the ONUs connected to a PON port on an OLT fail to be auto discovered by the OLT.	<ul style="list-style-type: none">• The ONU auto discovery function is disabled on the PON port.• The laser on the PON port is disabled.• The PON port is faulty.
	All the ONUs connected to a board on an OLT fail to be auto discovered by the OLT.	The board or the slot is faulty.
ODN	The PON port reports alarms described in ODN-Related Alarms, including 0x2e11a001 The feed fiber is broken or OLT can not receive any expected optical signals(LOS) and etc.	<p>ODN failures are generally caused by large reflection and attenuation caused by improper optical components, design, or construction. For details, see Common ODN Faults.</p> <ul style="list-style-type: none">• If a single ONU or multiple ONUs connected to an OLT fail to be auto discovered by the OLT, the branch fiber and the optical component may have faults.• If all ONUs connected to a PON port on an OLT fail to be auto discovered by the OLT, the backbone fiber and the optical component may have faults.
ONU	A single ONU or some ONUs connected to an OLT fail to be auto discovered by the OLT.	<ul style="list-style-type: none">• The ONU is not powered on.• A rogue ONU exists on the network and affects other ONUs.• The ONU hardware is faulty.• The optical module of the ONU is faulty.• The Patch cord of the ONU is broken or bent excessively.

NOTICE

The parameters of the optical module in this topic comply with Class B+. Note that such parameters are slightly different from the parameters in Class C.

6.4.2 OLT Fault

Procedure

Check for the possible causes on the OLT and troubleshoot the faults accordingly.

Possible Cause	Judgment Criterion	Troubleshooting Method
The ONU auto discovery function is disabled on the PON port.	Run the display port info command to query the information about the PON port. It is found that Autofind is in the Disable state.	Run the port ont-auto-find command to enable the auto discovery function of the PON port. NOTE By default, the ONU auto discovery function is disabled on a PON port.
The actual distance between the ONU and OLT exceeds the ranging compensation distance configured on the OLT.	Run the display port info command to query the minimum logical reach (Min distance) and maximum logical reach (Max distance) configured for the PON port. It is found that the actual distance between the ONU and OLT exceeds the ranging compensation distance. For example, the actual length of the optical fiber between the ONU and OLT is about 25 km, which exceeds the ranging compensation distance of 0-20 km.	Run the port range command to adjust the minimum logical reach and maximum logical reach so that the actual distance between the ONU and OLT is within the ranging compensation distance. NOTE <ul style="list-style-type: none">By default, the ranging compensation distance of a GPON port is from 0 km to 20 km.According to Class B+, the maximum logical reach of a GPON port must not exceed 60 km, and the difference between the minimum logical reach and maximum logical reach must not exceed 20 km.
The laser on the PON port is disabled.	Run the display port info command to query the information about the PON port. It is found that Admin State is in the Off state.	Run the port laser-switch command to enable the laser on the PON port. NOTE By default, the laser on a GPON port is enabled.

Possible Cause	Judgment Criterion	Troubleshooting Method
The PON port is faulty.	If either of the following two situations occurs, the PON port is faulty. <ul style="list-style-type: none"> Run the display port state command to query the status of the PON port. It is found that abnormal items exist in the query result. For example, the laser status (Laser state) is abnormal and the transmit optical power (TX power) exceeds the normal range (1.5-5.0 dBm). Migrate the service to another port. It is found that the ONU is auto discovered by the OLT. 	Replace the optical module of the PON port or replace the board.
The type of the optical module of the PON port is incorrect.	Run the display port state command to query the port status. xxx NRZ indicates that the optical module is of the GPON type. xxx 10BBB indicates that the optical module is of the EPON type.	Replace the optical module.
The board or the slot is faulty.	Run the display board command to query the status of the board. It is found that the board status is not Normal .	Run the board reset command to reset the board or change the board to another slot. If the fault persist, replace the board.

6.4.3 ODN Fault

Procedure

Check for the possible causes on the ODN and troubleshoot the faults accordingly.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The optical fiber connector is not clean.</p> <p>NOTE An unclean optical fiber connector will cause excessive attenuation and abnormal reflection.</p>	<ol style="list-style-type: none"> Test the backbone fiber and branch fiber by using the OTDR. It is found that the reflection and return loss are abnormal. Check the optical fiber connector on site by using the optical fiber endface detector. It is found that the optical fiber connector is not clean. 	Clean the optical fiber connector. For details about how to clean the connector, see Cleaning the Connector of an Optical Fiber .
<p>The optical fiber is bent excessively.</p> <p>NOTE Optical signals attenuate seriously on an optical fiber with an excessively small bending radius.</p>	<ol style="list-style-type: none"> Test the backbone fiber and branch fiber by using the OTDR. It is found that abnormal return loss points exist on the optical fiber. Check the optical fiber on site. It is found that the optical fiber is bent excessively. 	Route and bundle the optical fiber in a proper manner.
<p>The optical fiber is not firmly connected or different types of optical fiber connectors are interconnected.</p> <p>NOTE If the optical fiber is not firmly connected or different types of optical fiber connectors are interconnected, the attenuation and reflection will be excessively large.</p>	<ol style="list-style-type: none"> Test the backbone fiber and branch fiber by using the OTDR. It is found that abnormal return loss points exist on the optical fiber. Check the optical fiber connectors on site. It is found that the optical fiber is not firmly connected or PC connector (blue) and APC connector (green) are interconnected. 	<ul style="list-style-type: none"> If the optical fiber is not firmly connected, reconnect the optical fiber firmly. If different types of optical fiber connectors are interconnected, replace the incompatible connector with a compatible one or replace relevant devices, such as the optical splitter. <p>NOTE In the scenario of the CATV service, it is recommended that you use APC connectors (green) only.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The multi-mode optical fiber is used as the backbone or branch optical fiber.</p> <p>NOTE If the multi-mode optical fiber is used as the backbone or branch optical fiber, the optical signal attenuates quickly and the return loss increases.</p>	<ol style="list-style-type: none"> Check the backbone fiber and branch fiber by using the OTDR. It is found that optical signals attenuate seriously. Check the optical path on site. It is found that the multi-mode optical fiber is used. The multi-mode optical fiber can be recognized by its physical features such as its color. 	Replace the multi-mode optical fiber with the single-mode optical fiber.
<p>The optical attenuation of the optical path is excessively small.</p> <p>NOTE</p> <ul style="list-style-type: none"> If the optical attenuation of the optical path is excessively small, the optical power received by the ONU will exceed the overload optical power of the ONU. Such a situation occurs usually in labs, where the OLT and ONU may be directly connected to each other through a short optical fiber. 	<p>If either of the following two situations occurs, the optical attenuation of the optical path is excessively small.</p> <ul style="list-style-type: none"> Measure the receive optical power of the ONU by using the optical power meter. It is found that the actual receive optical power of the ONU is greater than -8 dBm. Check the optical path between the OLT and ONU. It is found that the optical attenuation of the optical path is excessively small. The normal attenuation range is 10-25 dB. 	Add an optical attenuator on the optical path between the OLT and ONU.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The ODN is not properly planned.</p> <p>NOTE</p> <ul style="list-style-type: none"> • The split ratio of the ODN link is not determined by the number of ONTs connected but by the split ratio of optical splitters. When an optical splitter is connected to the ODN, attenuation occurs and the split ratio of the optical splitter needs to be calculated. • The differences between the OLT-received optical power from the two adjacent ONUs must be smaller than or equal to 15 dB. 	<p>The ODN does not meet the requirements of the ODN link plan or GPON Class B+.</p> <ul style="list-style-type: none"> • Three-level splitting exists in the ODN. • The network coverage of the ODN exceeds 20 km by far. • The split ratio exceeds the maximum split ratio that the board allows. Assuming that the maximum split ratio of a board is 1:64. If the first-level split ratio is 1:8 and the second-level split ratio is 1:16, the actual split ratio is 1:128, which exceeds the maximum split ratio of the board. • The optical attenuation difference of two optical paths exceeds 15 dB. 	Optimize the ODN to meet Huawei's ODN planning requirements and protocol requirements.
<p>The optical splitter is faulty or the connectors on the optical splitter are not clean.</p>	<p>Measure the input and output optical power of the optical splitter by using the optical power meter. It is found that the actual attenuation exceeds the theoretical attenuation.</p> <p>NOTE The faults in the optical splitter cannot be located by the OTDR because the OTDR cannot penetrate the optical splitter.</p>	Replace the faulty optical splitter or clean the connectors on the optical splitter.

Possible Cause	Judgment Criterion	Troubleshooting Method
A backbone fiber break occurs.	<ol style="list-style-type: none"> Check the backbone fiber by using the OTDR. It is found that a backbone fiber break occurs. Check the optical fiber on site. It is found that the optical fiber is broken or not connected. 	Reconnect the backbone optical fiber.
A branch fiber break occurs.	<ol style="list-style-type: none"> Check the branch fiber by using the OTDR. It is found that a branch fiber break occurs. Check the optical fiber on site. It is found that the optical fiber is broken or not connected. 	Reconnect the branch optical fiber.

6.4.4 ONU Fault

Procedure

Check for the possible causes on the ONU and troubleshoot the faults accordingly.

Possible Cause	Judgment Criterion	Troubleshooting Method
The ONU is not powered on.	Check the power supply of the ONU. It is found that the power supply of the ONU fails or is turned off.	Restore the power supply of the ONU.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>A rogue ONU exists on the network and affects other ONUs.</p> <p>NOTE If a rogue ONU exists, the ONU that fails to go online may be a normal one and the ONU that can go online may be a rogue one.</p>	<p>If either of the following two situations occurs, a rogue ONU exists.</p> <ul style="list-style-type: none"> • The 0x2e314021 There are illegal incursionary rogue ONTs under the port alarm is generated on the OLT. • The 0x2e314022 The ONT is rogue ONT alarm is generated on the OLT. • Remove the optical fiber from the OLT port and connect the optical fiber to the optical power meter for measurement. If a value can be read from the optical power meter, a continuous-mode ONU or irregular-mode ONU exists. <p>NOTICE Measuring the optical power interrupt services, Therefore, it is recommended that you measure the optical power when a PON port does not run any services, such as deployment.</p>	Replace the rogue ONU with a normal one.
The ONU hardware is faulty.	<p>If either of the following two situations occurs, the ONU hardware is faulty.</p> <ul style="list-style-type: none"> • The LEDs of the ONU are off when the ONU is powered on. • After the ONU is replaced with another ONU, the new ONU is auto discovered by the OLT. 	Replace the faulty ONU or the optical module of the ONU.

Possible Cause	Judgment Criterion	Troubleshooting Method
The optical module of the ONU is abnormal. For example, the transmit optical power of the optical module is excessively small or its receiver sensitivity is low.	<p>Replace the faulty ONU with a normal one. It is found that the new ONU is auto discovered by the OLT.</p> <p>An alternative is to locate the fault as follows:</p> <ul style="list-style-type: none"> Set the optical module of the ONU to the continuous mode, and measure the transmit optical power by using the optical power meter. It is found that the actual transmit optical power is beyond the normal range (0.5 dBm to +5 dBm). Measure the receive optical power of the ONU by using the optical power meter. It is found that the actual receive optical power is within the normal range (-27 dBm to -8 dBm). <p>NOTE The transmit optical power of a 10G GPON optical module ranges from 2 dBm to 7 dBm, and the receive optical power ranges from -29.5 dBm to -9 dBm.</p>	Replace the faulty ONU or the optical module of the ONU.
The Patch cord of the ONU is broken or bent excessively.	Check the Patch cord of the ONU. It is found that the Patch cord is broken or bent excessively.	Replace the Patch cord of the ONU.

6.5 GPON ONU Frequently Goes Online and Offline

ONUs connected to a GPON port frequently go online and offline and therefore the OLT reports a large number of ONU LOS alarms and relevant recovery alarms.

6.5.1 Fault Identification and Demarcation

ONUs connected to a GPON port frequently go online and offline and therefore the OLT reports a large number of ONU LOS alarms and relevant recovery alarms.

Location Method

An ONU frequently goes online and offline because the OLT receives weak ONU signals. As a result, packets exchanged between the OLT and the ONU are lost.

- If an ONU frequently goes online and offline, such as every several seconds, the ODN may have a fault.
- If an ONU goes offline every one hour or longer, the ONU may be faulty.

When an ONU frequently goes online and offline, locate the fault based on the following fault symptoms and possible causes.

Fault Scope	Symptom	Possible Cause
OLT	All the ONUs connected to a PON port on an OLT frequently go online and offline.	The PON port is faulty.
	All the ONUs connected to a board frequently go online and offline.	The board or the slot is faulty.
ODN	The PON port reports alarms described in ODN-Related Alarms, including: <ul style="list-style-type: none">• 0xe112002 The loss of GEM channel delineation (LCDGi) occurs• 0xe112003 The signal degrade of ONTi (SDi) occurs• 0xe112004 The signal fail of ONTi (SFi) occurs• 0xe112006 The loss of frame of ONTi (LOFi) occurs	The quality of the optical line is poor. ODN failures are generally caused by large reflection and attenuation caused by improper optical components, design, or construction. For details, see Common ODN Faults . <ul style="list-style-type: none">• If a single ONU or multiple ONUs frequently go online and offline, the branch fiber and the optical component may have faults.• If all ONUs frequently go online and offline, the backbone fiber and the optical component may have faults.

Fault Scope	Symptom	Possible Cause
ONU	A single ONU or some ONUs connected to an OLT frequently go online and offline.	<ul style="list-style-type: none">• A rogue ONU exists on the network and affects other ONUs.• The ONU is restarted repeatedly.

NOTICE

The parameters of the optical module in this topic comply with Class B+. Note that such parameters are slightly different from the parameters in Class C.

6.5.2 Alarming Handling

Procedure

When the "ONU frequently goes online and offline" alarm is generated, run the **display ont info** command to query the **last down cause** of the ONU. Check whether the OLT generates the following alarms. If such alarms are generated, clear them and check whether the fault is rectified.

When an ONU frequently goes online and offline, the following alarms may be generated:

Fault Scope	Alarms
ODN	<p>ODN-Related Alarms, including:</p> <ul style="list-style-type: none">• 0x2e112002 The loss of GEM channel delineation (LCDGi) occurs• 0x2e112003 The signal degrade of ONTi (SDi) occurs• 0x2e112004 The signal fail of ONTi (SFi) occurs• 0x2e112006 The loss of frame of ONTi (LOFi) occurs• 0x2e11a001 The feed fiber is broken or OLT can not receive any expected optical signals(LOS)• 0x2e112007 The distribute fiber is broken or the OLT cannot receive expected optical signals from the ONT(LOSi/LOBi)
ONU	<ul style="list-style-type: none">• 0x2e314021 There are illegal incursionary rogue ONTs under the port• 0x2e314022 The ONT is rogue ONT

6.5.3 OLT Fault

Procedure

Check for the possible causes on the OLT and troubleshoot the faults accordingly.

Possible Cause	Judgment Criterion	Troubleshooting Method
The PON port is faulty.	If either of the following two situations occurs, the PON port is faulty. <ul style="list-style-type: none">• Run the display port state command to query the status of the PON port. It is found that abnormal items exist in the query result. For example, the laser status (Laser state) is abnormal and the transmit optical power (TX power) exceeds the normal range (1.5-5.0 dBm).• Migrate the service to another port. It is found that the ONU functions properly.	Replace the optical module of the PON port or replace the board.
The board or the slot is faulty.	All the ONUs connected to a board frequently go online and offline.	Change the board to another slot. If the fault persist, replace the board.

6.5.4 ODN Fault

Procedure

Check for the possible causes on the ODN and troubleshoot the faults accordingly.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The optical fiber connector is not clean.</p> <p>NOTE An unclean optical fiber connector will cause excessive attenuation and abnormal reflection.</p>	<ol style="list-style-type: none"> Test the backbone fiber and branch fiber by using the OTDR. It is found that the reflection and return loss are abnormal. Check the optical fiber connector on site by using the optical fiber endface detector. It is found that the optical fiber connector is not clean. 	Clean the optical fiber connector. For details about how to clean the connector, see Cleaning the Connector of an Optical Fiber .
<p>The optical fiber is bent excessively.</p> <p>NOTE Optical signals attenuate seriously on an optical fiber with an excessively small bending radius.</p>	<ol style="list-style-type: none"> Test the backbone fiber and branch fiber by using the OTDR. It is found that abnormal return loss points exist on the optical fiber. Check the optical fiber on site. It is found that the optical fiber is bent excessively. 	Route and bundle the optical fiber in a proper manner.
<p>The optical fiber is not firmly connected or different types of optical fiber connectors are interconnected.</p> <p>NOTE If the optical fiber is not firmly connected or different types of optical fiber connectors are interconnected, the attenuation and reflection will be excessively large.</p>	<ol style="list-style-type: none"> Test the backbone fiber and branch fiber by using the OTDR. It is found that abnormal return loss points exist on the optical fiber. Check the optical fiber connectors on site. It is found that the optical fiber is not firmly connected or PC connector (blue) and APC connector (green) are interconnected. 	<ul style="list-style-type: none"> If the optical fiber is not firmly connected, reconnect the optical fiber firmly. If different types of optical fiber connectors are interconnected, replace the incompatible connector with a compatible one or replace relevant devices, such as the optical splitter. <p>NOTE In the scenario of the CATV service, it is recommended that you use APC connectors (green) only.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The multi-mode optical fiber is used as the backbone or branch optical fiber.</p> <p>NOTE If the multi-mode optical fiber is used as the backbone or branch optical fiber, the optical signal attenuates quickly and the return loss increases.</p>	<ol style="list-style-type: none"> Check the backbone fiber and branch fiber by using the OTDR. It is found that optical signals attenuate seriously. Check the optical path on site. It is found that the multi-mode optical fiber is used. The multi-mode optical fiber can be recognized by its physical features such as its color. 	Replace the multi-mode optical fiber with the single-mode optical fiber.
<p>The optical splitter is faulty or the connectors on the optical splitter are not clean.</p>	<p>Measure the input and output optical power of the optical splitter by using the optical power meter. It is found that the actual attenuation exceeds the theoretical attenuation.</p> <p>NOTE The faults in the optical splitter cannot be located by the OTDR because the OTDR cannot penetrate the optical splitter.</p>	Replace the faulty optical splitter or clean the connectors on the optical splitter.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The ODN is not properly planned.</p> <p>NOTE</p> <ul style="list-style-type: none">• The split ratio of the ODN link is not determined by the number of ONTs connected but by the split ratio of optical splitters. When an optical splitter is connected to the ODN, attenuation occurs and the split ratio of the optical splitter needs to be calculated.• The differences between the OLT-received optical power from the two adjacent ONUs must be smaller than or equal to 15 dB.	<p>The ODN does not meet the requirements of the ODN link plan or GPON Class B+.</p> <ul style="list-style-type: none">• Three-level splitting exists in the ODN.• The network coverage of the ODN exceeds 20 km by far.• The split ratio exceeds the maximum split ratio that the board allows. Assuming that the maximum split ratio of a board is 1:64. If the first-level split ratio is 1:8 and the second-level split ratio is 1:16, the actual split ratio is 1:128, which exceeds the maximum split ratio of the board.• The optical attenuation difference of two optical paths exceeds 15 dB.	Optimize the ODN to meet Huawei's ODN planning requirements and protocol requirements.

6.5.5 ONU Fault

Procedure

Check for the possible causes on the ONU and troubleshoot the faults accordingly.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>A rogue ONU exists on the network and affects other ONUs.</p> <p>NOTE If a rogue ONU exists, the ONU that fails to go online may be a normal one and the ONU that can go online may be a rogue one.</p>	<p>If either of the following two situations occurs, a rogue ONU exists.</p> <ul style="list-style-type: none"> • The 0xe314021 There are illegal incursionary rogue ONTs under the port alarm is generated on the OLT. • The 0xe314022 The ONT is rogue ONT alarm is generated on the OLT. • Remove the optical fiber from the OLT port and connect the optical fiber to the optical power meter for measurement. If a value can be read from the optical power meter, a continuous-mode ONU or irregular-mode ONU exists. <p>NOTICE Measuring the optical power interrupt services, Therefore, it is recommended that you measure the optical power when a PON port does not run any services, such as deployment.</p>	Replace the rogue ONU with a normal one.
The ONU is restarted repeatedly.	Check whether the ONU is faulty or whether the power voltage is unstable.	Replace the ONU or ensure that the power supply of the ONU is normal.

7

Troubleshooting the FTTH Service

This chapter describes how to troubleshoot common faults in Internet access and multicast (IPTV)services in FTTH scenarios.

[7.1 Troubleshooting the Internet Access Service](#)

This topic describes how to troubleshoot common faults in the Internet access service, including the following faults: PPPoE dialup failure, DHCP dialup failure, failure to access the Internet after successful dialup, Internet access service interruption, and low Internet access rate. The following uses the bridging ONT as an example to describe how to troubleshoot a fault.

[7.2 IPTV Service Failure](#)

This topic describes how to troubleshoot an IPTV service fault in a FTTH network.

[7.3 Troubleshooting Voice Service Faults](#)

This topic describes how to troubleshoot voice service faults in a fiber to the home (FTTH) network. Common voice service faults include: no tone after offhook, busy tone after offhook, one-way audio in a voice call, noise in a voice call, voice interruptions in a voice call, and failure to dial certain phone numbers.

7.1 Troubleshooting the Internet Access Service

This topic describes how to troubleshoot common faults in the Internet access service, including the following faults: PPPoE dialup failure, DHCP dialup failure, failure to access the Internet after successful dialup, Internet access service interruption, and low Internet access rate. The following uses the bridging ONT as an example to describe how to troubleshoot a fault.

Prerequisites

The ONT and the OLT must communicate with each other normally. If a fault occurs in communication between the ONT and the OLT, all the services of the ONT may be interrupted. In this case, troubleshoot the fault first by referring to the methods described in [6 GPON ONU Abnormal State](#).

 NOTE

ONTs can be classified into two types: bridging ONT and gateway ONT. The following uses the bridging ONT as an example. The bridging ONT and gateway ONT have the following difference in the Internet access service:

- Gateway ONT: The ONT serves as a DHCP client for proxy to obtain the public IP addresses of user PCs and serves as a DHCP server to assign private IP addresses for user PCs.
- Bridging ONT: The ONT transparently transmits all user packets but does not process them.

7.1.1 Internet Access Service Fails

This topic describes how to troubleshoot Internet access service failures in fiber to the home (FTTH) networks.

7.1.1.1 Fault Identification and Demarcation

Description

The Internet access service failure is a fault in which users provided with the Internet access service cannot obtain network resources. For example, they cannot open a web page.

Fault Locating Guide

If a user fails to access the Internet in FTTH networks: If the user uses a static IP address, check whether the IP address of the PC is correct; if the user uses a dynamic IP address, check whether the user's PC can normally obtain an IP address.

 NOTE

To query the IP address of the PC for a Windows user, do as follows:

1. Choose **Start > Run** on the task bar of the PC. Enter the **cmd** command in the **Run** dialog box, and then press **Enter**.
2. In the displayed CLI, enter the **ipconfig** command to query the IP address of the PC.

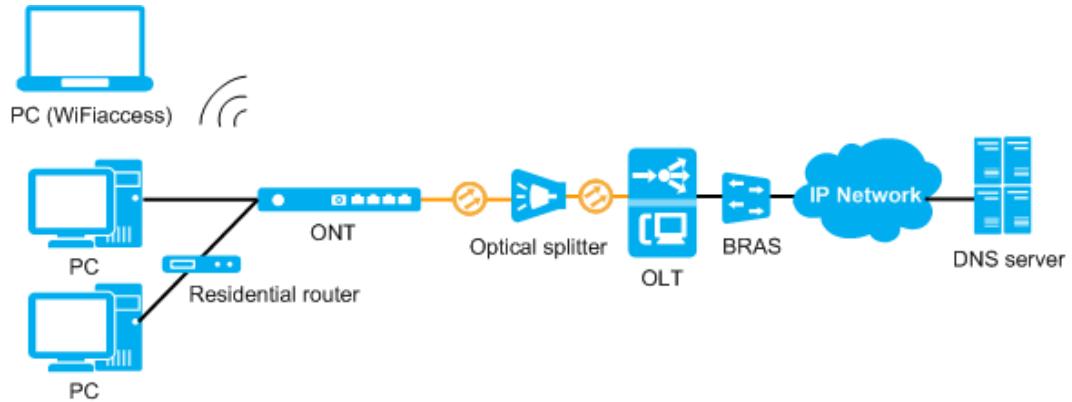
User's PC Fails to Obtain an IP Address

When a user's PC fails to obtain an IP address:

- For a PPPoE user, see [7.1.4 PPPoE Dialup Failure](#).
- For a DHCP user, see [7.1.5 Failure to Obtain an IP Address in the DHCP Mode](#).

User's PC Successfully Obtains an IP Address

Demarcate the fault based on the fault symptom.



Checking Scope	Determination Basis	Possible Cause
User's PC	Use a test PC, instead of the user's PC, for testing. The user can normally access the Internet through this PC.	<ul style="list-style-type: none"> The user's PC is infected with viruses. The IE browser of the PC is faulty. The PC responds slowly after having run for a long time. The network interface card (NIC) of the PC malfunctions or fails.
DNS server	Websites can be visited through entering the website IP addresses.	<ul style="list-style-type: none"> The DNS server is faulty and fails to resolve domain names. The communications between the user's PC and DNS server are abnormal.

NOTE

Faults can be located according to specific scenarios because the deployment scenario and the routine O&M scenario involve different fault scopes.

- If the fault occurs during a new deployment, check the hardware and initial software configurations.
- If the fault occurs during O&M, check only the hardware, because the software configurations of a user are generally not modified in this scenario. Therefore, if the user state changes from normal to abnormal, it may be caused by a hardware fault. If the fault occurs after a new user is added or an existing user is modified, check the software configurations of the user.

7.1.1.2 User's PC Is Faulty

Determining the Fault

Use a test PC, instead of the user's PC, for testing. The user can normally access the Internet through this PC.

Procedure

- Step 1** Use the antivirus software to remove viruses.
 - Step 2** Restart the IE. If the fault persists, re-install the IE.
 - Step 3** Restart the PC.
 - Step 4** Update the driver of the NIC. If the fault persists, replace the NIC.
- End

7.1.1.3 DNS Server Is Faulty

Determining the Fault

Enter the IP address (such as http://192.168.0.2) of a known website to the IE address bar and you can visit this web page. This indicates that the link between the PC to DNS server or the DNS server fails, causing a domain name parse failure.

Troubleshooting

Check whether the PC can ping the IP address of the DNS server.



To query the IP address of the DNS server connected to the PC, do as follows:

1. Choose **Start > Run**. Enter **cmd** in the **Run** dialog box, and then press **Enter**.
2. In the DoS window of the PC, enter the **ipconfig/all** command to query the IP address (**DNS Servers**) of the DNS server obtained by the PC.
 - If the ping operation fails, the link between the PC and DNS server fails. Check the link.
 - If the ping operation succeeds, the DNS server fails. Contact the maintenance personnel to check the DNS server.

7.1.2 Internet Access Is Interrupted Frequently

Internet access is interrupted frequently in fiber to the home (FTTH) networks.

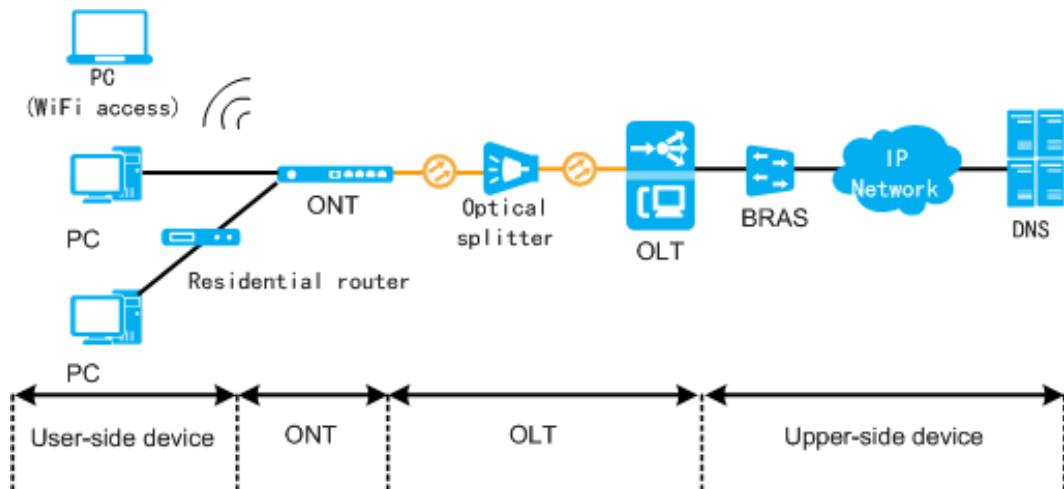
7.1.2.1 Fault Identification and Demarcation

Symptoms Description

Internet access is interrupted frequently in fiber to the home (FTTH) networks.

Fault Locating Guide

Figure 7-1 shows an example network of the FTTH Internet access service.

Figure 7-1 Example network of the FTTH Internet access service

When the Internet access service is interrupted, locate the fault according to the fault scope and possible causes, as described in the following table.

Table 7-1 Possible causes of the fault in different scopes

Fault Scope	Judgment Criterion	Possible Cause
User-side device	The Internet access service of a single user is interrupted but the Internet access service of other users connected to the same ONT is normal.	<ul style="list-style-type: none">The PC is infected by viruses.A network device such as the residential router between the ONT and the PC is faulty.The driver of the network interface card (NIC) on the PC is damaged or the hardware of the NIC is faulty.
ONT	The Internet access service of multiple users connected to the same ONT is interrupted.	<ul style="list-style-type: none">The wireless signals received by the PC using Wi-Fi access are of poor quality.The hardware of the ONT malfunctions or is faulty.
OLT	The Internet access service of users on multiple ONTs connected to the same OLT is interrupted.	<ul style="list-style-type: none">Packet loss occurs because of incorrect configurations, such as link aggregation and port negotiation between the OLT and the port of the upper-layer device.Packet loss occurs because of a large volume of traffic on the upstream port.MAC address transfer occurs because a network encounters a loop or a device improperly forwards packets.The hardware, such as the optical module, service board, and control board of the OLT malfunctions or is faulty.

Fault Scope	Judgment Criterion	Possible Cause
Upper-layer device	The Internet access service of users connected to multiple OLTs is interrupted.	<ul style="list-style-type: none">Packet loss occurs on the upper-layer device.

7.1.2.2 User's PC Is Faulty

Determining the Fault

Use a test PC, instead of the user's PC, for testing. The user can normally access the Internet through this PC.

Procedure

Step 1 Restart the PC.

Step 2 Use the antivirus software to remove viruses.

Step 3 Update the driver of the NIC. If the fault persists, replace the NIC.

----End

7.1.2.3 Residential Router Is Faulty

Determining the Fault

The fault is rectified after the PC is directly connected to an ONT.

Troubleshooting

Restart user's residential router, if the fault persists, replace it.

7.1.2.4 User's ONT Is Faulty

Determining the Fault

The fault is rectified after the ONT is replaced.

Troubleshooting

1. Adjust the position of the PC and ensure that the quality of signals exchanged between the PC and the ONT meets the requirement.
2. Restart the ONT. If the fault persists, replace the ONT.

7.1.2.5 Packet loss of OLT Occurs

Determining the Fault

1. The link aggregation, port protection pair, and port negotiation configurations of the OLT are different from those of the upper-layer interconnected device.
2. **Number of discarded frames** increases in the output of the **display port statistics** command that is executed multiple times, packet loss occurs on the upstream port due to the large traffic.

Troubleshooting

1. Modify the configurations of the OLT or the upper-layer interconnected device to ensure that configurations of the OLT are the same as those of the upper-layer interconnected device.
2. If packet loss occurs because of a large volume of traffic on the upstream port, share traffic with other ports or increase the rate of the port.

NOTE

Increasing the rate of the OLT upstream port forcibly may result in a failure to negotiation between the OLT upstream port and its interconnected port. As a result, the OLT upstream port is unavailable. If such a failure occurs, plan the rate of both the OLT upstream port and its interconnected port according to the live network.

7.1.2.6 OLT Is Faulty

Determining the Fault

The fault is rectified by resetting the service board, replacing the optical module, or restarting the system.

Troubleshooting

1. Resetting the service board, replacing the optical module, or restarting the system.
2. If multiple devices have the same hardware fault, contact Huawei technical support engineers for help.
3. If the fault recurs after a period of time, the software fails. In this case, contact Huawei technical support engineers for help.

7.1.2.7 OLT Has MAC Address Duplication

Determining the Fault

MAC address transfer occurs on the upstream port or other service ports in the output of the **display location** command that is executed multiple times for querying the MAC address of the user encounters the fault.

Troubleshooting

1. Run the **ring check enable** command to check whether a ring network is generated.

2. Capture packets to locate the device that improperly forwards packets.

 **NOTE**

Enable the anti-MAC spoofing function to prevent MAC address transfer on service ports.

7.1.2.8 The Upper-layer Device Loss Packet

Determining the Fault

Packet loss is found in the output of the **ping** command for testing the quality of the link between the OLT and the network server.

Troubleshooting

Capture packets along the service route section by section to locate the device that discards packets or improperly forwards packets.

7.1.3 Low Internet Access Rate

The actual Internet access rate of a user is far lower than the applied rate.

7.1.3.1 Fault Identification and Demarcation

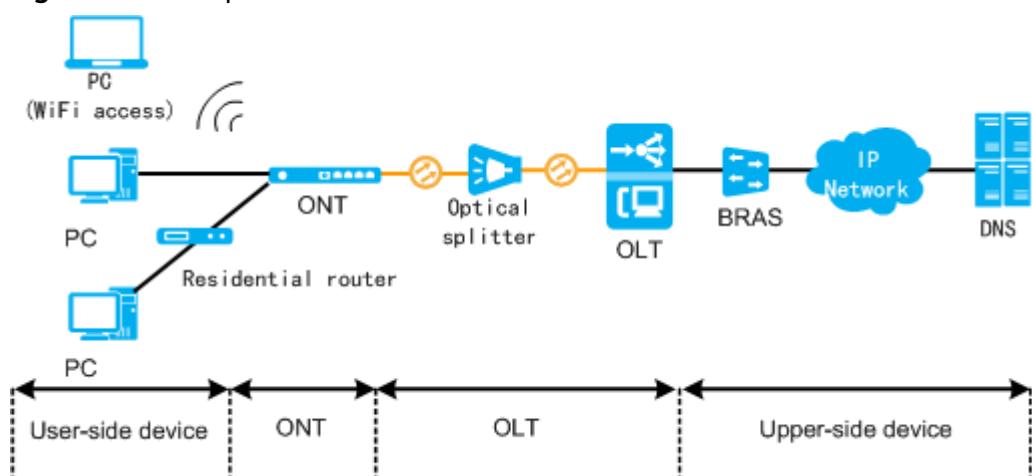
Symptoms Description

The actual Internet access rate of a user is far lower than the applied rate.

Fault Locating Guide

[Figure 7-2](#) shows an example network of the FTTH Internet access service.

Figure 7-2 Example network of the FTTH Internet access service



When the Internet access rate is low, locate the fault according to the fault scope and possible causes, as described in the following table.

Table 7-2 Possible causes of the fault in different scopes

Fault Scope	Judgment Criterion	Possible Cause
User-side device	The Internet access rate of a single user is low but the Internet access rate of other users connected to the same ONT is normal.	<ul style="list-style-type: none">• The PC runs for a long time.• The PC is infected by viruses.• The Internet Explorer (IE) of the PC fails.• The network interface card (NIC) of the PC is faulty or• A network device such as the residential router between the ONT and the PC is faulty.
ONT	The Internet access rate of multiple users connected to the same ONT is low.	<ul style="list-style-type: none">• The wireless signals received by the PC using Wi-Fi access are of poor quality.• The hardware of the ONT malfunctions or is faulty.• The user number of ONT is too large.
OLT	The Internet access rate of users on multiple ONTs connected to the same OLT is low.	<ul style="list-style-type: none">• The limited rate of the OLT is lower than the provisioned rate.• Packet loss occurs because of a large volume of traffic on the upstream port.• The OLT has unknown traffic, occupying user bandwidth.• The hardware, such as the optical module, service board, and control board of the OLT malfunctions or is faulty.
Upper-layer device	The Internet access rate of users of multiple OLTs is low.	<ul style="list-style-type: none">• The limited rate of the BRAS is lower than the provisioned rate.• Packet loss occurs on the upper-layer device or the delay is excessive long.

7.1.3.2 User's PC Is Faulty

Determining the Fault

Use a test PC, instead of the user's PC, for testing. The user can normally access the Internet through this PC.

Troubleshooting

1. Restart the PC.
2. Use the antivirus software to remove viruses.

3. Restart the IE. If the fault persists, re-install the IE.
4. Update the driver of the NIC. If the fault persists, replace the NIC.

7.1.3.3 Residential Router Is Faulty

Determining the Fault

The fault is rectified after the PC is directly connected to an ONT.

Troubleshooting

Restart user's residential router. If the fault persists, replace it.

7.1.3.4 User's ONT Is Faulty

Location Method

The fault is rectified after the ONT is replaced.

Troubleshooting

1. Adjust the position of the PC and ensure that the quality of signals exchanged between the PC and the ONT meets the requirement.
2. Restart the ONT. If the fault persists, replace the ONT.

7.1.3.5 The Limited Rate of the OLT Is Faulty

Location Method

The available rate is lower than the applied rate by checking the rate limit configurations of the OLT.

Troubleshooting

Modify the configurations to ensure that the available rate reaches the applied rate. For details, see "Configuring GPON Rate Limitation" in the *Commissioning and Configuration Guide*.

Keywords of main rate limit nodes are displayed as follows:

- Service port: **service-port**
- ONT port: **port eth**
- ONT T-CONT: **tcont**
- PON port: **car-port**
- Upstream port: **line-rate**

7.1.3.6 Large Volume of Traffic Cause Packet Loss

Determining the Fault

Number of discarded frames increases in the output of the **display port statistics** command that is executed multiple times, packet loss occurs on the upstream port due to the large traffic.

Troubleshooting

Share traffic with other ports or increase the rate of both the OLT upstream port and its interconnected port according to the live network.



Increasing the rate of the OLT upstream port forcibly may result in a failure to negotiation between the OLT upstream port and its interconnected port. As a result, the OLT upstream port is unavailable. If such a failure occurs, plan the rate of both the OLT upstream port and its interconnected port according to the live network.

7.1.3.7 Unknown Traffic Occupies User's Bandwidth

Determining the Fault

There is a large volume of traffic when no service is configured by running the **display port traffic** command to query the data traffic of the upstream port or the service port.

Troubleshooting

1. Use the antivirus software to remove viruses.
2. Capture packets to analyze the source of the unknown traffic to troubleshoot the fault.



More than 200 users in a VLAN may lead to an oversize broadcast domain. Then, a broadcast storm will occur in peak hours. As a result, the Internet access rate of users in the VLAN is low.

7.1.3.8 OLT Is Faulty

Determining the Fault

The fault is rectified by resetting the service board, replacing the optical module, or restarting the system.

Troubleshooting

1. Resetting the service board, replacing the optical module, or restarting the system.
2. If multiple devices have the same hardware fault, contact Huawei technical support engineers for help.
3. If the fault recurs after a period of time, the software fails. In this case, contact Huawei technical support engineers for help.

7.1.3.9 The Rate Limited on the BRAS is Lower Than the Applied Rate

Determining the Fault

The rate limited on the BRAS is lower than the applied rate.

Troubleshooting

Modify the limited rate to ensure that the rate meets the applied rate.

7.1.3.10 The Upper-layer Device Loss Packet

Determining the Fault

Packet loss or excessive long delay is found in the output of the **ping** command for testing the quality of the link between the OLT and the network server.

Troubleshooting

Capture packets along the service route section by section to locate the device that discards packets or has excessive long delay.

7.1.4 PPPoE Dialup Failure

The user encounters errors during PPPoE dialup to access the Internet and consequently the IP address cannot be obtained.

7.1.4.1 Fault Identification and Demarcation

Symptoms Description

The user encounters errors (such as error 678) during PPPoE dialup to access the Internet and consequently the IP address cannot be obtained.

Fault Locating Guide

PPPoE dialup can be initiated by the user PC, residential router, or ONT. This section uses the PPPoE dialup initiated by the user PC as an example to describe how to troubleshoot common faults.

When a user fails to obtain an IP address through PPPoE dialup, demarcate the fault scope according to PPPoE Dialup Emulation, as shown in [Figure 7-3](#).

Figure 7-3 Example network of the FTTH Internet access service

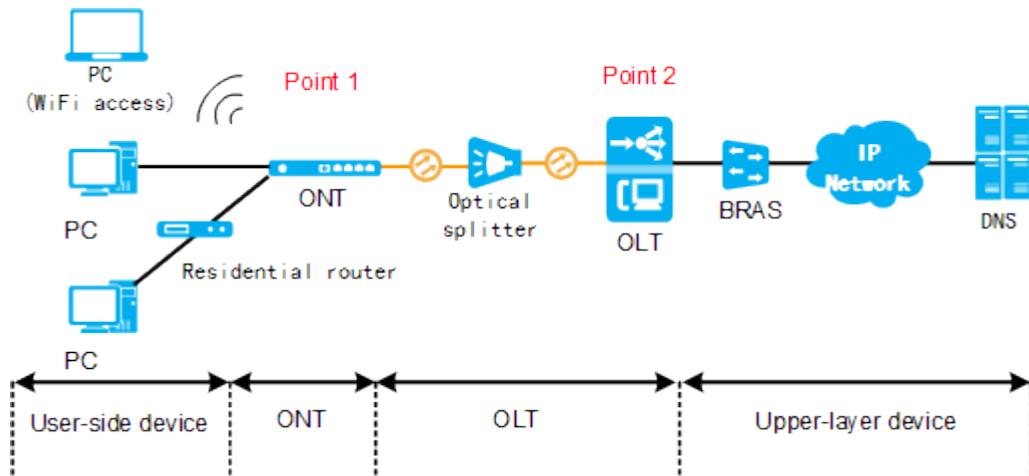


Table 7-3 Possible causes of PPPoE dialup failure

Fault Scope	Judgment Criterion	Possible Cause
User-side device	<ol style="list-style-type: none"> Dialup of a single user PC fails but other user PCs of the same ONT are normal. The result of emulation point 1 is "success". 	<ul style="list-style-type: none"> The PPPoE dialup software is not installed correctly or does not run properly. The PPPoE dialup software is not correctly installed. The driver of the user PC NIC (network interface card) is damaged or the NIC hardware is faulty. Configurations for the authentication mode or encryption mode on the PC (Wi-Fi access) are different from the configurations on the ONT. The network device (such as residential router) between the ONT and the user PC has problems.
ONT	<ol style="list-style-type: none"> Dialup of multiple user PCs of the same ONT fails. The result on emulation point 1 is not "success", but the result on emulation point 2 is "success". 	<ul style="list-style-type: none"> The WLAN function of the ONT is disabled. The SSID broadcast function of the ONT is disabled and the Wi-Fi terminal cannot search for the SSID. The ONT hardware is abnormal or faulty. The DHCP server of the ONT is faulty. The ONT user has charges overdue.

Fault Scope	Judgment Criterion	Possible Cause
OLT	<ol style="list-style-type: none">1. Dialup of multiple ONTs of the same OLT fails.2. The results of emulation points 1 and 2 are not "success".	<ul style="list-style-type: none">• Configuration problems of the VLAN translation in the OLT and ONT traffic streams.• The PTP protocol configuration is different on the OLT and the BRAS.• The number of MAC addresses in the service port access reaches the maximum number of learned MAC addresses.• The OLT discards the interaction packets between the user PC and the BRAS.• The OLT hardware (optical module, service board, or control board) is abnormal or faulty.
Upper-layer device (BRAS, convergence switch, or router)	<ol style="list-style-type: none">1. Dialup of users of multiple OLTs fails.2. The results of emulation points 1 and 2 are not "success".	<ul style="list-style-type: none">• The BRAS restricts the number of connection users.

7.1.4.2 User's PC Is Faulty

Determining the Fault

Use a test PC, instead of the user's PC, for testing. The user can normally access the Internet through this PC.

Troubleshooting

1. "Error 606" or "error 617" is returned during dialup. Check the network connection of the user PC and find that the connection is in the disabled state or in another abnormal state.
2. "Error 602", "error 605", "error 608", "error 609", "error 611", "error 617", or "error 633" is returned during dialup. After the PPPoE dialup software is uninstalled and then reinstalled.
3. "Error 691" is returned during dialup. Check the user name and password. If they are right, find the FCS and replace the board.
4. Connect the PC to the ONT in the wireless mode and check the configurations of the ONT and PC (Wi-Fi access). If the configurations for the authentication mode or encryption mode on the PC are different from the configurations on the ONT, modify the configurations.

5. Reinstall the NIC driver. If the fault persists, replace the NIC.

7.1.4.3 Residential Router Is Faulty

Determining the Fault

The fault is rectified after the PC is directly connected to an ONT.

Troubleshooting

Restart user's residential router. If the fault persists, replace it.

7.1.4.4 User's ONT Is Faulty

Determining the Fault

The fault is rectified after the ONT is replaced.

Troubleshooting

1. If the PC cannot search for the SSID of the wireless network, log in to the web page of the ONT and enable the SSID broadcast function.

 NOTE

To ensure that the wireless network is not embezzled, you must manually input on the PC the same SSID that is set on the ONT if the SSID broadcast function of the ONT is disabled.

2. If the WLAN indicator of the ONT is not in the always on state, press and hold the WLAN button or set the WLAN function on the ONT web page to enable the WLAN function.
3. Restart the ONT. If the fault persists, replace the ONT.

7.1.4.5 PITP Configuration Is Incorrect

Determining the Fault

Perform a PPPoE dialup emulation on the MDU and error code 732 is returned. This indicates that the MDU and upper-layer device have different PPP control protocols.

Troubleshooting

1. Run the `display pitp config` command to confirm that Policy Information Transfer Protocol (PITP) is enabled globally.
2. Run the `display pitp config` command to check the current PITP mode.
3. Confirm whether the current protocol type is the same as that set on the upper-layer device.
 - If the current mode is pmode, run the `display pitp permit-forwarding service-port` command to check whether the service port allows user-side PPPoE packets to carry the vendor tag. If this function is not enabled, run the `pitp permit-forwarding service-port` command to enable it and then check whether PPPoE dialup can be successfully performed.

- If the current mode is vmode, run the **display pitp vmode ether-type** command to check whether the Ethernet protocol type for VBRAS packets on the MDU is consistent with that on upper-layer device. If they are different, run the **pitp vmode ether-type** command to modify the Ethernet protocol type on the MDU so that it is consistent with that on the upper-layer device. Then, check whether the PPPoE dialup can be successfully performed.

 NOTE

Refer to "Configuring Anti-Theft or Roaming of User Accounts Through DHCP" in the *Commissioning and Configuration Guide* and configure parameters based on the data plan.

7.1.4.6 User Number Reaches the Maximum Number of Learned MAC Addresses.

Determining the Fault

Run the **display mac-address service-port** command to query the number of MAC addresses already learned by the service port, run the **display mac-address max-mac-count service-port** command to query the maximum number of learned dynamic MAC addresses, and find that the number of already learned MAC addresses reaches the maximum number of learned MAC addresses.

Troubleshooting

Run the **mac-address max-mac-count** command to reconfigure the maximum number of learned MAC addresses for this traffic stream, and increase the number of access users on this service port.

 NOTE

By default, the maximum number of learned MAC addresses is not restricted.

7.1.4.7 OLT Discards the Interaction Packets

Determining the Fault

Capture packets for analysis on the OLT user port and upstream port, and find that packets are lost.

Troubleshooting

1. Run the **display packet-filter port frameid/slotid/portid** command to check whether the user port is configured with the ACL rule.
2. Run the **display acl** command to check whether this ACL rule restricts PPPoE packets. Modify the ACL rule on PPPoE packets or delete the ACL rule from the port.
3. Check the problems such as broadcast storm, extremely large traffic, and port rate limitation on the OLT.

7.1.4.8 OLT Is faulty

Determining the Fault

The fault is rectified by resetting the service board, replacing the optical module, or restarting the system.

Troubleshooting

1. Resetting the service board, replacing the optical module, or restarting the system.
2. If multiple devices have the same hardware fault, contact Huawei technical support engineers for help.
3. If the fault recurs after a period of time, the software fails. In this case, contact Huawei technical support engineers for help.

7.1.4.9 User's Account Is Restricted on the BRAS

Determining the Fault

Perform a PPPoE dialup emulation on the MDU. Then, error code 668 is returned, indicating that the server forcibly terminates the PPPoE emulation.

Troubleshooting

1. Check whether user data of the upper-layer BRAS is correct or whether the user's account is restricted on the BRAS.
2. If the user data of the upper-layer BRAS is incorrect or whether the user's account is restricted on the BRAS, modify the BRAS configurations and check whether the IP address can be obtained successfully.

Capture packets along the service route section by section to locate the device that discards packets or has excessive long delay.

7.1.4.10 The Upper-layer Device Loss Packet

Determining the Fault

Packet loss or excessive long delay is found in the output of the **ping** command for testing the quality of the link between the OLT and the network server.

Troubleshooting

Capture packets along the service route section by section to locate the device that discards packets or has excessive long delay.

7.1.5 Failure to Obtain an IP Address in the DHCP Mode

The user uses the DHCP mode to access the Internet but fails to obtain an IP address.

7.1.5.1 Fault Identification and Demarcation

Symptoms Description

The user user uses the DHCP mode to access the Internet but fails to obtain an IP address.

Fault Locating Guide

The DHCP client can be the user PC, IPTV set top box, IP phone, residential router, or ONT. This section uses the user PC that functions as the DHCP client as an example to describe how to troubleshoot common faults.

When "Failure to Obtain an IP Address in the DHCP Mode" occurs, locate the fault based on the following fault symptoms and possible causes.

Figure 7-4 Example network of the FTTH Internet access service

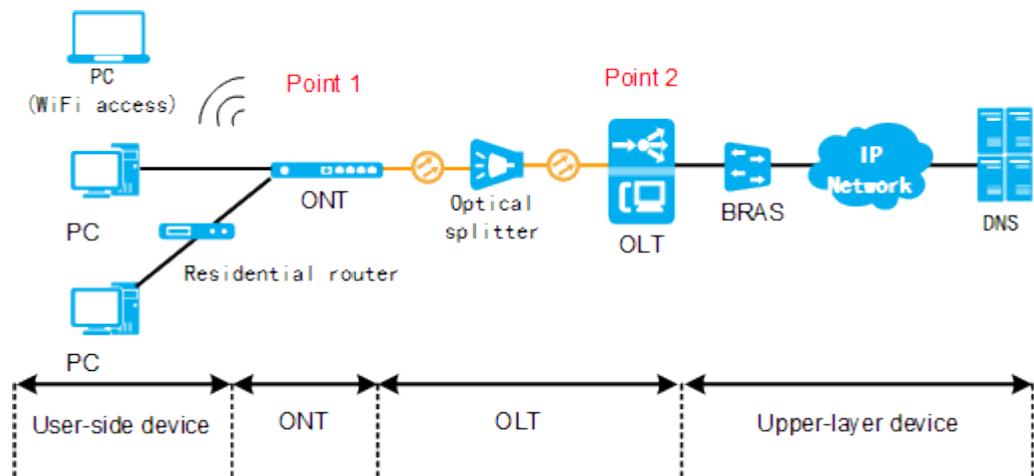


Table 7-4 Possible causes of failure to obtain an IP address in the DHCP mode

Fault Scope	Judgment Criterion	Possible Cause
User-side device	<ol style="list-style-type: none">1. Dialup of a single user PC fails but other user PCs of the same ONT are normal.2. The result of emulation point 1 is "success".	<ul style="list-style-type: none">• The network connection of the user PC is abnormal or disabled.• The IP obtaining mode of the PC is not set to "Obtain an IP address automatically."• The driver of the user PC NIC (network interface card) is damaged or the NIC hardware is faulty.• Configurations for the authentication mode or encryption mode on the PC (Wi-Fi access) are different from the configurations on the ONT.• The network device (such as residential router) between the ONT and the user PC has problems.
ONT	<ol style="list-style-type: none">1. Dialup of multiple user PCs of the same ONT fails.2. The result on emulation point 1 is not "success", but the result on emulation point 2 is "success".	<ul style="list-style-type: none">• The WAN port of an ONT is not created.• The SSID broadcast function of the ONT is disabled and the Wi-Fi terminal cannot search for the SSID.• The ONT hardware is abnormal or faulty.• The DHCP server of the ONT is faulty.• The ONT user has charges overdue.

Fault Scope	Judgment Criterion	Possible Cause
OLT	<ol style="list-style-type: none"> 1. Dialup of multiple ONTs of the same OLT fails. 2. The results of emulation points 1 and 2 are not "success". 	<ul style="list-style-type: none"> • Configuration problems of the VLAN translation in the OLT and ONT traffic streams: <ul style="list-style-type: none"> - VLAN tag translation on the ONT - VLAN tag translation on the OLT - Configuration for the native VLAN of the OLT upstream port and the ONT user port - Configuration for the mappings between user VLAN, ONT port, ONT ID, service VLAN, and upstream port • Configurations for the DHCP option 82 function on the OLT are different from the configurations on the DHCP server. • The number of MAC addresses in the service port access reaches the maximum number of learned MAC addresses. • The OLT enables a special function (such as anti-MAC spoofing) and modifies the RAIO information in the DHCP option 82 packet. • The OLT hardware (optical module, service board, or control board) is abnormal or faulty.
Upper-layer device	<ol style="list-style-type: none"> 1. Dialup of users of multiple OLTs fails. 2. The results of emulation points 1 and 2 are not "success". 	<ul style="list-style-type: none"> • The BRAS restricts the number of connection users.

7.1.5.2 User's PC Is Faulty

Determining the Fault

Use a test PC, instead of the user's PC, for testing. The user can normally access the Internet through this PC.

Troubleshooting

1. Check the network connection of the user PC, if the connection is in the disabled state or in another abnormal state, rectify the network connection of the user PC to ensure that the connection is in the normal state.

2. Check the properties of the network connection, if the IP obtaining mode is static IP address, set the property of the network connection to "Obtain an IP address automatically."
3. Check the configurations of the ONT and PC (Wi-Fi access), if configurations for the authentication mode or encryption mode on the PC are different from the configurations on the ONT, modify the configurations for the authentication mode and encryption mode on the PC (Wi-Fi access) to be the same as the configurations on the ONT.
4. Reinstall the NIC driver. If the fault persists, replace the NIC.

7.1.5.3 Residential Router Is Faulty

Determining the Fault

The fault is rectified after the PC is directly connected to an ONT.

Troubleshooting

Restart user's residential router, if the fault persists, replace it.

7.1.5.4 User's ONT Is Faulty

Determining the Fault

The fault is rectified after the ONT is replaced.

Troubleshooting

1. If the PC cannot search for the SSID of the wireless network, log in to the web page of the ONT and enable the SSID broadcast function.

NOTE

To ensure that the wireless network is not embezzled, you must manually input on the PC the same SSID that is set on the ONT if the SSID broadcast function of the ONT is disabled.

2. If the WLAN indicator of the ONT is not in the always on state, press and hold the WLAN button or set the WLAN function on the ONT web page to enable the WLAN function.
3. Restart the ONT. If the fault persists, replace the ONT.

7.1.5.5 ONT Configuration Is Incorrect

Determining the Fault

1. Run the **display dhcp option82 config** command to query whether DHCP option 82 is enabled globally. The query result is different from the data plan.
2. When DHCP option 82 is enabled and you run the **display dhcp-option82 permit-forwarding service-port** command to check whether the OLT allows the user-side DHCP packet to carry the device information, the query result is different from the data plan.

Troubleshooting

Refer to "Configuring Anti-Theft or Roaming of User Accounts Through DHCP" in the *Commissioning and Configuration Guide* and configure parameters based on the data plan.



Pay attention to the following data plan:

- Whether the DHCP server requires the DHCP packet to carry the option 82 information.
- Whether the option 82 information is added by the user device or the OLT.
- The option 82 information cannot be added repeatedly.

7.1.5.6 User Number Reaches the Maximum Number of Learned MAC Addresses.

Determining the Fault

Run the **display mac-address service-port** command to query the number of MAC addresses already learned by the service port, run the **display mac-address max-mac-count service-port** command to query the maximum number of learned dynamic MAC addresses, and find that the number of already learned MAC addresses reaches the maximum number of learned MAC addresses.

Troubleshooting

Run the **mac-address max-mac-count** command to reconfigure the maximum number of learned MAC addresses for this traffic stream, and increase the number of access users on this service port.



By default, the maximum number of learned MAC addresses is not restricted.

7.1.5.7 OLT is faulty

Determining the Fault

The fault is rectified by resetting the service board, replacing the optical module, or restarting the system.

Troubleshooting

1. Resetting the service board, replacing the optical module, or restarting the system.
2. If multiple devices have the same hardware fault, contact Huawei technical support engineers for help.
3. If the fault recurs after a period of time, the software fails. In this case, contact Huawei technical support engineers for help.

7.1.5.8 User's Account Is Restricted on the BRAS

Determining the Fault

Perform a PPPoE dialup emulation on the OLT. Then, error code 668 is returned, indicating that the server forcibly terminates the PPPoE emulation.

Troubleshooting

1. Check whether user data of the upper-layer BRAS is correct or whether the user's account is restricted on the BRAS.
2. If the user data of the upper-layer BRAS is incorrect or whether the user's account is restricted on the BRAS, modify the BRAS configurations and check whether the IP address can be obtained successfully.

Capture packets along the service route section by section to locate the device that discards packets or has excessive long delay.

7.1.5.9 The Upper-layer Device Loss Packet

Determining the Fault

Packet loss or excessive long delay is found in the output of the **ping** command for testing the quality of the link between the OLT and the network server.

Troubleshooting

Capture packets along the service route section by section to locate the device that discards packets or has excessive long delay.

7.2 IPTV Service Failure

This topic describes how to troubleshoot an IPTV service fault in a FTTH network.

Prerequisites

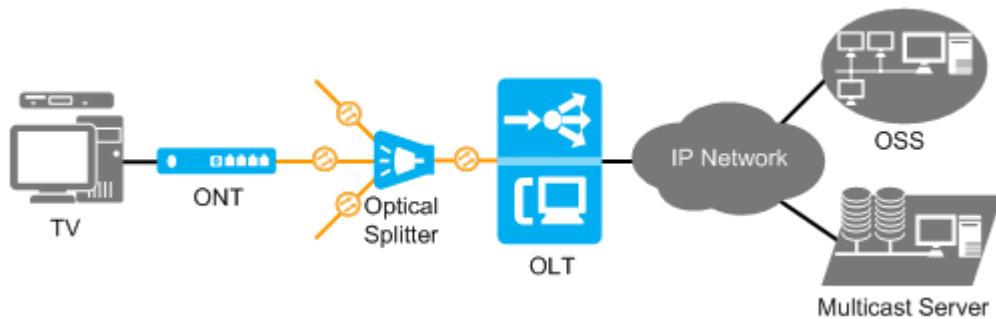
The ONT and the OLT must communicate with each other normally.



If a fault occurs in communication between the ONT and the OLT, all the services of the ONT may be interrupted. In this case, troubleshoot the fault first by referring to the methods described in [GPON ONU Abnormal State](#).

Context

The follow figure show an IPTV service in a FTTH network.



7.2.1 Online Access Failures

This section describes how to identify and resolve online access failures that occur on a fiber to the home (FTTH) network.

7.2.1.1 Symptoms

Description

A multicast user fails to go online, and this user is in **offline** or **block** state. In this case, when this user orders a video, a blank screen appears.

To query the status of a multicast user, run the **display igmp user** command.

- This user is **offline**.

```
huawei#display igmp user service-port 500
User : 0/1/0/500
State : offline
Authentication : auth
Quick leave : MAC-based
.....
```

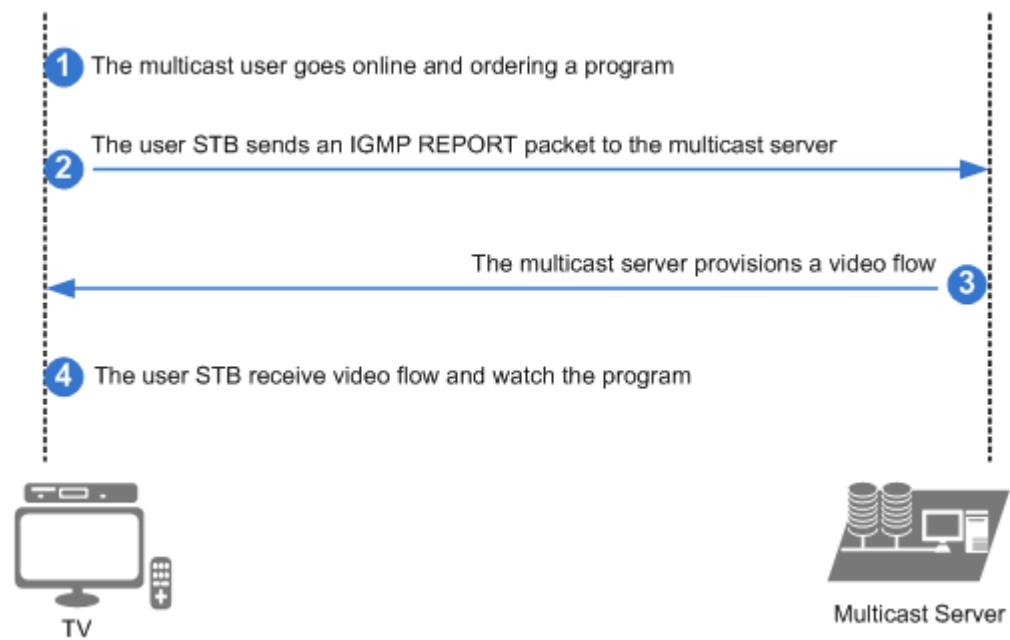
- This user is **block**.

```
huawei#display igmp user service-port 400
User : 0/1/1/400
State : block
Authentication : auth
Quick leave : MAC-based
.....
```

7.2.1.2 Fault Identification and Demarcation

Overview

The process of ordering a video is as follows:



1. The multicast user goes online and ordering a video.
2. The user STB sends an IGMP REPORT packet to the multicast server.
3. Based on the received IGMP REPORT packet, the multicast server provisions a video flow.
4. The network device forward the video flow to the user STB.

Fault Demarcation

If the multicast user is in **block** state, run the **undo igmp user block** command to unblock this user.

If the multicast user is in **offline** state, identify offline causes. In this case, Enable multicast debugging on the OLT and locate the fault based on the displayed multicast debugging information.

NOTE

In config mode, enable multicast debugging on the OLT.

```
terminal monitor //Enable debugging display on the user terminal.  
terminal debugging //Enable debugging data output on the user terminal.  
debugging igmp service-port index //Enable fault diagnosis for multicast users. In this command,  
parameter "index" is the index of the multicast user.
```

After locating the fault, disable multicast debugging on the OLT.

```
undo debugging igmp service-port index  
undo terminal debugging  
undo terminal monitor
```

The cause of user offline may differ from the scenario, and errors may have occurred during deployment or maintenance. Locate the fault based on application scenarios.

- If this fault occurs during site deployment, check the device hardware and the initial device software configuration.

- If this fault occurs during routine maintenance, this fault is unlikely to be caused by the device software. In this case, check the device hardware. If new users have been added or user configurations have been modified during routine maintenance, check user configurations.

7.2.1.3 Handling Process

7.2.1.3.1 Multicast User Is Blocked

Fault Information

After multicast debugging is enabled on the OLT, whenever a user fails to order a video due to blocked user status, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
 2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
  Type: REPORT, Version: V2, Group IP: 224.1.1.2
  Ethernet, src: 00-e0-fc-c4-80-34
  IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
  Warning: the user has been blocked
Debugging information: "Warning: the user has been blocked"
```

Determining the Fault

The status of this user is **block**. This status is queried by running the **display igmp user service-port index** command.

Troubleshooting

Run the **undo igmp user block** command to unblock the user if necessary.

NOTE

If a user, such as an overdue user, is expected to remain in a multicast group but is forbidden to order videos, run the **igmp user block** command to block this user. The OLT forces this user to go offline in the video being watched and rejects any initiated order requests until the user is unblocked.

7.2.1.3.2 The User Fails to Pass Bandwidth CAC

Fault Information

After multicast debugging is enabled on the OLT, whenever a user fails to order a video due to a bandwidth connection admission control (CAC) failure, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
 2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
  Type: REPORT, Version: V2, Group IP: 224.1.1.2
  Ethernet, src: 00-e0-fc-c4-80-34
  IP, src: 10.1.1.11
```

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
  Warning: the user fails to pass bandwidth CAC
Debugging information: "Warning: the user fails to pass bandwidth CAC"
```

Determining the Fault

The maximum bandwidth allocated to this user is less than the bandwidth of the video ordered by this user.

To query the maximum bandwidth allocated to this user, run the **display igmp user service-port index** command. To query the bandwidth of the video ordered by this user, run the **display igmp program name** command.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- Notify this user of insufficient bandwidth, which leads to inability to order videos.
- Run the **igmp user modify service-port index max-bandwidth** command to increase the maximum bandwidth allocated to this user.

7.2.1.3.3 Number of Specific Videos Ordered Has Reached the Upper Limit

Fault Information

After multicast debugging is enabled on the OLT, whenever a user fails to order a video due to number limitation, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
  2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
  Type: REPORT, Version: V2, Group IP: 224.1.1.2
  Ethernet, src: 00-e0-fc-c4-80-34
  IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
  Warning: the number of the grade program that the user is allowed to watch has reached maximum
Debugging information: "Warning: the number of the grade program that the user is allowed to watch has reached maximum"
```

Determining the Fault

The maximum number (**watch limit**) of specific videos that can be ordered by this user is **0**. To query the maximum number, run the **display igmp user extended-attributes user-index** command.



- If the value of **watch limit** is **0**, this user is forbidden to watch this type of video. For example, if the value of **HDTV watch limit** is **0**, this user has no rights to watch high definition (HD) videos.
- If the value of **watch limit** is **no-limit**, the maximum number of specific videos that can be ordered by this user is not limited. However, the total number of videos that can be concurrently watched by this user is limited.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- Inform the user that they have no rights to watch this type of video.
- Run the **igmp user watch-limit** command to increase the number of specific videos that can be ordered by this user.

7.2.1.3.4 Total Number of Ordered Videos Has Reached the Upper Limit

Fault Information

After multicast debugging is enabled on the OLT, whenever a user fails to order a video due to number limitation, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
Type: REPORT, Version: V2, Group IP: 224.1.1.2
Ethernet, src: 00-e0-fc-c4-80-34
IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
Warning: the number of program that the user is allowed to watch has reached maximum
Debugging information: "Warning: the number of program that the user is
allowed to watch has reached maximum"
```

Determining the Fault

The total number of ordered videos has reached the maximum number that can be ordered by this user. To query the two numbers, run the **display igmp user service-port index** command.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- Inform the user that they have no rights to watch more videos.
- Run the **igmp user modify service-port index max-program max-program-num** command to increase the total number of videos that can be ordered by this user.

7.2.1.3.5 User Has No Rights to Watch a Video

Fault Information

After multicast debugging is enabled on the OLT, whenever a user fails to order a video due to rights limitation, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
Type: REPORT, Version: V2, Group IP: 224.1.1.2
```

```
Ethernet, src: 00-e0-fc-c4-80-34
IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
Warning: the user has no right
Debugging information: "Warning: the user has no right"
```

Determining the Fault

To determine whether the failure in ordering videos is caused by rights limitation, run the **display igmp service-port 100** command. In this command, the index of this service-port is assumed to be 100.

- If the number of **Bind profiles** is **0**, no rights profile has been bound to this user and no videos can be ordered.
- If the number of **Bind profiles** is **1** or larger, this user can order only permitted videos. In queried results, identify the index (which is assumed to be **1**) and name of the rights profile bound to this user, then, run the **display igmp profile profile-index 1** command to query the rights of this user.
 - If the queried result is **forbidden** or **idle**, this user has no rights to watch this video.
 - If the queried result is **watch** or **preview**, this user has rights to watch this video, which is excluded from the possible offline causes. **preview** right is after a user watches a video for a period of time (for example, a few minutes), the video stops playing, or a blank screen occurs.

NOTE

Multiple rights profiles can be bound to one user. If these profiles specify different rights for a video, the rights with the highest priority take effect for this user. By default, the rights priorities of **forbidden**, **preview**, **watch**, and **idle** are in descending order. This order can be changed by running the **igmp right-priority** command.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- If this user does not require authentication and can watch all videos, run the **igmp user modify service-port 100 no-auth** command in BTV mode to configure this user to not require authentication. In this command, the index of this service-port is assumed to be 100.
- If this user requires authentication and can watch only some videos, inform the user that they have no rights to watch this video.
- If this user can only preview the video, inform the user that they can only watch for the permitted duration.
- If this user has viewing rights, modify or replace the rights profile bound to this user.
 - Modifying the rights profile: Run the **igmp profile profile-index 0 program-name PROGRAM-0 watch** to change the viewing rights from **preview** to **watch**.
 - Replacing the rights profile: Run the **undo igmp user bind-profile** command to unbind the original rights profile, then, run the **igmp user bind-profile** command to bind a new rights profile for this user.

7.2.1.3.6 Match Program Fail

Fault Information

After multicast debugging is enabled on the OLT, whenever a user fails to order a video due to rights limitation, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
Type: REPORT, Version: V2, Group IP: 224.1.1.2
Ethernet, src: 00-e0-fc-c4-80-34
IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
Warning: match program fail
Debugging information: "Warning: match program fail"
```

Determining the Fault

Possible Cause	Determination Basis
This user is not an M-VLAN member	To query M-VLAN members, run the display igmp multicast-vlan member vlanid command. NOTE A user can watch videos configured in an M-VLAN only if this user is a member in this M-VLAN.
Ordered Video Is Not Contained in the M-VLAN Video List	The video list of the M-VLAN does not contain the ordered video. To query an M-VLAN video list, run the display igmp program vlan command.
No Multicast Uplink Port Has Been Configured in the M-VLAN	No multicast uplink port has been configured in the M-VLAN. To query the uplink port of an M-VLAN, run the display igmp uplink-port all command.

Troubleshooting

Possible Cause	Handling Method
This user is not an M-VLAN member	Use either of the following methods to rectify this fault based on the user's service type: <ul style="list-style-type: none">• Inform the user that they have no rights to watch this video.• In M-VLAN mode, run the igmp multicast-vlan member service-port index command to add this user to the M-VLAN.

Possible Cause	Handling Method
Ordered Video Is Not Contained in the M-VLAN Video List	<p>Use either of the following methods to rectify this fault based on the user's service type:</p> <ul style="list-style-type: none">• If this user has not subscribed to this video, inform the user that they have no rights to watch this type of video.• If this user has subscribed to this video, perform the following operations:<ol style="list-style-type: none">1. Run the display igmp config vlan command to query the video mapping mode (Program match mode) supported by the M-VLAN.<ul style="list-style-type: none">– If the value of Program match mode is enable, this video is a static one and requires configuration before it can be ordered.– If the value of Program match mode is disable, this video is a dynamic one and automatically generated when a user orders it.2. Add this video to the M-VLAN video list.<ul style="list-style-type: none">– For a static video, run the igmp program add command.– For a dynamic video, run the igmp match group command to configure the address range for the M-VLAN video list. Ensure that the IP address of this ordered video is within the address range.
No Multicast Uplink Port Has Been Configured in the M-VLAN	In M-VLAN mode, run the igmp uplink-port command to configure the uplink port on the OLT as the multicast uplink port. Then, all multicast packets in this M-VLAN can be forwarded using this uplink port.

7.2.1.3.7 IGMP Has Been Incorrectly Configured

Fault Locating Guide

The OLT does not receive the IGMP REPORT packet sent by a user, and all other members in the M-VLAN fail to go online. In this case, the fault may be caused by the disabled status of the IGMP function in this M-VLAN.

Procedure

In M-VLAN mode, run the **display igmp config vlan** command to query the IGMP status (**IGMP mode**) in the M-VLAN.

- If the value of **IGMP mode** is **off**, IGMP is disabled in this M-VLAN. In this case, run the **igmp mode** command in M-VLAN mode to configure the IGMP status to **proxy** or **snooping**.
- If the value of **IGMP mode** is **proxy** or **snooping**, IGMP has been enabled in this M-VLAN, which is excluded from the possible offline causes.

7.2.1.3.8 Subscriber Line or Terminal Is Faulty

Fault Locating Guide

Locate the fault based on symptoms.

- If this user could initially go online and then failed, the software configuration is correct. Pay special attention to hardware, including the STB, ONT, and physical line between the ONT and the STB.
- If this user has never succeeded in going online, check both hardware and OLT data configuration.

Procedure

Possible Cause	Judgment Criterion	Troubleshooting Method
The STB is faulty.	The user can go online after resetting the STB or replacing the STB with a functional one and ordering the program.	Reset the STB or replace the STB with a functional one.
The ONT is faulty.	The user can go online after resetting the ONT or replacing the ONT with a functional one and ordering the program.	Reset the ONT or replace the ONT with a functional one.
The physical line between the STB and ONT is faulty. For example, the network cable is not securely connected, is damaged, or is incorrectly connected.	<p>Check the LAN indicator on the ONT (the HG8245 is used as an example) to determine the status of the physical line between the STB and ONT.</p> <ul style="list-style-type: none">• If the LAN indicator is off, the line is faulty.• If the LAN indicator is steady on or blinks, the line is in the normal state.	Connect the network cable again or replace the network cable with a functional one.

7.2.2 Blank Screens on the Multicast Service

This section describes how to identify and resolve blank screens on the multicast service for a fiber to the home (FTTH) network.

7.2.2.1 Symptoms

Description

After ordering a video, the multicast user experiences a blank screen but not the ordered video.

To query the status of a multicast user, run the **display igmp user** command.

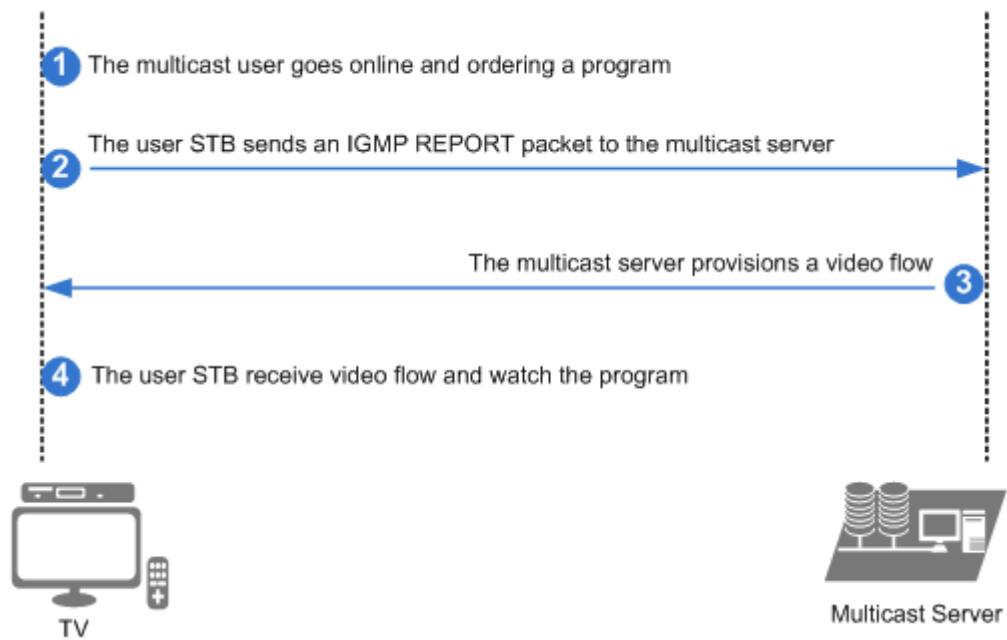
This user is **online**.

```
huawei#display igmp user service-port 500
User : 0/1/0/500
State : online
Authentication : auth
Quick leave : MAC-based
.....
```

7.2.2.2 Fault Identification and Demarcation

Overview

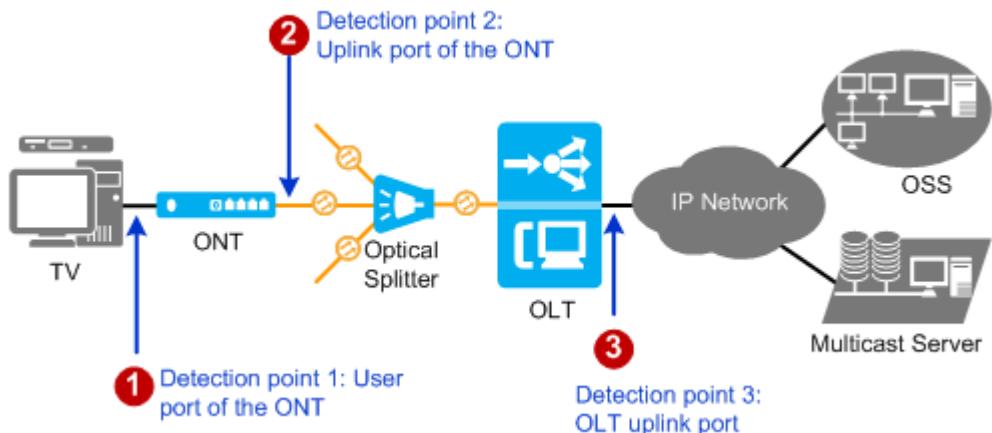
The process of ordering a video is as follows:



1. The multicast user goes online and ordering a video.
2. The user STB sends an IGMP REPORT packet to the multicast server.
3. Based on the received IGMP REPORT packet, the multicast server provisions a video flow.
4. The network device forward the video flow to the user STB.

Fault Demarcation

When a blank screen occurs on an FTTH network, demarcate the fault where the video stream was interrupted, as shown in .



Detection point	Symptom	Possible Cause
Detection point 1	Multicast streams reach the user port of the ONT	User terminal is faulty.
Detection point 2	Multicast streams reach the upstream port of the ONT but do not reach the user port of the ONT.	<ul style="list-style-type: none"> The remaining multicast bandwidth is lower than the required bandwidth of the ordered program. The number of programs watched by the multicast user reaches the upper limit. The number of programs at a level watched by the multicast user reaches the upper limit. The multicast user does not have the permission to watch the program. The program ordered is not in the MVLAN to which the multicast user belongs. There are too many prejoined static programs, occupying too many bandwidths.
Detection point 3	Multicast streams reach the upstream port of the OLT but do not reach the upstream port of the ONT. Multicast streams do not reach the upstream port of the OLT.	<ul style="list-style-type: none"> The program ordered is not in the MVLAN to which the multicast user belongs. The maximum multicast bandwidth assigned to the PON port is very low.

NOTE

The cause of blank screens may differ from the scenario, and errors may have occurred during deployment or maintenance. Locate the fault based on applicable scenarios.

- If this fault occurs during site deployment, check the device hardware and the initial device software configuration.
- If this fault occurs during routine maintenance, this fault is unlikely to be caused by the device software. In this case, check the device hardware. If new users have been added or user configurations have been modified during routine maintenance, check user configurations.

7.2.2.3 Handling Process

7.2.2.3.1 The User Fails to Pass Bandwidth CAC

Fault Information

After multicast debugging is enabled on the OLT, whenever a user fails to order a video due to a bandwidth connection admission control (CAC) failure, the debugging information in the following figure is displayed.

```
huawei(config)#  
*0.367341940 huawei BTV/8/ALL:  
 2015-04-13 18:09:52 service-port index 0 receive an IGMP packet  
  Type: REPORT, Version: V2, Group IP: 224.1.1.2  
  Ethernet, src: 00-e0-fc-c4-80-34  
  IP, src: 10.1.1.11  
huawei(config)#  
*0.367341940 huawei BTV/8/ALL:  
  Warning: the user fails to pass bandwidth CAC  
Debugging information: "Warning: the user fails to pass bandwidth CAC"
```

Determining the Fault

The maximum bandwidth allocated to this user is less than the bandwidth of the video ordered by this user.

To query the maximum bandwidth allocated to this user, run the **display igmp user service-port index** command. To query the bandwidth of the video ordered by this user, run the **display igmp program name** command.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- Notify this user of insufficient bandwidth, which leads to inability to order videos.
- Run the **igmp user modify service-port index max-bandwidth** command to increase the maximum bandwidth allocated to this user.

7.2.2.3.2 Number of Specific Videos Ordered Has Reached the Upper Limit

Fault Information

After multicast debugging is enabled on the OLT, whenever a user fails to order a video due to number limitation, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
Type: REPORT, Version: V2, Group IP: 224.1.1.2
Ethernet, src: 00-e0-fc-c4-80-34
IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
Warning: the number of the grade program that the user is allowed to watch has reached maximum
Debugging information: "Warning: the number of the grade program that the user is allowed to watch has reached maximum"
```

Determining the Fault

The maximum number (**watch limit**) of specific videos that can be ordered by this user is **0**. To query the maximum number, run the **display igmp user extended-attributes user-index** command.



NOTE

- If the value of **watch limit** is **0**, this user is forbidden to watch this type of video. For example, if the value of **HDTV watch limit** is **0**, this user has no rights to watch high definition (HD) videos.
- If the value of **watch limit** is **no-limit**, the maximum number of specific videos that can be ordered by this user is not limited. However, the total number of videos that can be concurrently watched by this user is limited.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- Inform the user that they have no rights to watch this type of video.
- Run the **igmp user watch-limit** command to increase the number of specific videos that can be ordered by this user.

7.2.2.3.3 Total Number of Ordered Videos Has Reached the Upper Limit

Fault Information

After multicast debugging is enabled on the OLT, whenever a user fails to order a video due to number limitation, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
Type: REPORT, Version: V2, Group IP: 224.1.1.2
Ethernet, src: 00-e0-fc-c4-80-34
IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
Warning: the number of program that the user is allowed to watch has reached maximum
Debugging information: "Warning: the number of program that the user is allowed to watch has reached maximum"
```

Determining the Fault

The total number of ordered videos has reached the maximum number that can be ordered by this user. To query the two numbers, run the **display igmp user service-port index** command.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- Inform the user that they have no rights to watch more videos.
- Run the **igmp user modify service-port index max-program max-program-num** command to increase the total number of videos that can be ordered by this user.

7.2.2.3.4 User Has No Rights to Watch a Video

Fault Information

After multicast debugging is enabled on the OLT, whenever a user fails to order a video due to rights limitation, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
 2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
  Type: REPORT, Version: V2, Group IP: 224.1.1.2
  Ethernet, src: 00-e0-fc-c4-80-34
  IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
  Warning: the user has no right
Debugging information: "Warning: the user has no right"
```

Determining the Fault

To determine whether the failure in ordering videos is caused by rights limitation, run the **display igmp service-port 100** command. In this command, the index of this service-port is assumed to be 100.

- If the number of **Bind profiles** is 0, no rights profile has been bound to this user and no videos can be ordered.
- If the number of **Bind profiles** is 1 or larger, this user can order only permitted videos. In queried results, identify the index (which is assumed to be 1) and name of the rights profile bound to this user, then, run the **display igmp profile profile-index 1** command to query the rights of this user.
 - If the queried result is **forbidden** or **idle**, this user has no rights to watch this video.
 - If the queried result is **watch** or **preview**, this user has rights to watch this video, which is excluded from the possible offline causes. **preview** right is after a user watches a video for a period of time (for example, a few minutes), the video stops playing, or a blank screen occurs.

 NOTE

Multiple rights profiles can be bound to one user. If these profiles specify different rights for a video, the rights with the highest priority take effect for this user. By default, the rights priorities of **forbidden**, **preview**, **watch**, and **idle** are in descending order. This order can be changed by running the **igmp right-priority** command.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- If this user does not require authentication and can watch all videos, run the **igmp user modify service-port 100 no-auth** command in BTV mode to configure this user to not require authentication. In this command, the index of this service-port is assumed to be 100.
- If this user requires authentication and can watch only some videos, inform the user that they have no rights to watch this video.
- If this user can only preview the video, inform the user that they can only watch for the permitted duration.
- If this user has viewing rights, modify or replace the rights profile bound to this user.
 - Modifying the rights profile: Run the **igmp profile profile-index 0 program-name PROGRAM-0 watch** to change the viewing rights from **preview** to **watch**.
 - Replacing the rights profile: Run the **undo igmp user bind-profile** command to unbind the original rights profile, then, run the **igmp user bind-profile** command to bind a new rights profile for this user.

7.2.2.3.5 Match Program Fail

Fault Information

After multicast debugging is enabled on the OLT, whenever a user fails to order a video due to rights limitation, the debugging information in the following figure is displayed.

```
huawei(config)#  
*0.367341940 huawei BTV/8/ALL:  
 2015-04-13 18:09:52 service-port index 0 receive an IGMP packet  
  Type: REPORT, Version: V2, Group IP: 224.1.1.2  
  Ethernet, src: 00-e0-fc-c4-80-34  
  IP, src: 10.1.1.11  
huawei(config)#  
*0.367341940 huawei BTV/8/ALL:  
  Warning: match program fail  
Debugging information: "Warning: match program fail"
```

Determining the Fault

Possible Cause	Determination Basis
This user is not an M-VLAN member	To query M-VLAN members, run the display igmp multicast-vlan member vlanid command. NOTE A user can watch videos configured in an M-VLAN only if this user is a member in this M-VLAN.
Ordered Video Is Not Contained in the M-VLAN Video List	The video list of the M-VLAN does not contain the ordered video. To query an M-VLAN video list, run the display igmp program vlan command.
No Multicast Uplink Port Has Been Configured in the M-VLAN	No multicast uplink port has been configured in the M-VLAN. To query the uplink port of an M-VLAN, run the display igmp uplink-port all command.

Troubleshooting

Possible Cause	Handling Method
This user is not an M-VLAN member	Use either of the following methods to rectify this fault based on the user's service type: <ul style="list-style-type: none">• Inform the user that they have no rights to watch this video.• In M-VLAN mode, run the igmp multicast-vlan member service-port index command to add this user to the M-VLAN.

Possible Cause	Handling Method
Ordered Video Is Not Contained in the M-VLAN Video List	<p>Use either of the following methods to rectify this fault based on the user's service type:</p> <ul style="list-style-type: none"> If this user has not subscribed to this video, inform the user that they have no rights to watch this type of video. If this user has subscribed to this video, perform the following operations: <ol style="list-style-type: none"> Run the display igmp config vlan command to query the video mapping mode (Program match mode) supported by the M-VLAN. <ul style="list-style-type: none"> If the value of Program match mode is enable, this video is a static one and requires configuration before it can be ordered. If the value of Program match mode is disable, this video is a dynamic one and automatically generated when a user orders it. Add this video to the M-VLAN video list. <ul style="list-style-type: none"> For a static video, run the igmp program add command. For a dynamic video, run the igmp match group command to configure the address range for the M-VLAN video list. Ensure that the IP address of this ordered video is within the address range.
No Multicast Uplink Port Has Been Configured in the M-VLAN	In M-VLAN mode, run the igmp uplink-port command to configure the uplink port on the OLT as the multicast uplink port. Then, all multicast packets in this M-VLAN can be forwarded using this uplink port.

7.2.2.3.6 Prejoined Videos Use an Excessively High Bandwidth

Fault Information

A blank screen occurs only in some ordered videos.

Determining the Fault

Video prejoin has been enabled for all videos. To query the prejoin status of all videos, run the **display igmp program all** command.

```
huawei(config-btv)#display igmp program all
```

Index	Create	IP	Program	User	VLAN	Prejoin	Priority
Flag	Address	name	num	ID			

0	S	224.1.1.1	PROGRAM-0	0	2	enable	7
1	S	224.1.1.2	PROGRAM-1	0	2	enable	7
2	S	224.1.1.3	PROGRAM-2	0	2	enable	7
3	S	224.1.1.4	PROGRAM-3	0	2	enable	7

Total: 4 program(s) (Static/Dynamic: 4/0)

The bandwidth used by prejoined static videos is so high that it reaches the maximum downstream bandwidth allocated to the PON port connected to the affected ONT. As a result, no more video can be ordered due to an insufficient bandwidth.

Perform the following operations on the OLT to query the maximum downstream bandwidth allocated to a PON port:

1. Run the **display igmp config global** command to query the status of bandwidth management, which should be **enable**.
2. Run the **display igmp bandwidth port** command to query the maximum downstream bandwidth allocated to the PON port.

Troubleshooting

Although the video prejoin function implements rapid video ordering, prejoined videos may use an excessively high bandwidth. Rectify the fault based on service scenarios.

Service Scenario	Handling Method
The video prejoin function is required for rapid video ordering.	Run the igmp bandwidth port command on the OLT to increase the maximum downstream bandwidth allocated to the PON port.
The video prejoin function is not required for rapid video ordering.	Run the igmp program modify command on the OLT to disable video prejoin.

NOTE

The status of video prejoin for all videos can be changed in any M-VLAN. However, the status cannot be changed for a video that is being played.

7.2.2.3.7 Maximum Downstream Bandwidth Allocated to a PON Port Is Excessively Low

Fault Information

Videos can be ordered properly at working hours. However, a blank screen occurs when videos are ordered during traffic rush hours at night.

Determining the Fault

The remaining bandwidth of the PON port connected to the affected ONT is less than the bandwidth required by the ordered video. As a result, this video fails to order due to an insufficient bandwidth.

Perform the following operations on the OLT to query the remaining bandwidth of a PON port:

1. Run the **display igmp config global** command to query the status of bandwidth management, which should be **enable**.
2. Run the **display igmp bandwidth port** command to query the maximum downstream bandwidth allocated to the PON port and the used bandwidth of this port.
3. Use the following formula to calculate the remaining bandwidth of the PON port: Remaining bandwidth = Maximum downstream bandwidth allocated to the PON port - Used bandwidth of this port

Troubleshooting

Run the **igmp bandwidth port** command on the OLT to increase the maximum downstream bandwidth allocated to the PON port.

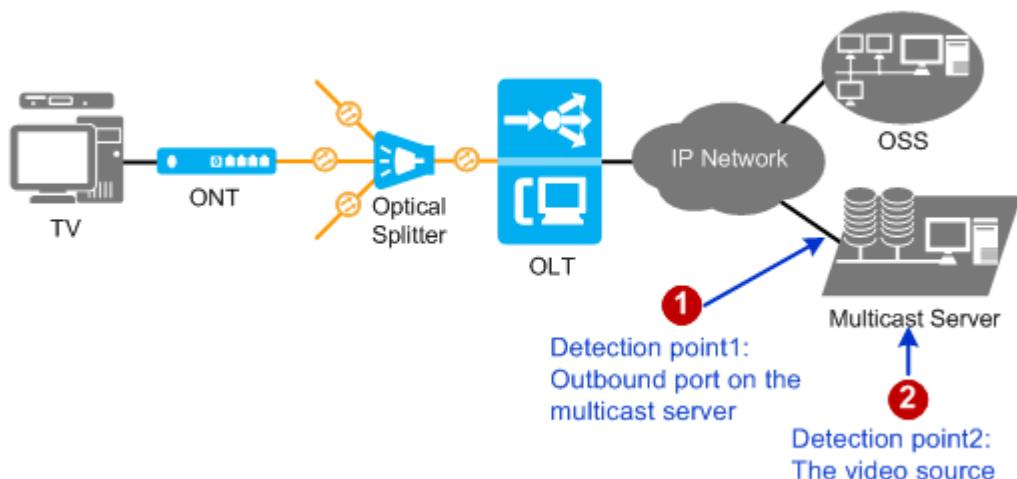
7.2.2.3.8 Poor Video Source Quality

Fault Information

Video stops or a blank screen occurs for all users connected to a multicast server.

Determining the Fault

If all users connected to the multicast server are affected, the fault occurs on the multicast server. The method of determining the fault is shown in the following figure.



Detection Point	Determination Basis
Detection point 1: video source	<p>View the video on the screen of the multicast server.</p> <ul style="list-style-type: none"> If the video is functional, the video source is excluded from the possible blank screen causes. If the video stops or a blank screen occurs, the media file of the video source is incorrect.
Detection point 2: outbound port on the multicast server	<p>Capture packets on the outbound port of the multicast server and restore the video from the packets. Alternatively, order a video on the outbound port.</p> <ul style="list-style-type: none"> If the video is functional, the video source is excluded from the possible blank screen causes. If the video stops or a blank screen occurs, the fault occurs on the multicast server. <ul style="list-style-type: none"> The multicast server is faulty. An error occurs in video codec. <p>NOTE</p> <p>Capture packets may involve obtaining the personal information, such as the IP address, MAC address, the personal data of users and the content of users' communications (the product does not save, parse, or process such information). Huawei alone is unable to collect or save the personal data of users and the content of users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the personal data of users and the content of users' communications are fully protected when the personal data and the content are being used and saved.</p>

Troubleshooting

Fault Point	Handling Method
Media file of the video source is incorrect.	Verify that parameter settings in the file comply with service requirements.
The multicast server is faulty.	<p>Check and rectify the following faults on the multicast server:</p> <ul style="list-style-type: none"> The load or CPU usage is excessively high, or the available memory is insufficient. The number of users connected by the multicast server has reached the upper limit. An alarm affecting services has been generated. The outbound port is faulty. Data configuration is incorrect.

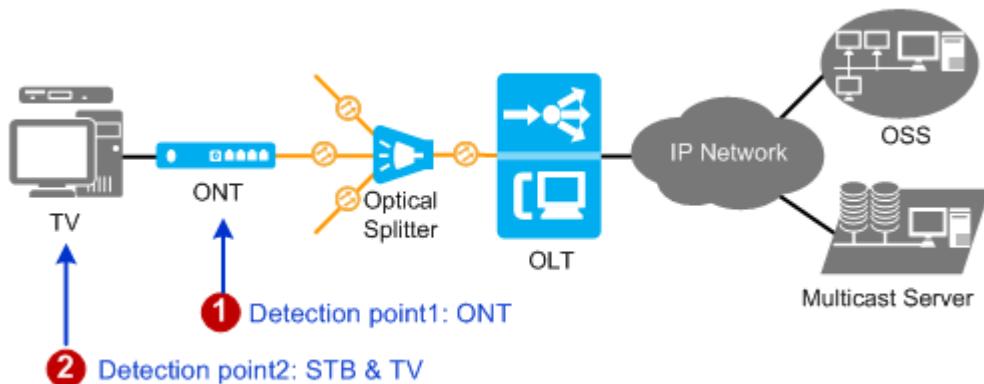
7.2.2.3.9 User Terminal Is Faulty

Fault Information

The user online, ordered video stream has reached the user port. However, a faulty occurs for this user.

Confirm the Fault

The ordered video stream has reached the user port. However, a faulty occurs for this user. In this case, the user terminal may be faulty.



Detection Point	Determination Basis
Detection point 1: ONT	The ONT indicator is faulty. After the ONT is restarted or replaced, this fault is rectified.
Detection point 2: STB and TV	<ul style="list-style-type: none">After the STB is restarted or replaced, this fault is rectified.After the TV video cable is connected to a video input device, such as a digital video disc (DVD) recorder or a video recorder, this fault persists.

To query the multicast video ordered by a user, run the following command:

```
huawei#display igmp user service-port 500
User          : 0/1/0/500
State         : online
.....
-----
Program name  VLAN  IP/MAC      State       Start time
-----
PROGRAM-0     1      224.1.1.1  watching    2015-03-15
                           16:02:38+08:00
```

The preceding terminal display shows that the IP address of the ordered video is 224.1.1.1 and the M-VLAN ID is 1.

To query real-time video traffic on the multicast uplink port, run the following command:

```
huawei#display multicast flow-statistic vlan 1 ip 224.1.1.1
Command is being executed. Please wait...
Multicast flow statistic result: 4096(kbps)
```

The preceding terminal display shows that the video traffic on the multicast uplink port is 4096 kbit/s, which is the same as the traffic of the ordered video. This indicates that the video stream has reached the multicast uplink port.

To query the traffic collected on the service port of the multicast user, run the **display statistics service-port 500** command. In this command, parameter **Number of downstream bytes** specifies the video traffic collected on the user terminal, which is the same as the traffic of the ordered video. This indicates that the video stream has reached the user terminal.

Troubleshooting

Possible Cause	Judgment Criterion	Troubleshooting Method
The STB is faulty.	The user can go online after resetting the STB or replacing the STB with a functional one and ordering the program.	Reset the STB or replace the STB with a functional one.
The ONT is faulty.	The user can go online after resetting the ONT or replacing the ONT with a functional one and ordering the program.	Reset the ONT or replace the ONT with a functional one.
The physical line between the STB and ONT is faulty. For example, the network cable is not securely connected, is damaged, or is incorrectly connected.	<p>Check the LAN indicator on the ONT (the HG8245 is used as an example) to determine the status of the physical line between the STB and ONT.</p> <ul style="list-style-type: none">• If the LAN indicator is off, the line is faulty.• If the LAN indicator is steady on or blinks, the line is in the normal state.	Connect the network cable again or replace the network cable with a functional one.

7.2.3 Multicast Video Artifacts and Intermittent Video Stops

This section describes how to identify and resolve the appearance of multicast video artifacts and intermittent video stops that occur on a fiber to the home (FTTH) network.

7.2.3.1 Symptoms

Multicast Video Artifacts

Artifacts appear on the screen during the display of a multicast video if one or multiple of the following cases continuously occur: pixelation, stripes, stains, color blocks, position reversal, video jitter, or image distortion, as shown in [Figure 7-5](#).

Figure 7-5 Example of multicast video artifacts



Intermittent Multicast Video Stops

Intermittent multicast video stops occur when the display of a multicast video is not smooth or stops for a long period of time (for example, a few minutes) for video loading, as shown in [Figure 7-6](#).

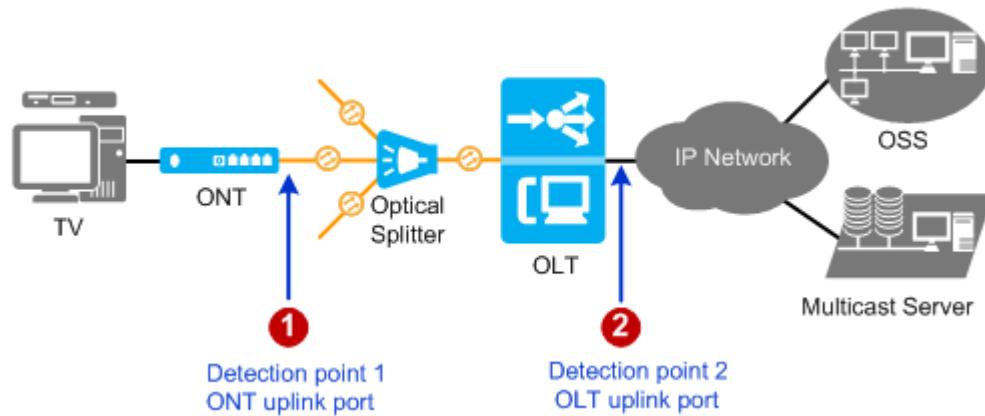
Figure 7-6 Example of intermittent multicast video stops



7.2.3.2 Fault Identification and Demarcation

Fault Demarcation

If multicast video artifacts appear or intermittent video stops occur on an FTTH network, identify the location where packet loss has occurred on demarcate the fault, as shown in [Figure 7-7](#).

Figure 7-7 Fault demarcation

Detection Point	Symptom	Possible Cause
Detection point 1	Packet loss does not occur on the ONT uplink port	<ul style="list-style-type: none">User bandwidth is insufficient.User terminal is faulty.
Detection point 1	Packet loss does not occur on the OLT uplink port, but packet loss occurs on the ONT uplink port	Poor ODN lines quality.
	Packet loss occurs on the OLT uplink port	<ul style="list-style-type: none">Poor video source quality.Poor OLT's upper-Layer network quality.

7.2.3.3 Handling Process

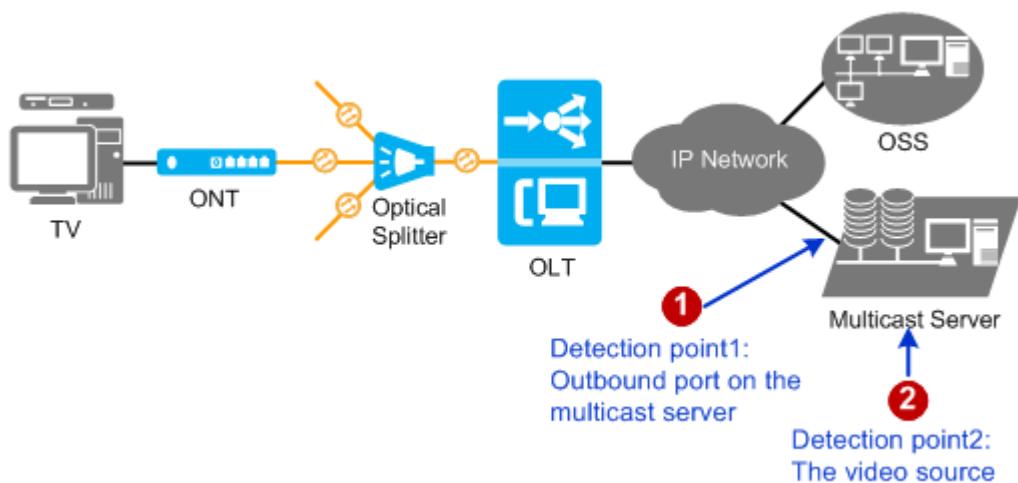
7.2.3.3.1 Poor Video Source Quality

Fault Information

Video stops or a blank screen occurs for all users connected to a multicast server.

Determining the Fault

If all users connected to the multicast server are affected, the fault occurs on the multicast server. The method of determining the fault is shown in the following figure.



Detection Point	Determination Basis
Detection point 1: video source	<p>View the video on the screen of the multicast server.</p> <ul style="list-style-type: none"> If the video is functional, the video source is excluded from the possible blank screen causes. If the video stops or a blank screen occurs, the media file of the video source is incorrect.
Detection point 2: outbound port on the multicast server	<p>Capture packets on the outbound port of the multicast server and restore the video from the packets. Alternatively, order a video on the outbound port.</p> <ul style="list-style-type: none"> If the video is functional, the video source is excluded from the possible blank screen causes. If the video stops or a blank screen occurs, the fault occurs on the multicast server. <ul style="list-style-type: none"> The multicast server is faulty. An error occurs in video codec. <p>NOTE Capture packets may involve obtaining the personal information, such as the IP address, MAC address, the personal data of users and the content of users' communications (the product does not save, parse, or process such information). Huawei alone is unable to collect or save the personal data of users and the content of users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the personal data of users and the content of users' communications are fully protected when the personal data and the content are being used and saved.</p>

Troubleshooting

Fault Point	Handling Method
Media file of the video source is incorrect.	Verify that parameter settings in the file comply with service requirements.
The multicast server is faulty.	<p>Check and rectify the following faults on the multicast server:</p> <ul style="list-style-type: none">• The load or CPU usage is excessively high, or the available memory is insufficient.• The number of users connected by the multicast server has reached the upper limit.• An alarm affecting services has been generated.• The outbound port is faulty.• Data configuration is incorrect.

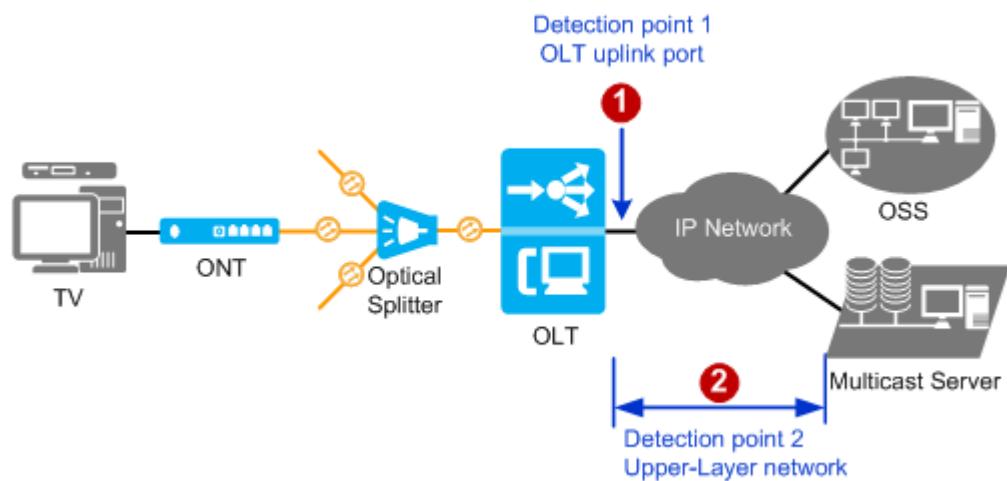
7.2.3.3.2 Poor OLT's Upper-Layer Network Quality

Fault Information

The ordered video stream has reached the OLT uplink port. However, packets have been lost.

Fault Locating Guide

The guide to locate an issue caused by poor OLT's upper-layer network quality.



Detection Point	Determination Basis
Detection point 1: OLT uplink port	<ul style="list-style-type: none">• The uplink port state is abnormal.• The status of the optical module installed in the uplink port is abnormal.

Detection Point	Determination Basis
Detection point 2: OLT upper-layer network	Packets have been lost before the video stream reaches the uplink port on the OLT.

Procedure

Step 1 Check whether the optical module installed in the uplink port on the OLT is functional.

1. Check whether the uplink port is functional.

An OLT equipped with a ETH board for upstream transmission is used as an example. Run the **display port state all** command to query the status of the optical module installed in the uplink port.

The value of the **Optic Status** parameter specifies the status of the optical module.

- **absence**: indicates that the optical module is not securely installed.
- **abnormal**: indicates that the optical module is faulty.
- **normal**: indicates that the optical module is securely installed.

2. Run the **display port ddm-info** command to query the diagnosis information about the optical module.

```
hauwei(config-if-eth-0/19)#display port ddm-info 0
Temperature(C)          : 38.375000
Supply voltage(V)       : 3.304000
TX bias current(mA)    : 16.541125
TX power(dBm)          : -6.623598
RX power(dBm)          : -6.292528
```

Both TX and RX optical power is generally -5 dBm. If the queried value is significantly different from this value, the optical path is unreachable. In this case, you must check the optical path.

Step 2 Check line quality on the upper-layer network.

Start a **multicast emulation test** on the OLT. After the test is complete, run the **display multicast flow-statistic vlan 3 ip 224.1.1.1** command to query the real-time traffic parameter **Multicast flow statistic result** of the multicast video. The multicast VLAN (M-VLAN) and IP address of the video are assumed to be 3 and 224.1.1.1, respectively. Then, perform operations listed in the following table based on queried results.

Queried Result	Handling Method
The real-time traffic of the multicast video is approximately the same as the rate of the video stream.	The video stream has reached the uplink port on the OLT properly. In this case, packets are not lost on the upper-layer network.

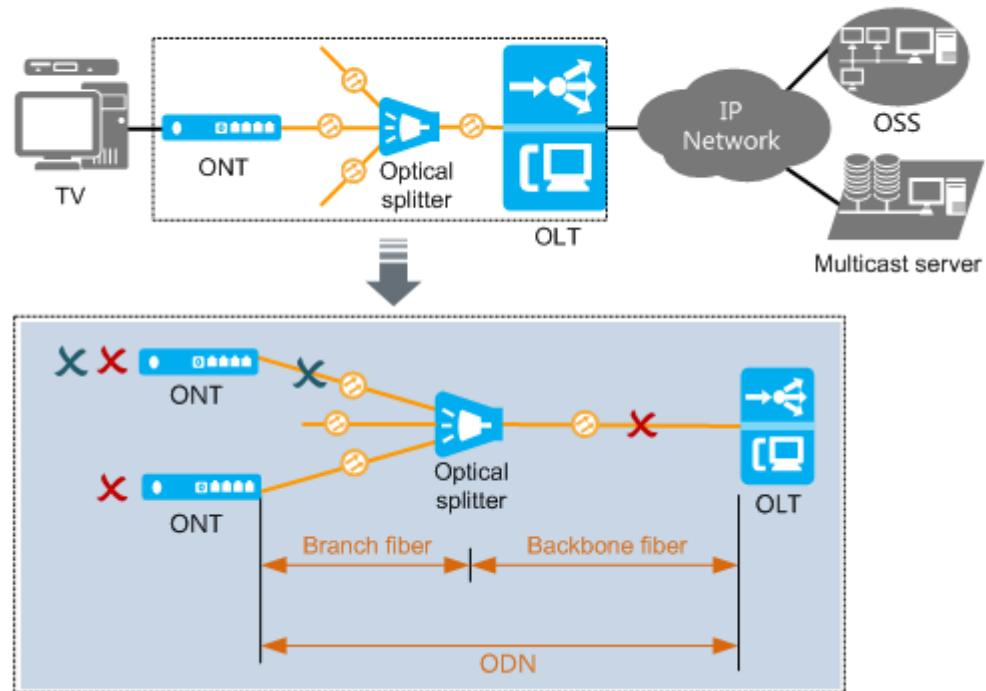
Queried Result	Handling Method
The real-time traffic of the multicast video is significantly less than the rate of the video stream.	<p>Packets have been lost before the video stream reaches the uplink port on the OLT. In this case, the line quality of the OLT's upper-layer network must be poor.</p> <ul style="list-style-type: none"> Check whether the optical fiber is securely connected to the uplink port and whether the fiber connector is clean. Connect the optical fiber to the uplink port again, or replace this optical fiber. Check upper-layer devices, such as the switch, router.

----End

7.2.3.3.3 Poor ODN Line Quality

Fault Locating Guide

The network between a PON port on an OLT and ONTs is shown in the following figure.



In this figure:

- Poor feeder fiber quality prevents service provisioning on all ONTs connected to the PON port.

- Poor branch fiber quality prevents service provisioning on oneONT.

Troubleshooting Guide

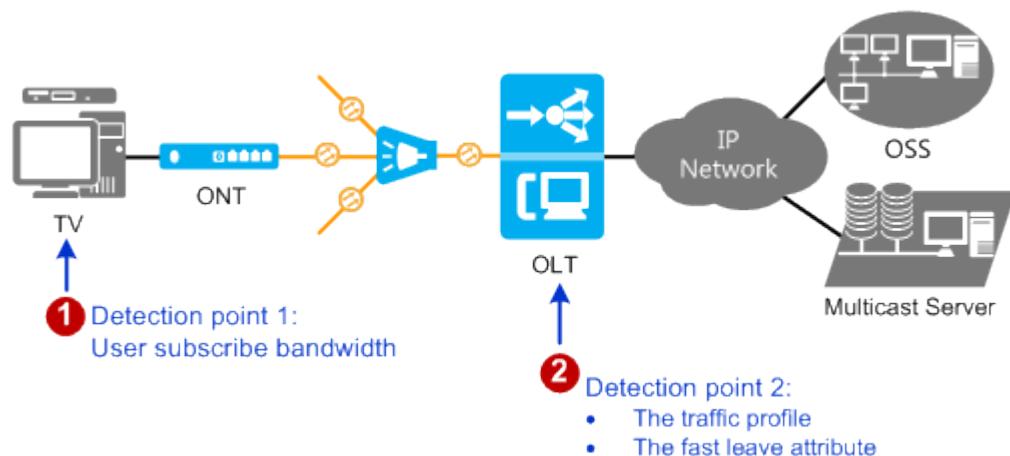
Please refer to [<Methods of Locating and Troubleshooting Common ODN Faults>](#).

7.2.3.3.4 User Bandwidth Is Insufficient

Fault Locating Guide

If a user port carries other services, such as Internet access, in addition to multicast, the bandwidth of all services on this user port must be less than or equal to the target rate. Otherwise, artifacts may appear due to insufficient multicast bandwidth.

The guide to locate an issue caused by an insufficient user bandwidth.



Detection Point	Determination Basis
Detection point 1: User subscribe bandwidth	The subscribed user bandwidth is too low to support the multicast service.
Detection point 2: <ul style="list-style-type: none">• The traffic profile• The fast leave attribute	<ul style="list-style-type: none">• The traffic profile bound to the multicast service is incorrect.• The function of quick leave is disable.

Procedure

Step 1 Check the subscribed user bandwidth.

If the subscribed user bandwidth is too low to support the multicast service, artifacts are caused by insufficient user bandwidth.

Use either of the following methods to rectify this fault based on the user's service type:

- Notify this user of insufficient bandwidth, which leads to inability to order videos.
- Increase the bandwidth allocated to this user.

 **NOTE**

If a user port carries other services, such as Internet access, in addition to multicast, the bandwidth of all services on this user port must be less than or equal to the target rate. Otherwise, artifacts may appear due to insufficient multicast bandwidth.

Step 2 Check whether the traffic profile bound to the ONT is correct.

Run the **display service-port** command on the OLT to query the index of the RX traffic for the multicast service flow. Then, run the **display traffic table ip** command to query the peak information rate (PIR) of the traffic profile bound to the multicast service flow.

If the service port carries other service flows in addition to the multicast service flow, the bandwidth of all services on this service port must be less than or equal to PIR.

 **NOTE**

Common and high definition (HD) videos require different bandwidths. Empirical values are as follows:

- Bandwidth required by common videos: < 5 Mbit/s
- Bandwidth required by HD videos: > 12 Mbit/s

Change the traffic profile bound to the multicast service flow based on site requirements.

- If a proper traffic profile is available, run the **service-port 100 outbound traffic-table index 6** command on the OLT to bind the new traffic profile to the multicast service flow. The indexes of the multicast service flow and the new traffic profile are assumed to be 100 and 6, respectively.
- If no proper traffic profile is available, run the **traffic table ip** command on the OLT to create a desired traffic profile. Bind the new traffic profile to the multicast service flow.

Step 3 Check the configured user attribute.

If multicast video artifacts appear only when videos are switched, the maximum bandwidth of this user must be higher than the downstream line rate, and the fast leave function is not enabled.

Determination Basis	Handling Method
Run the display igmp user service-port index command to query the fast leave attribute (quick leave).	If the value of quick leave is disable , change the attribute based on the application scenario of this user. <ul style="list-style-type: none">• If this user connects to multiple VoD terminals, change the attribute to mac-based.• If this user connects to only one VoD terminal, change the attribute to immediate.

Determination Basis	Handling Method
Run the display igmp user service-port index command to query the maximum bandwidth of the video (User MaxBandWidth).	If the value of User MaxBandWidth is greater than the downstream line rate, artifacts appear due to insufficient line bandwidth. Run the igmp user modify user-index max-bandwidth command to change the maximum bandwidth for this user to be lower than the line rate.

----End

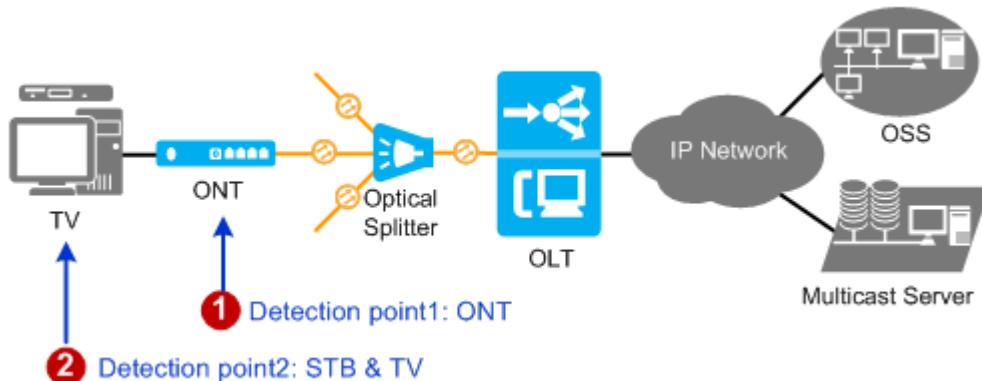
7.2.3.3.5 User Terminal Is Faulty

Fault Information

The user online, ordered video stream has reached the user port. However, a faulty occurs for this user.

Confirm the Fault

The ordered video stream has reached the user port. However, a faulty occurs for this user. In this case, the user terminal may be faulty.



Detection Point	Determination Basis
Detection point 1: ONT	The ONT indicator is faulty. After the ONT is restarted or replaced, this fault is rectified.
Detection point 2: STB and TV	<ul style="list-style-type: none"> After the STB is restarted or replaced, this fault is rectified. After the TV video cable is connected to a video input device, such as a digital video disc (DVD) recorder or a video recorder, this fault persists.

To query the multicast video ordered by a user, run the following command:

```
huawei#display igmp user service-port 500
User          : 0/1/0/500
State         : online
.....
-----
Program name  VLAN IP/MAC      State       Start time
-----
PROGRAM-0     1    224.1.1.1   watching    2015-03-15
                           16:02:38+08:00
```

The preceding terminal display shows that the IP address of the ordered video is 224.1.1.1 and the M-VLAN ID is 1.

To query real-time video traffic on the multicast uplink port, run the following command:

```
huawei#display multicast flow-statistic vlan 1 ip 224.1.1.1
Command is being executed. Please wait...
Multicast flow statistic result: 4096(kbps)
```

The preceding terminal display shows that the video traffic on the multicast uplink port is 4096 kbit/s, which is the same as the traffic of the ordered video. This indicates that the video stream has reached the multicast uplink port.

To query the traffic collected on the service port of the multicast user, run the **display statistics service-port 500** command. In this command, parameter **Number of downstream bytes** specifies the video traffic collected on the user terminal, which is the same as the traffic of the ordered video. This indicates that the video stream has reached the user terminal.

Troubleshooting

Possible Cause	Judgment Criterion	Troubleshooting Method
The STB is faulty.	The user can go online after resetting the STB or replacing the STB with a functional one and ordering the program.	Reset the STB or replace the STB with a functional one.
The ONT is faulty.	The user can go online after resetting the ONT or replacing the ONT with a functional one and ordering the program.	Reset the ONT or replace the ONT with a functional one.
The physical line between the STB and ONT is faulty. For example, the network cable is not securely connected, is damaged, or is incorrectly connected.	<p>Check the LAN indicator on the ONT (the HG8245 is used as an example) to determine the status of the physical line between the STB and ONT.</p> <ul style="list-style-type: none">If the LAN indicator is off, the line is faulty.If the LAN indicator is steady on or blinks, the line is in the normal state.	Connect the network cable again or replace the network cable with a functional one.

7.3 Troubleshooting Voice Service Faults

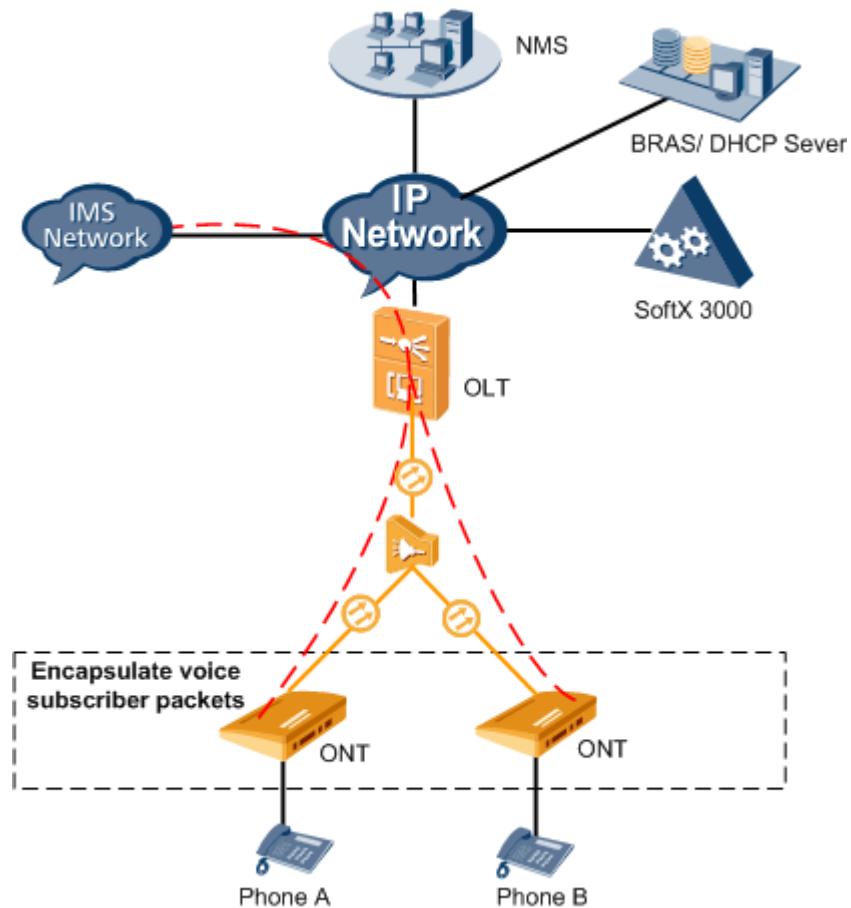
This topic describes how to troubleshoot voice service faults in a fiber to the home (FTTH) network. Common voice service faults include: no tone after offhook, busy tone after offhook, one-way audio in a voice call, noise in a voice call, voice interruptions in a voice call, and failure to dial certain phone numbers.

Prerequisites

- The ONT and OLT communicate with each other normally. If a fault occurs in a voice call between the ONT and OLT, all the services on the ONT may be interrupted. In this case, troubleshoot the fault first by referring to the methods described in [ONT Abnormal State](#).
- For different types of ONTs, methods for troubleshooting voice service faults are different. This topic uses HG8240, HG8245 and HG8247 series as examples.

Context

In an FTTH network, voice subscribers access the network by using ONTs, and the ONTs work together with an upper-layer softswitch or IMS network to achieve the VoIP service. After encapsulated by ONTs that serve as MG or SIP interfaces, voice packets are forwarded to the next generation network (NGN) through the OLT. The following figure shows an FTTH network for voice service.



 NOTE

Voice signaling tracing and voice VBD fault diagnosis may be used in voice service troubleshooting.

Based on your requirements, signaling tracing may obtain some contents of users' communications

(integrity communication contents are not obtained and user information will not be disclosed)

for the purpose of safeguarding network operations and protecting services.

Huawei alone is unable to collect or save the content of users' communications.

You must comply with the laws and regulations of the countries concerned for using the signaling tracing feature.

You are obligated to take considerable measures to ensure that the content of users' communications is fully protected when the content is being used and saved.

7.3.1 No Power Feed After Offhook

This section describes how to troubleshoot the fault where there is no power feed when a phone goes offhook. When this fault occurs, the phone does not respond after going offhook, and the "phone in use" indicator is off, which means that the phone has no power feed.

Location Method

When an FTTH subscriber hears no power feed after offhook, possible causes are as follows:

- The phone is faulty.
- The line between the phone and the POTS port (POTS refers to plain old telephone service) is faulty.
- The line between the phone and the POTS port is not properly connected.
- The ONT POTS port is faulty.

 NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Perform the voice loop line test on the ONT. If a fault occurs, rectify it according to the test conclusion. If the subscriber hears no tone after offhook after the rectification, go to [Step 2](#).

Test Result	Possible Cause	Troubleshooting Method
<ul style="list-style-type: none">• Normal• Phone disconnected	-	No process is needed because the loop line and phone are normal.

Test Result	Possible Cause	Troubleshooting Method
<ul style="list-style-type: none"> ● AC current abnormal ● DC current abnormal ● Loop current abnormal ● Loop resistance abnormal ● Insulating resistance abnormal ● Capacitance abnormal ● Impedance abnormal ● Insulating not good ● Broken lines ● Line mixing ● Connected to ground ● AB Line reversal ● Line leaking 	The line between the phone and the POTS port is faulty.	Replace the line between the phone and the POTS port.
Broken lines	<ul style="list-style-type: none"> ● The phone is faulty. ● The line between the phone and the POTS port is faulty. ● The line between the phone and the POTS port is not properly connected. 	<ul style="list-style-type: none"> ● Replace the phone. ● Replace the line between the phone and the POTS port. ● Re-connect the line between the phone and the POTS port properly.

Step 2 Connect the phone that encounters the fault to another POTS port. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, the original ONT POTS port is faulty. In this case, replace the ONT by referring to [Replacing an ONT](#). Then, go to **Step 4**.
- Then, go to **Step 3**.

Step 3 Connect Technical Support.

Step 4 The fault is rectified.

----End

7.3.2 No Tone After Offhook

No tone after offhook indicates that a subscriber hears no tone or only a weak current noise after offhook. When such a fault occurs in an FTTH network, locate the fault according to the following procedure.

Cause Analysis

When an FTTH subscriber hears no tone after offhook, possible causes are as follows:

- The ONT domain name set on the softswitch is inconsistent with the domain name set on the ONT.
- The phone is faulty.
- The line between the phone and the POTS (POTS refers to plain old telephone service) port is faulty.
- The line between the phone and the POTS port is not properly connected.
- The POTS port is faulty.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Perform the voice loop line test on the ONT. If a fault occurs, rectify it according to the test conclusion. If the subscriber hears no tone after offhook after the rectification, go to [Step 2](#).

Test Result	Possible Cause	Troubleshooting Method
<ul style="list-style-type: none">• Normal• Phone disconnected	-	No process is needed because the loop line and phone are normal.
<ul style="list-style-type: none">• AC current abnormal• DC current abnormal• Loop current abnormal• Loop resistance abnormal• Insulating resistance abnormal• Capacitance abnormal• Impedance abnormal• Insulating not good• Broken lines• Line mixing• Connected to ground• AB Line reversal• Line leaking	The line between the phone and the POTS port is faulty.	Replace the line between the phone and the POTS port.

Test Result	Possible Cause	Troubleshooting Method
Broken lines	<ul style="list-style-type: none"> The phone is faulty. The line between the phone and the POTS port is faulty. The line between the phone and the POTS port is not properly connected. 	<ul style="list-style-type: none"> Replace the phone. Replace the line between the phone and the POTS port. Re-connect the line between the phone and the POTS port properly.

Step 2 Check whether the ONT domain name set on the softswitch is consistent with the domain name set on the ONT.

- If they are inconsistent, go to [Step 3](#).
- If they are consistent, go to [Step 4](#).

Step 3 Modify the ONT domain name set on the softswitch to be consistent with the domain name set on the ONT. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to [Step 7](#).
- If the fault persists, go to [Step 4](#).

Step 4 Connect the phone that encounters the fault to another POTS port. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to [Step 7](#).
- If the fault persists, go to [Step 5](#).

Step 5 The original ONT POTS port is faulty. In this case, replace the ONT by referring to [Replacing an ONT](#). Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to [Step 7](#).
- If the fault persists, go to [Step 6](#).

Step 6 Connect Technical Support.

Step 7 The fault is rectified.

----End

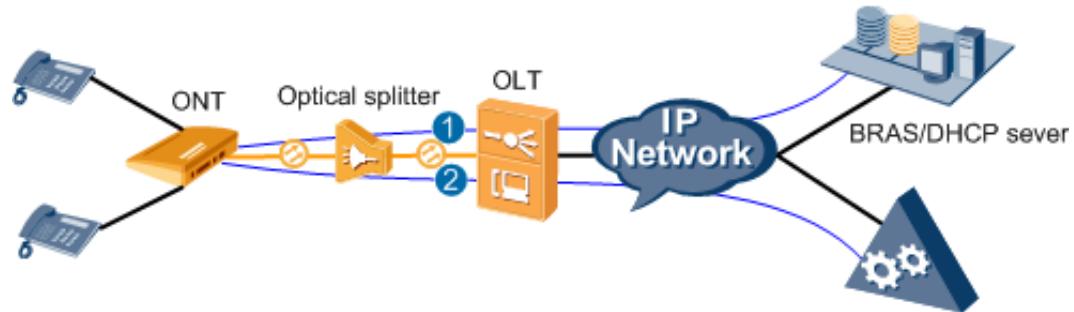
7.3.3 Busy Tone After Off-hook

After a user picks up the phone, no dial tone can be heard but only the busy tone can be heard. When a user hears the busy tone after off-hook in an FTTH network, locate and troubleshoot the fault by using the following location methods and troubleshooting procedure.

Location Method

The root cause of this fault is that the voice user is not registered with the MGC/IMS. It is recommended that you locate the fault by referring to [Figure 7-8](#).

Figure 7-8 Location method



- ① Checking scope: ONT → OLT → BRAS/DHCP sever
Judgment criterion: The ONT obtains the IP address.
- ② Checking scope: ONT → OLT → SoftX3000
Judgment criterion: The ONT voice user is successfully registered.

1. Network topology: ONT -> OLT -> BRAS or DHCP server. Check whether WAN connections for the voice service on the ONT are normal and whether they obtain IP addresses. If a WAN connection is abnormal and fails to obtain the IP address, the PPPoE dialup fails or the DHCP server fails to obtain the IP address. Rectify the fault that the DHCP server fails to obtain the IP address, see [7.1.4 PPPoE Dialup Failure](#) or [7.1.5 Failure to Obtain an IP Address in the DHCP Mode](#).
2. Network topology: ONT -> OLT -> MGC or IMS (SoftX3000 is used as an example). Check whether the voice user of the ONT is registered with the MGC or IMS. If the voice user is not registered with the MGC or IMS, the link from the ONT to the MGC or IMS is faulty or voice parameters of the MGC or IMS are incorrect. Rectify the corresponding fault.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Check whether WAN connections for the voice service on the ONT are normal and whether they obtain IP addresses. If a WAN connection is abnormal and fails to obtain the IP address, the PPPoE dialup fails or the DHCP server fails to obtain the IP address. Rectify the fault that the DHCP server fails to obtain the IP address, see [7.1.4 PPPoE Dialup Failure](#) or [7.1.5 Failure to Obtain an IP Address in the DHCP Mode](#).

Check and locate the fault through CLI, NMS, or web page, as described in the following table.

Checking Mode	Procedure	Judgment Criterion
CLI	Run the display ont wan-info command to check whether the WAN connection for the voice service is normal and whether the WAN connection obtains the IP address.	<ul style="list-style-type: none"> If IPv4 addresses are used and IPv4 Connection status is Connected, the WAN connection for the voice service is normal. If IPv4 address displays the IP address, the WAN connection for the voice service obtains the IP address.
NMS	Select the ONT to be queried from GPON ONU . On the WAN Interface tab page in the lower pane, check whether the WAN connection for the voice service is normal and whether the WAN connection obtains the IP address.	<ul style="list-style-type: none"> If IPv6 addresses are used and IPv6 Connection status is Connected, the WAN connection for the voice service is normal. If IPv6 address displays the IP address, the WAN connection for the voice service obtains the IP address. If IPv4 and IPv6 dual addresses are used and both IPv4 Connection status and IPv6 Connection status are Connected, the WAN connection for the voice service is normal. If IPv4 address and IPv6 address display the IP addresses, the WAN connections for the voice service obtain the IP addresses.
Web page	Choose Status > WAN Information from the navigation tree. In the right pane, check whether the WAN connection for the voice service is normal and whether the WAN connection obtains the IP address.	If Status is Connected , the WAN connection is normal. If IP Address displays the IP address, the WAN connection obtains the IP address.

Step 2 Check whether the voice user of the ONT is registered with the MGC or IMS. If the voice user is not registered with the MGC or IMS, the link from the ONT to the MGC or IMS is faulty or voice parameters of the MGC or IMS are incorrect. Rectify the fault by perform [Step 3](#) or [Step 4](#).

Check and locate the fault through CLI, NMS, or web page, as described in the following table.

Checking Mode	Procedure	Judgment Criterion
CLI	Run the display ont port state command to check whether the voice service is normal.	If Service state is InService , the service is normal.
NMS	Select the ONT to be queried from GPON ONU . On the POTS User tab page in the lower pane, check whether the voice service is normal.	If Service Status is In Service , the voice service is normal.
Web page	Choose Status > VoIP Information from the navigation tree. In the right pane, check whether the voice service is normal.	If User Status is Up , the voice service is normal.

Step 3 Rectify the fault on the link from the ONT to the MGC or IMS.

Check the quality of the link from the OLT to the MGC or IMS by referring to [5.7.6 Pinging from an ONT Remotely](#). If packets are lost or delay is very large, capture packets in an exclusive way to locate the device that drops packets or incorrectly forwards packets. Then, rectify the fault.

Step 4 Rectify the incorrect voice parameters of the MGC or IMS, as described in the following table.

There are various of voice parameters and methods of configuring these voice parameters. See the FTTx Solution Configuration to rectify such faults.

Possible Cause	Judgment Criterion	Troubleshooting Method
The type of the WAN connection for the voice service is incorrect.	Confirm that the WAN connection type of the voice service is not set to VoIP or VoIP combination.	Modify the WAN connection type of the voice service to VoIP or VoIP combination.
Voice users of the ONT are disabled.	Check whether voice users of the ONT are enabled.	Enable voice users of the ONT.

Possible Cause	Judgment Criterion	Troubleshooting Method
Voice parameters on the ONT or MGC or IMS are not configured or incorrectly configured.	<p>Voice parameters on the ONT or MGC or IMS are not configured or incorrectly configured if one of the following situations occurs:</p> <ul style="list-style-type: none"> • Confirm that voice parameters on the ONT or MGC or IMS are not configured. • Data configurations are different from the data plan. (Data configurations on the ONT must be the same as those on the MGC or IMS) <p>Key parameters of the H.248 voice service:</p> <ul style="list-style-type: none"> • MGC address and port ID • MID format, MG domain name, and device name • Prefix and digital length of the RTP TID • Terminal name (terminal ID) • Associated physical port (associated POTS port) <p>Key parameters of the SIP voice service:</p> <ul style="list-style-type: none"> • IP address and port ID of the SIP server • Home domain name • Registered user name (phone number of a voice user, which is unique on the ONT under the same softswitch) • Authentication user name and password • Associated physical port (associated POTS port) 	Configure the data correctly based on the data plan.

Possible Cause	Judgment Criterion	Troubleshooting Method
	<p>NOTE</p> <p>You can trace H.248 signaling on the MGC and check for error 502 to determine whether the RTP TID format of the MG is the same as that of the MGC.</p> <p>In the protocol, error 502 indicates that the terminal is invalid, including the RTP terminal and physical terminal. If error 502 is traced in the H.248 signaling on the MGC, the RTP TID format of the MG is different from that of the MGC. For example, RTPs on the MGC are RTP1000, RTP1001, and RTP1002,..., but RTPs on the MG are RTP500, RTP501, and RTP501...</p>	

Step 5 Make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 7**.
- If the fault persists, go to **Step 6**.

Step 6 Connect Technical Support.

Step 7 The fault is rectified.

----End

7.3.4 One-Way Audio in a Voice Call

One-way audio indicates that a subscriber can dial a phone number and hear the ring tone, but only the tone of one party can be heard in a voice call. When such a fault occurs in an FTTH network, locate the fault according to the following procedure.

Cause Analysis

When one-way audio occurs in an FTTH network, possible causes are as follows:

ACL (ACL refers to access control list) rules on the bearer network, OLT or ONT are not configured correctly.



- A subscriber can dial the phone number and hear the ring tone. Hence the signaling streams are normal.
- If a fault occurs on the bearer network, locate the fault by making phone calls between subscribers of the same OLT. In this case, media streams are forwarded inside the device instead of the bearer network. If the subscribers can call each other normally, the link between the device and the bearer network is faulty.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Check whether subscribers of the same OLT can call each other normally.
- If the subscribers can call each other normally, the link between the device and the bearer network is faulty. In this case, proceed to **Step 2**.
 - If the subscribers fail to call each other normally, go to **Step 3**.
- Step 2** Run the **ip address** command to configure the SVLAN interface of the voice service and then run the **arp proxy** command to enable ARP proxy globally and ARP proxy of the SVLAN interface of the voice service. Check whether the subscribers can call each other normally.
- If the subscribers can call each other normally, the link between the device and the bearer network is faulty. In this case, go to **Step 3**.
 - If the subscribers fail to call each other normally, go to **Step 4**.
- Step 3** Check whether ACL rules are correctly configured on the router of the IP bearer network.
- If ACL rules are correctly configured, go to **Step 8**.
 - If ACL rules are not correctly configured, modify or cancel ACL rules of the IP bearer network. Then, go to **Step 7**.
- Step 4** Check whether subscribers of the same ONT can call each other normally.
- If the subscribers can call each other normally, configurations on the OLT are incorrect. In this case, proceed to **Step 5**.
 - If the subscribers fail to call each other normally, configurations on the ONT are incorrect. In this case, go to **Step 6**.
- Step 5** On the OLT, run the **display acl all** command to check whether ACL rules are used to filter upstream or downstream voice media streams.
- If ACL rules are used, run the **undo acl** command on the OLT to cancel the ACL rules, and go to **Step 7**.
 - If ACL rules are not used, proceed to **Step 6**.
-  **NOTE**
- The ACL that has been delivered to a port cannot be deleted. To delete such an ACL, cancel the ACL delivery before deleting by running the **undo packet-filter** command on the OLT.
- Step 6** On the ONT, check whether IP filtering and MAC address filtering functions are configured to filter upstream or downstream voice media streams.
- If IP filtering and MAC address filtering functions are configured, disable them and proceed to **Step 7**.
 - If IP filtering and MAC address filtering functions are not configured, go to **Step 8**.
- Step 7** Make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 9**.
- If the fault persists, proceed to **Step 8**.

Step 8 Connect Technical Support.

Step 9 The fault is rectified.

----End

7.3.5 Noise in a Voice Call

Noise in a voice call indicates that a subscriber hears a strong current noise and broadcast noise in a voice call, excluding the environment noise of both parties. When such a fault occurs in an FTTH network, locate the fault according to the following procedure.

Cause Analysis

When noise in a voice call occurs in an FTTH network, locate the fault according to the fault scope, as described in the following table.

Fault Scope	Possible Cause
Subscribers of the same OLT	<ul style="list-style-type: none">• Packet loss occurs in the bearer network.• Electromagnetic interference exists in the environment of the OLT.
Subscribers of two POTS ports on an ONT	<ul style="list-style-type: none">• Electromagnetic interference exists in the environment of the ONT and the line between the ONT and the phones.• The ONT or power adapter is faulty.
Subscriber of a POTS port on an ONT	<ul style="list-style-type: none">• The POTS port is faulty.• The line between the phone and the POTS port is faulty.• The line between the phone and the POTS port is not properly connected.• The phone is faulty.• The subscriber line is not correctly connected. For example, an extra xDSL (DSL refers to digital subscriber line) distribution box is connected.
Subscribers calling certain numbers	The phone number configured on the ONT is different from that configured on the softswitch.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check the fault scope.

- If all subscribers of the same OLT hear the noise, proceed to **Step 2**.
- If the subscribers of two POTS ports on an ONT hear the noise, go to **Step 3**.
- If the subscriber of a POTS port on an ONT hears the noise, go to **Step 5**.
- If the subscribers calling certain numbers hear the noise, go to **Step 7**.

Step 2 Rectify packet loss failure in the bearer network and eliminate electromagnetic interference (such as interference brought by the broadcast tower and high voltage wire) in the environment of the OLT. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 9**.
- If the fault persists, go to **Step 8**.

Step 3 Eliminate electromagnetic interference (such as interference brought by a radio or stereo) in the environment of the ONT and the line between the ONT and the phones. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 9**.
- If the fault persists, proceed to **Step 4**.

Step 4 Replace the **ONT** or power adapter. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 9**.
- If the fault persists, go to **Step 8**.

Step 5 Run the **ont pots-test** command to perform a loop line test for the ONT, and rectify the fault according to the test result. If the noise persists in a voice call after the rectification, proceed to **Step 6**.

Test Result	Possible Cause	Troubleshooting Method
<ul style="list-style-type: none">• Normal• Phone disconnected	-	No process is needed because the loop line and phone are normal.

Test Result	Possible Cause	Troubleshooting Method
<ul style="list-style-type: none"> ● AC current abnormal ● DC current abnormal ● Loop current abnormal ● Loop resistance abnormal ● Insulating resistance abnormal ● Capacitance abnormal ● Impedance abnormal ● Insulating not good ● Broken lines ● Line mixing ● Connected to ground ● AB Line reversal ● Line leaking 	The line between the phone and the POTS port is faulty.	Replace the line between the phone and the POTS port.
Broken lines	<ul style="list-style-type: none"> ● The phone is faulty. ● The line between the phone and the POTS port is faulty. ● The line between the phone and the POTS port is not properly connected. 	<ul style="list-style-type: none"> ● Replace the phone. ● Replace the line between the phone and the POTS port. ● Re-connect the line between the phone and the POTS port properly.

Step 6 Re-connect the subscriber line properly. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to [Step 9](#).
- If the fault persists, go to [Step 8](#).

Step 7 Check the phone numbers configured on the softswitch and ONT, and modify the phone number configured on the phone that encounters the fault to be the same as the phone number configured on a normal phone. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to [Step 9](#).
- If the fault persists, proceed to [Step 8](#).

Step 8 Connect Technical Support.

Step 9 The fault is rectified.

----End

7.3.6 Voice Interruptions in a Voice Call

Voice interruptions in a voice call indicate that the voice heard by a subscriber in a voice call is interrupted at times. When such a fault occurs in an FTTH network, locate the fault according to the following procedure.

Cause Analysis

When voice interruptions in a voice call occur in an FTTH network, possible causes are as follows:

- The 802.1p priority of the voice service is too low on the ONT.
- The POTS port is faulty.
- The line between the POTS port and the phone is faulty.
- The line between the phone and the POTS port is not properly connected.
- The phone is faulty.
- The network connection is abnormal.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Run the **ont pots-test** command to perform a loop line test for the ONT, and rectify the fault according to the test result. If voice interruptions persist after the rectification, proceed to **Step 2**.

Test Result	Possible Cause	Troubleshooting Method
<ul style="list-style-type: none">• Normal• Phone disconnected	-	No process is needed because the loop line and phone are normal.

Test Result	Possible Cause	Troubleshooting Method
<ul style="list-style-type: none"> ● AC current abnormal ● DC current abnormal ● Loop current abnormal ● Loop resistance abnormal ● Insulating resistance abnormal ● Capacitance abnormal ● Impedance abnormal ● Insulating not good ● Broken lines ● Line mixing ● Connected to ground ● AB Line reversal ● Line leaking 	The line between the phone and the POTS port is faulty.	Replace the line between the phone and the POTS port.
Broken lines	<ul style="list-style-type: none"> ● The phone is faulty. ● The line between the phone and the POTS port is faulty. ● The line between the phone and the POTS port is not properly connected. 	<ul style="list-style-type: none"> ● Replace the phone. ● Replace the line between the phone and the POTS port. ● Re-connect the line between the phone and the POTS port properly.

Step 2 Rectify the network fault (for example, improper optical fiber connection). Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to [Step 8](#).
- If the fault persists, proceed to [Step 3](#).

Step 3 Connect the phone that encounters the fault to another POTS port. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, the POTS port on the original ONT is faulty. In this case, [replace the ONT](#) and go to [Step 8](#).
- If the fault persists, proceed to [Step 4](#).

Step 4 Check whether the 802.1p priority of the voice service is too low on the ONT.

 **NOTE**

- When packet loss occurs in case of network congestion, packets with a lower QoS (QoS refers to quality of service) priority are discarded first. Priorities of QoS packets are from 0 to 7 in an ascending order.
- The voice service requires a high network quality. Hence, it is recommended that you set the priority of the voice service on the ONT to 7.

- If the 802.1p priority of the voice service is too low on the ONT, set it to a high priority, and proceed to **Step 5**.
- If the 802.1p priority of the voice service is high on the ONT, go to **Step 6**.

Step 5 Make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 8**.
- If the fault persists, proceed to **Step 6**.

Step 6 **Replace the ONT**. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 8**.
- If the fault persists, proceed to **Step 7**.

Step 7 Connect Technical Support.

Step 8 The fault is rectified.

----End

7.3.7 Failure to Dial Certain Phone Numbers

Failure to dial certain phone numbers indicates that when dialing certain phone numbers, the subscriber hears "the number you dialed does not exist". When such a fault occurs in an FTTH network, locate the fault according to the following procedure.

Cause Analysis

When a subscriber fails to dial certain phone numbers, possible causes are as follows:

1. Packet loss occurs in the network between the OLT and the MGC/IMS.
2. Digitmaps associated with the phone numbers are not configured on the MGC or ONT.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check whether packet loss occurs in the network between the OLT and the MGC/IMS.



In the VLANIF/MEth mode on the OLT, run the **ip address** command to configure a Layer 3 interface, and run the **ping** command to ping the IP address of the MGC/IMS repeatedly to check whether packet loss occurs in the network between the OLT and the MGC/IMS.

- If packet loss occurs in the network, rectify the fault (for example, improper optical fiber connection) in the link between the OLT and the MGC/IMS, and proceed to **Step 2**.
- If no packet loss occurs in the network, go to **Step 3**.

Step 2 Make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 6**.
- If the fault persists, proceed to **Step 3**.

Step 3 Check whether digitmaps associated with the phone numbers are configured on the MGC or ONT.

- If the digitmaps are configured, go to **Step 5**.
- If the digitmaps are not configured, configure them, and proceed to **Step 4**.

Step 4 Make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 6**.
- If the fault persists, proceed to **Step 5**.

Step 5 Connect Technical Support.

Step 6 The fault is rectified.

----End

8 Troubleshooting the xPON power distribution service

The ONU supports video surveillance data transmission and intelligent collection of power consumption information in the electrical power system through an Ethernet port. It also supports automatic transmission of site information in electrical power system through an Ethernet port or serial port. This topic describes how to troubleshoot common Ethernet and serial port access faults.

[8.1 Troubleshooting Ethernet Access Services](#)

This topic describes how to troubleshoot ethernet access service faults on the ONU.

[8.2 Troubleshooting Serial Port Access Services](#)

The ONU supports intelligent collection of power consumption information through a serial port.

8.1 Troubleshooting Ethernet Access Services

This topic describes how to troubleshoot ethernet access service faults on the ONU.

8.1.1 Troubleshooting Video Surveillance Data Transmission Services

The ONU supports video surveillance data transmission services using Ethernet access.

Context

Working with the optical line terminal (OLT), the ONU provides transparent channels for transmitting video surveillance information and allows the monitoring center to monitor desired sites in real time.

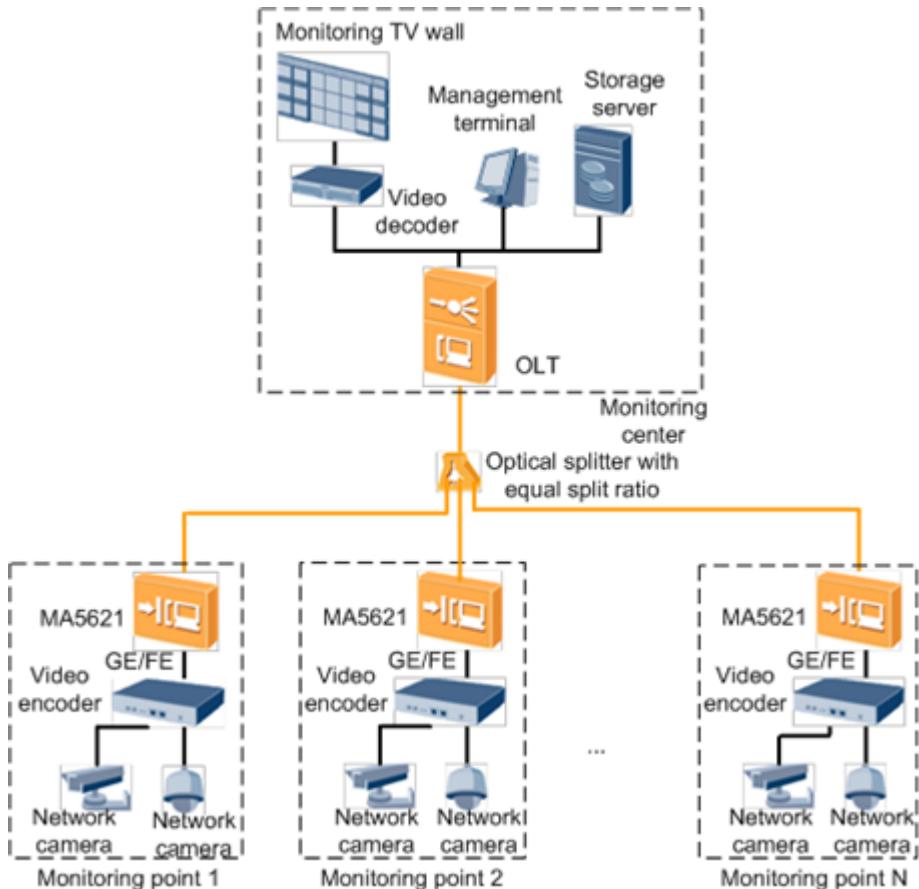
- A video monitor encapsulates the monitoring information in Ethernet frames, and sends the frames to the ONU.

- The ONU uses the uplink passive optical network (PON) port to send the received information to the OLT located in the monitoring center.
- The OLT forwards the received information to a monitoring device, such as a storage server, management terminal, or video decoder.
- The monitoring device decodes the information and saves it.

Fault Location

Figure 8-1 shows the network for video surveillance data transmission using Ethernet access.

Figure 8-1 Network for video surveillance data transmission



Use the following guidelines to locate the fault based on **Figure 8-1**.

Fault Scope	Possible Causes
Link between the video terminal and the ONU	<ul style="list-style-type: none">The video monitor is faulty.The line between the video monitor and the ONU is faulty.Port negotiation between the video monitor and the ONU failed.The data configurations of the ONU are incorrect.
Link between the ONU and the OLT	The line between the ONU and the OLT is faulty.
Monitoring center	The monitoring device is faulty, such as a storage server, management terminal, or video decoder.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check whether the video monitor is working properly. Replace it if it is faulty.

Step 2 Check whether the line between the ONU and the OLT is faulty.

Run the **display alarm history** command on the OLT to query alarms associated with the line. If an alarm, such as **The distribute fiber is broken or OLT cannot receive expected optical signals from GPON ONT(LOSi)** is generated, the line quality is poor. Check whether any of the following is true:

- The transmit power of the uplink PON port on the ONU is wrong.
- The optical distribution network (ODN) plan is wrong. Specifically, the optical split ratio is too large, the reach is too long, or the signal is too attenuated.
- The optical fiber is bent severely.
- The types of the optical fiber connectors do not match each other.
- The optical fiber connector is dirty.

Step 3 Check whether the data configurations of the ONU are correct.

- Run the **display service-port** command to query the service port configuration. Check whether the VLAN ID and port ID match the data plan.

If the parameters do not match the data plan, perform the following operations to modify them:

- Run the **undo service-port** command to delete the original service port.
- Run the **service-port** command to create a service port according to the data plan.

- Run the **display port vlan** command to query whether the uplink port has been added to the upstream VLAN.

If the uplink port has not been added to the upstream VLAN, run the **port vlan** command to add it to the upstream VLAN.

Step 4 Check the Ethernet port parameter settings on the video monitor and the ONU.

- Run the **display port state** command to query the Ethernet port parameter settings on the ONU. The parameters include port auto-negotiation mode and network cable auto-sensing mode.
- Check whether the Ethernet port parameter settings on the ONU match those on the peer video monitor. If they do not match, perform the following operations to modify the settings on the ONU:
 - Run the **auto-neg** command to enable or disable the auto-negotiation mode of the Ethernet port.
 - Run the **duplex** command to set the duplex mode of the Ethernet port.
 - Run the **speed** command to set the Ethernet port rate.
 - Run the **mdi** command to set the network cable auto-sensing mode of the Ethernet port.

Step 5 Check whether the line between the video monitor and the ONU is functional.

Run the **display port statistics** command at least 10 times to query the Ethernet port statistics every 20 seconds. Check whether **Number of CRC error frames** increases during testing. If it increases, the line is faulty. Check whether any of the following is true:

- The network cable is old or short-circuited.
- The connectors at the end of the network cable are loose or in poor contact.
- The signal is too attenuated because the network cable is too long.

Step 6 Check whether the monitoring device in the monitoring center is working properly.

Video encoding and decoding each form part of a single process that requires negotiation between the encoder and decoder. Ensure that the parameter settings on the decoder match those on the video monitor and the decoder is working properly in the monitoring center.

Step 7 Contacting Huawei for Assistance.

Step 8 End.

----End

8.1.2 Troubleshooting Intelligent Collection of Power Consumption Information

The ONU intelligently collects power consumption information in the electrical power system using Ethernet access.

Context

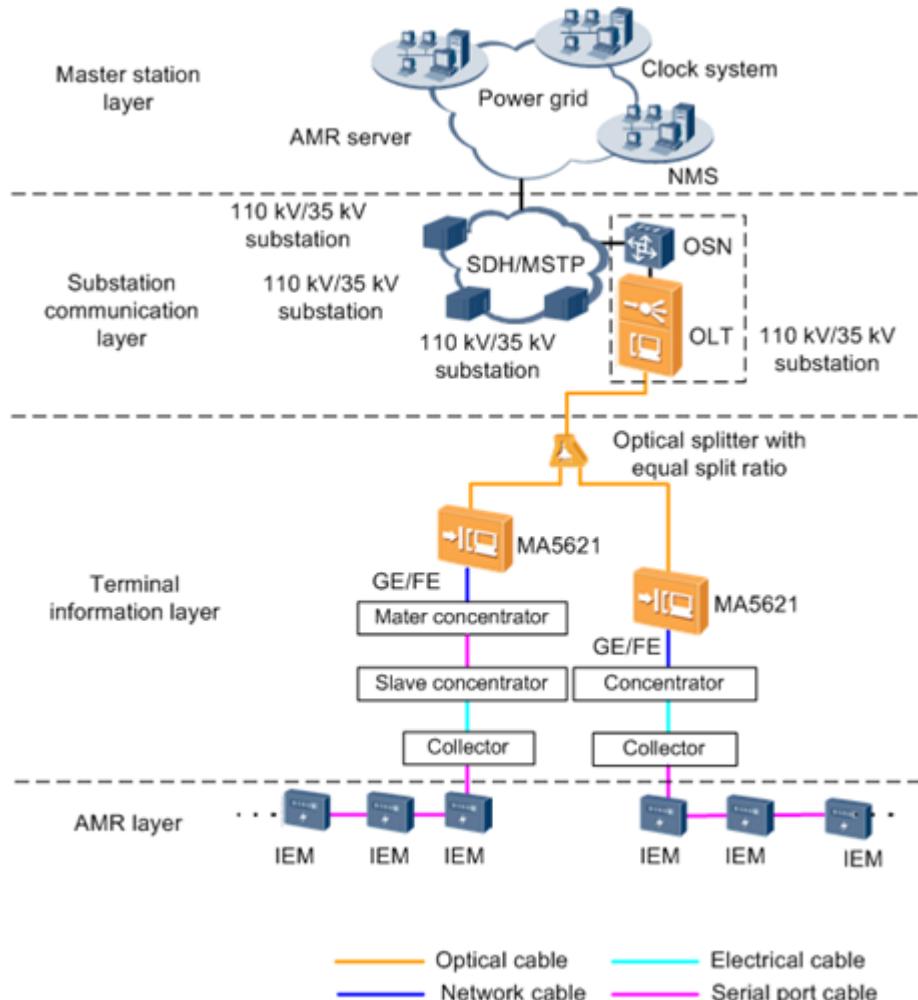
Working with an optical line terminal (OLT), the ONU provides transparent channels for collecting power consumption information intelligently and allows the automatic meter reading system (AMR) server to obtain the power consumption information about users in real time.

- The collector collects power consumption information from smart meters and transmits the information upstream to a concentrator using power line carrier (PLC) technologies, with the electrical cable functioning as a transmission channel.
- The concentrator encapsulates the power consumption information into Ethernet frames and transmits them to the ONU.
- The ONU sends the received information to the OLT through an uplink passive optical network (PON) port.
- The OLT forwards the received information upstream to a transmission device at the substation communication layer. In a synchronous digital hierarchy (SDH) or Multiple Spanning Tree Protocol (MSTP) network, the OLT forwards the information to an optical switch node (OSN).
- The transmission device transmits the received information to the AMR server.

Fault Location

Figure 8-2 shows the network for intelligent collection of power consumption information using Ethernet access.

Figure 8-2 Network for intelligent collection of power consumption information



Use the following guidelines to locate the fault based on [Figure 8-2](#).

Fault Scope	Possible Causes
Link between the smart meter and the master concentrator	<ul style="list-style-type: none">The smart meter is faulty.The collector is faulty.The master or slave concentrator is faulty.
Link between the master concentrator and the ONU	<ul style="list-style-type: none">The line between the ONU and the master concentrator is faulty.Port negotiation between the ONU and the master concentrator failed.The data configurations of the ONU are incorrect.
Link between the ONU and the OLT	The line between the ONU and the OLT is faulty.
Monitoring device in the master station	The monitoring device in the master station is faulty.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check whether the line between the ONU and the OLT is faulty.

Run the **display alarm history** command on the OLT to query alarms associated with the line. If an alarm, such as **The distribute fiber is broken or OLT cannot receive expected optical signals from GPON ONT(LOSi)** is generated, the line quality is poor. Check whether any of the following is true:

- The transmit power of the uplink PON port on the ONU is wrong.
- The optical distribution network (ODN) plan is wrong. Specifically, the optical split ratio is too large, the reach is too long, or the signal is too attenuated.
- The optical fiber is severely bent.
- The types of the optical fiber connectors do not match each other.
- The optical fiber connector is dirty.

Step 2 Check whether the data configurations of the ONU are correct.

- Run the **display service-port** command to query the service port configuration. Check whether the VLAN ID and port ID match the data plan.

If the parameters do not match the data plan, perform the following operations to modify them:

- Run the **undo service-port** command to delete the original service port.

- Run the **service-port** command to create a service port according to the data plan.
- 2. Run the **display port vlan** command to query whether the uplink port has been added to the upstream VLAN.
If the uplink port has not been added to the upstream VLAN, run the **port vlan** command to add it to the upstream VLAN.

Step 3 Check the Ethernet port parameter settings on the master concentrator and the ONU.

- Run the **display port state** command to query the Ethernet port parameter settings on the ONU. The parameters include the port auto-negotiation mode and network cable auto-sensing mode.
- Check whether the Ethernet port parameter settings on the ONU match those on the master concentrator. If they do not match, perform the following operations to modify the settings on the ONU:
 - Run the **auto-neg** command to enable or disable the auto-negotiation mode of the Ethernet port.
 - Run the **duplex** command to set the duplex mode of the Ethernet port.
 - Run the **speed** command to set the Ethernet port rate.
 - Run the **mdi** command to set the network cable auto-sensing mode of the Ethernet port.

Step 4 Check whether the line between the master concentrator and the ONU is functional.

Run the **display port statistics** command at least 10 times to query the Ethernet port statistics every 20 seconds. Check whether **Number of CRC error frames** increases during testing. If it increases, the line is faulty. Check whether any of the following is true:

- The network cable is old or short-circuited.
- The connectors at the end of the network cable are loose or in poor contact.
- The signal is too attenuated because the network cable is too long.

Step 5 Check whether the link between the smart meter and the master concentrator is functional.

1. Check whether the smart meter is working properly. Replace the smart meter if it is faulty.
2. Check whether the collector and the master concentrator are working properly and whether they are communicating with each other properly.

Step 6 Check whether the monitoring device in the master station is working properly.

Step 7 Contacting Huawei for Assistance.

Step 8 End.

----End

8.2 Troubleshooting Serial Port Access Services

The ONU supports intelligent collection of power consumption information through a serial port.

8.2.1 Troubleshooting Intelligent Collection of Power Consumption Information

The ONU intelligently collects power consumption information in the electrical power system through a serial port.

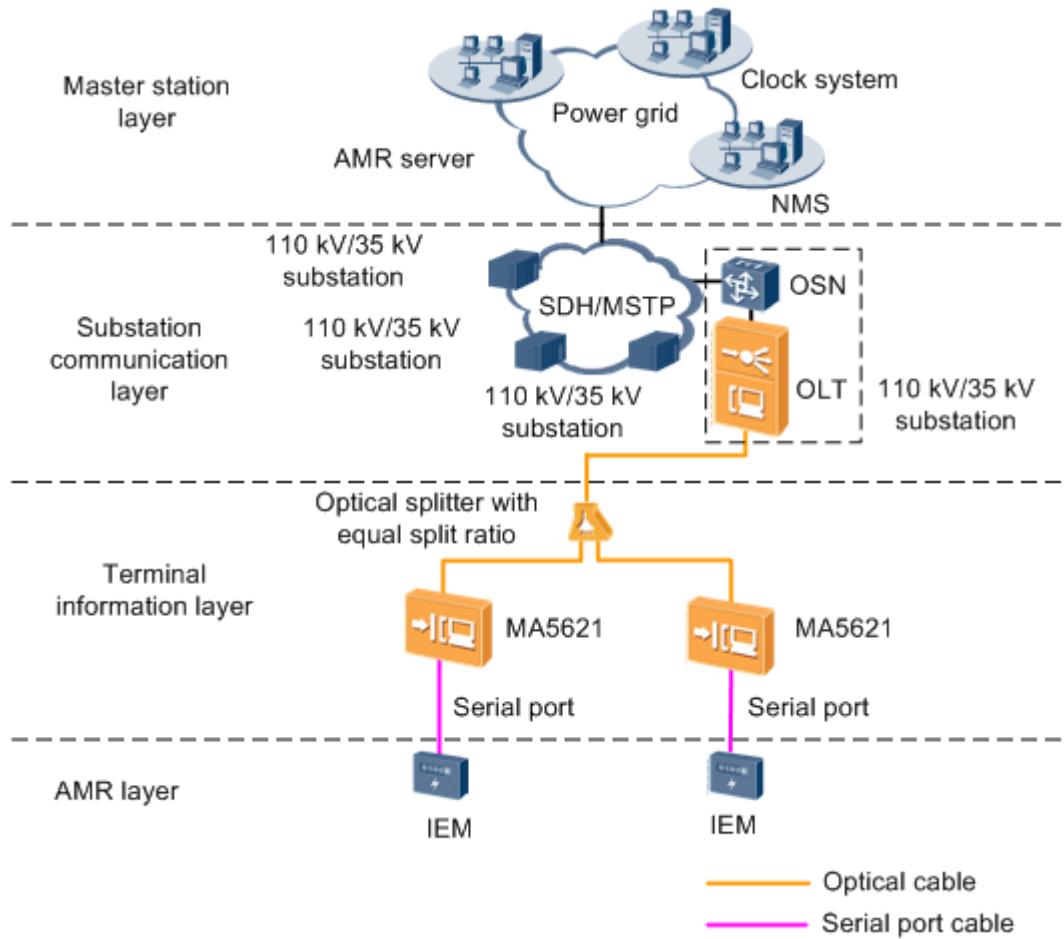
Context

Working with an optical line terminal (OLT), the ONU provides transparent channels for collecting power consumption information intelligently and allows the automatic meter reading system (AMR) server to obtain the power consumption information about users in real time.

- The ONU collects power consumption information from smart meters.
- The ONU sends the received information to the OLT through an uplink passive optical network (PON) port.
- The OLT forwards the received information upstream to a transmission device at the substation communication layer. In a synchronous digital hierarchy (SDH) or Multiple Spanning Tree Protocol (MSTP) network, the OLT forwards the information to an optical switch node (OSN).
- The transmission device transmits the received information to the AMR server.

Fault Location

Figure 8-3 shows the network for intelligent collection of power consumption information using serial port access.

Figure 8-3 Network for intelligent collection of power consumption information

Use the following guidelines to locate the fault based on [Figure 8-3](#).

Fault Scope	Possible Causes
Smart meter	The smart meter is faulty.
Link between the smart meter and the ONU	<ul style="list-style-type: none">The line between the ONU and the smart meter is faulty.Serial port parameter settings on the ONU do not match those on the smart meter.The data configurations of the ONU are incorrect.
Link between the ONU and the OLT	The line between the ONU and the OLT is faulty.
Monitoring device in the master station	The monitoring device in the master station is faulty.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check whether the line between the ONU and the OLT is faulty.

Run the **display alarm history** command on the OLT to query alarms associated with the line. If an alarm, such as **The distribute fiber is broken or OLT cannot receive expected optical signals from GPON ONT(LOSi)** is generated, the line quality is poor. Check whether any of the following is true:

- The transmit power of the uplink PON port on the ONU is wrong.
- The optical distribution network (ODN) plan is wrong. Specifically, the optical split ratio is too large, the reach is too long, or the signal is too attenuated.
- The optical fiber is severely bent.
- The types of the optical fiber connectors do not match each other.
- The optical fiber connector is dirty.

Step 2 Check whether the data configurations of the ONU are correct.

1. Run the **display serialop-connection** command to query the Transmission Control Protocol/Internet Protocol (TCP/IP) connection bound to the serial port.

Check whether the parameters match the data plan. The parameters include the serial port ID, transmission mode, local IP address, local port ID, peer IP address, peer port ID, and serial port frame type.

2. If the parameters do not match the data plan, perform the following operations to modify them:
 - Run the **undo serialop-connection** command to delete the TCP/IP connection bound to the serial port.
 - Run the **serialop-connection** command to reconfigure the TCP/IP connection connected to the serial port according to the data plan.

Step 3 Check the serial port parameter settings on the smart meter and the ONU.

- Run the **display port state(serial)** command to query the serial port parameter settings. The serial port parameters include the baud rate, data bit, parity, stop bit, and flow control.
- Check whether the serial port parameter settings on the ONU match those on the terminal unit. If they do not match, run the **port config** command to set the baud rate, data bit, parity, stop bit, and flow control.

Step 4 Check whether the serial port line between the smart meter and the ONU is functional.

Check whether any of the following is true:

- The serial cable is old or short-circuited.
- The connectors at the end of the serial cable are loose or in poor contact.
- The signal is too attenuated because the serial cable is too long.

Step 5 Check the smart meter.

Check whether the smart meter is working properly. Replace it if it is faulty.

Step 6 Check whether the monitoring device in the master station is working properly.

Step 7 Contacting Huawei for Assistance.

Step 8 End.

----End

9

Troubleshooting the FTTO Service

This chapter describes how to troubleshoot common faults in Internet access, multicast (IPTV), and voice (VoIP) services in FTTO scenarios.

9.1 Troubleshooting the Internet Access Service

This topic describes how to troubleshoot common faults in the Internet access service, including the following faults: PPPoE dialup failure, DHCP dialup failure, failure to access the Internet after successful dialup, Internet access service interruption, and low Internet access rate. The following uses the bridging ONU as an example to describe how to troubleshoot a fault.

9.2 IPTV Service Failure

This topic describes how to troubleshoot IPTV service faults.

9.3 Troubleshooting Voice Service Faults

This topic describes how to troubleshoot voice service faults. Common voice service faults include: no tone after offhook, busy tone after offhook, one-way audio in a voice call, noise in a voice call, voice interruptions in a voice call, and failure to dial certain phone numbers.

9.1 Troubleshooting the Internet Access Service

This topic describes how to troubleshoot common faults in the Internet access service, including the following faults: PPPoE dialup failure, DHCP dialup failure, failure to access the Internet after successful dialup, Internet access service interruption, and low Internet access rate. The following uses the bridging ONU as an example to describe how to troubleshoot a fault.

Prerequisites

The ONU and the OLT must communicate with each other normally. If a fault occurs in communication between the ONU and the OLT, all the services of the ONU may be interrupted. In this case, troubleshoot the fault first by referring to the methods described in [6 GPON ONU Abnormal State](#).

9.1.1 Internet Access Failure

This topic describes how to troubleshoot the fault when a user provisioned with the Internet access service obtains the IP address but fails to obtain resources in a

network (for example, the user fails to open a web page or fails to download a file).

Context

NOTE

ONUs can be classified into two types: bridging ONU and gateway ONU. The following uses the bridging ONU as an example. The bridging ONU and gateway ONU have the following difference in the Internet access service:

- **Gateway ONU:** The ONU serves as a DHCP client for proxy to obtain the public IP addresses of user PCs and serves as a DHCP server to assign private IP addresses for user PCs.
- **Bridging ONU:** The ONU transparently transmits all user packets but does not process them.

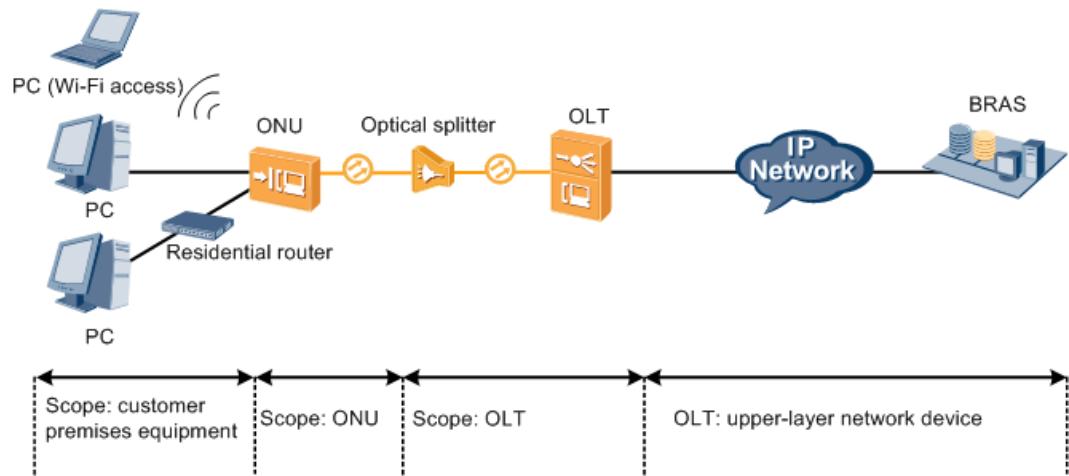
The following uses the bridging ONU as an example to describe how to troubleshoot a fault.

Figure 9-1 shows an example network of the FTTO Internet access service.

NOTE

If a user fails to obtain the IP address, see [9.1.4 PPPoE Dialup Failure](#) or [9.1.5 Failure to Obtain an IP Address in the DHCP Mode](#) to troubleshoot the fault of failing to obtain the IP address.

Figure 9-1 Example network of the FTTO Internet access service



Location Method

When Internet access failure occurs in an FTTO network, locate the fault according to the fault scope and possible causes, as described in the following table.

Table 9-1 Possible causes of the fault in different scopes

Fault Scope	Judgment Criterion	Possible Cause
User-side device	A single user fails to access the Internet but other users connected to the same ONU access the Internet successfully.	<ul style="list-style-type: none">The user fails to obtain the IP address.The PC is infected by viruses.The Internet Explorer (IE) of the PC is faulty.The PC is in slow response because of its long-term operating.The network interface card (NIC) of the PC is abnormal or is faulty.
OLT/ONU	None	NOTE Generally, this fault is not caused by the OLT or the ONU if the IP address is obtained.
Upper-layer device (such as the web page server and DNS server)	Users connected to multiple OLTs fail to access the Internet.	<ul style="list-style-type: none">The web page server is faulty.The DNS server is faulty.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Run the **display alarm active** command to check whether a line-related alarm that is not cleared is in the system. If such an alarm is generated, clear the alarm by referring to the relevant instruction documents.
- If the fault persists even after the alarm is cleared, go to [Step 2](#).
 - If the fault is rectified after the alarm is cleared, go to [Step 5](#).

- Step 2** Troubleshoot the fault of the user-side device according to the following table. If the Internet access failure persists, go to [Step 3](#).

Possible Cause	Judgment Criterion	Troubleshooting Method
The PC is infected by viruses.	Viruses are found by using the antivirus software.	Use the antivirus software to remove viruses.

Possible Cause	Judgment Criterion	Troubleshooting Method
The IE of the PC fails.	The fault is rectified by restarting the IE or re-installing the IE.	Restart the IE. If the fault persists, re-install the IE.
The PC is in slow response because of its long-term operating.	The fault is rectified after the PC is restarted.	Restart the PC.
The NIC of the PC malfunctions or fails.	The fault persists after all the above-mentioned operations are performed.	Update the driver of the NIC. If the fault persists, replace the NIC.

Step 3 Troubleshoot the fault of the upper-layer device according to the following table. If the Internet access failure persists, go to **Step 4**.

Possible Cause	Judgment Criterion	Troubleshooting Method
The web page server is faulty.	Another web page can be visited.	Check the web page server. If the web page server is faulty, troubleshoot the fault.
The DNS server is faulty.	A known web page can be visited by entering its IP address (such as http://192.168.0.2) to the IE address bar.	The DNS server fails to resolve the domain name. In this case, check the DNS server and troubleshoot the fault.

Step 4 Connect Technical Support.

Step 5 The fault is rectified.

----End

9.1.2 Internet Access Service Interruption

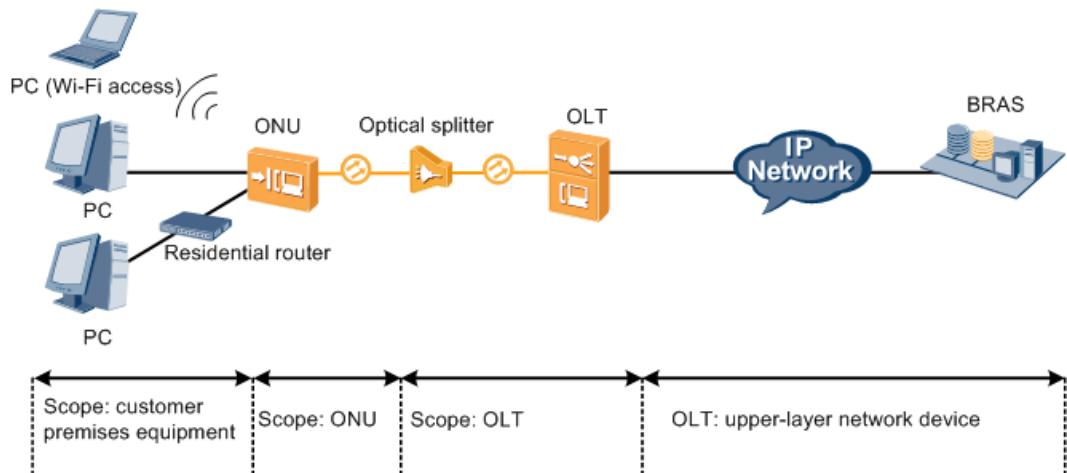
This topic describes how to troubleshoot the fault when the Internet access service is interrupted.

Context

Figure 9-2 shows an example network of the FTTO Internet access service.



Internet access service interruption may occur by various causes, for example, the ONU goes offline frequently and the IP address fails to be obtained.

Figure 9-2 Example network of the FTTO Internet access service

Location Method

When the Internet access service is interrupted, locate the fault according to the fault scope and possible causes, as described in the following table.

Table 9-2 Possible causes of the fault in different scopes

Fault Scope	Judgment Criterion	Possible Cause
User-side device	The Internet access service of a single user is interrupted but the Internet access service of other users connected to the same ONU is normal.	<ul style="list-style-type: none">The PC is infected by viruses.A network device such as the residential router between the ONU and the PC is faulty.The driver of the network interface card (NIC) on the PC is damaged or the hardware of the NIC is faulty.
ONU	The Internet access service of multiple users connected to the same ONU is interrupted.	<ul style="list-style-type: none">The wireless signals received by the PC using Wi-Fi access are of poor quality.The hardware of the ONU malfunctions or is faulty.

Fault Scope	Judgment Criterion	Possible Cause
OLT	The Internet access service of users on multiple ONUs connected to the same OLT is interrupted.	<ul style="list-style-type: none">Packet loss occurs because of incorrect configurations, such as link aggregation and port negotiation between the OLT and the port of the upper-layer device.Packet loss occurs because of a large volume of traffic on the upstream port.MAC address transfer occurs because a network encounters a loop or a device improperly forwards packets.The hardware, such as the optical module, service board, and control board of the OLT malfunctions or is faulty.
Upper-layer device (including the convergence switch, router, and BRAS)	The Internet access service of users connected to multiple OTTs is interrupted.	<ul style="list-style-type: none">Packet loss occurs on the upper-layer device.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Run the **display alarm active** command to check whether a line-related alarm that is not cleared is in the system. If such an alarm is generated, clear the alarm by referring to the relevant instruction documents.
- If the fault persists even after the alarm is cleared, go to **Step 2**.
 - If the fault is rectified after the alarm is cleared, go to **Step 7**.
- Step 2** Troubleshoot the fault of the user-side device according to the following table. If the Internet access service interruption persists, go to **Step 3**.

Possible Cause	Judgment Criterion	Troubleshooting Method
The PC is infected by viruses.	Viruses are found by using the antivirus software.	Use the antivirus software to remove viruses.

Possible Cause	Judgment Criterion	Troubleshooting Method
A network device such as the residential router between the ONU and the PC is faulty.	The fault is rectified after the PC is directly connected to an ONU.	Replace the device between the ONU and the PC.
The driver of the NIC on the PC is damaged or the hardware of the NIC is faulty.	The fault persists after all the above-mentioned operations are performed.	Update the driver of the NIC. If the fault persists, replace the NIC.

Step 3 Troubleshoot the fault of the ONU according to the following table. If the Internet access service interruption persists, go to [Step 4](#).

Possible Cause	Judgment Criterion	Troubleshooting Method
The wireless signals received by the PC using Wi-Fi access are of poor quality.	The quality of signals checked on the PC is poor.	Adjust the position of the PC and ensure that the quality of signals exchanged between the PC and the ONU meets the requirement.
The hardware of the ONU malfunctions or is faulty.	The fault is rectified after the ONU is restarted or replaced.	Restart the ONU. If the fault persists, replace the ONU.

Step 4 Troubleshoot the fault of the OLT according to the following table. If the Internet access service interruption persists, go to [Step 5](#).

Possible Cause	Judgment Criterion	Troubleshooting Method
Packet loss occurs because of incorrect configurations, such as link aggregation and port negotiation between the OLT and the port of the upper-layer device. NOTE Packets will be forwarded to a non-destination port or discarded because of incorrect configurations of the OLT's upstream port.	The link aggregation, port protection pair, and port negotiation configurations of the OLT are different from those of the upper-layer interconnected device.	Modify the configurations of the OLT or the upper-layer interconnected device to ensure that configurations of the OLT are the same as those of the upper-layer interconnected device.

Possible Cause	Judgment Criterion	Troubleshooting Method
Packet loss occurs because of a large volume of traffic on the upstream port.	If Number of discarded frames increases in the output of the display port statistics command that is executed multiple times, packet loss occurs on the upstream port due to the large traffic.	In this case, share traffic with other ports or increase the rate of the port. NOTICE Increasing the rate of the OLT upstream port forcibly may result in a failure to negotiation between the OLT upstream port and its interconnected port. As a result, the OLT upstream port is unavailable. If such a failure occurs, plan the rate of both the OLT upstream port and its interconnected port according to the live network.
MAC address transfer occurs because a network encounters a loop or a device improperly forwards packets.	MAC address transfer occurs on the upstream port or other service ports in the output of the display location command that is executed multiple times for querying the MAC address of the user encounters the fault. NOTE Enable the anti-MAC spoofing function to prevent MAC address transfer on service ports.	1. Run the ring check enable command to check whether a ring network is generated. 2. Capture packets to locate the device that improperly forwards packets.
The hardware, such as the optical module, service board, and control board of the OLT malfunctions or is faulty.	The fault is rectified by resetting the service board, replacing the optical module, or restarting the system. NOTE If the fault recurs after a period of time, the software fails. In this case, contact Huawei technical support engineers for help.	Exclude hardware faults by resetting the service board, replacing the optical module, or restarting the system. NOTE If multiple devices have the same hardware fault, contact Huawei technical support engineers for help.

Step 5 Troubleshoot the fault of the upper-layer device according to the following table. If the Internet access service interruption persists, go to [Step 6](#).

Possible Cause	Judgment Criterion	Troubleshooting Method
Packet loss occurs on the upper-layer device.	Packet loss is found in the output of the ping command for testing the quality of the link between the OLT and the network server.	Capture packets along the service route section by section to locate the device that discards packets or improperly forwards packets.

Step 6 Connect Technical Support.

Step 7 The fault is rectified.

----End

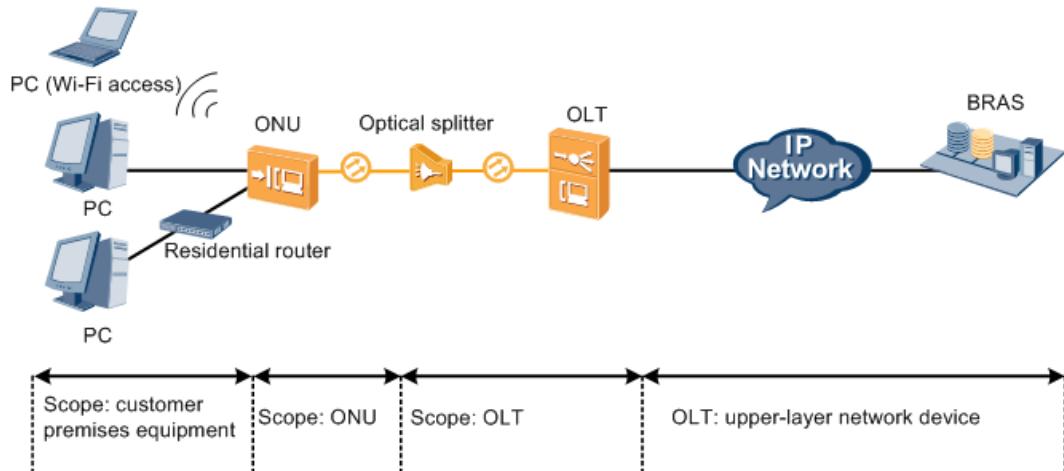
9.1.3 Low Internet Access Rate

This topic describes how to troubleshoot the fault when the actual Internet access rate of a user is far lower than the applied rate.

Context

Figure 9-3 shows an example network of the FTTO Internet access service.

Figure 9-3 Example network of the FTTO Internet access service



Location Method

When the Internet access rate is low, locate the fault according to the fault scope and possible causes, as described in the following table.

Table 9-3 Possible causes of the fault in different scopes

Fault Scope	Judgment Criterion	Possible Cause
User-side device	The Internet access rate of a single user is low but the Internet access rate of other users connected to the same ONU is normal.	<ul style="list-style-type: none">• The PC is infected by viruses.• The Internet Explorer (IE) of the PC fails.• The network interface card (NIC) of the PC is faulty or the PC runs for a long time.• The Internet connection of the PC is abnormal or is prohibited.• A network device such as the residential router between the ONU and the PC is faulty.
ONU	The Internet access rate of multiple users connected to the same ONU is low.	<ul style="list-style-type: none">• The wireless signals received by the PC using Wi-Fi access are of poor quality.• The hardware of the ONU malfunctions or is faulty.
OLT	The Internet access rate of users on multiple ONUs connected to the same OLT is low.	<ul style="list-style-type: none">• The limited rate of the OLT is lower than the provisioned rate.• Packet loss occurs because of a large volume of traffic on the upstream port.• The OLT has unknown traffic, occupying user bandwidth.• The hardware, such as the optical module, service board, and control board of the OLT malfunctions or is faulty.
Upper-layer device (including the convergence switch, router, and BRAS)	The Internet access rate of users of multiple OLTs is low.	<ul style="list-style-type: none">• The limited rate of the BRAS is lower than the provisioned rate.• Packet loss occurs on the upper-layer device or the delay is excessive long.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Run the **display alarm active** command to check whether a line-related alarm that is not cleared is in the system. If such an alarm is generated, clear the alarm by referring to the relevant instruction documents.

- If the fault persists even after the alarm is cleared, go to **Step 2**.
- If the fault is rectified after the alarm is cleared, go to **Step 7**.

Step 2 Troubleshoot the fault of the user-side device according to the following table. If the low Internet access rate persists, go to **Step 3**.

Possible Cause	Judgment Criterion	Troubleshooting Method
The PC is infected by viruses.	Viruses are found by using the antivirus software.	Use the antivirus software to remove viruses.
The Internet Explorer (IE) of the PC fails.	The fault is rectified by restarting the IE or re-installing the IE.	Restart the IE. If the fault persists, re-install the IE.
The PC is in slow response because of its long-term operating.	The fault is rectified after the PC is restarted.	Restart the PC.
The NIC of the PC malfunctions or fails.	The fault persists after all the above-mentioned operations are performed.	Update the driver of the NIC. If the fault persists, replace the NIC.
A network device such as the residential router between the ONU and the PC is faulty.	The fault is rectified after the PC is directly connected to an ONU.	Replace the device between the ONU and the PC.

Step 3 Troubleshoot the fault of the ONU according to the following table. If the low Internet access rate persists, go to **Step 4**.

Possible Cause	Judgment Criterion	Troubleshooting Method
The wireless signals received by the PC using Wi-Fi access are of poor quality.	The quality of signals checked on the PC is poor.	Adjust the position of the PC and ensure that the quality of signals exchanged between the PC and the ONU meets the requirement.
The hardware of the ONU malfunctions or is faulty.	The fault is rectified after the ONU is restarted or replaced.	Restart the ONU. If the fault persists, replace the ONU.

Step 4 Troubleshoot the fault of the OLT according to the following table. If the low Internet access rate persists, go to **Step 5**.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The limited rate of the OLT is lower than the provisioned rate.</p> <p>NOTE The rate limit scheme is formulated in service planning. Rates of multiple nodes will be limited if the rate limit scheme is not clear. In this case, the available rate is the lowest limited rate.</p>	<p>The available rate is lower than the applied rate by checking the rate limit configurations of the OLT.</p> <p>NOTE Keywords of main rate limit nodes are displayed as follows:</p> <ul style="list-style-type: none"> • Service port: service-port • ONU port: port eth • ONU T-CONT: tcont • PON port: car-port • Upstream port: line-rate 	<p>Modify the configurations to ensure that the available rate reaches the applied rate. For details, see "Configuring GPON Rate Limitation" in the <i>Commissioning and Configuration Guide</i>.</p>
<p>Packet loss occurs because of a large volume of traffic on the upstream port.</p>	<p>If Number of discarded frames increases in the output of the display port statistics command that is executed multiple times, packet loss occurs on the upstream port due to the large traffic.</p>	<p>In this case, share traffic with other ports or increase the rate of the port.</p> <p>NOTICE Increasing the rate of the OLT upstream port forcibly may results in a failure to negotiation between the OLT upstream port and its interconnected port. As a result, the OLT upstream port is unavailable. If such a failure occurs, plan the rate of both the OLT upstream port and its interconnected port according to the live network.</p>
<p>The OLT has unknown traffic, occupying user bandwidth.</p>	<p>Run the display port traffic command to query the data traffic of the upstream port or the service port, the unknown traffic exists because there is a large volume of traffic when no service is running.</p>	<p>Capture packets to analyze the source of the unknown traffic to troubleshoot the fault.</p> <p>NOTE More than 200 users in a VLAN may lead to an oversize broadcast domain. Then, a broadcast storm will occur in peak hours. As a result, the Internet access rate of users in the VLAN is low.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
The hardware, such as the optical module, service board, and control board of the OLT malfunctions or is faulty.	<p>The fault is rectified by resetting the service board, replacing the optical module, or restarting the system.</p> <p>NOTE If the fault recurs after a period of time, the software fails. In this case, contact Huawei technical support engineers for help.</p>	<p>Exclude hardware faults by resetting the service board, replacing the optical module, or restarting the system.</p> <p>NOTE If multiple devices have the same hardware fault, contact Huawei technical support engineers for help.</p>

Step 5 Troubleshoot the fault of the upper-layer device according to the following table. If the low Internet access rate persists, go to [Step 6](#).

Possible Cause	Judgment Criterion	Troubleshooting Method
The limited rate of the BRAS is lower than the provisioned rate.	The rate limited on the BRAS is lower than the applied rate.	Modify the limited rate to ensure that the rate meets the applied rate.
Packet loss occurs on the upper-layer device or the delay is excessive long.	Packet loss or excessive long delay is found in the output of the ping command for testing the quality of the link between the OLT and the network server.	Capture packets along the service route section by section to locate the device that discards packets or has excessive long delay.

Step 6 Connect Technical Support.

Step 7 The fault is rectified.

----End

9.1.4 PPPoE Dialup Failure

This topic describes how to troubleshoot the fault when a user encounters errors (such as error 678) during PPPoE dialup to access the Internet and consequently the IP address cannot be obtained.

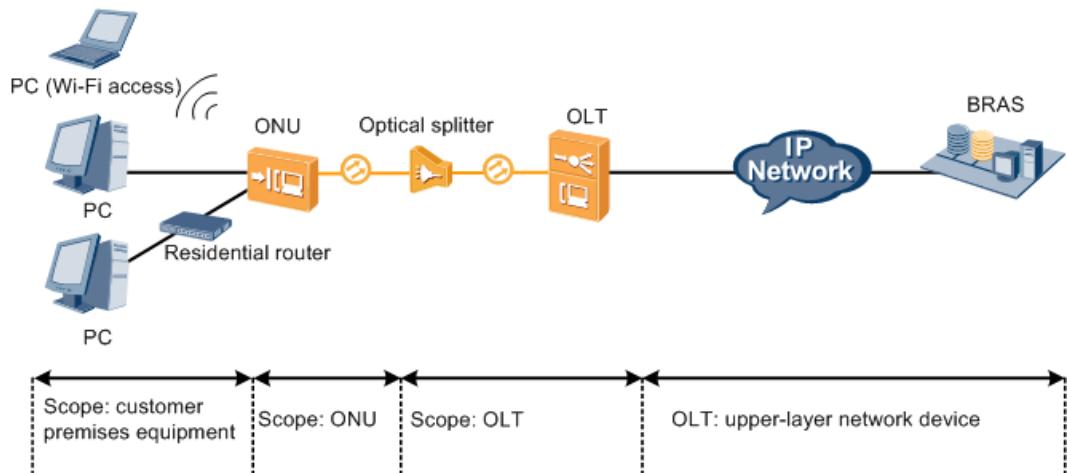
Context

[Figure 9-4](#) shows an example network of the FTTO Internet access service.



PPPoE dialup can be initiated by the user PC, residential router, or ONU. This section uses the PPPoE dialup initiated by the user PC as an example to describe how to troubleshoot common faults.

Figure 9-4 Example network of the FTTO Internet access service



Location Method

NOTE

- If the OLT supports the PPPoE dialup emulation, you can run the PPPoE dialup emulation command on the OLT for the OLT to emulate a user to initiate PPPoE dialup. If the emulation dialup succeeds, you can preliminarily judge that the OLT and the upper-layer device are normal.
- If the ONU supports the PPPoE dialup emulation, you can run the PPPoE dialup emulation command on the ONU for the ONU to emulate a user to initiate PPPoE dialup. If the emulation dialup succeeds, you can preliminarily judge that the ONU, OLT, and the upper-layer device are normal.

When "PPPoE Dialup Failure" occurs, locate the fault based on the following fault symptoms and possible causes.

Table 9-4 Possible causes of PPPoE dialup failure

Fault Scope	Judgment Criterion	Possible Cause
User-side device	Dialup of a single user PC fails but other user PCs of the same ONU are normal.	<ul style="list-style-type: none">● The PPPoE dialup software is not installed correctly or does not run properly.● The network connection of the user PC is abnormal or disabled.● The PPPoE user name or password is incorrect.● The network device (such as residential router) between the ONU and the user PC has problems.● The ONU port is incorrectly connected.● Configurations for the authentication mode or encryption mode on the PC (Wi-Fi access) are different from the configurations on the ONU.● The driver of the user PC NIC (network interface card) is damaged or the NIC hardware is faulty.
ONU	Dialup of multiple user PCs of the same ONU fails.	<ul style="list-style-type: none">● The WLAN function of the ONU is disabled.● The SSID broadcast function of the ONU is disabled and the Wi-Fi terminal cannot search for the SSID.● The ONU hardware is abnormal or faulty.

Fault Scope	Judgment Criterion	Possible Cause
OLT	Dialup of multiple ONUs of the same OLT fails.	<ul style="list-style-type: none"> • Configuration problems of the VLAN translation in the OLT and ONU traffic streams: <ul style="list-style-type: none"> - VLAN tag translation on the ONU - VLAN tag translation on the OLT - Configuration for the native VLAN of the OLT upstream port and the ONU user port - Configuration for the mappings between user VLAN, ONU port, ONU ID, GEM port, service VLAN, and upstream port • The PTP protocol configuration is different on the OLT and the BRAS. • The number of MAC addresses in the service port access reaches the maximum number of learned MAC addresses. • When PPPoE VMAC is set to be in the single-mac mode, the number of PPPoE sessions reaches the configured maximum number of PPPoE sessions for the port. • The OLT discards the interaction packets between the user PC and the BRAS. • The OLT hardware (optical module, service board, or control board) is abnormal or faulty.
Upper-layer device (BRAS, convergence switch, or router)	Dialup of users of multiple OLTs fails.	<ul style="list-style-type: none"> • The user name or account is not configured properly on the BRAS. • The BRAS restricts the number of connection users. • In the link between the OLT and the BRAS, some device discards the interaction packets between the user PC and the BRAS.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Run the **display alarm active** command to check whether a line-related alarm that is not cleared is in the system. If such an alarm is generated, clear the alarm by referring to the relevant instruction documents.

- If the fault persists even after the alarm is cleared, go to **Step 2**.
- If the fault is rectified after the alarm is cleared, go to **Step 8**.

Step 2 Run the **display mac-address vlan** command to check MAC address learning on the user side and network side.

- If the user side does not learn a MAC address, the user-side device is faulty. Then, go to **Step 3**.
- If the network side does not learn a MAC address, the upper-layer device is faulty. Then, go to **Step 6**.

Step 3 Handle the user-side device problems based on the following table. If dialup still fails after these problems are solved, go to **Step 4**.

Possible Cause	Judgment Criterion	Troubleshooting Method
The PPPoE dialup software is not installed correctly or does not run properly.	"Error 602", "error 605", "error 606", "error 608", "error 609", "error 611", "error 617", or "error 633" is returned during dialup. After the PPPoE dialup software is uninstalled and then reinstalled, the dialup succeeds.	Uninstall and then reinstall the PPPoE dialup software. NOTE In the Windows operating system (OS), set up a network connection again to reinstall the PPPoE dialup software.
The network connection of the user PC is abnormal or disabled.	"Error 606" or "error 617" is returned during dialup. Check the network connection of the user PC and find that the connection is in the disabled state or in another abnormal state.	Rectify the network connection of the user PC to ensure that the connection is in the normal state. NOTE In the Windows OS, after the user PC is connected to the ONU, no configuration is required and the network will automatically enter the normal state.
The PPPoE user name or password is incorrect.	"Error 691" is returned during dialup.	Use the correct user name and password.
The network device (such as residential router) between the ONU and the user PC has problems.	Connect the user PC directly to the ONU and dialup can succeed.	Replace the network device between the ONU and the user PC.

Possible Cause	Judgment Criterion	Troubleshooting Method
The ONU port is incorrectly connected.	PPPoE dialup is normal after the PC is connected to a correct ONU port.	Connect the PC to the correct ONU port.
Configurations for the authentication mode or encryption mode on the PC (Wi-Fi access) are different from the configurations on the ONU.	Connect the PC to the ONU in the wireless mode and check the configurations of the ONU and PC (Wi-Fi access). Configurations for the authentication mode or encryption mode on the PC are different from the configurations on the ONU.	Modify the configurations for the authentication mode and encryption mode on the PC (Wi-Fi access) to be the same as the configurations on the ONU. NOTE If the OS is Windows 2003 and the patch version is Service Pack 2, only the Tkip encryption mode is supported. The patch version must be upgraded to Service Pack 3 to support the Tkip, Tkip&Aes, and Aes encryption modes.
The driver of the user PC NIC (network interface card) is damaged or the NIC hardware is faulty.	After all the preceding possible causes are excluded, dialup still fails.	Reinstall the NIC driver. If the fault persists, replace the NIC.

Step 4 Handle the ONU problems based on the following table. If dialup still fails after these problems are solved, go to **Step 5**.

Possible Cause	Judgment Criterion	Troubleshooting Method
The WLAN function of the ONU is disabled.	The WLAN indicator of the ONU is not in the always on state.	Press and hold the WLAN button or set the WLAN function on the ONU web page to enable the WLAN function.

Possible Cause	Judgment Criterion	Troubleshooting Method
The SSID broadcast function of the ONU is disabled and the Wi-Fi terminal cannot search for the SSID.	The PC cannot search for the SSID of the wireless network.	<p>Log in to the web page of the ONU and enable the SSID broadcast function.</p> <p>NOTE</p> <ul style="list-style-type: none"> • By default, the SSID broadcast function is enabled. • To ensure that the wireless network is not embezzled, you must manually input on the PC the same SSID that is set on the ONU if the SSID broadcast function of the ONU is disabled.
The ONU hardware is abnormal or faulty.	Restart or replace the ONU, and dialup can succeed.	Restart the ONU. If the fault persists, replace the ONU.

Step 5 Handle the OLT problems based on the following table. If dialup still fails after these problems are solved, go to **Step 6**.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>Configuration problems of the traffic stream:</p> <ul style="list-style-type: none"> • VLAN tag translation on the ONU • VLAN tag translation on the OLT • Configuration for the native VLAN of the OLT upstream port and the ONU user port • Configuration for the mappings between user VLAN, ONU port, ONU ID, GEM port, service VLAN, and upstream port 	<ul style="list-style-type: none"> • If the user once succeeded in dialup, run the display log command to check the system log and find that the problem occurs because the data configuration is modified. • If the user never succeeded in dialup, check the data configuration based on the data plan and find that the data configuration is different from the plan. 	Configure the data correctly based on the data plan.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>The PITP protocol configuration is different on the OLT and the BRAS.</p> <p>NOTE After the PITP function is enabled, the user device information is carried in a PPPoE packet and the PPPoE packet is then authenticated on the BRAS. The dialup succeeds only when the device information (added by OLT or by a user-side device) is the same as that configured on the BRAS.</p>	<ul style="list-style-type: none"> Run the display pitp config command to query whether global PITP is enabled. The query result is different from the data plan. When PITP is enabled, run the display pitp permit-forwarding service-port command to check whether the OLT allows the user-side PPPoE packet to carry the device information. The query result is different from the data plan. 	Refer to "Configuring Anti-Theft or Roaming of User Accounts Through DHCP" in the <i>Commissioning and Configuration Guide</i> and configure parameters based on the data plan.
The number of users in the service port access reaches the maximum number of learned MAC addresses.	Run the display mac-address service-port command to query the number of MAC addresses already learned by the service port, run the display mac-address max-mac-count service-port command to query the maximum number of learned dynamic MAC addresses, and find that the number of already learned MAC addresses reaches the maximum number of learned MAC addresses.	Run the mac-address max-mac-count command to reconfigure the maximum number of learned MAC addresses for this traffic stream, and increase the number of access users on this service port. <p>NOTE By default, the maximum number of learned MAC addresses is not restricted.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>When PPPoE VMAC is set to be in the single-mac mode, the number of PPPoE sessions reaches the configured maximum number of PPPoE sessions for the port.</p> <p>NOTE If the number of online PPPoE sessions is larger than the preset maximum number for the port, the system does not allow a new PPPoE session to be set up.</p>	Run the display pppoe mac-mode command to query the current MAC address allocation mode for the PPPoE user and find that the mode is single-mac.	<p>Run the pppoe max-session-count command to set the maximum number of PPPoE sessions for a service port to 8 (the largest value).</p> <p>NOTE When the MAC address allocation mode of VMAC is single-mac, a service port allows a maximum of eight PPPoE sessions. Therefore, make a proper plan before network deployment to prevent that the number of online PPPoE sessions exceeds eight.</p>
The OLT discards the interaction packets between the user PC and the BRAS.	Capture packets for analysis on the OLT user port and upstream port, and find that packets are lost.	<p>Based on the packet capture result and the device configuration, analyze the cause for packet loss and take measures to rectify the fault.</p> <p>NOTE Possible causes of OLT packet loss are as follows:</p> <ul style="list-style-type: none"> • Packets are filtered due to the ACL configuration problem. • Packets are discarded due to the problems such as broadcast storm, extremely large traffic, and port rate limitation on the OLT.
The OLT hardware (optical module, service board, or control board) is abnormal or faulty.	<p>Perform operations such as resetting the service board, replacing the optical module, and restarting the system, and the fault is rectified.</p> <p>NOTE If the fault occurs again after a period of time, the software has problems. Then, go to Step 7.</p>	<p>Perform operations such as resetting the service board, replacing the optical module, and restarting the system to rectify the hardware problems.</p> <p>NOTE If multiple devices have the same hardware problem, go to Step 7.</p>

Step 6 Handle the upper-layer device problems based on the following table. If dialup still fails after these problems are solved, go to [Step 7](#).

Possible Cause	Judgment Criterion	Troubleshooting Method
The number of users reaches that maximum number of connected users supported by the BRAS.	Check the maximum number of connections allowed by the BRAS and the number of already connected users, and find that the number of already connected users reaches the maximum number of connections.	Expand the capacity of the BRAS.
The user name or account is not configured properly on the BRAS.	Check the data configuration of the BRAS and find that the user name and password of the user with problems are not configured or are configured incorrectly.	Configure the user name and password correctly on the BRAS.
In the link between the OLT and the BRAS, some device discards the packets sent by the user PC.	Run the ping command to test the quality of the link between the OLT and the network server, and find packet loss.	Capture packets section by section, locate the device where packets are discarded or forwarded incorrectly, and rectify the problem.

Step 7 Connect Technical Support.

Step 8 The fault is rectified.

----End

9.1.5 Failure to Obtain an IP Address in the DHCP Mode

This topic describes how to troubleshoot the fault when a user uses the DHCP mode to access the Internet but fails to obtain an IP address.

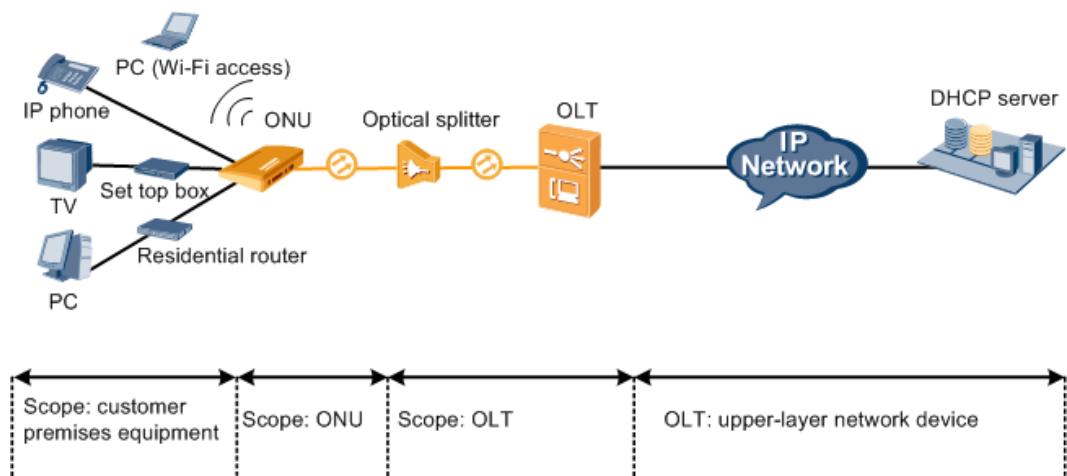
Context

Figure 9-5 shows an example network of the FTTO Internet access service.



The DHCP client can be the user PC, IPTV set top box, IP phone, residential router, or ONU. This section uses the user PC that functions as the DHCP client as an example to describe how to troubleshoot common faults.

Figure 9-5 Example network of the FTTO Internet access service



Location Method

When "Failure to Obtain an IP Address in the DHCP Mode" occurs, locate the fault based on the following fault symptoms and possible causes.

Table 9-5 Possible causes of failure to obtain an IP address in the DHCP mode

Fault Scope	Judgment Criterion	Possible Cause
User-side device	A single user PC fails to obtain an IP address but other user PCs of the same ONU are normal.	<ul style="list-style-type: none"> The IP obtaining mode of the PC is not set to "Obtain an IP address automatically." The network connection of the user PC is abnormal or disabled. The network device (such as residential router) between the ONU and the user PC has problems. The ONU port is incorrectly connected. Configurations for the authentication mode or encryption mode on the PC (Wi-Fi access) are different from the configurations on the ONU. The driver of the user PC NIC (network interface card) is damaged or the NIC hardware is faulty.

Fault Scope	Judgment Criterion	Possible Cause
ONU	Multiple user PCs of the same ONU fail to obtain IP addresses.	<ul style="list-style-type: none"> The WAN port of an ONU is not created. The SSID broadcast function of the ONU is disabled and the Wi-Fi terminal cannot search for the SSID. The ONU hardware is abnormal or faulty.
OLT	Multiple ONUs of the same OLT fail to obtain IP addresses.	<ul style="list-style-type: none"> Configuration problems of the VLAN translation in the OLT and ONU traffic streams: <ul style="list-style-type: none"> VLAN tag translation on the ONU VLAN tag translation on the OLT Configuration for the native VLAN of the OLT upstream port and the ONU user port Configuration for the mappings between user VLAN, ONU port, ONU ID, service VLAN, and upstream port Configurations for the DHCP option 82 function on the OLT are different from the configurations on the DHCP server. The number of MAC addresses in the service port access reaches the maximum number of learned MAC addresses. The OLT enables a special function (such as anti-MAC spoofing) and modifies the RAIO information in the DHCP option 82 packet. The OLT hardware (optical module, service board, or control board) is abnormal or faulty.
Upper-layer device (DHCP server, convergence switch, or router)	Users of multiple OLTs fail to obtain IP addresses.	<ul style="list-style-type: none"> The IP address pool resources of the DHCP server are exhausted. In the link between the OLT and the DHCP server, some device discards the packets sent by the user PC. The OLT enables a special function (such as anti-MAC spoofing) and modifies the RAIO information in the DHCP option 82 packet. The upper-layer device modifies the information in the DHCP option 82 packet.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Run the **display alarm active** command to check whether a line-related alarm that is not cleared is in the system. If such an alarm is generated, clear the alarm by referring to the relevant instruction documents.
- If the fault persists even after the alarm is cleared, go to **Step 2**.
 - If the fault is rectified after the alarm is cleared, go to **Step 8**.
- Step 2** Run the **display mac-address vlan** command to check MAC address learning on the user side and network side.
- If the user side does not learn a MAC address, the user-side device is faulty. Then, go to **Step 3**.
 - If the network side does not learn a MAC address, the upper-layer device is faulty. Then, go to **Step 6**.
- Step 3** Handle the user-side device problems based on the following table. If the IP address still cannot be obtained after these problems are solved, go to **Step 4**.

Possible Cause	Judgment Criterion	Troubleshooting Method
The IP obtaining mode of the PC is not set to "Obtain an IP address automatically."	Check the properties of the network connection and find that the IP obtaining mode is static IP address.	<p>Set the property of the network connection to "Obtain an IP address automatically."</p> <p>NOTE In the Windows operating system (OS), the default property of the network connection is "Obtain an IP address automatically."</p>
The network connection of the user PC is abnormal or disabled.	Check the network connection of the user PC and find that the connection is in the disabled state or in another abnormal state.	<p>Rectify the network connection of the user PC to ensure that the connection is in the normal state.</p> <p>NOTE In the Windows OS, after the user PC is connected to the ONU, no configuration is required and the network will automatically enter the normal state.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
The network device (such as residential router) between the ONU and the user PC has problems.	Connect the user PC directly to the ONU and an IP address can be obtained.	Replace the network device between the ONU and the user PC.
The ONU port is incorrectly connected.	The PC can obtain the IP address after being connected to a correct ONU port.	Connect the PC to the correct ONU port.
Configurations for the authentication mode or encryption mode on the PC (Wi-Fi access) are different from the configurations on the ONU.	Connect the PC to the ONU in the wireless mode and check the configurations of the ONU and PC (Wi-Fi access). Configurations for the authentication mode or encryption mode on the PC are different from the configurations on the ONU.	Modify the configurations for the authentication mode and encryption mode on the PC (Wi-Fi access) to be the same as the configurations on the ONU. NOTE If the OS is Windows 2003 and the patch version is Service Pack 2, only the Tkip encryption mode is supported. The patch version must be upgraded to Service Pack 3 to support the Tkip, Tkip&Aes, and Aes encryption modes.
The driver of the user PC NIC (network interface card) is damaged or the NIC hardware is faulty.	After all the preceding possible causes are excluded, dialup still fails.	Reinstall the NIC driver. If the fault persists, replace the NIC.

Step 4 Handle the ONU problems based on the following table. If the IP address still cannot be obtained after these problems are solved, go to [Step 5](#).

Possible Cause	Judgment Criterion	Troubleshooting Method
The WLAN function of the ONU is disabled.	The WLAN indicator of the ONU is not in the always on state.	Press and hold the WLAN button or set the WLAN function on the ONU web page to enable the WLAN function.

Possible Cause	Judgment Criterion	Troubleshooting Method
The SSID broadcast function of the ONU is disabled and the Wi-Fi terminal cannot search for the SSID.	The PC cannot search for the SSID of the wireless network.	<p>Log in to the web page of the ONU and enable the SSID broadcast function.</p> <p>NOTE</p> <ul style="list-style-type: none"> By default, the SSID broadcast function is enabled. To ensure that the wireless network is not embezzled, you must manually input on the PC the same SSID that is set on the ONU if the SSID broadcast function of the ONU is disabled.
The ONU hardware is abnormal or faulty.	Restart or replace the ONU, and an IP address can be obtained.	Restart the ONU. If the fault persists, replace the ONU.

Step 5 Handle the OLT problems based on the following table. If the IP address still cannot be obtained after these problems are solved, go to **Step 7**.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>Configuration problems of the traffic stream:</p> <ul style="list-style-type: none"> VLAN tag translation on the ONU VLAN tag translation on the OLT Configuration for the native VLAN of the OLT upstream port and the ONU user port Configuration for the mappings between user VLAN, ONU port, ONU ID, service VLAN, and upstream port 	<ul style="list-style-type: none"> If the user once obtained an IP address successfully, run the display log command to check the system log and find that the problem occurs because the data configuration is modified. If the user never obtained an IP address successfully, check the data configuration based on the data plan and find that the data configuration is different from the plan. 	Configure the data correctly based on the data plan.

Possible Cause	Judgment Criterion	Troubleshooting Method
<p>Configurations for the DHCP option 82 function on the OLT are different from the configurations on the DHCP server.</p> <p>NOTE</p> <ul style="list-style-type: none"> After the DHCP option 82 function is enabled, the device information is carried in a DHCP packet and the DHCP packet is then authenticated on the DHCP server. The authentication succeeds only when the device information (added by OLT or by a user-side device) is the same as that configured on the DHCP server. If the DHCP server authenticates the user based on the added information of the user device, run the dhcp-option82 permit-forwarding service-port 100 enable command on the OLT for the device to allow the DHCP packet with the information added by the user device to pass (assume that the traffic stream ID of the user is 100). 	<ul style="list-style-type: none"> Run the display dhcp option82 config command to query whether DHCP option 82 is enabled globally. The query result is different from the data plan. When DHCP option 82 is enabled and you run the display dhcp-option82 permit-forwarding service-port command to check whether the OLT allows the user-side DHCP packet to carry the device information, the query result is different from the data plan. <p>NOTE</p> <ol style="list-style-type: none"> Run the dhcp l2 statistics service-port 100 command to enable Layer 2 DHCP statistics on the service port to which the user belongs. Assume that the service port index is 100. Run the display dhcp l2 statistics command to query the statistics of the Layer 2 DHCP packets. In the statistics, "Number of received packets with untrusted option82" indicates that the OLT receives the DHCP packet with the information added by the user device. 	<p>Refer to "Configuring Anti-Theft or Roaming of User Accounts Through DHCP" in the <i>Commissioning and Configuration Guide</i> and configure parameters based on the data plan.</p> <p>NOTE</p> <p>Pay attention to the following data plan:</p> <ul style="list-style-type: none"> Whether the DHCP server requires the DHCP packet to carry the option 82 information. Whether the option 82 information is added by the user device or the OLT. The option 82 information cannot be added repeatedly.

Possible Cause	Judgment Criterion	Troubleshooting Method
The number of users in the service port access reaches the maximum number of learned MAC addresses.	Run the display mac-address service-port command to query the number of MAC addresses already learned by the service port, run the display mac-address max-mac-count service-port command to query the maximum number of learned dynamic MAC addresses, and find that the number of already learned MAC addresses reaches the maximum number of learned MAC addresses.	<p>Run the mac-address max-mac-count command to reconfigure the maximum number of learned MAC addresses for this traffic stream, and increase the number of access users on this service port.</p> <p>NOTE By default, the maximum number of learned MAC addresses is not restricted.</p>
<p>The OLT enables a special function (such as anti-MAC spoofing) and modifies the RAIO information in the DHCP option 82 packet.</p> <p>NOTE If the DHCP server verifies the RAIO information in the DHCP option 82 packet and the RAIO information is modified by the OLT or other devices, the RAIO information cannot pass the verification and an IP address fails to be obtained.</p>	Capture the DHCP option 82 packets that enter the OLT and that are forwarded out of the OLT. Analyze the packets and find that the packet contents are modified.	<p>Analyze the captured packets, find out the cause for the packet modification, and adjust the configuration accordingly.</p> <p>NOTE After enabling anti-MAC spoofing, the OLT will add the 802.1q information flag to the low 16 bits of the XID in the DHCP DISCOVER packets sent by users. If the DHCP server does not allow the information to be added to the XID parameter, anti-MAC spoofing must be disabled.</p>
The OLT hardware (optical module, service board, or control board) is abnormal or faulty.	<p>Perform operations such as resetting the service board, replacing the optical module, and restarting the system, and the fault is rectified.</p> <p>NOTE If the fault occurs again after a period of time, the software has problems and you need to contact Huawei engineers to carry out further analysis.</p>	<p>Perform operations such as resetting the service board, replacing the optical module, and restarting the system to rectify the hardware problems.</p> <p>NOTE If multiple devices have the same hardware problem, contact Huawei engineers to analyze the hardware fault and fundamentally rectify the hardware fault.</p>

Step 6 Handle the upper-layer device problems based on the following table. If the IP address still cannot be obtained after these problems are solved, go to **Step 7**.

Possible Cause	Judgment Criterion	Troubleshooting Method
The IP address pool resources of the DHCP server are exhausted.	Check the number of remaining IP addresses on the DHCP server and find that the number is 0.	Expand the capacity of the DHCP server.
In the channel between the OLT and the DHCP server, some device discards the packets sent by the user PC.	Run the ping command to test the quality of the link between the OLT and the network server, and find packet loss.	Capture packets section by section, locate the device where packets are discarded or forwarded incorrectly, and rectify the problem.
The upper-layer device modifies the information in the DHCP option 82 packet.	Capture the DHCP option 82 packets that enter the device and that are forwarded out of the device. Analyze the packets and find that the packet contents are modified.	Analyze the captured packets, find out the cause for the packet modification, and adjust the configuration accordingly.

Step 7 Connect Technical Support.

Step 8 The fault is rectified.

----End

9.2 IPTV Service Failure

This topic describes how to troubleshoot IPTV service faults.

Prerequisites

- The ONU and OLT communicate with each other properly. If a communication fault occurs between the ONU and OLT, all the services on the ONU may be interrupted. In this case, troubleshoot the fault first by referring to the methods described in **ONU Abnormal State**.
- The multicast mode of an ONU is the dynamic controllable mode. That is, when the **display ont info** command is run in global config mode, the **multicast mode** of an ONU is displayed as **olt-control**. In this case, the OLT configures and manages the users and programs of an ONU. That is, the ONU does not manage its multicast users and programs.

Precautions

The described methods for troubleshooting multicast service faults are applicable only to dynamic-controllable-mode ONUs.

9.2.1 Multicast User Fails to Go Online

This topic describes how to troubleshoot the fault when a multicast user fails to order any program because the multicast user fails to go online (the queried user status is **offline** or **block** on the OLT). When such a fault occurs in an FTTO network, locate and troubleshoot the fault by using the following location methods and troubleshooting procedure.

Location Method

When a multicast user in an FTTO network is blocked, run the **undo igmp user block** command to unblock the user.

When a multicast user in an FTTO network is offline, enable the OLT debugging function and check whether the OLT receives a report packet from the multicast user for ordering the specified program.

- If the OLT does not receive the report packet, the multicast link fails. This is mainly caused by incorrect software configurations of the OLT and hardware faults of user terminals.
- If the OLT receives the report packet, the multicast link is normal. Run the **undo igmp user block** command to check whether the forwarding path for a program is created on the control board, service board, and ONU. This is generally caused by incorrect multicast configurations on the OLT.

Table 9-6 provides more details about using the location methods.

Table 9-6 Location methods

Fault Scope	Judgment Criterion	Possible Cause
OLT	The OLT receives the report packet.	<ul style="list-style-type: none">• The program ordered by the multicast user is not included in the MVLAN to which the multicast user belongs.• No upstream port is configured in the MVLAN to which the multicast user belongs.• The multicast user does not have the permission to watch the program.• The maximum multicast bandwidth of the user is lower than the bandwidth required by the ordered program.• The multicast user does not have the permission to order certain types of programs (such as HDTV).

Fault Scope	Judgment Criterion	Possible Cause
	The OLT is faulty if both the following situations occur: <ul style="list-style-type: none">• The OLT does not receive the report packet.• The user fails to go online from the beginning or fails to go online after configuration modification.	<ul style="list-style-type: none">• The IGMP function is disabled in the MVLAN to which the OLT belongs. In this case, all users in the MVLAN fail to go online.• Multicast configurations of the ONU ETH port are incorrect. For example, the native VLAN is not configured on the ONU.
ONU and user terminal	The ONU and user terminal are faulty if both the following situations occur: <ul style="list-style-type: none">• The OLT does not receive the report packet.• The user can go online at first but fails to go online later.	<ul style="list-style-type: none">• The set top box (STB) is faulty.• The ONU is faulty.• The physical line between the STB and ONU is faulty.

NOTE

Faults can be located according to specified scenarios because the deployment scenario and the routine OM scenario involve different fault scopes.

- If the fault occurs during deployment, check the hardware and initial software configurations.
- If the fault occurs during OM, check only the hardware because the software configurations of a user are generally not modified in this scenario. Hence, if the status of a user changes from normal to abnormal, it is generally caused by hardware failures. If the fault occurs after a new user is added or an existing user is modified, check the software configurations of the user.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Run the **display mac-address vlan** command to check MAC address learning on the user side and network side.

- If the user side does not learn a MAC address, the user-side device is faulty. Then, go to [Step 7](#).
- If the network side does not learn a MAC address, the upper-layer device is faulty. Then, go to [Step 2](#).

Step 2 Run the **display igmp user service-port** command to query the multicast user status (check the **State** parameter).

- If **State** is **block**, the multicast user is blocked. In this case, run the **undo igmp user block** command to unblock the user. Then, go to [Step 3](#).
- If **State** is **offline**, go to [Step 4](#).

 NOTE

If you need to block a multicast user from watching programs temporarily without deleting the user (for example, when the user has charges overdue), run the **igmp user block** command to block the user. When the user is blocked, the OLT forces the user to go offline from the current program. In addition, the OLT rejects the user's requests for ordering programs until the user is unblocked.

Step 3 Order a program and check whether the user can go online.

- If the user can go online, go to [Step 10](#).
- If the user fails to go online, go to [Step 4](#).

Step 4 Enable the OLT debugging function and collect information as follows:

1. Enable the function of multicast user monitoring.

```
huawei(config)#terminal monitor  
huawei(config)#terminal debugging  
huawei(config)#debugging igmp service-port
```

2. Order a program again and go to [Step 5](#).

 NOTE

After the preceding steps are performed, run the following commands to disable the debugging function.

```
huawei(config)#undo debugging igmp  
huawei(config)#undo terminal debugging  
huawei(config)#undo terminal monitor
```

Step 5 Locate the fault according to the reception result (received or not) of the report packet and the fault scope.

- If the OLT displays a prompt message for the program, the OLT receives the report packet successfully. In this case, go to [Step 6.1](#).
- If the OLT does not display a prompt message for the program, the OLT fails to receive the report packet. In this case, locate the fault according to the fault scope.
 - If the user fails to go online from the beginning or fails to go online after configuration modification, go to [Step 6.2](#).
 - If the user can go online at first but fails to go online later, go to [Step 7](#).

Step 6 Check multicast configurations of the OLT.

1. If the OLT receives the report packet successfully, find the possible cause according to the judgment criteria described in [Table 9-7](#) and troubleshoot the fault. Then, go to [Step 6.4](#) to verify whether the fault is rectified.

Table 9-7 Incorrect multicast configurations of the OLT and troubleshooting methods

Possible Cause	Judgment Criterion	Troubleshooting Method
The maximum multicast bandwidth of the user is lower than the bandwidth required by the ordered program if one of the following situations occurs: <ul style="list-style-type: none"> - The OLT receives the report packet and displays "the user fails to pass bandwidth CAC". - User MaxBandWidth in the display igmp user service-port command output is lower than Bandwidth in the display igmp program name command output. NOTE If User MaxBandWidth is no-limit , the multicast bandwidth of the user is not limited.	Choose one of the following troubleshooting methods according to the purchased service type: <ul style="list-style-type: none"> - Inform the user that the program cannot be watched because of insufficient bandwidth, and ask the user to order a program with a lower bandwidth than the maximum bandwidth of the user. - Increase the user bandwidth and ask the user to order the program again. NOTE Run the igmp user modify service-port 100 max-bandwidth command to modify the maximum bandwidth of the user to ensure that it is higher than the program bandwidth (this example assumes that the service port index of the multicast user is 100).	

Possible Cause	Judgment Criterion	Troubleshooting Method
The multicast user does not have the permission to order certain types of programs (such as HDTV).	<p>The multicast user does not have the permission to order certain types of programs if one of the following situations occurs:</p> <ul style="list-style-type: none"> - The OLT receives the report packet and displays "the number of the grade program that the user is allowed to watch has reached maximum". - The maximum number of programs at a level that the user can watch (watch limit) is 0 in the display igmp user extended-attributes service-port command output. <p>NOTE</p> <ul style="list-style-type: none"> - If watch limit is 0, the user cannot order any programs at this level. That is, the user's permission to the programs of the corresponding type is limited. For example, if HDTV watch limit is 0, the user cannot watch HDTV programs. - If watch limit is no-limit, the maximum number of programs at this level that a user can watch is not limited, but the total number of programs that can be concurrently watched is limited. 	<p>Choose one of the following troubleshooting methods according to the purchased service type:</p> <ul style="list-style-type: none"> - Inform the user that the program cannot be watched because the user does not have the permission to watch the program, and ask the user to order a program that has not reached the maximum watch limit at its level. - Add the permission for ordering the programs at this level for the user so that the user can order the program. <p>NOTE</p> <p>You can run the igmp user watch-limit service-port command to set the number of programs at each level that a user can watch.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
The multicast user does not have the permission to watch the program.	<p>The multicast user does not have the permission to watch the program if one of the following situations occurs:</p> <ul style="list-style-type: none"> - The OLT receives the report packet and displays "the user has no right". - Run the display igmp user service-port 100 command to query the right profile bound to the multicast user (this example assumes that the service port index of the multicast user is 100). ■ If Bind profiles is 0, the user is not bound to a right profile so the user cannot order any programs. ■ If Bind profiles is equal to or larger than 1, the user can watch only the program to which the user has the watch permission. In this case, perform operations for further check. In the query result, find the index (this example assumes that the index is 1) and name of the right profile bound to the user and run the display igmp profile profile-index 1 command to query the user permission for ordering the program. <ul style="list-style-type: none"> ○ If the permission of a program is forbidden or idle, the user does not have the permission to order the program. ○ If the permission of a program is watch or preview, the user can order the program. If so, the user's permission to 	<p>Choose one of the following troubleshooting methods according to the purchased service type:</p> <ul style="list-style-type: none"> - If the user can watch all programs without authentication, perform the following operations: <ol style="list-style-type: none"> 1. In BTV mode, run the igmp user modify service-port 100 no-auth command to modify the authentication mode of the user to "no authentication" (this example assumes that the service port index of the multicast user is 100). 2. Order the program again. - If the user can watch only certain programs with authentication, inform the user that the user has no permission to watch the program and ask the user to order a program with the watch or preview permission. <p>NOTE To set permissions of the user for ordering some programs, run the igmp user bind-profile service-port 100 profile-index-list 1 command to bind a correct right profile to the multicast user (this example assumes that the service port index of the multicast user is 100 and the right profile index is 1).</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
	<p>the program is not the cause of this fault.</p> <p>NOTE</p> <p>A multicast user can be bound to multiple right profiles. If these right profiles are configured with different permissions to the same program, the permission with the highest priority prevails. By default, the priorities of the program permissions are forbidden > preview > watch > idle. You can run the igmp right-priority command to set the priorities.</p>	

Possible Cause	Judgment Criterion	Troubleshooting Method
The program ordered by the multicast user is not included in the MVLAN to which the multicast user belongs.	<p>The program ordered is not included in the MVLAN to which the multicast user belongs if both the following situations occur:</p> <ul style="list-style-type: none"> - The OLT receives the report packet and displays "match program fail". - In the display igmp program vlan command output, the program ordered is not in the program list of the MVLAN. 	<p>Choose one of the following troubleshooting methods according to the purchased service type:</p> <ul style="list-style-type: none"> - Inform the user that the program cannot be watched because the user has no permission to watch the program, and ask the user to order a program that is included in the MVLAN to which the multicast user belongs. - Perform the following steps to add the program to the user's MVLAN and ask the user to order the program again. <ol style="list-style-type: none"> 1. Run the display igmp config vlan command to query Program match mode of the MVLAN. <ul style="list-style-type: none"> o If Program match mode is enable, the program is a static program, which is manually added. o If Program match mode is disable, the program is a dynamic program, which is automatically generated upon ordering. 2. Add programs to the MVLAN. <ul style="list-style-type: none"> o To add a static program to an MVLAN, run the igmp program add command. o To add dynamic programs to an

Possible Cause	Judgment Criterion	Troubleshooting Method
		MVLAN, run the igmp match group command to set the IP address range of program groups that can be generated dynamically in the MVLAN, and include the IP address of the ordered program in the IP address range.

2. In MVLAN mode, run the **display igmp config vlan** command to query **IGMP mode** of the MVLAN.
 - If **IGMP mode** is **off**, the IGMP function is disabled in the MVLAN. In this case, run the **igmp mode** command in MVLAN mode to set **IGMP mode** to **proxy**. Then, order the program again and go to [Step 6.4](#).
 - If **IGMP mode** is **proxy** or **snooping**, the IGMP function is enabled in the MVLAN and this is not the cause of the fault. Then, go to [Step 6.3](#).

 **NOTE**

If the terminal (ONU or STB) used by the user does not support multicast management, enable the IGMP function on the OLT. Otherwise, the multicast service cannot be provisioned to the user.

3. Run the **display ont info** command to query the configurations of the ONU ETH port. Specially, query the port VLAN and native VLAN of the ETH port carrying the multicast service. Compare the queried data with the data of a normal multicast user to verify whether the configurations are correct.
 - If the configurations are correct, go to [Step 7](#).
 - If the configurations are incorrect, modify configurations by referring to the configurations of a common user. Then, order the program again and go to [Step 6.4](#).

 **NOTE**

The configurations of the ONU ETH port carrying the multicast service depend on the network topology and data plan and therefore the configurations are flexible. The typical configurations are: **Port VLAN** is **CVLAN** and **Native VLAN** is not configured. If the default native VLAN is different from the port VLAN, the untagged multicast packets sent from the user side will be dropped by the ONU ETH port. As a result, the user fails to go online.

4. Check whether the user can go online.
 - If the user can go online, go to [Step 10](#).
 - If the user fails to go online, go to [Step 7](#).

Step 7 If the OLT does not receive the report packet and the other users in the MVLAN can go online, find the possible cause according to the judgment criteria described

in **Table 9-8** and troubleshoot the fault. Then, go to **Step 8** to verify whether the fault is rectified.

Table 9-8 Line and terminal faults and troubleshooting methods

Possible Cause	Judgment Criterion	Troubleshooting Method
The STB is faulty.	The user can go online after resetting the STB or replacing the STB with a functional one and ordering the program.	Reset the STB or replace the STB with a functional one.
The ONU is faulty.	The user can go online after resetting the ONU or replacing the ONU with a functional one and ordering the program.	Reset the ONU or replace the ONU with a functional one. NOTE Some ONUs can be reset remotely by running commands on the OLT. For details, see 5.7.8 Resetting an ONT .
The physical line between the STB and ONU is faulty. For example, the network cable is not securely connected, is damaged, or is incorrectly connected.	Check the LAN indicator on the ONU to determine the status of the physical line between the STB and ONU. For MA567x: <ul style="list-style-type: none">If the LAN indicator is off, the line is faulty.If the LAN indicator is steady on or blinks, the line is in the normal state.	Connect the network cable again or replace the network cable with a functional one.

Step 8 Order a program and check whether the user can go online.

- If the user can go online, go to **Step 10**.
- If the user fails to go online, go to **Step 9**.

Step 9 Connect Technical Support.

Step 10 The fault is rectified.

----End

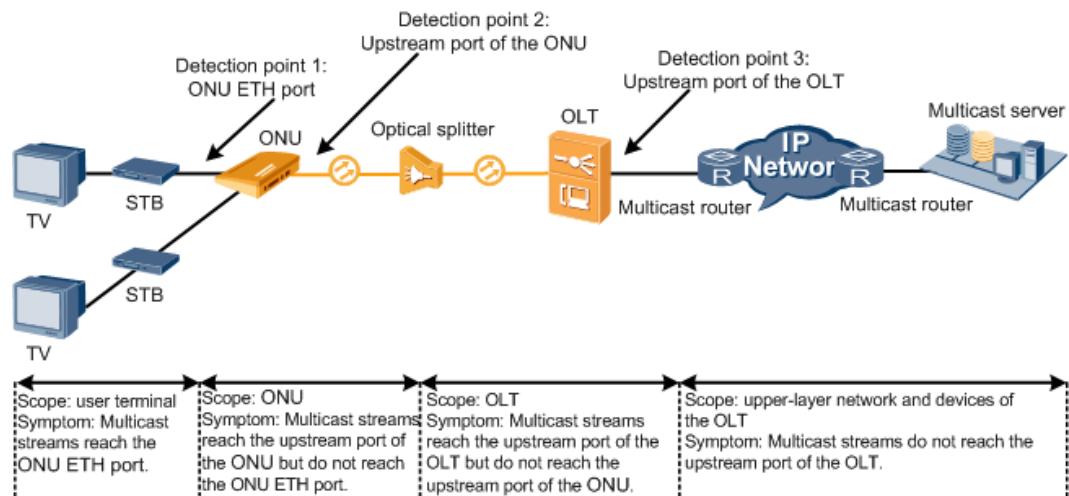
9.2.2 Blank Screen After a Program Is Ordered

When such a fault occurs, a user cannot watch the program after the user goes online and orders a program. When such a fault occurs in an FTTO network, locate and troubleshoot the fault by using the following location methods and troubleshooting procedure.

Location Method

When blank screen occurs after a user orders a program in an FTTO network, the fault scope can be determined by the location where program traffic interruption occurs, as shown in [Figure 9-6](#).

Figure 9-6 Locating the fault



[Table 9-9](#) describes possible causes of the fault in different scopes.

Table 9-9 Possible causes of the fault in different scopes

Fault Scope	Possible Cause
User terminal	<ul style="list-style-type: none"> The TV cable connecting the TV set to the set top box (STB) is not properly connected or is damaged. The STB is faulty.
ONU	The ONU is faulty.

Fault Scope	Possible Cause
OLT	<p>On the OLT, check whether the multicast user is online and then troubleshoot the fault according to the following symptoms:</p> <ul style="list-style-type: none">• If the multicast user is offline or blocked, troubleshoot the fault by referring to related description in 9.2.1 Multicast User Fails to Go Online.• If the multicast user goes online but the multicast program still has a blank screen, the fault is generally caused by incorrect multicast configurations on the OLT. In this case, enable the OLT debugging function and locate the fault according to the debugging information displayed on the OLT CLI. Possible causes are as follows:<ul style="list-style-type: none">- The remaining multicast bandwidth of the user is lower than the bandwidth required by the ordered program.- The number of programs that the user watches reaches the upper limit so that the user cannot order a new program.- The multicast user does not have the permission to watch the program.- The program ordered is not in the MVLAN to which the multicast user belongs.- The multicast user does not have the permission to order certain types of programs (such as HDTV).- The number of programs at a level that the user can watch reaches the upper limit so that the user cannot order a new program at this level.- The rate configured in the traffic profile that is bound to the service port is far lower than the bandwidth of the multicast program.- There are too many prejoin static programs, occupying too much bandwidth.- The maximum multicast bandwidth assigned to the PON port is very low.
Upper-layer network and devices (including the multicast router and multicast server) of the OLT	<ul style="list-style-type: none">• The program is not configured on the multicast server.• The time to live (TTL) value set on the multicast server for the multicast stream is very small.• Network communication fails between the OLT and multicast router, or between the multicast router and multicast server.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Order a program again and perform the following steps to determine the location where program traffic interruption occurs.

1. Run the **display multicast flow-statistic vlan 3 ip 224.1.1.1** command to query the traffic statistics of the ordered program on the OLT upstream port (this example assumes that the MVLAN ID is 3 and the IP address of the multicast program is 224.1.1.1). If the queried program traffic is not 0, the program traffic has reached the OLT upstream port.
2. On the OLT, run the **display statistics ont** command in global config mode two or three times to query the statistics of the traffic sent from PON port to the ONU. If the value of **Sent frames** changes obviously every time, the program traffic has reached the upstream port of the ONU.

 **NOTE**

The following prerequisites must be met before you run the **display statistics ont** command to query the traffic statistics so as to prevent the query results from being affected by other services.

- The multicast user is not watching other programs.
 - The ONU is not carrying other heavy-traffic services, such as file download from the Internet.
3. According to the preceding query results, determine the fault scope by referring to **Table 9-10** and perform operations accordingly.

 **NOTE**

When multiple NEs need to be checked, generally locate the fault from lower-layer devices to upper-layer devices, that is, in the sequence of user terminal -> ONU -> OLT -> multicast router -> multicast server, section by section along the service route.

Table 9-10 Fault scope and troubleshooting methods

Fault Scope	Judgment Criterion	Troubleshooting Method
User terminal, ONU	Multicast streams reach the upstream port of the ONU but do not reach the user port of the ONU.	<ol style="list-style-type: none">1. Check the user terminal following Step 2.2. Check the ONU following Step 3.
User terminal, ONU, and OLT	Multicast streams reach the upstream port of the OLT but do not reach the upstream port of the ONU.	<ol style="list-style-type: none">1. Check the user terminal following Step 2.2. Check the ONU following Step 3.3. Check the OLT following Step 4.

Fault Scope	Judgment Criterion	Troubleshooting Method
User terminal, ONU, OLT, and upper-layer network and devices of the OLT	Multicast streams do not reach the upstream port of the OLT.	<ol style="list-style-type: none">1. Check the user terminal following Step 2.2. Check the ONU following Step 3.3. Check the OLT following Step 4.4. Check the upper-layer network and devices of the OLT following Step 5.

Step 2 Check the user terminal.

1. Verify that the TV cable is properly connected to the STB.
2. Check the indicator status of the STB. If the indicator of the STB ETH port connected to the ONU blinks quickly, the STB decoding may be incorrect. Reset the STB or replace the STB with a functional one.
3. Order a program to check whether the user can watch the program successfully.
 - If the user can watch the program successfully, go to [Step 7](#).
 - If the user fails to watch the program, go to [Step 2.4](#).
4. Check whether all NEs have been checked according to [Table 9-10](#).
 - If all NEs have been checked, go to [Step 6](#).
 - If some NEs have not been checked, check these NEs according to [Table 9-10](#).

Step 3 Check the ONU.

1. Reset the ONU by referring to [Resetting an ONU](#). Order the program to check whether the user can watch the program.
 - If the user can watch the program successfully, go to [Step 7](#).
 - If the user fails to watch the program, go to [Step 3.2](#).
2. Replace the ONU with a functional one by referring to [Replacing an ONU](#). Order the program to check whether the user can watch the program.
 - If the user can watch the program successfully, go to [Step 7](#).
 - If the user fails to watch the program, go to [Step 3.3](#).
3. Check whether all NEs have been checked according to [Table 9-10](#).
 - If all NEs have been checked, go to [Step 6](#).
 - If some NEs have not been checked, check these NEs according to [Table 9-10](#).

Step 4 Check the OLT.

1. Run the **display igmp user service-port** command to query the multicast user status (check the **State** parameter).
 - If **State** is **online**, go to [Step 4.2](#).

- If State is **offline** or **block**, perform operations by referring to [9.2.1 Multicast User Fails to Go Online](#). Then, go to [Step 7](#).
2. Enable the OLT debugging function and collect information as follows:
 - a. Enable the function of multicast user monitoring.

```
huawei(config)#terminal monitor
huawei(config)#terminal debugging
huawei(config)#debugging igmp service-port
```
 - b. Order a program again and go to [Step 4.3](#).

 **NOTE**

After the preceding steps are performed, run the following commands to disable the debugging function.

```
huawei(config)#undo debugging igmp
huawei(config)#undo terminal debugging
huawei(config)#undo terminal monitor
```

3. Find the possible cause according to the judgment criteria described in [Table 9-11](#) and troubleshoot the fault. Then, go to [Step 4.4](#) to verify whether the fault is rectified.

Table 9-11 Incorrect multicast configurations of the OLT and troubleshooting methods

Possible Cause	Judgment Criterion	Troubleshooting Method
No upstream port is configured in the MVLAN to which the multicast user belongs if both the following situations occur: NOTE In this case, multicast streams do not reach the upstream port of the OLT.	No upstream port is configured in the MVLAN to which the multicast user belongs if both the following situations occur: <ul style="list-style-type: none"> - The OLT receives the report packet and displays "match program fail". - No upstream port maps the user's MVLAN in the display igmp uplink-port all command output. 	Add an upstream port to the MVLAN and ask the user to order the program again. NOTE In MVLAN mode, run the igmp uplink-port command to set the upstream port as the upstream port of the MVLAN. This allows the upstream port to forward the multicast packets of this MVLAN.

Possible Cause	Judgment Criterion	Troubleshooting Method
The maximum multicast bandwidth of the user is lower than the bandwidth required by the ordered program if one of the following situations occurs:	<p>The maximum multicast bandwidth of the user is lower than the bandwidth required by the ordered program if one of the following situations occurs:</p> <ul style="list-style-type: none"> - The OLT receives the report packet and displays "the user fails to pass bandwidth CAC". - Run the display igmp user service-port command to query the maximum bandwidth (User MaxBandWidth) and used bandwidth (Used bandwidth) of the user and run the display igmp program name command to query the bandwidth (Bandwidth) of the ordered program. As shown by the command output, the user's remaining bandwidth (maximum bandwidth minus used bandwidth) is lower than the bandwidth of the ordered program. <p>NOTE If User MaxBandWidth is no-limit, the multicast bandwidth of the user is not limited.</p>	<p>Choose one of the following troubleshooting methods according to the purchased service type:</p> <ul style="list-style-type: none"> - Inform the user that no more programs can be ordered because the user's remaining bandwidth is insufficient, and ask the user to close some programs first and then order the program again. - Increase the user bandwidth and ask the user to order the program again. <p>NOTE</p> <ul style="list-style-type: none"> - You can run the igmp user modify service-port index max-bandwidth command to modify the maximum bandwidth of the user. - When multicast bandwidth management (multicast CAC) is disabled, the system does not guarantee the bandwidth of the program requested by the user. - Because the downstream rate of a line is limited, multicast packets will be lost if the bandwidth of the downstream multicast streams is higher than the maximum rate of the line. In this case, the user can watch the program but pixelation or delay occurs. If a large number of multicast packets are lost, blank screen occurs.

Possible Cause	Judgment Criterion	Troubleshooting Method
The maximum number of programs that the user can concurrently watch reaches the preset maximum value if one of the following situations occurs: <ul style="list-style-type: none"> - The OLT receives the report packet and displays "the number of program that the user is allowed to watch has reached maximum". - The number of programs that the user is watching is equal to the available programs (Available programs) in the display igmp user service-port command output. 	<p>The maximum number of programs that the user can concurrently watch reaches the preset maximum value if one of the following situations occurs:</p> <ul style="list-style-type: none"> - The OLT receives the report packet and displays "the number of program that the user is allowed to watch has reached maximum". - The number of programs that the user is watching is equal to the available programs (Available programs) in the display igmp user service-port command output. 	<p>Choose one of the following troubleshooting methods according to the purchased service type:</p> <ul style="list-style-type: none"> - Inform the user that no more programs can be ordered because the available programs reach the preset maximum value, and ask the user to close some programs and order the program again. - Increase the available programs for the user and ask the user to order the program again. <p>NOTE You can run the igmp user modify service-port index max-program command to modify the number of available programs.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
The multicast user does not have the permission to watch the program.	<p>The multicast user does not have the permission to watch the program if one of the following situations occurs:</p> <ul style="list-style-type: none"> - The OLT receives the report packet and displays "the user has no right". - Run the display igmp user service-port 100 command to query the right profile bound to the multicast user (this example assumes that the service port index of the multicast user is 100). ■ If Bind profiles is 0, the user is not bound to a right profile so the user cannot order any programs. ■ If Bind profiles is equal to or larger than 1, the user can watch only the program to which the user has the watch permission. In this case, perform operations for further check. In the query result, find the index (this example assumes that the index is 1) and name of the right profile bound to the user and run the display igmp profile profile-index 1 command to query the user permission for ordering the program. <ul style="list-style-type: none"> ○ If the permission of a program is forbidden or idle, the user does not have the permission to order the program. ○ If the permission of a program is watch or preview, the user can order the program. If so, the user's permission to 	<p>Choose one of the following troubleshooting methods according to the purchased service type:</p> <ul style="list-style-type: none"> - If the user can watch all programs without authentication, perform the following two operations: <ol style="list-style-type: none"> 1. In BTV mode, run the igmp user modify service-port 100 no-auth command to modify the authentication mode of the user to "no authentication" (this example assumes that the service port index of the multicast user is 100). 2. Order the program again. - If the user can watch only certain programs with authentication, inform the user that the user has no permission to watch the program and ask the user to order a program with the watch or preview permission. <p>NOTE To set permissions of the user for ordering some programs, run the igmp user bind-profile service-port 100 profile-index-list 1 command to bind a correct right profile to the multicast user (this example assumes that the service port index of the multicast user is 100 and the right profile index is 1).</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
	<p>the program is not the cause of this fault.</p> <p>NOTE</p> <p>A multicast user can be bound to multiple right profiles. If these right profiles are configured with different permissions to the same program, the permission with the highest priority prevails. By default, the priorities of the program permissions are forbidden > preview > watch > idle. You can run the igmp right-priority command on the OLT to set the priorities.</p>	

Possible Cause	Judgment Criterion	Troubleshooting Method
The program ordered is not included in the MVLAN to which the multicast user belongs.	<p>The program ordered is not included in the MVLAN to which the multicast user belongs if both the following situations occur:</p> <ul style="list-style-type: none"> - The OLT receives the report packet and displays "match program fail". - In the display igmp program vlan command output, the program ordered is not in the program list of the MVLAN. 	<p>Choose one of the following troubleshooting methods according to the purchased service type:</p> <ul style="list-style-type: none"> - Inform the user that the user has no permission to watch the program, and ask the user to order a program that is included in the MVLAN to which the multicast user belongs. - Perform the following steps to add the program to the user's MVLAN and ask the user to order the program again. <ol style="list-style-type: none"> 1. Run the display igmp config vlan command to query Program match mode of the MVLAN. <ul style="list-style-type: none"> o If Program match mode is enable, the program is a static program, which is manually added. o If Program match mode is disable, the program is a dynamic program, which is automatically generated upon ordering. 2. Add programs to the MVLAN. <ul style="list-style-type: none"> o To add a static program to an MVLAN, run the igmp program add command. o To add dynamic programs to an MVLAN, run the

Possible Cause	Judgment Criterion	Troubleshooting Method
		<p>igmp match group command to set the IP address range of program groups that can be generated dynamically in the MVLAN, and include the IP address of the ordered program in the IP address range.</p>
The multicast user does not have the permission to order certain types of programs (such as HDTV).	<p>The multicast user does not have the permission to order certain types of programs if one of the following situations occurs:</p> <ul style="list-style-type: none"> - The OLT receives the report packet and displays "the number of the grade program that the user is allowed to watch has reached maximum". - The maximum number of programs at a level that the user can watch (watch limit) is 0 in the display igmp user extended-attributes service-port command output. <p>NOTE If the maximum number of the programs at a certain level is 0, the user cannot order any programs at this level. That is, the user's permission to the programs of the corresponding type is limited. For example, if HDTV watch limit is 0, the user cannot watch HDTV programs.</p>	<p>Choose one of the following troubleshooting methods according to the purchased service type:</p> <ul style="list-style-type: none"> - Inform the user that the program cannot be watched because the user does not have the permission to watch the program, and ask the user to order a program that has not reached the maximum watch limit at its level. - Add the permission for ordering the programs at this level for the user so that the user can order the program. <p>NOTE You can run the igmp user watch-limit service-port command to set the number of programs at each level that a user can watch.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
The number of programs at a level that the user can watch reaches the upper limit so that the user cannot order a new program at this level.	<p>Such is the case if one of the following situations occurs:</p> <ul style="list-style-type: none"> - The OLT receives the report packet and displays "the number of the grade program that the user is allowed to watch has reached maximum". - The number of programs that the user is watching is equal to the maximum number (watch limit) of programs at a level that the user can watch in the display igmp user extended-attributes service-port command output. <p>NOTE If watch limit is no-limit, the maximum number of programs at this level that a user can watch is not limited, but the total number of programs that can be concurrently watched is limited.</p>	<p>Choose one of the following troubleshooting methods according to the purchased service type:</p> <ul style="list-style-type: none"> - Inform the user that the ordered program has not been purchased by the user and ask the user to order other programs. - Increase the maximum number of programs at this level and ask the user to order the program again. <p>NOTE You can run the igmp user watch-limit service-port command to set the number of programs at each level that a user can watch.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
There are too many prejoin static programs, occupying too much bandwidth.	<p>The prejoin static programs occupy too much bandwidth, which is close to the maximum downstream bandwidth of multicast programs provided by the PON port.</p> <ul style="list-style-type: none"> - You can obtain the bandwidth of prejoin static programs following the steps below: <ol style="list-style-type: none"> 1. Run the display igmp program all command to query the prejoin attribute (Prejoin) of the program. 2. Calculate the bandwidth of prejoin static programs (Prejoin is enable) according to the data plan. For example, if 100 programs are enabled with the prejoin function and the bandwidth of each program is 5 Mbit/s, the total bandwidth of the prejoin static programs is 500 Mbit/s. - You can obtain the maximum downstream bandwidth of multicast programs provided by the PON port following the steps below: <ol style="list-style-type: none"> 1. Run the display igmp config global command to query the bandwidth management function (Bandwidth management switch). 2. Run the display igmp bandwidth port command to query the bandwidth (Max bandwidth) assigned to the PON port. <ul style="list-style-type: none"> ▪ If Bandwidth management switch is disable, the OLT does not perform multicast 	<p>Run the igmp program modify command to modify Prejoin to disable and then order the program again.</p> <p>NOTE You can modify the attributes of all multicast programs in any MVLAN. When a program is being watched or previewed by a user, however, its attributes cannot be modified.</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
	<p>bandwidth management. The maximum bandwidth in this case is the maximum downstream transmission rate supported by the PON line.</p> <ul style="list-style-type: none"> ▪ If Bandwidth management switch is enable and Max bandwidth is no-limit, the OLT performs multicast bandwidth management but the OLT PON port does not limit the multicast program bandwidth. The maximum bandwidth in this case is the maximum downstream transmission rate supported by the PON line. ▪ If Bandwidth management switch is enable and Max bandwidth has a specific value, the OLT PON port limits the multicast program bandwidth. The maximum bandwidth in this case is the bandwidth (Max bandwidth) assigned to the PON port. 	

Possible Cause	Judgment Criterion	Troubleshooting Method
The maximum multicast bandwidth assigned to the PON port is very low if both the following situations occur: <ul style="list-style-type: none"> - In the display igmp config global command output, the bandwidth management function (Bandwidth management switch) is enable. - Run the display igmp bandwidth port command to query the bandwidth (Max bandwidth) assigned to the PON port and the used bandwidth (Used bandwidth). As shown by the command output, the remaining bandwidth (the assigned bandwidth minus the used bandwidth) is lower than the bandwidth of the ordered program. - The bandwidth assigned to the PON port is very small, which does not meet the total bandwidth requirement of OLT multicast users. 	Run the igmp bandwidth port command to modify the maximum bandwidth provided by the PON port for multicast programs to meet the total bandwidth requirement of the OLT multicast user. Then order the program again.	

4. Check whether the user can watch the program successfully.
 - If the user can watch the program successfully, go to [Step 7](#).
 - If the user fails to watch the program, go to [Step 4.5](#).
5. Check whether all NEs have been checked according to [Table 9-10](#).
 - If all NEs have been checked, go to [Step 6](#).
 - If some NEs have not been checked, check these NEs according to [Table 9-10](#).

Step 5 Check the upper-layer network and devices of the OLT.

1. Find the possible cause according to the judgment criteria described in [Table 9-12](#) and troubleshoot the fault. Then, go to [Step 5.2](#) to check whether the fault is rectified.

Table 9-12 Faulty upper-layer network and devices of the OLT and troubleshooting methods

Possible Cause	Judgment Criterion	Troubleshooting Method
The program is not configured on the multicast server.	<p>The multicast server does not have the program.</p> <p>NOTE If the user can watch the program, it indicates that the multicast server has the program.</p>	Add the program to the multicast server.
The TTL value set on the multicast server for the multicast stream is very small.	<p>All users of the OLT fail to watch all programs configured on the multicast server.</p> <p>NOTE If the TTL value of multicast packets on the upstream port of the OLT is smaller than 2, the OLT drops the multicast packets.</p>	Increase the TTL value of multicast packets on the multicast server.
The upper-layer network communication of the OLT fails.	<p>Ping the multicast router and the multicast server from the OLT separately. It is found that the OLT fails to ping the multicast router or the multicast server.</p> <p>NOTE If other users of the OLT can watch the program, the network between the OLT and the multicast server is functional.</p>	Troubleshoot the fault in the network between the OLT and the multicast router or between the OLT and the multicast server.

2. Order a program again and check whether the user can watch the program.
 - If the user can watch the program successfully, go to [Step 7](#).
 - If the user fails to watch the program, go to [Step 5.3](#).
3. Check whether all NEs have been checked according to [Table 9-10](#).
 - If all NEs have been checked, go to [Step 6](#).
 - If some NEs have not been checked, check these NEs according to [Table 9-10](#).

Step 6 Connect Technical Support.

Step 7 The fault is rectified.

----End

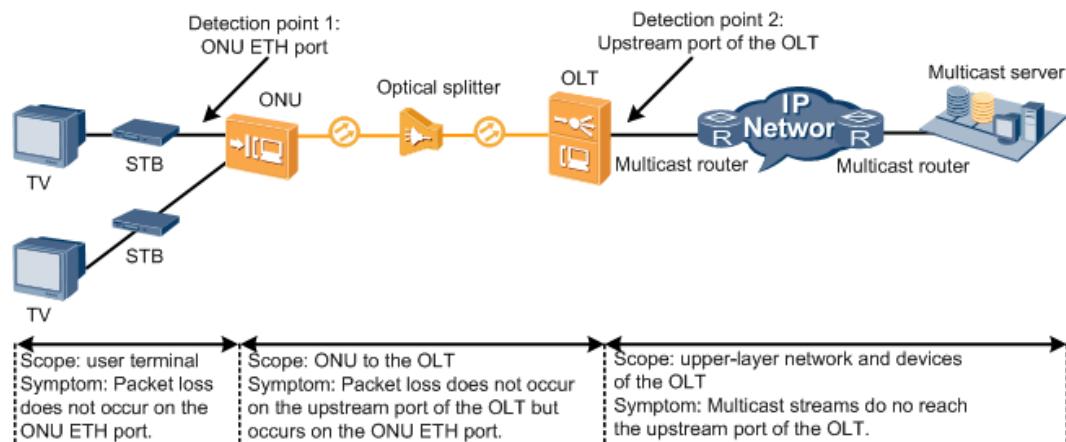
9.2.3 Pixelation in a Multicast Program

Pixelation in a multicast program is a fault that a user goes online successfully and orders a program but the quality of the program is poor. For example, the program has pixelation. When pixelation occurs in a program in a fiber to the office (FTTO) network, locate and troubleshoot the fault using the following location methods and troubleshooting procedure.

Location Method

When pixelation occurs, the fault scope can be determined by the location where packet loss occurs, as shown in [Figure 9-7](#).

Figure 9-7 Locating the pixelation fault



[Table 9-13](#) describes possible causes of the fault in different scopes. When the fault scope cannot be determined, generally locate the fault from upper-layer devices to low-layer devices, that is, in the sequence of multicast server -> multicast router -> OLT -> ODN -> ONU -> user terminal, section by section along the service route.

Table 9-13 Possible causes of the fault in different scopes

Fault Scope	Possible Cause
User terminal	<ul style="list-style-type: none"> The STB is faulty. The TV set is faulty.
ONU	The ONU is faulty.
ODN	Packet loss occurs over the physical line between the OLT and the ONU.

Fault Scope	Possible Cause
OLT	<ul style="list-style-type: none">The bandwidth configured in the traffic profile bound to the traffic stream is lower than the bandwidth of the multicast program.The QoS rate limited on the port is excessively low.The DBA bandwidth allocated to the MDU from the OLT is insufficient.The MAC address aging time is excessively short.The index of the unknown multicast or unicast traffic suppression table is excessively small.
Upper-layer network and devices of the OLT	<ul style="list-style-type: none">The multicast source is abnormal.Network communication fails on the physical line between the OLT and multicast router, or between the multicast router and multicast server.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Order a program again and perform the following steps to determine the location where multicast packets are lost.

Run the **display multicast flow-statistic vlan 3 ip 224.1.1.1** command to query the traffic statistics of the ordered program on the OLT upstream port (this example assumes that the MVLAN ID is 3 and the IP address of the multicast program is 224.1.1.1).

- If the query result is close to the rate of the program traffic, the program traffic has reached the OLT upstream port. Then, go to **Step 3** and **Step 4**.
- If the query result is far lower than the rate of the program traffic, the program traffic encounters packet loss before reaching the OLT upstream port. This indicates that the upper-layer network and devices of the OLT are faulty. Then, go to **Step 2**.

Step 2 Check the upper-layer network and devices of the OLT.

- Find the possible cause according to judgment criteria described in **Table 9-14** and troubleshoot the fault. Then, go to **Step 2.2** to check whether the fault is rectified.

Table 9-14 Faulty upper-layer network and devices of the OLT and troubleshooting methods

Possible Cause	Judgment Criterion	Troubleshooting Method
The multicast source is abnormal.	<p>Pixelation occurs when a user watches a program on the multicast server.</p> <p>NOTE If other users can watch the program properly, the multicast source is functional.</p>	Replace the multicast source.
The upper-layer network of the OLT is of poor quality.	<p>Ping the multicast router and multicast server from the OLT separately. It is found that packet loss occurs.</p> <p>NOTE If other users of the OLT can watch the program, the network between the OLT and the multicast server is functional.</p>	Troubleshoot the fault in the network between the OLT and the multicast router or between the OLT and the multicast server.

2. Order the program and check whether the user can watch the program.
 - If the user can watch the program successfully, go to [Step 8](#).
 - If the user fails to watch the program, go to [Step 2.3](#).
3. Check whether packet loss occurs on the upstream port of the OLT.
 - If packet loss occurs on the upstream port of the OLT, go to [Step 7](#).
 - If no packet is lost on the upstream port of the OLT, the fault on the physical line between the OLT and the multicast server is cleared. Then, troubleshoot the fault in other fault scopes according to the location where packet loss occurs and go to [Step 1](#).

Step 3 Check the quality of the optical path between the OLT PON and the ONU.

1. Run the **display statistics ont-line-quality** command to query the quality statistics of the ONU line connected to the PON port multiple times.
 - If bit errors increase, the optical path is of poor quality. Then, rectify the fault on the optical path and physical line and check whether the fault has been rectified according to [Step 3.2](#).
 - If bit errors are within the normal range, the optical path is functional. Then, go to [Step 4](#).
2. Order the program and check whether the user can watch the program.
 - If the user can watch the program, go to [Step 8](#).
 - If the user cannot watch the program, go to [Step 4](#).

Step 4 Check the OLT.

1. Run the **display alarm history all** command to query historical alarms and check whether the OLT generates an ODN-related alarm.

- If an ODN-related alarm is generated, the ODN is faulty. In this case, clear the alarm by referring to relevant instruction documents. Then, go to [Step 4.3](#).
 - If no ODN-related alarm is generated, go to [Step 4.2](#).
2. Find the possible cause according to judgment criteria described in [Table 9-15](#) and troubleshoot the fault. Then, go to [Step 4.3](#) to check whether the fault is rectified.

Table 9-15 Incorrect configurations of the OLT and troubleshooting methods

Possible Cause	Judgment Criterion	Troubleshooting Method
The QoS rate limited on the port is excessively low.	<p>Run the display qos-info traffic-limit port command to query the target rate of the user port. The query result shows that the target rate is less than the rate required for ordering the program.</p> <p>NOTE If the user port carries other services, such as the Internet access service, the traffic of all services must be lower than or equal to the target rate. Otherwise, other services may occupy the majority bandwidths and the multicast bandwidth is insufficient, leading to the pixelation.</p>	Run the traffic-limit command to change the target rate to a proper value or run the undo traffic-limit command to cancel QoS rate limitation on the port.
The DBA bandwidth allocated to the ONU from the OLT is insufficient.	<ol style="list-style-type: none">1. Run the display ont info portid ontid command to query the ID of the DBA profile (DBA Profile-ID) configured for the ONU.2. Run the display DBA-profile profile-id command to query the maximum bandwidth configured in the DBA profile. The query result shows that the maximum bandwidth is less than the ordered program bandwidth. <p>NOTE If the user port carries other services, such as the Internet access service, the traffic of all services must be lower than or equal to the maximum bandwidth. Otherwise, other services may occupy the majority bandwidths and the multicast bandwidth is insufficient, leading to the pixelation.</p>	For a GPON ONU, run the tcont command to bind a DBA profile with a proper maximum bandwidth to the ONU.

Possible Cause	Judgment Criterion	Troubleshooting Method
The MAC address aging time is excessively short.	Run the display mac-address timer command to query the MAC address aging time. The default value 300s is recommended.	Run the mac-address timer command to change the MAC address aging time to a proper value.
The index of the unknown multicast or unicast traffic suppression table is excessively small.	Run the display traffic-suppress command to query the index of the unknown traffic suppression table and the suppressed traffic.	Run the traffic-suppress command to change the index of the unknown multicast or unicast traffic suppression table to a proper value. The unknown multicast or unicast traffic suppression table is based on the video source.

3. Order the program and check whether the user can watch the program.

- If the user can watch the program successfully, go to [Step 8](#).
- If the user fails to watch the program, go to [Step 5](#).

Step 5 Check the ONU.

1. Reset the ONU by referring to [Resetting an ONU](#). Order a program again and check whether the user can watch the program.
 - If the user can watch the program successfully, go to [Step 8](#).
 - If the user fails to watch the program, go to [Step 5.2](#).
2. Replace the ONU with a functional one by referring to [Replacing an ONU](#). Order a program again and check whether the user can watch the program.
 - If the user can watch the program successfully, go to [Step 8](#).
 - If the user fails to watch the program, go to [Step 5.3](#).
3. Check whether packet loss occurs on the ONU ETH port.
 - If packets are lost on the ONU ETH port, go to [Step 7](#).
 - If no packet is lost on the ONU ETH port, the fault on the physical line between the ONU and OLT is cleared. Then, go to [Step 6](#).

Step 6 Check the user terminal.

1. Reset the STB. Order a program again and check whether the user can watch the program.

- If the user can watch the program successfully, go to [Step 8](#).
 - If the user fails to watch the program, go to [Step 6.2](#).
2. Replace the STB. Order a program again and check whether the user can watch the program.
 - If the user can watch the program successfully, go to [Step 8](#).
 - If the user fails to watch the program, go to [Step 6.3](#).
 3. Check whether the TV set is faulty. If the TV set is faulty, troubleshoot the fault. Order a program again and check whether the user can watch the program.
 - If the user can watch the program successfully, go to [Step 8](#).
 - If the user fails to watch the program, go to [Step 7](#).

 **NOTE**

You can connect the TV cable to another video input device such as a DVD player or VCR player to check whether the TV set is faulty. If pixelation persists, the TV set is faulty.

Step 7 Connect Technical Support.

Step 8 The fault is rectified.

----End

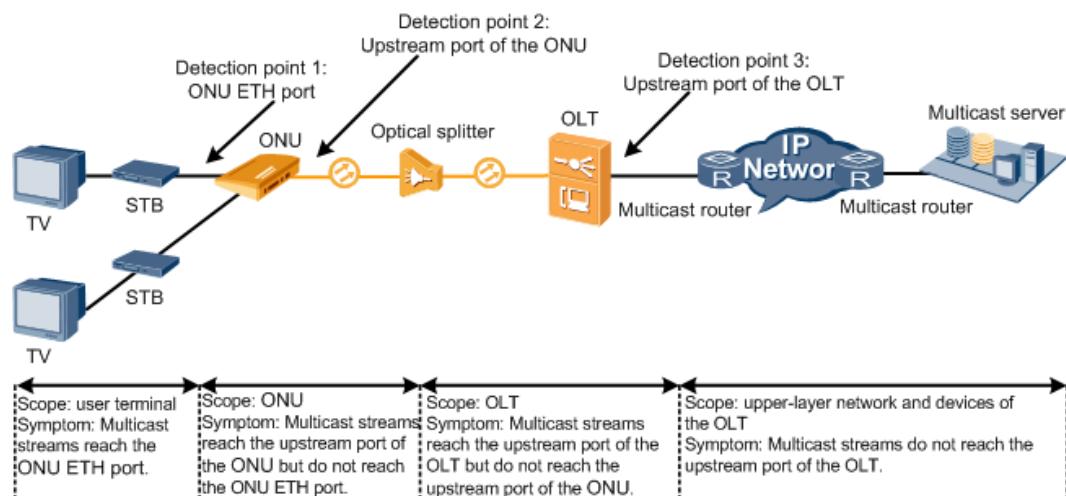
9.2.4 Abnormal Interruption of a Multicast Program

Abnormal interruption of a multicast program is a fault that a program is abnormally interrupted when a multicast user is watching the program. When abnormal program interruption occurs in an FTTO network, locate and troubleshoot the fault by using the following location methods and troubleshooting procedure.

Location Method

When abnormal interruption occurs after a user orders a program in an FTTO network, the fault scope can be determined by the location where program traffic interruption occurs, as shown in [Figure 9-8](#).

Figure 9-8 Locating the fault



When abnormal multicast program interruption occurs in an FTTO network, generally locate the fault from upper-layer devices to lower-layer devices, that is, in the sequence of multicast server -> multicast router -> OLT -> ODN -> ONU -> user terminal, section by section along the service route. **Table 9-16** describes possible causes of the fault in different scopes.

Table 9-16 Possible causes of the fault in different scopes

Fault Scope	Judgment Criterion	Possible Cause
Upper-layer network and devices of the OLT	All users encounter the fault.	The multicast source is abnormal.
	All users of the OLT encounter the fault.	Network communication fails on the physical line between the OLT and multicast router, or between the multicast router and multicast server.
OLT	The OLT is faulty if both the following symptoms occur: <ul style="list-style-type: none">● A single user encounters the fault.● Other programs can still be watched when a program is interrupted.	The viewing duration of the user reaches the preview duration.
	The OLT is faulty if both the following symptoms occur: <ul style="list-style-type: none">● The ONU is connected to multiple STBs.● Programs of an STB are frequently interrupted when a program is switched on another STB.	The quick leave mode of the user is immediate .
ODN	The ODN is faulty if the OLT generates the following alarms: <ul style="list-style-type: none">● 0x2e11a001 The feeder fiber is broken or OLT can not receive any expected optical signals(LOS)● 0x2e112007 The distribute fiber is broken or the OLT cannot receive expected optical signals from the ONT(LOSi/LOBi)	The backbone fiber or branch fiber is faulty.

Fault Scope	Judgment Criterion	Possible Cause
ONU and user terminal	The ONU and user terminal are faulty if both the following symptoms occur: <ul style="list-style-type: none">• A single user encounters the fault.• Other programs cannot be watched when a program is interrupted.	<ul style="list-style-type: none">• The ONU is faulty.• The STB is faulty.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check the upper-layer network and devices of the OLT.

1. Find the possible cause according to the judgment criteria described in [Table 9-17](#) and troubleshoot the fault. Then, go to [Step 1.2](#) to check whether the fault is rectified.

Table 9-17 Faulty upper-layer network and devices of the OLT and troubleshooting methods

Possible Cause	Judgment Criterion	Troubleshooting Method
The multicast source is abnormal.	Program interruption occurs when a user is watching a program ordered from the multicast server. NOTE If other users can watch the program properly, the multicast source is functional.	Replace the multicast source.

Possible Cause	Judgment Criterion	Troubleshooting Method
The upper-layer network communication of the OLT fails.	<p>Ping the multicast router and the multicast server from the OLT separately. It is found that the OLT fails to ping the multicast router or the multicast server.</p> <p>NOTE If other users of the OLT can watch the program, the network between the OLT and the multicast server is functional.</p>	Troubleshoot the fault in the network between the OLT and the multicast router or between the OLT and the multicast server.

2. Order the program to check whether the user can watch the program.
 - If the user can watch the program successfully, go to [Step 5](#).
 - If the user fails to watch the program, go to [Step 2](#).

Step 2 Check the OLT.

1. Run the **display alarm history all** command to query historical alarms and check whether the OLT generates the following alarms:

GPON:

 - **0x2e11a001 The feeder fiber is broken or OLT can not receive any expected optical signals(LOS)**
 - **0x2e112007 The distribute fiber is broken or the OLT cannot receive expected optical signals from the ONT(LOSi/LOBi)**
 - If the preceding alarms are generated, the fiber is faulty. In this case, clear the alarms by referring to relevant instruction documents. Then, go to [Step 2.3](#).
 - If the preceding alarms are not generated, go to [Step 2.2](#).
2. Find the possible cause according to the judgment criteria described in [Table 9-18](#) and troubleshoot the fault. Then, go to [Step 2.3](#) to check whether the fault is rectified.

Table 9-18 Incorrect configurations of the OLT and troubleshooting methods

Possible Cause	Judgment Criterion	Troubleshooting Method
The viewing duration of the user reaches the preview duration.	<p>The viewing duration of the user reaches the preview duration if both the following symptoms occur:</p> <ul style="list-style-type: none"> - A single user encounters the fault. - Other programs can still be watched when a program is interrupted. <p>NOTE A program is suspended when its viewing duration reaches the preset preview duration.</p>	<p>Choose one of the following troubleshooting methods according to the purchased service type:</p> <ul style="list-style-type: none"> - Inform the user that the user has no permission to watch the program and ask the user to order a program with the watch permission. - Add the permission for watching the program for the user. <p>NOTE To set permissions of the user for ordering some programs, run the igmp user bind-profile service-port 100 profile-index-list 1 command to bind a correct right profile to the multicast user (this example assumes that the service port index of the multicast user is 100 and the right profile index is 1).</p>

Possible Cause	Judgment Criterion	Troubleshooting Method
The quick leave mode of the user is immediate .	<p>The quick leave mode of the user is immediate if the ONU is connected to multiple STBs and one of the following symptoms occurs:</p> <ul style="list-style-type: none"> - Programs of an STB are frequently interrupted when a program is switched on another STB. - As shown by the display igmp user service-port command output, the quick leave mode of the user is immediate. <p>NOTE</p> <ul style="list-style-type: none"> - If an ONU without the IGMP proxy function is connected to multiple STBs, quick leave can only be disable or mac-based. - If immediate is selected, the OLT stops forwarding the program traffic to the user after receiving the leave packet sent from the user. All services of an ONU are carried through a service port and all STBs connected to the ONU share the service port. As a result, if a program that is provided by an STB but being watched by other STBs is switched to another program, the program being watched by other STBs is interrupted. - For details about principles and data processing of the fast leave attribute, see Feature Guide > Multicast > Implementation Principles of Multicast > Multicast Forwarding > Leave Flow. 	In BTV mode, run the igmp user modify service-port 100 quickleave mac-based command to modify quick leave to mac-based (this example assumes that the service port index is 100). Order the program again and switch a program on another STB.

3. Check whether the user can watch the program.
 - If the user can watch the program successfully, go to [Step 5](#).
 - If the user fails to watch the program, go to [Step 3](#).

Step 3 Check the ONU and user terminal.

1. Check the indicator status of the STB. If the indicator of the STB ETH port connected to the ONU blinks quickly, the STB decoding may be incorrect. Reset the STB or replace the STB with a functional one. Order a program again and check whether the user can watch the program.
 - If the user can watch the program successfully, go to [Step 5](#).

- If the user fails to watch the program, go to [Step 3.2](#).
- 2. Reset the ONU by referring to [Resetting an ONU](#). Order a program again and check whether the user can watch the program.
 - If the user can watch the program successfully, go to [Step 5](#).
 - If the user fails to watch the program, go to [Step 3.3](#).
- 3. Replace the ONU with a functional one by referring to [Replacing an ONU](#). Order a program again and check whether the user can watch the program.
 - If the user can watch the program successfully, go to [Step 5](#).
 - If the user fails to watch the program, go to [Step 4](#).

Step 4 Connect Technical Support.

Step 5 The fault is rectified.

----End

9.2.5 Long Program Switching Time

Long program switching time is a fault that a very long time is required in switching the current program to a new one; however, the programs can be switched and the new program can be watched. When such a fault occurs in an FTTO network, locate and troubleshoot the fault using the following location methods and troubleshooting procedure.

Location Method

When the fault occurs in an FTTO network, check whether the fast leave attribute is correctly configured on the OLT.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Run the **display igmp user service-port** command to query the fast leave attribute (**quick leave**) of the user who encounters the fault, and check whether the fast leave attribute is correctly configured. The fast leave attribute can be configured by referring to [Table 9-19](#) according to user network's configurations.
- If the fast leave attribute is correctly configured, go to [Step 3](#).
 - If the fast leave attribute is incorrectly configured, run the **igmp user modify service-port quickleave** command to modify the fast leave attribute of the user. Then, go to [Step 2](#).

Table 9-19 Configuring the fast leave attribute of a multicast user

ONU IGMP Settings	Number of STBs	Reserved Bandwidth	Fast Leave Disabled	Immediate Fast Leave	MAC-Based Fast Leave
IGMP disabled	One	Insufficient		✓	✓
		Sufficient	✓	✓	✓
	More than one	Insufficient			✓ (fewer than or equal to eight STBs)
		Sufficient	✓		✓ (fewer than or equal to eight STBs)
	One	Insufficient		✓	✓
		Sufficient	✓	✓	✓
IGMP snooping	More than one	Insufficient			✓ (fewer than or equal to eight STBs)
		Sufficient	✓		✓ (fewer than or equal to eight STBs)
	One	Insufficient		✓	✓
		Sufficient	✓	✓	✓
IGMP proxy	One	Insufficient		✓	✓
		Sufficient	✓	✓	✓
	More than one	Insufficient		✓	✓ (not limited)
		Sufficient	✓	✓	✓ (not limited)

NOTE

- In [Table 9-19](#), ✓ indicates that the corresponding fast leave attribute can be selected.
- If MAC address-based fast leave is used, the OLT records the MAC addresses of multicast members in a multicast group, which are MAC addresses of the ONUs the multicast members connected to. The OLT records a maximum of eight MAC addresses for each program. The number of STBs connected to an ONU is not controlled by the OLT but based on ONU hardware and software.
- For details about principles and data processing of the fast leave attribute, see Feature Guide > Multicast > Implementation Principles of Multicast > Multicast Forwarding > Leave Flow.

Step 2 Order the program again to check whether the time of switching a program is of a proper length.

- If the time of switching a program is of a proper length, go to **Step 4**.
- If the time of switching a program is still too long, go to **Step 3**.

Step 3 Connect Technical Support.

Step 4 The fault is rectified.

----End

9.3 Troubleshooting Voice Service Faults

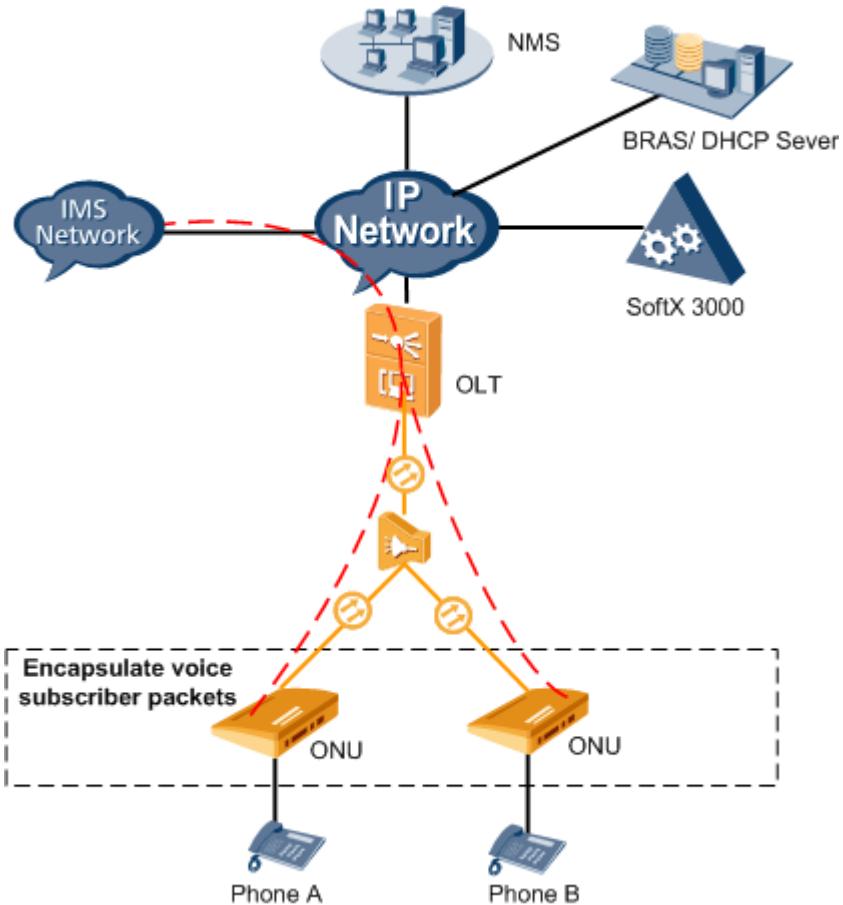
This topic describes how to troubleshoot voice service faults. Common voice service faults include: no tone after offhook, busy tone after offhook, one-way audio in a voice call, noise in a voice call, voice interruptions in a voice call, and failure to dial certain phone numbers.

Prerequisites

The ONU and OLT communicate with each other normally. If a fault occurs in a voice call between the ONU and OLT, all the services on the ONU may be interrupted. In this case, troubleshoot the fault first by referring to the methods described in **ONU Abnormal State**.

Context

In an FTTO network, voice subscribers access the network by using ONUs, and the ONUs work together with an upper-layer softswitch or IMS network to achieve the VoIP service. After encapsulated by ONUs that serve as MG or SIP interfaces, voice packets are forwarded to the next generation network (NGN) through the OLT. The following figure shows an FTTO network for voice service.



NOTE

Voice signaling tracing and voice VBD fault diagnosis may be used in voice service troubleshooting.

Based on your requirements, signaling tracing and VBD fault diagnosis may obtain some contents of users' communications

(integrity communication contents are not obtained and user information will not be disclosed)

for the purpose of safeguarding network operations and protecting services.

Huawei alone is unable to collect or save the content of users' communications.

You must comply with the laws and regulations of the countries concerned for using the functions.

You are obligated to take considerable measures to ensure that the content of users' communications is fully protected when the content is being used and saved.

9.3.1 No Power Feed After Offhook

This section describes how to troubleshoot the fault where there is no power feed when a phone goes offhook. When this fault occurs, the phone does not respond after going offhook, and the "phone in use" indicator is off, which means that the phone has no power feed.

Location Method

When an FTTO subscriber hears no power feed after offhook, possible causes are as follows:

- The phone is faulty.
- The line between the phone and the POTS port (POTS refers to plain old telephone service) is faulty.
- The line between the phone and the POTS port is not properly connected.
- The ONU POTS port is faulty.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Perform the voice loop line test on the ONU. If a fault occurs, rectify it according to the test conclusion. If the subscriber hears no tone after offhook after the rectification, go to [Step 2](#).

Test Result	Possible Cause	Troubleshooting Method
<ul style="list-style-type: none">• Normal• Phone disconnected	-	No process is needed because the loop line and phone are normal.
<ul style="list-style-type: none">• AC current abnormal• DC current abnormal• Loop current abnormal• Loop resistance abnormal• Insulating resistance abnormal• Capacitance abnormal• Impedance abnormal• Insulating not good• Broken lines• Line mixing• Connected to ground• AB Line reversal• Line leaking	The line between the phone and the POTS port is faulty.	Replace the line between the phone and the POTS port.

Test Result	Possible Cause	Troubleshooting Method
Broken lines	<ul style="list-style-type: none">The phone is faulty.The line between the phone and the POTS port is faulty.The line between the phone and the POTS port is not properly connected.	<ul style="list-style-type: none">Replace the phone.Replace the line between the phone and the POTS port.Re-connect the line between the phone and the POTS port properly.

Step 2 Connect the phone that encounters the fault to another POTS port. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, the original ONU POTS port is faulty. In this case, replace the ONU by referring to [Replacing an ONU](#). Then, go to **Step 4**.
- Then, go to **Step 3**.

Step 3 Connect Technical Support.

Step 4 The fault is rectified.

----End

9.3.2 No Tone After Offhook

No tone after offhook indicates that a subscriber hears no tone or only a weak current noise after offhook. When such a fault occurs in an FTTO network, locate the fault according to the following procedure.

Cause Analysis

When an FTTO subscriber hears no tone after offhook, possible causes are as follows:

- The domain name conflict occurs on ONUs connected to the same softswitch.
- The phone is faulty.
- The line between the phone and the POTS (POTS refers to plain old telephone service) port is faulty.
- The line between the phone and the POTS port is not properly connected.
- The POTS port is faulty.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Perform the voice loop line test on the ONU. If a fault occurs, rectify it according to the test conclusion. If the subscriber hears no tone after offhook after the rectification, go to [Step 2](#).

Test Result	Possible Cause	Troubleshooting Method
<ul style="list-style-type: none">● Normal● Phone disconnected	-	No process is needed because the loop line and phone are normal.
<ul style="list-style-type: none">● AC current abnormal● DC current abnormal● Loop current abnormal● Loop resistance abnormal● Insulating resistance abnormal● Capacitance abnormal● Impedance abnormal● Insulating not good● Broken lines● Line mixing● Connected to ground● AB Line reversal● Line leaking	The line between the phone and the POTS port is faulty.	Replace the line between the phone and the POTS port.
Broken lines	<ul style="list-style-type: none">● The phone is faulty.● The line between the phone and the POTS port is faulty.● The line between the phone and the POTS port is not properly connected.	<ul style="list-style-type: none">● Replace the phone.● Replace the line between the phone and the POTS port.● Re-connect the line between the phone and the POTS port properly.

Step 2 Check whether domain name conflict occurs on ONUs connected to the same softswitch.

- If domain name conflict occurs, go to [Step 3](#).
- If no domain name conflict, go to [Step 4](#).

Step 3 Change the name to ensure that there is no identical domain name. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to [Step 7](#).

- If the fault persists, go to **Step 4**.

Step 4 Connect the phone that encounters the fault to another POTS port. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 7**.
- If the fault persists, go to **Step 5**.

Step 5 The original ONU POTS port is faulty. In this case, replace the ONU by referring to [Replacing an ONU](#). Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 7**.
- If the fault persists, go to **Step 6**.

Step 6 Connect Technical Support.

Step 7 The fault is rectified.

----End

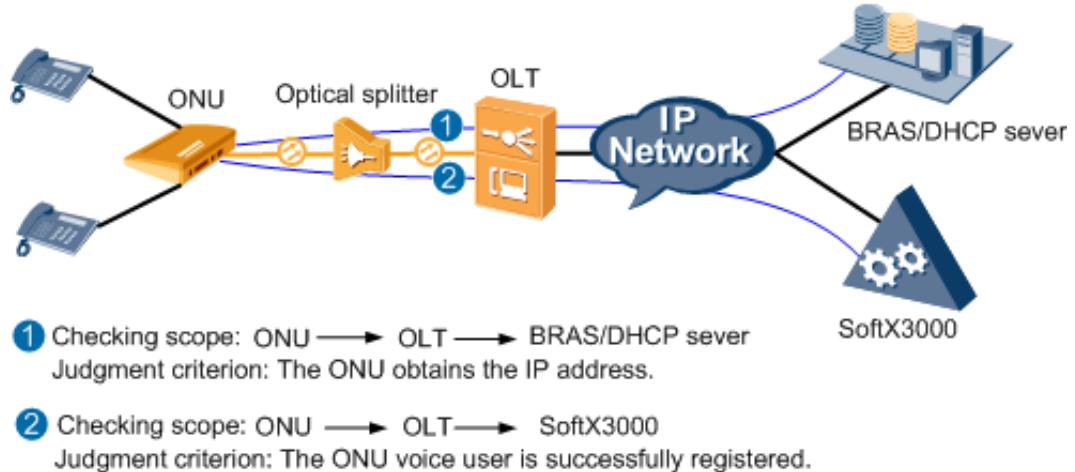
9.3.3 Busy Tone After Off-hook

After a user picks up the phone, no dial tone can be heard but only the busy tone can be heard. When a user hears the busy tone after off-hook in an FTTO network, locate and troubleshoot the fault by using the following location methods and troubleshooting procedure.

Location Method

The root cause of this fault is that the voice user is not registered with the MGC/IMS. It is recommended that you locate the fault by referring to [Figure 9-9](#).

Figure 9-9 Location method



1. Network topology: ONU -> OLT -> BRAS or DHCP server. Check whether WAN connections for the voice service on the ONU are normal and whether they obtain IP addresses. If a WAN connection is abnormal and fails to obtain the IP address, the PPPoE dialup fails or the DHCP server fails to obtain the IP

address. Rectify the fault that the DHCP server fails to obtain the IP address, see [9.1.4 PPPoE Dialup Failure](#) or [9.1.5 Failure to Obtain an IP Address in the DHCP Mode](#).

2. Network topology: ONU -> OLT -> MGC or IMS (SoftX3000 is used as an example). Check whether the voice user of the ONU is registered with the MGC or IMS. If the voice user is not registered with the MGC or IMS, the link from the ONU to the MGC or IMS is faulty or voice parameters of the MGC or IMS are incorrect. Rectify the corresponding fault.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Check whether WAN connections for the voice service on the ONU are normal and whether they obtain IP addresses. If a WAN connection is abnormal and fails to obtain the IP address, the PPPoE dialup fails or the DHCP server fails to obtain the IP address. Rectify the fault that the DHCP server fails to obtain the IP address, see [9.1.4 PPPoE Dialup Failure](#) or [9.1.5 Failure to Obtain an IP Address in the DHCP Mode](#).

Check and locate the fault through CLI, NMS, or web page, as described in the following table.

Checking Mode	Procedure	Judgment Criterion
CLI	Run the display ont wan-info command to check whether the WAN connection for the voice service is normal and whether the WAN connection obtains the IP address.	<ul style="list-style-type: none">• If IPv4 addresses are used and IPv4 Connection status is Connected, the WAN connection for the voice service is normal. If IPv4 address displays the IP address, the WAN connection for the voice service obtains the IP address.• If IPv6 addresses are used and IPv6 Connection status is Connected, the WAN connection for the voice service is normal. If IPv6 address displays the IP address, the WAN connection for the voice service obtains the IP address.• If IPv4 and IPv6 dual addresses are used and both IPv4 Connection status and

Checking Mode	Procedure	Judgment Criterion
NMS	Select the ONU to be queried from GPON ONU . On the WAN Interface tab page in the lower pane, check whether the WAN connection for the voice service is normal and whether the WAN connection obtains the IP address.	IPv6 Connection status are Connected, the WAN connection for the voice service is normal. If IPv4 address and IPv6 address display the IP addresses, the WAN connections for the voice service obtain the IP addresses.
Web page	Choose Status > WAN Information from the navigation tree. In the right pane, check whether the WAN connection for the voice service is normal and whether the WAN connection obtains the IP address.	If Status is Connected , the WAN connection is normal. If IP Address displays the IP address, the WAN connection obtains the IP address.

Step 2 Check whether the voice user of the ONU is registered with the MGC or IMS. If the voice user is not registered with the MGC or IMS, the link from the ONU to the MGC or IMS is faulty or voice parameters of the MGC or IMS are incorrect. Rectify the fault by perform [Step 3](#) or [Step 4](#).

Check and locate the fault through CLI, NMS, or web page, as described in the following table.

Checking Mode	Procedure	Judgment Criterion
CLI	Run the display ont port state command to check whether the voice service is normal.	If Service state is InService , the service is normal.
NMS	Select the ONU to be queried from GPON ONU . On the POTS User tab page in the lower pane, check whether the voice service is normal.	If Service Status is In Service , the voice service is normal.
Web page	Choose Status > VoIP Information from the navigation tree. In the right pane, check whether the voice service is normal.	If User Status is Up , the voice service is normal.

Step 3 Rectify the fault on the link from the ONU to the MGC or IMS.

Check the quality of the link from the OLT to the MGC or IMS by referring to [5.7.6 Pinging from an ONT Remotely](#). If packets are lost or delay is very large, capture

packets in an exclusive way to locate the device that drops packets or incorrectly forwards packets. Then, rectify the fault.

Step 4 Rectify the incorrect voice parameters of the MGC or IMS, as described in the following table.

There are various of voice parameters and methods of configuring these voice parameters. See the FTTx Solution Configuration to rectify such faults.

Possible Cause	Judgment Criterion	Troubleshooting Method
The type of the WAN connection for the voice service is incorrect.	Confirm that the WAN connection type of the voice service is not set to VoIP or VoIP combination.	Modify the WAN connection type of the voice service to VoIP or VoIP combination.
Voice users of the ONU are disabled.	Check whether voice users of the ONU are enabled.	Enable voice users of the ONU.

Possible Cause	Judgment Criterion	Troubleshooting Method
Voice parameters on the ONU or MGC or IMS are not configured or incorrectly configured.	<p>Voice parameters on the ONU or MGC or IMS are not configured or incorrectly configured if one of the following situations occurs:</p> <ul style="list-style-type: none"> • Confirm that voice parameters on the ONU or MGC or IMS are not configured. • Data configurations are different from the data plan. (Data configurations on the ONU must be the same as those on the MGC or IMS) <p>Key parameters of the H.248 voice service:</p> <ul style="list-style-type: none"> • MGC address and port ID • MID format, MG domain name, and device name • Prefix and digital length of the RTP TID • Terminal name (terminal ID) • Associated physical port (associated POTS port) <p>Key parameters of the SIP voice service:</p> <ul style="list-style-type: none"> • IP address and port ID of the SIP server • Home domain name • Registered user name (phone number of a voice user, which is unique on the ONU under the same softswitch) • Authentication user name and password • Associated physical port (associated POTS port) 	Configure the data correctly based on the data plan.

Possible Cause	Judgment Criterion	Troubleshooting Method
	<p>NOTE</p> <p>You can trace H.248 signaling on the MGC and check for error 502 to determine whether the RTP TID format of the MG is the same as that of the MGC.</p> <p>In the protocol, error 502 indicates that the terminal is invalid, including the RTP terminal and physical terminal. If error 502 is traced in the H.248 signaling on the MGC, the RTP TID format of the MG is different from that of the MGC. For example, RTPs on the MGC are RTP1000, RTP1001, and RTP1002,..., but RTPs on the MG are RTP500, RTP501, and RTP501...</p>	

Step 5 Make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 7**.
- If the fault persists, go to **Step 6**.

Step 6 Connect Technical Support.

Step 7 The fault is rectified.

----End

9.3.4 One-Way Audio in a Voice Call

One-way audio indicates that a subscriber can dial a phone number and hear the ring tone, but only the tone of one party can be heard in a voice call. When such a fault occurs in an FTTO network, locate the fault according to the following procedure.

Cause Analysis

When one-way audio occurs in an FTTO network, possible causes are as follows:

ACL (ACL refers to access control list) rules on the bearer network, OLT or ONU are not configured correctly.



- A subscriber can dial the phone number and hear the ring tone. Hence the signaling streams are normal.
- If a fault occurs on the bearer network, locate the fault by making phone calls between subscribers of the same OLT. In this case, media streams are forwarded inside the device instead of the bearer network. If the subscribers can call each other normally, the link between the device and the bearer network is faulty.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Check whether subscribers of the same OLT can call each other normally.
- If the subscribers can call each other normally, the link between the device and the bearer network is faulty. In this case, proceed to **Step 2**.
 - If the subscribers fail to call each other normally, go to **Step 4**.
- Step 2** Run the **ip address** command to configure the SVLAN interface of the voice service and then run the **arp proxy** command to enable ARP proxy globally and ARP proxy of the SVLAN interface of the voice service. Check whether the subscribers can call each other normally.
- If the subscribers can call each other normally, the link between the device and the bearer network is faulty. In this case, go to **Step 3**.
 - If the subscribers fail to call each other normally, go to **Step 4**.
- Step 3** Check whether ACL rules are correctly configured on the router of the IP bearer network.
- If ACL rules are correctly configured, go to **Step 8**.
 - If ACL rules are not correctly configured, modify or cancel ACL rules of the IP bearer network. Then, go to **Step 7**.
- Step 4** Check whether subscribers of the same ONU can call each other normally.
- If the subscribers can call each other normally, configurations on the OLT are incorrect. In this case, proceed to **Step 5**.
 - If the subscribers fail to call each other normally, configurations on the ONU are incorrect. In this case, go to **Step 6**.
- Step 5** On the OLT, run the **display acl all** command to check whether ACL rules are used to filter upstream or downstream voice media streams.
- If ACL rules are used, run the **undo acl** command on the OLT to cancel the ACL rules, and go to **Step 7**.
 - If ACL rules are not used, proceed to **Step 6**.
-  **NOTE**
- The ACL that has been delivered to a port cannot be deleted. To delete such an ACL, cancel the ACL delivery before deleting by running the **undo packet-filter** command on the OLT.
- Step 6** On the ONU, check whether IP filtering and MAC address filtering functions are configured to filter upstream or downstream voice media streams.
- If IP filtering and MAC address filtering functions are configured, disable them and proceed to **Step 7**.
 - If IP filtering and MAC address filtering functions are not configured, go to **Step 8**.
- Step 7** Make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 9**.
- If the fault persists, proceed to **Step 8**.

Step 8 Connect Technical Support.

Step 9 The fault is rectified.

----End

9.3.5 Noise in a Voice Call

Noise in a voice call indicates that a subscriber hears a strong current noise and broadcast noise in a voice call, excluding the environment noise of both parties. When such a fault occurs in an FTTO network, locate the fault according to the following procedure.

Cause Analysis

When noise in a voice call occurs in an FTTO network, locate the fault according to the fault scope, as described in the following table.

Fault Scope	Possible Cause
Subscribers of the same OLT	<ul style="list-style-type: none">• Packet loss occurs in the bearer network.• Electromagnetic interference exists in the environment of the OLT.
Subscribers of two POTS ports on an ONU	<ul style="list-style-type: none">• Electromagnetic interference exists in the environment of the ONU and the line between the ONU and the phones.• The ONU or power adapter is faulty.
Subscriber of a POTS port on an ONU	<ul style="list-style-type: none">• The POTS port is faulty.• The line between the phone and the POTS port is faulty.• The line between the phone and the POTS port is not properly connected.• The phone is faulty.• The subscriber line is not correctly connected. For example, an extra xDSL (DSL refers to digital subscriber line) distribution box is connected.
Subscribers calling certain numbers	The phone number configured on the ONU is different from that configured on the softswitch.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check the fault scope.

- If all subscribers of the same OLT hear the noise, proceed to **Step 2**.
- If the subscribers of two POTS ports on an ONU hear the noise, go to **Step 3**.
- If the subscriber of a POTS port on an ONU hears the noise, go to **Step 5**.
- If the subscribers calling certain numbers hear the noise, go to **Step 7**.

Step 2 Rectify packet loss failure in the bearer network and eliminate electromagnetic interference (such as interference brought by the broadcast tower and high voltage wire) in the environment of the OLT. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 9**.
- If the fault persists, go to **Step 8**.

Step 3 Eliminate electromagnetic interference (such as interference brought by a radio or stereo) in the environment of the ONU and the line between the ONU and the phones. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 9**.
- If the fault persists, proceed to **Step 4**.

Step 4 Replace the ONU or power adapter. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 9**.
- If the fault persists, go to **Step 8**.

Step 5 Run the **ont pots-test** command to perform a loop line test for the ONU, and rectify the fault according to the test result. If the noise persists in a voice call after the rectification, proceed to **Step 6**.

Test Result	Possible Cause	Troubleshooting Method
<ul style="list-style-type: none">• Normal• Phone disconnected	-	No process is needed because the loop line and phone are normal.

Test Result	Possible Cause	Troubleshooting Method
<ul style="list-style-type: none"> ● AC current abnormal ● DC current abnormal ● Loop current abnormal ● Loop resistance abnormal ● Insulating resistance abnormal ● Capacitance abnormal ● Impedance abnormal ● Insulating not good ● Broken lines ● Line mixing ● Connected to ground ● AB Line reversal ● Line leaking 	The line between the phone and the POTS port is faulty.	Replace the line between the phone and the POTS port.
Broken lines	<ul style="list-style-type: none"> ● The phone is faulty. ● The line between the phone and the POTS port is faulty. ● The line between the phone and the POTS port is not properly connected. 	<ul style="list-style-type: none"> ● Replace the phone. ● Replace the line between the phone and the POTS port. ● Re-connect the line between the phone and the POTS port properly.

Step 6 Re-connect the subscriber line properly. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to [Step 9](#).
- If the fault persists, go to [Step 8](#).

Step 7 Check the phone numbers configured on the softswitch and ONU, and modify the phone number configured on the phone that encounters the fault to be the same as the phone number configured on a normal phone. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to [Step 9](#).
- If the fault persists, proceed to [Step 8](#).

Step 8 Connect Technical Support.

Step 9 The fault is rectified.

----End

9.3.6 Voice Interruptions in a Voice Call

Voice interruptions in a voice call indicate that the voice heard by a subscriber in a voice call is interrupted at times. When such a fault occurs in an FTTO network, locate the fault according to the following procedure.

Cause Analysis

When voice interruptions in a voice call occur in an FTTO network, possible causes are as follows:

- The 802.1p priority of the voice service is too low on the ONU.
- The POTS port is faulty.
- The line between the POTS port and the phone is faulty.
- The line between the phone and the POTS port is not properly connected.
- The phone is faulty.
- The network connection is abnormal.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Run the **ont pots-test** command to perform a loop line test for the ONU, and rectify the fault according to the test result. If voice interruptions persist after the rectification, proceed to **Step 2**.

Test Result	Possible Cause	Troubleshooting Method
<ul style="list-style-type: none">• Normal• Phone disconnected	-	No process is needed because the loop line and phone are normal.

Test Result	Possible Cause	Troubleshooting Method
<ul style="list-style-type: none"> ● AC current abnormal ● DC current abnormal ● Loop current abnormal ● Loop resistance abnormal ● Insulating resistance abnormal ● Capacitance abnormal ● Impedance abnormal ● Insulating not good ● Broken lines ● Line mixing ● Connected to ground ● AB Line reversal ● Line leaking 	The line between the phone and the POTS port is faulty.	Replace the line between the phone and the POTS port.
Broken lines	<ul style="list-style-type: none"> ● The phone is faulty. ● The line between the phone and the POTS port is faulty. ● The line between the phone and the POTS port is not properly connected. 	<ul style="list-style-type: none"> ● Replace the phone. ● Replace the line between the phone and the POTS port. ● Re-connect the line between the phone and the POTS port properly.

Step 2 Rectify the network fault (for example, improper optical fiber connection). Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to [Step 8](#).
- If the fault persists, proceed to [Step 3](#).

Step 3 Connect the phone that encounters the fault to another POTS port. Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, the POTS port on the original ONU is faulty. In this case, [replace the ONU](#) and go to [Step 8](#).
- If the fault persists, proceed to [Step 4](#).

Step 4 Check whether the 802.1p priority of the voice service is too low on the ONU.

 **NOTE**

- When packet loss occurs in case of network congestion, packets with a lower QoS (QoS refers to quality of service) priority are discarded first. Priorities of QoS packets are from 0 to 7 in an ascending order.
- The voice service requires a high network quality. Hence, it is recommended that you set the priority of the voice service on the ONU to 7.

- If the 802.1p priority of the voice service is too low on the ONU, set it to a high priority, and proceed to **Step 5**.
- If the 802.1p priority of the voice service is high on the ONU, go to **Step 6**.

Step 5 Make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 8**.
- If the fault persists, proceed to **Step 6**.

Step 6 **Replace the ONU.** Then, make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 8**.
- If the fault persists, proceed to **Step 7**.

Step 7 Connect Technical Support.

Step 8 The fault is rectified.

----End

9.3.7 Failure to Dial Certain Phone Numbers

Failure to dial certain phone numbers indicates that when dialing certain phone numbers, the subscriber hears "the number you dialed does not exist". When such a fault occurs in an FTTO network, locate the fault according to the following procedure.

Cause Analysis

When a subscriber fails to dial certain phone numbers, possible causes are as follows:

1. Packet loss occurs in the network between the OLT and the MGC/IMS.
2. Digitmaps associated with the phone numbers are not configured on the MGC or ONU.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check whether packet loss occurs in the network between the OLT and the MGC/IMS.



In the VLANIF/MEth mode on the OLT, run the **ip address** command to configure a Layer 3 interface, and run the **ping** command to ping the IP address of the MGC/IMS repeatedly to check whether packet loss occurs in the network between the OLT and the MGC/IMS.

- If packet loss occurs in the network, rectify the fault (for example, improper optical fiber connection) in the link between the OLT and the MGC/IMS, and proceed to **Step 2**.
- If no packet loss occurs in the network, go to **Step 3**.

Step 2 Make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 6**.
- If the fault persists, proceed to **Step 3**.

Step 3 Check whether digitmaps associated with the phone numbers are configured on the MGC or ONU.

- If the digitmaps are configured, go to **Step 5**.
- If the digitmaps are not configured, configure them, and proceed to **Step 4**.

Step 4 Make a call again to check whether the fault is rectified.

- If the fault is rectified, go to **Step 6**.
- If the fault persists, proceed to **Step 5**.

Step 5 Connect Technical Support.

Step 6 The fault is rectified.

----End

10 Troubleshooting the FTTB and FTTC Service

This chapter describes how to troubleshoot common faults in Internet access and multicast (IPTV) services in FTTB and FTTC scenarios.

10.1 Internet Access Service Failure

This topic describes how to troubleshoot Internet access service failures in fiber to the building (FTTB) or fiber to the curb (FTTC) networks. Common Internet access service failures include: users fail to access the Internet, Internet access is interrupted frequently, PPPoE dialup fails to obtain an IP address, and DHCP dialup fails to obtain an IP address.

10.2 IPTV Service Failure

This topic describes how to troubleshoot an IPTV service fault in a FTTB or FTTC network.

10.3 Troubleshooting the Voice Service

This topic describes how to troubleshoot common faults in the voice service, including the following faults: no tone after offhook, busy tone after offhook, one-way audio in communication, noise in communication, poor voice service in communication, and failure to dial certain phone numbers.

10.1 Internet Access Service Failure

This topic describes how to troubleshoot Internet access service failures in fiber to the building (FTTB) or fiber to the curb (FTTC) networks. Common Internet access service failures include: users fail to access the Internet, Internet access is interrupted frequently, PPPoE dialup fails to obtain an IP address, and DHCP dialup fails to obtain an IP address.

Prerequisites

The ONU and OLT communicate with each other normally. If the communication between them fails, all services provided by the ONU may be interrupted. See [6 GPON ONU Abnormal State](#) to rectify faults occur in PON upstream transmission between the ONU and OLT.

10.1.1 Internet Access Service Fails

This topic describes how to troubleshoot Internet access service failures in fiber to the building (FTTB) or fiber to the curb (FTTC) networks.

10.1.1.1 Symptoms

Description

The Internet access service failure is a fault in which users provided with the Internet access service cannot obtain network resources. For example, they cannot open a web page.

10.1.1.2 Fault Identification and Demarcation

Fault Locating Guide

If a user fails to access the Internet in FTTB or FTTC networks: If the user uses a static IP address, check whether the IP address of the PC is correct; if the user uses a dynamic IP address, check whether the user's PC can normally obtain an IP address.



To query the IP address of the PC for a Windows user, do as follows:

1. Choose **Start > Run** on the task bar of the PC. Enter the **cmd** command in the **Run** dialog box, and then press **Enter**.
2. In the displayed CLI, enter the **ipconfig** command to query the IP address of the PC.

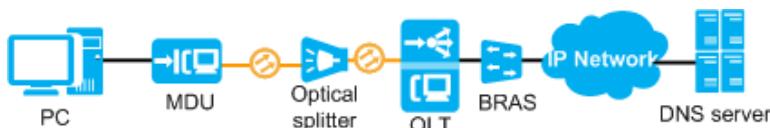
- **User's PC Fails to Obtain an IP Address**

When a user's PC fails to obtain an IP address:

- For a PPPoE user, see [10.1.4 IP Address Fails to Be Obtained Through PPPoE Dialup](#).
- For a DHCP user, see [10.1.5 IP Address Fails to Be Obtained Through DHCP Dialup](#).

- **User's PC Successfully Obtains an IP Address**

Demarcate the fault based on the fault symptom.



Checking Scope	Determination Basis	Possible Cause
User's PC	Use a test PC, instead of the user's PC, for testing. The user can normally access the Internet through this PC.	<ul style="list-style-type: none">• The user's PC is infected with viruses.• The IE browser of the PC is faulty.• The PC responds slowly after having run for a long time.

Checking Scope	Determination Basis	Possible Cause
DNS server	Websites can be visited through entering the website IP addresses.	<ul style="list-style-type: none">The DNS server is faulty and fails to resolve domain names.The communications between the user's PC and DNS server are abnormal.

NOTE

Faults can be located according to specific scenarios because the deployment scenario and the routine O&M scenario involve different fault scopes.

- If the fault occurs during a new deployment, check the hardware and initial software configurations.
- If the fault occurs during O&M, check only the hardware, because the software configurations of a user are generally not modified in this scenario. Therefore, if the user state changes from normal to abnormal, it may be caused by a hardware fault. If the fault occurs after a new user is added or an existing user is modified, check the software configurations of the user.

10.1.1.3 User's PC Is Faulty

Determining the Fault

Use a test PC, instead of the user's PC, for testing. The user can normally access the Internet through this PC.

Troubleshooting

Check whether the user's PC is affected by viruses, whether the IE browser fails, or whether the PC responds slowly after having run for a long time.

10.1.1.4 DNS Server Is Faulty

Determining the Fault

Enter the IP address (such as `http://192.168.0.2`) of a known website to the IE address bar and you can visit this web page. This indicates that the link between the PC to DNS server or the DNS server fails, causing a domain name parse failure.

Troubleshooting

Check whether the PC can ping the IP address of the DNS server.

NOTE

To query the IP address of the DNS server connected to the PC, do as follows:

- Choose **Start > Run**. Enter **cmd** in the **Run** dialog box, and then press **Enter**.
- In the DoS window of the PC, enter the **ipconfig/all** command to query the IP address (**DNS Servers**) of the DNS server obtained by the PC.

- If the ping operation fails, the link between the PC and DNS server fails. Check the link.
- If the ping operation succeeds, the DNS server fails. Contact the maintenance personnel to check the DNS server.

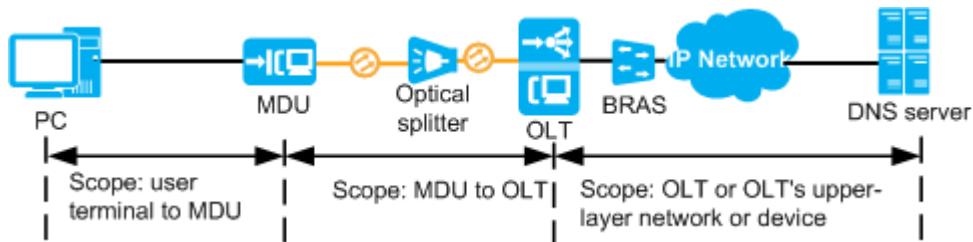
10.1.2 Internet Access Is Interrupted Frequently

This topic describes how to troubleshoot the fault that Internet access is interrupted frequently in fiber to the building (FTTB) or fiber to the curb (FTTC) networks.

10.1.2.1 Fault Identification and Demarcation

Handling Guide

If this fault occurs in FTTB or FTTC networks, determine the fault scope according to fault symptoms.



Checking Scope	Determination Basis	Possible Cause
User terminal to the MDU	A user encounters this fault.	<ul style="list-style-type: none">• The user's PC is infected with viruses, or its network interface card (NIC) is faulty.• The user terminal is faulty.• The line from the user terminal to the MDU has serious packet loss.
MDU to the OLT	Users under a port on the MDU encounter this fault.	The MDU port is faulty.
	All users under the MDU encounter this fault.	<ul style="list-style-type: none">• The MDU is affected by strong interference sources.• The MDU has MAC address duplication.
OLT or upper-layer BRAS	All users under the BRAS encounter this fault.	The BRAS has MAC address duplication.

 NOTE

Faults can be located based on the actual scenarios, because the new deployment scenario and the routine O&M scenario involve different fault scopes.

- If the fault occurs during a new deployment, check the hardware and initial software configurations.
- If the fault occurs during O&M, it is usually necessary to check only the hardware, because the software configurations of a user are generally not modified in the O&M scenario. Therefore, if the user status changes from normal to abnormal in O&M scenarios, it may be caused by a hardware fault. If the fault occurs after a new user is added or an existing user is modified, check whether the software configurations of the user are correct.

10.1.2.2 User's PC Is Faulty

Determining the Fault

Use a test PC, instead of the user's PC, for testing. The user can normally access the Internet through this PC.

Troubleshooting

Check whether the network interface card (NIC) of the PC is faulty, whether the PC is infected with viruses, whether the PC responds slowly after having run for a long time, or whether the PC has low configurations.

10.1.2.3 User's Modem Is Faulty

Determining the Fault

In DSL access, the modem is activated and deactivated frequently and the activation indicator of the modem is abnormal. Use a test modem, instead of the user's modem, for testing. The user can normally access the Internet through this modem.

Troubleshooting

1. Reset the modem.
2. Replace the modem if the fault persists after a reset.

10.1.2.4 Line from the User Terminal to the MDU Has Serious Packet Loss

Determining the Fault

Check whether CRC packet loss occurs in the line between the service port and the user terminal.

 NOTE

Query the statistics of the faulty port for multiple times at an interval of 20s and check whether the statistics increase. Based on this, determine whether packet loss occurs in the line between the service port and the user terminal (recommended times: 10; recommended interval: 20s).

- DSL access scenario

Run the **display xdsl statistics performance frameid/slotid/portid line-showtime co ever-before** command in the xDSL mode on the MDU to query all the performance statistics after the line is initialized. Then, check whether the **Count of errored seconds** and **Count of severely errored seconds** increase. If any of the counts increases, packet loss occurs.

```
huawei(config)#display xdsl statistics performance
{ frameid/slotid/portid<S><Length 5-15> }:0/1/0
{ line-initial<K>|line-showtime<K>|channel<K> }:line-showtime
{ co<K>|cpe<K> }:co
{ current-15minutes<K>|current-24hours<K>|historic-15minutes<K>|historic-24hours
<K>|ever-before<K> }:ever-before
```

Command:

```
display xdsl statistics performance 0/1/0 line-showtime co ever-before
```

```
-----  
Count of forward error correction seconds : 0  
Count of errored seconds : 0  
Count of severely errored seconds : 0  
Count of loss of signal seconds : 0  
Count of unavailable seconds : 0  
Count of lefr defects seconds : 7  
Count of the number of error-free bits passed(64kBit) : 8  
Minimum error-free throughput : 9  
Count of loss of frame seconds : 0  
Count of loss of link seconds : 0  
Count of loss of power seconds : 0
```

- LAN access scenario

Run the **display port statistics portid** command in the ETH mode on the MDU to query all the performance statistics after the line is initialized. Then, check whether **Number of CRC error frames** increases. If the count increases, packet loss occurs.

```
huawei(config-if-eth-0/1)#display port statistics 0
```

```
Number of transmitted frames : 0
Number of received frames : 0
Total number of frames : 0
Number of transmitted multicast frames : 0
Number of received multicast frames : 0
Total number of multicast frames : 0
Number of transmitted broadcast frames : 0
Number of received broadcast frames : 0
Total number of broadcast frames : 0
Number of transmitted unicast frames : 0
Number of received unicast frames : 0
Total number of unicast frames : 0
Number of transmitted pause frames : 0
Number of received pause frames : 0
Number of transmitted octets : 0
Number of received octets : 0
Total number of octets : 0
Number of alignment error frames : 0
Number of discarded frames : 0
Number of CRC error frames : 0
Number of collision frames : 0
Number of discarded undersized frames : 0
Number of oversized frames : 0
Number of CRC error frames(less than 64 octets in length) : 0
Number of CRC error frames(longer than 1518 octets in length) : 0
```

Troubleshooting

1. Check the quality of the physical line between the MDU and the user terminal, that is, whether the physical line is excessively long, has any unreliable connection, or has deteriorated. If so, reconnect the physical line or replace the deteriorated physical line.
2. Check whether strong interference sources exist near the user's home, such as a radio base station (RBS) or a high frequency switch mode power supply (SMPS). If so, contact the responsible party to handle it.

10.1.2.5 MDU Port Is Faulty

Determining the Fault

Use another port and configure corresponding data. It is found that services have recovered.

Troubleshooting

Use another port and reconfigure data.

10.1.2.6 MDU Has MAC Address Duplication

Determining the Fault

Run the **display location mac-addr** command for multiple times (more than 3 times as recommended) on the MDU to query the port that learns the user MAC address. The port that learns the user MAC address is different from the port that connects to the user.

```
huawei#display location  
{ mac-addr<P><XXXX-XXXX-XXXX> }:00e0-fc00-1111
```

Command:

display location 00e0-fc00-1111

It will take several minutes, and console may be timeout, please use command idle-timeout to set time limit

Are you sure to query MAC address location ? (y/n)[n]:y

NOTE

- **mac-addr** in the command output indicates the user MAC address. If dialing is initiated from a modem, the MAC address of the user is that of the modem. If dialing is initiated from the user's computer, the MAC address of the user is that of the user's computer.
- **F/S/P** in the command output indicates the port that learns the user's MAC address. Normally, the queried port is the user access port. Otherwise, the user's MAC address is duplicated.

Troubleshooting

Check whether the ports related to MAC address duplication are located on a loopback network or are attacked. If yes, disconnect the loopback network or deactivate the port from which the attacks come. Check whether services are normal.

10.1.2.7 BRAS MAC Address Duplication

Determining the Fault

Run the **display location mac-addr** command for multiple times (more than 3 times as recommended) on the MDU to query the port that learns the user MAC address. The port that learns the user MAC address is different from the port that connects to the user.

```
huawei#display location
{ mac-addr<P><XXXX-XXXX-XXXX> }:00e0-fc00-1111
```

Command:

```
display location 00e0-fc00-1111
```

It will take several minutes, and console may be timeout, please use command idle-timeout to set time limit

```
Are you sure to query MAC address location ? (y/n)[n]:y
```



- **mac-addr** in the command output indicates the BRAS MAC address.
- **F/S/P** in the command output indicates the upstream port that learns the MAC address of the BRAS. Normally, the queried port is the upstream port connected to the BRAS. Otherwise, the BRAS MAC address is duplicated.

Troubleshooting

Check whether the ports related to MAC address duplication are located on a loopback network or are attacked. If yes, disconnect the loopback network or deactivate the port from which the attacks come. Check whether services are normal.

10.1.3 Internet Access Rate Is Low

This topic describes how to troubleshoot low Internet access rate in fiber to the building (FTTB) or fiber to the curb (FTTC) networks.

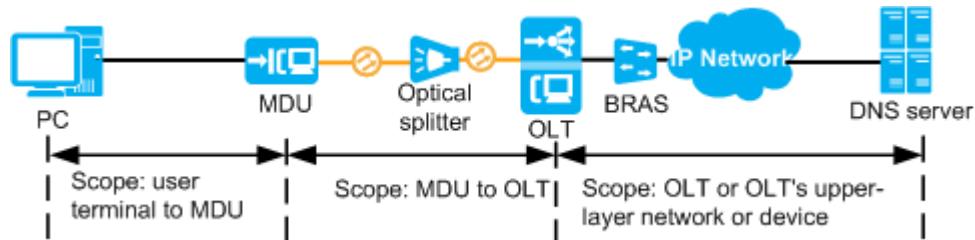
10.1.3.1 Fault Identification and Demarcation

Description

Low Internet access rate is a fault that the Internet access rate of a user is far lower than the provided Internet access rate.

Fault Locating Guide

If this fault occurs in FTTB or FTTC networks, determine the fault scope according to fault symptoms.



Checking Scope	Determination Basis	Possible Cause
User terminal to the MDU	A user connected to the MDU encounters this fault.	<ul style="list-style-type: none">The user's PC is infected with viruses, or its network interface card (NIC) is faulty.The user terminal is faulty.The line from the user terminal to the MDU has serious packet loss.Unknown traffic occupies user bandwidth.
MDU to the OLT	Users under a port encounter this fault.	The user rate limitation configuration is improper.
		The broadband remote access server (BRAS) restricts the user access rate.
	All users connected to the MDU encounter this fault.	The MDU has MAC address duplication.
OLT or BRAS	All users connected to the MDU encounter this fault.	Bandwidth allocated by the OLT to the MDU is insufficient.
	All users connected to the BRAS encounter this fault.	The BRAS has MAC address duplication.

NOTE

Faults can be located according to specific scenarios because the deployment scenario and the routine O&M scenario involve different fault scopes.

- If the fault occurs during a new deployment, check the hardware and initial software configurations.
- If the fault occurs during O&M, check only the hardware, because the software configurations of a user are generally not modified in this scenario. Therefore, if the user state changes from normal to abnormal, it may be caused by a hardware fault. If the fault occurs after a new user is added or an existing user is modified, check the software configurations of the user.

10.1.3.2 NIC of the User's PC Is Faulty

Determining the Fault

Use a test PC, instead of the user's PC, for testing. The Internet access rate is normal.

Troubleshooting

Check whether the network interface card (NIC) of the user's PC is faulty.

10.1.3.3 User's Modem Is Faulty

Determining the Fault

Use a test modem, instead of the user's modem, for testing. The Internet access rate is normal.

Troubleshooting

Replace the user's modem.

10.1.3.4 Line from the User Terminal to the MDU Has Serious Packet Loss

Determining the Fault

Check whether CRC packet loss occurs in the line between the service port and the user terminal.



Query the statistics of the faulty port for multiple times at an interval of 20s and check whether the statistics increase to determine whether packet loss occurs in the line between the service port and the user terminal (recommended times: 10; recommended interval: 20s).

- DSL access scenario

Run the **display xdsl statistics performance frameid/slotid/portid line-showtime co ever-before** command in the xDSL mode on the MDU to query all the performance statistics after the line is initialized. Then, check whether the **Count of errored seconds** and **Count of severely errored seconds** increase. If any of the counts increases, packet loss occurs.

```
huawei(config)#display xdsl statistics performance
{ frameid/slotid/portid<S><Length 5-15> }:0/1/0
{ line-initial<K>|line-showtime<K>|channel<K> }:line-showtime
{ co<K>|cpe<K> }:co
{ current-15minutes<K>|current-24hours<K>|historic-15minutes<K>|historic-24hours
<K>|ever-before<K> }:ever-before
```

Command:

```
display xdsl statistics performance 0/1/0 line-showtime co ever-before
```

```
-----
Count of forward error correction seconds      : 0
Count of errored seconds                      : 0
Count of severely errored seconds              : 0
Count of loss of signal seconds               : 0
Count of unavailable seconds                 : 0
Count of lefr defects seconds                : 7
Count of the number of error-free bits passed(64kBit) : 8
Minimum error-free throughput                 : 9
Count of loss of frame seconds               : 0
Count of loss of link seconds                : 0
Count of loss of power seconds               : 0
```

- LAN access scenario

Run the **display port statistics portid** command in the ETH mode on the MDU to query all the performance statistics after the line is initialized. Then, check whether **Number of CRC error frames** increases. If the count increases, packet loss occurs.

```
huawei(config-if-eth-0/1)#display port statistics 0
```

Number of transmitted frames	: 0
Number of received frames	: 0
Total number of frames	: 0
Number of transmitted multicast frames	: 0
Number of received multicast frames	: 0
Total number of multicast frames	: 0
Number of transmitted broadcast frames	: 0
Number of received broadcast frames	: 0
Total number of broadcast frames	: 0
Number of transmitted unicast frames	: 0
Number of received unicast frames	: 0
Total number of unicast frames	: 0
Number of transmitted pause frames	: 0
Number of received pause frames	: 0
Number of transmitted octets	: 0
Number of received octets	: 0
Total number of octets	: 0
Number of alignment error frames	: 0
Number of discarded frames	: 0
Number of CRC error frames	: 0
Number of collision frames	: 0
Number of discarded undersized frames	: 0
Number of oversized frames	: 0
Number of CRC error frames(less than 64 octets in length)	: 0
Number of CRC error frames(longer than 1518 octets in length)	: 0

Troubleshooting

1. Check the quality of the physical line between the MDU and the user terminal, that is, whether the physical line has unreliable connection or has deteriorated. If so, reconnect the physical line or replace the deteriorated physical line. Check whether the user terminal is normal.
2. Use a test modem, instead of the user's modem, for testing. Then, check whether the Internet access rate becomes normal. If the Internet access rate becomes normal, the user's modem is faulty and needs to be replaced.

10.1.3.5 Unknown Traffic Occupies User Bandwidth

Determining the Fault

- DSL access scenario

Run the **display line operation** command in the xDSL mode on the MDU to query the actual line rate downstream and determine whether the actual downstream line rate (**actual line rate downstream (kbit/s)**) differs greatly from the user's subscription rate.

Ask the user to stop Internet access and run the **display statistics service-port index** command on the MDU to query the traffic information about the faulty service port for multiple times (recommended times: 5; recommended interval: 20s). If the upstream or downstream traffic increases rapidly, unknown traffic occupies the user bandwidth.

```
huawei#display statistics service-port  
{ index<U><0,1999> }:2
```

Command:
display statistics service-port 2
Number of upstream bytes : 0
Number of upstream packets : 0
Number of upstream discard packets : 0
Number of downstream bytes : 0

```
Number of downstream packets      : 0
Number of downstream discard packets : 0
```

NOTE

In normal situations, the traffic has no drastic changes after multiple queries when the user stops Internet access.

- Number of upstream bytes: current upstream traffic of the user
 - Number of downstream bytes: current downstream traffic of the user
 - LAN access scenario
- Ask the user to stop Internet access and run the **display port statistics portid** command on the MDU to query the Ethernet port statistics for multiple times (recommended times: 5; recommended interval: 20s). If the upstream or downstream traffic increases rapidly, unknown traffic occupies the user bandwidth.

```
huawei(config-if-eth-0/1)#display port statistics 0
```

```
Number of transmitted frames      : 0
Number of received frames        : 0
Total number of frames          : 0
Number of transmitted multicast frames : 0
Number of received multicast frames : 0
Total number of multicast frames : 0
Number of transmitted broadcast frames : 0
Number of received broadcast frames : 0
Total number of broadcast frames : 0
Number of transmitted unicast frames : 0
Number of received unicast frames : 0
Total number of unicast frames : 0
Number of transmitted pause frames : 0
Number of received pause frames : 0
Number of transmitted octets      : 0
Number of received octets        : 0
Total number of octets          : 0
Number of alignment error frames : 0
Number of discarded frames       : 0
Number of CRC error frames       : 0
Number of collision frames       : 0
Number of discarded undersized frames : 0
Number of oversized frames       : 0
Number of CRC error frames(less than 64 octets in length) : 0
Number of CRC error frames(longer than 1518 octets in length) : 0
```

NOTE

In normal situations, the traffic has no drastic changes after multiple queries when the user stops Internet access.

- Number of transmitted octets: current downstream traffic of the user
- Number of received octets: current upstream traffic of the user

Troubleshooting

Check and remove viruses from the user's PC.

10.1.3.6 MDU Has MAC Address Duplication

Determining the Fault

Run the **display location mac-addr** command for multiple times (more than 3 times as recommended) on the MDU to query the port that learns the user MAC

address. The port that learns the user MAC address is different from the port that connects to the user.

```
huawei#display location
{ mac-addr<P><XXXX-XXXX-XXXX> }:00e0-fc00-1111
```

Command:

display location 00e0-fc00-1111

It will take several minutes, and console may be timeout, please use command idle-timeout to set time limit

Are you sure to query MAC address location ? (y/n)[n]:y

NOTE

- **mac-addr** in the command output indicates the user MAC address. If dialing is initiated from a modem, the MAC address of the user is that of the modem. If dialing is initiated from the user's computer, the MAC address of the user is that of the user's computer.
- **F/S/P** in the command output indicates the port that learns the user's MAC address. Normally, the queried port is the user access port. Otherwise, the user's MAC address is duplicated.

Troubleshooting

Check whether the ports related to MAC address duplication are located on a loopback network or are attacked. If yes, disconnect the loopback network or deactivate the port from which the attacks come. Check whether services are normal.

10.1.3.7 BRAS MAC Address Duplication

Determining the Fault

Run the **display location mac-addr** command for multiple times (more than 3 times as recommended) on the MDU to query the port that learns the user MAC address. The port that learns the user MAC address is different from the port that connects to the user.

```
huawei#display location
{ mac-addr<P><XXXX-XXXX-XXXX> }:00e0-fc00-1111
```

Command:

display location 00e0-fc00-1111

It will take several minutes, and console may be timeout, please use command idle-timeout to set time limit

Are you sure to query MAC address location ? (y/n)[n]:y

NOTE

- **mac-addr** in the command output indicates the BRAS MAC address.
- **F/S/P** in the command output indicates the upstream port that learns the MAC address of the BRAS. Normally, the queried port is the upstream port connected to the BRAS. Otherwise, the BRAS MAC address is duplicated.

Troubleshooting

Check whether the ports related to MAC address duplication are located on a loopback network or are attacked. If yes, disconnect the loopback network or deactivate the port from which the attacks are initiated. Check whether services are normal.

10.1.4 IP Address Fails to Be Obtained Through PPPoE Dialup

This topic describes how to troubleshoot the fault that an IP address fails to be obtained through PPPoE dialup in fiber to the building (FTTB) or fiber to the curb (FTTC) networks.

10.1.4.1 Fault Identification and Demarcation

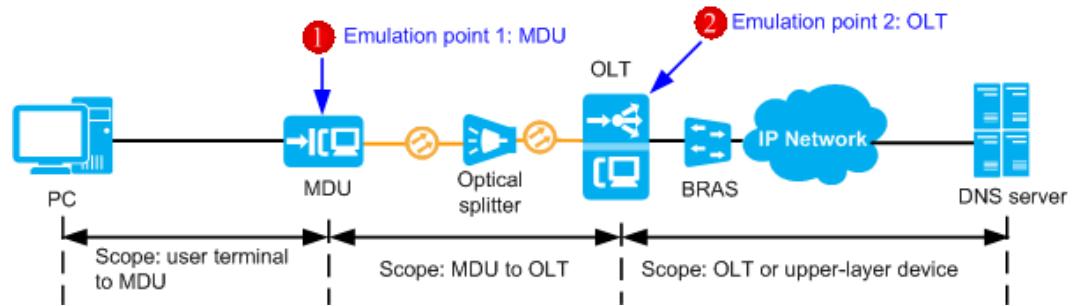
Description

An IP address cannot be obtained through PPPoE dialup.

Fault Locating Guide

When a user fails to obtain an IP address through PPPoE dialup, demarcate the fault scope according to "PPPoE Dialup Emulation", as shown in [Figure 10-1](#).

Figure 10-1 PPPoE dialup emulation



Checking Scope	Determination Basis	Possible Cause
User terminal to the MDU	The result of emulation point 1 is "success".	The network interface card (NIC) of the user's PC is faulty or disabled, or the user PPPoE dialup software is not correctly installed.
		The user terminal is faulty.
		The MDU port is faulty.
MDU to the OLT	The result on emulation point 1 is not "success", but the result on emulation point 2 is "success".	An access control list (ACL) that restricts PPPoE packets is configured.
		The Policy Information Transfer Protocol (PITP) configuration is incorrect.
		The MDU has MAC address duplication.

Checking Scope	Determination Basis	Possible Cause
		The BRAS has MAC address duplication.
OLT or BRAS	The results of emulation points 1 and 2 are not "success".	The user's account is restricted on the BRAS.

NOTE

Faults can be located according to specific scenarios because the deployment scenario and the routine O&M scenario involve different fault scopes.

- If the fault occurs during a new deployment, check the hardware and initial software configurations.
- If the fault occurs during O&M, check only the hardware, because the software configurations of a user are generally not modified in this scenario. Therefore, if the user state changes from normal to abnormal, it may be caused by a hardware fault. If the fault occurs after a new user is added or an existing user is modified, check the software configurations of the user.

10.1.4.2 NIC of the User's PC Is Faulty or Is Disabled

Determining the Fault

Use a test PC, instead of the user's PC, for testing. PPPoE dialup is successful and the IP address can be obtained.

Troubleshooting

Check whether the network interface card (NIC) of the user's PC is faulty or disabled, or whether the user PPPoE dialup software is not correctly installed.

10.1.4.3 User's Modem Is Faulty

Determining the Fault

Use a test modem, instead of the user's modem, for testing. PPPoE dialup is successful and the IP address can be obtained.

Troubleshooting

Replace the user's modem.

10.1.4.4 MDU Port Is Faulty

Determining the Fault

- DSL access scenario

Run the **display port state portid** command in the xDSL mode on the MDU to query the activation status of the port to which the user is connected. The port is in the deactivated state (**Deactivated**). Connect the user to another port and check the port activation status. The port is in the activated state (**Activated**).

- LAN access scenario

The MDU port is faulty when one of the following conditions is met:

- Run the **display port state all** command in the ETH mode on the MDU to query the activation status (**Active State**) of the Ethernet port. The Ethernet port is in the deactivated state (**deactive**).
- Run the **display port state portid** command in the ETH mode on the MDU to query the link status (**Link**) of the Ethernet port. The Ethernet port is in the offline link state (**offline**).
- Run the **display port state portid** command in the ETH mode on the MDU to query the duplex mode, rate, and network cable adaptation mode of the Ethernet port. The duplex mode, rate, or network cable adaptation mode does not match that of the user terminal.

Troubleshooting

- DSL access scenario

- a. Run the **activate portid** command in the xDSL mode to activate the xDSL port, and check whether the activation status of the port to which the user is connected is activated (**Activated**).
- b. Connect the user to another port and configure the related data if the port to which the user is connected is faulty.

- LAN access scenario

- a. Run the **undo shutdown portid** command to activate the port, and check whether the activation status of the Ethernet port is activated (**activated**).
- b. Check the quality of the physical line between the ONU and the user terminal, that is, whether the connector is loose or the physical line has deteriorated. If so, reconnect the connector or replace the physical line. Then, check whether the link status (**Link**) of the Ethernet port is online (**online**).
- c. Change the Ethernet port configurations, ensuring that the configurations are consistent with those of the user terminal.

NOTE

To change the Ethernet port parameter configurations in the ETH mode:

- Run the **auto-neg** command to enable or disable auto-negotiation of the Ethernet port. After auto-negotiation of the Ethernet port is enabled, the Ethernet port automatically negotiates the port rate and duplex mode with the peer port.
 - Run the **duplex** command to configure the duplex mode of the Ethernet port to full-duplex or half-duplex.
 - Run the **mdi** command to configure the network cable adaptation mode of the Ethernet port.
 - Run the **speed** command to configure the Ethernet port rate.
- d. Connect the user to another port and configure the related data if the port to which the user is connected is faulty.

10.1.4.5 PITP Configuration Is Incorrect

Determining the Fault

Perform a PPPoE dialup emulation on the MDU and error code 732 is returned. This indicates that the MDU and upper-layer device have different PPP control protocols.

Troubleshooting

1. Run the **display pitp config** command to confirm that Policy Information Transfer Protocol (PITP) is enabled globally.
2. Run the **display pitp config** command to check the current PITP mode.
3. Confirm whether the current protocol type is the same as that set on the upper-layer device.
 - If the current mode is **pmode**, run the **display pitp permit-forwarding service-port service-portid** command to check whether the service port allows user-side PPPoE packets to carry the vendor tag. If this function is not enabled, run the **pitp permit-forwarding service-port service-portid enable** command to enable it and then check whether PPPoE dialup can be successfully performed.
 - If the current mode is **vmode**, run the **display pitp vmode ether-type** command to check whether the Ethernet protocol type for VBRAS packets on the MDU is consistent with that on upper-layer device. If they are different, run the **pitp vmode ether-type** command to modify the Ethernet protocol type on the MDU so that it is consistent with that on the upper-layer device. Then, check whether the PPPoE dialup can be successfully performed.

10.1.4.6 ACL That Restricts PPPoE Packets Is Configured

Determining the Fault

Perform a PPPoE dialup emulation on the MDU and error code 638 is returned. This indicates that PPPoE emulation has entered the link setup phase of the PPP session, but the creation of a Link Control Protocol (LCP) link is abnormal. The abnormality may be caused by the access control list (ACL) that restricts PPPoE packets is configured on the MDU or OLT.

Troubleshooting

Follow steps below on the MDU and OLT respectively:

1. Run the **display packet-filter port frameid/slotid/portid** command to check whether the user port is configured with the ACL rule.
2. Run the **display acl** command to check whether this ACL rule restricts PPPoE packets.
3. Modify the ACL rule on PPPoE packets or delete the ACL rule from the port. Then, check whether the PPPoE dialup can be successfully performed.

10.1.4.7 MDU Has MAC Address Duplication

Determining the Fault

Run the **display location mac-addr** command for multiple times (more than 3 times as recommended) on the MDU to query the port that learns the user MAC address. The port that learns the user MAC address is different from the port that connects to the user.

```
huawei#display location
{ mac-addr<P><XXXX-XXXX-XXXX> }:00e0-fc00-1111
```

Command:

display location 00e0-fc00-1111

It will take several minutes, and console may be timeout, please use command idle-timeout to set time limit

Are you sure to query MAC address location ? (y/n)[n]:y



NOTE

- **mac-addr** in the command output indicates the user MAC address. If dialing is initiated from a modem, the MAC address of the user is that of the modem. If dialing is initiated from the user's computer, the MAC address of the user is that of the user's computer.
- **F/S/P** in the command output indicates the port that learns the user's MAC address. Normally, the queried port is the user access port. Otherwise, the user's MAC address is duplicated.

Troubleshooting

Check whether the ports related to MAC address duplication are located on a loopback network or are attacked. If yes, disconnect the loopback network or deactivate the port from which the attacks are initiated. Check whether services are normal.

10.1.4.8 BRAS MAC Address Duplication

Determining the Fault

Run the **display location mac-addr** command for multiple times (more than 3 times as recommended) on the MDU to query the port that learns the user MAC address. The port that learns the user MAC address is different from the port that connects to the user.

```
huawei#display location
{ mac-addr<P><XXXX-XXXX-XXXX> }:00e0-fc00-1111
```

Command:

display location 00e0-fc00-1111

It will take several minutes, and console may be timeout, please use command idle-timeout to set time limit

Are you sure to query MAC address location ? (y/n)[n]:y



NOTE

- **mac-addr** in the command output indicates the BRAS MAC address.
- **F/S/P** in the command output indicates the upstream port that learns the MAC address of the BRAS. Normally, the queried port is the upstream port connected to the BRAS. Otherwise, the BRAS MAC address is duplicated.

Troubleshooting

Check whether the ports related to MAC address duplication are located on a loopback network or are attacked. If yes, disconnect the loopback network or deactivate the port from which the attacks are initiated. Check whether services are normal.

10.1.4.9 User's Account Is Restricted on the BRAS

Determining the Fault

Perform a PPPoE dialup emulation on the MDU. Then, error code 668 is returned, indicating that the server forcibly terminates the PPPoE emulation.

Troubleshooting

1. Check whether user data of the upper-layer BRAS is correct or whether the user's account is restricted on the BRAS.
2. If the user data of the upper-layer BRAS is incorrect or whether the user's account is restricted on the BRAS, modify the BRAS configurations and check whether the IP address can be obtained successfully.

10.1.5 IP Address Fails to Be Obtained Through DHCP Dialup

This topic describes how to troubleshoot the fault that an IP address fails to be obtained through DHCP dialup in fiber to the building (FTTB) or fiber to the curb (FTTC) networks.

10.1.5.1 Fault Identification and Demarcation

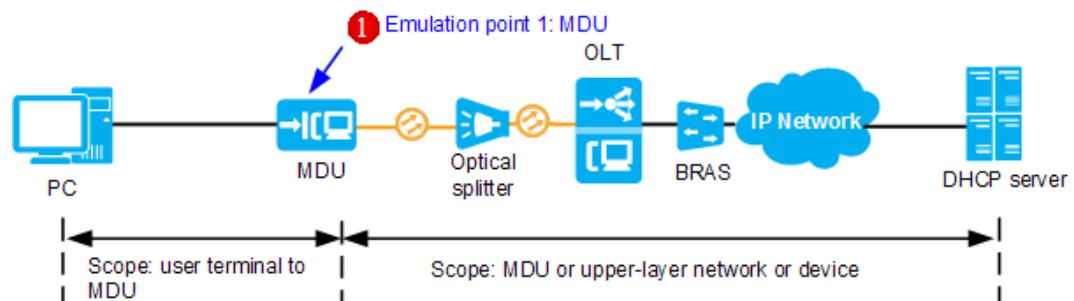
Description

An IP address fails to be obtained through DHCP dialup.

Fault Locating Guide

When a user fails to obtain an IP address through DHCP dialup, demarcate the fault scope according to "DHCP Dialup Emulation", as shown in [Figure 10-2](#).

Figure 10-2 DHCP emulation



Checking Scope	Determination Basis	Possible Cause
User terminal to the MDU	The emulation result on the MDU is "get IP successful".	The network interface card (NIC) of the user's PC is faulty or disabled.
		The user terminal is faulty.
		The MDU port is faulty.
		Static IP address binding is configured.
		The MDU has MAC address duplication.
MDU or upper-layer device	The emulation result on the MDU is not "get IP successful".	The link from the MDU to DHCP server fails.
		The DHCP server is faulty.
		The user's account is restricted on the BRAS.

NOTE

Faults can be located based on the actual scenarios, because the new deployment scenario and the routine O&M scenario involve different fault scopes.

- If the fault occurs during a new deployment, check the hardware and initial software configurations.
- If the fault occurs during O&M, it is usually necessary to check only the hardware, because the software configurations of a user are generally not modified in the O&M scenario. Therefore, if the user status changes from normal to abnormal in O&M scenarios, it may be caused by a hardware fault. If the fault occurs after a new user is added or an existing user is modified, check whether the software configurations of the user are correct.

10.1.5.2 NIC of the User's PC Is Faulty or Is Disabled

Determining the Fault

Use a test PC, instead of the user's PC, for testing. The IP address can be obtained through DHCP dialup.

Troubleshooting

Check whether the network interface card (NIC) of the user's PC is faulty or is disabled.

10.1.5.3 User's Modem Is Faulty

Determining the Fault

Use a test modem, instead of the user's modem, for testing. DHCP dialup is successful and the IP address can be obtained.

Troubleshooting

Replace the user's modem.

10.1.5.4 MDU Port Is Faulty

Determining the Fault

- DSL access scenario

Run the **display port state portid** command in the xDSL mode on the MDU to query the activation status of the port to which the user is connected. The port is in the deactivated state (**Deactivated**). Connect the user to another port and check the port activation status. The port is in the activated state (**Activated**).

- LAN access scenario

The MDU port is faulty when one of the following conditions is met:

- Run the **display port state all** command in the ETH mode on the MDU to query the activation status (**Active State**) of the Ethernet port. The Ethernet port is in the deactivated state (**deactive**).
- Run the **display port state portid** command in the ETH mode on the MDU to query the link status (**Link**) of the Ethernet port. The Ethernet port is in the offline link state (**offline**).
- Run the **display port state portid** command in the ETH mode on the MDU to query the duplex mode, rate, and network cable adaptation mode of the Ethernet port. The duplex mode, rate, or network cable adaptation mode does not match that of the user terminal.

Troubleshooting

- DSL access scenario
 - a. Run the **activate portid** command in the xDSL mode to activate the xDSL port, and check whether the activation status of the port to which the user is connected is activated (**Activated**).
 - b. Connect the user to another port and configure the related data if the port to which the user is connected is faulty.
- LAN access scenario
 - a. Run the **undo shutdown portid** command to activate the port, and check whether the activation status of the Ethernet port is activated (**activated**).
 - b. Check the quality of the physical line between the ONU and the user terminal, that is, whether the connector is loose or the physical line has deteriorated. If so, reconnect the connector or replace the physical line.

Then, check whether the link status (**Link**) of the Ethernet port is online (**online**).

- c. Change the Ethernet port configurations, ensuring that the configurations are consistent with those of the user terminal.

 **NOTE**

To change the Ethernet port parameter configurations in the ETH mode:

- Run the **auto-neg** command to enable or disable auto-negotiation of the Ethernet port. After auto-negotiation of the Ethernet port is enabled, the Ethernet port automatically negotiates the port rate and duplex mode with the peer port.
- Run the **duplex** command to configure the duplex mode of the Ethernet port to full-duplex or half-duplex.
- Run the **mdi** command to configure the network cable adaptation mode of the Ethernet port.
- Run the **speed** command to configure the Ethernet port rate.

- d. Connect the user to another port and configure the related data if the port to which the user is connected is faulty.

10.1.5.5 MDU Has MAC Address Duplication

Determining the Fault

Run the **display location mac-addr** command for multiple times (more than 3 times as recommended) on the MDU to query the port that learns the user MAC address. The port that learns the user MAC address is different from the port that connects to the user.

```
huawei#display location  
{ mac-addr<P><XXXX-XXXX-XXXX> }:00e0-fc00-1111
```

Command:

display location 00e0-fc00-1111

It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
e

 **NOTE**

- **mac-addr** in the command output indicates the user MAC address. If dialing is initiated from a modem, the MAC address of the user is that of the modem. If dialing is initiated from the user's computer, the MAC address of the user is that of the user's computer.
- **F/S/P** in the command output indicates the port that learns the user's MAC address. Normally, the queried port is the user access port. Otherwise, the user's MAC address is duplicated.

Troubleshooting

Check whether the ports related to MAC address duplication are located on a loopback network or are attacked. If yes, disconnect the loopback network or deactivate the port from which the attacks are initiated.

10.1.5.6 Link from the MDU to DHCP Server Fails

Determining the Fault

Perform a DHCP dialup on the MDU and "DHCP server not found" is returned. Then, run the **Ping** command to ping the DHCP server and the ping operation fails.

Troubleshooting

1. Run the **display dhcp option82 config** command on the MDU to check whether its DHCP option 82 configuration is consistent with that configured on the DHCP server.
2. If they are different, run the **dhcp option82** command to modify the DHCP option 82 configuration so that it is consistent with that configured on the DHCP server.

10.1.5.7 DHCP Server Is Faulty

Determining the Fault

Perform a DHCP emulation on the MDU. Then, "DHCP server refuse request" is returned, indicating that the DHCP server rejects the DHCP request from the access node.

Troubleshooting

Check the DHCP server. Specifically, check whether the DHCP server is faulty and whether IP addresses are exhausted. Ensure that the DHCP server is available and can obtain the IP address.

10.1.5.8 User's Account Is Restricted on the BRAS

Troubleshooting

1. Check whether user data of the upper-layer BRAS is correct or whether the user's account is restricted on the BRAS.
2. If the user data of the upper-layer BRAS is incorrect or whether the user's account is restricted on the BRAS, modify the BRAS configurations and check whether the IP address can be obtained successfully.

10.2 IPTV Service Failure

This topic describes how to troubleshoot an IPTV service fault in a FTTB or FTTC network.

Prerequisites

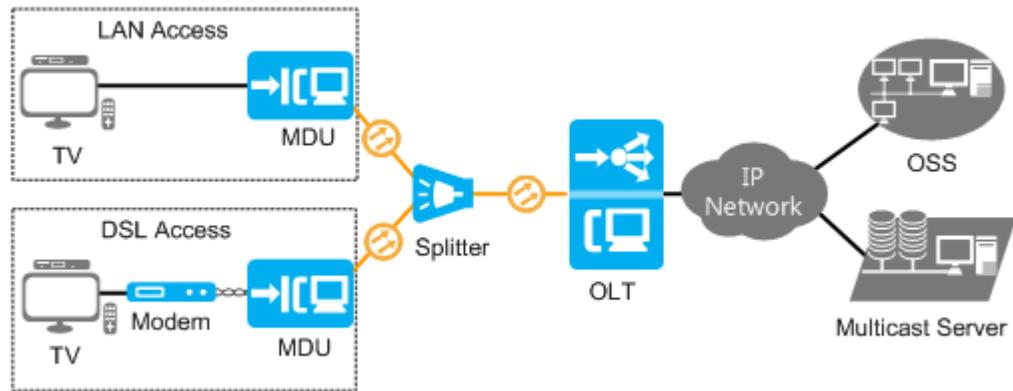
The ONU and the OLT must communicate with each other normally.

 NOTE

If a fault occurs in communication between the ONU and the OLT, all the services of the ONU may be interrupted. In this case, troubleshoot the fault first by referring to the methods described in [GPON ONU Abnormal State](#).

Context

The follow figure show an IPTV service in a FTTB or FTTC network.



 NOTE

Different MDUs support different functions and commands. In troubleshooting the IPTV service faults, the MA5616 is used as an example.

10.2.1 Online Access Failures

This section describes how to identify and resolve online access failures that occur on a fiber to the building (FTTB) or fiber to the curb (FTTC) network.

10.2.1.1 Symptoms

Description

A multicast user fails to go online, and this user is in **offline** or **block** state. In this case, when this user orders a video, a blank screen appears.

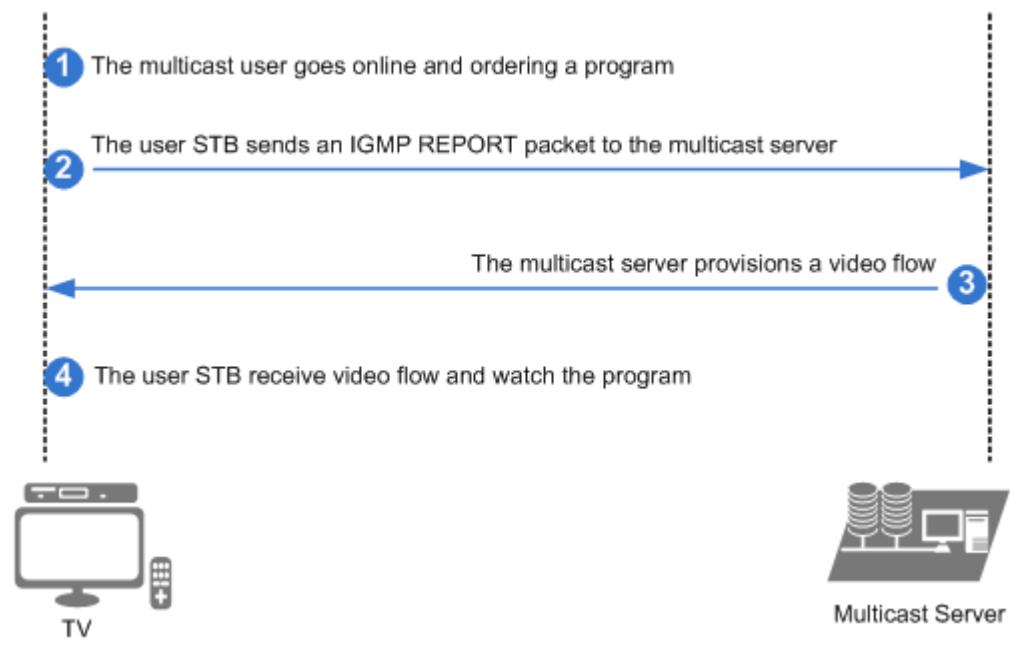
To query the status of a multicast user, run the **display igmp user** command.

- The user "State" is **offline**.
- The user "State" is **block**.

10.2.1.2 Fault Identification and Demarcation

Overview

The process of ordering a video is as follows:



1. The multicast user goes online and ordering a video.
2. The user STB sends an IGMP REPORT packet to the multicast server.
3. Based on the received IGMP REPORT packet, the multicast server provisions a video flow.
4. The network device forward the video flow to the user STB.

Fault Demarcation

If the multicast user is in **block** state, run the **undo igmp user block** command to unblock this user.

If the multicast user is in **offline** state, identify offline causes. In this case, enable multicast debugging on the MDU and check whether the MDU has received the IGMP REPORT packet sent by this user.

NOTE

The cause of user offline may differ from the scenario, and errors may have occurred during deployment or maintenance. Locate the fault based on application scenarios.

- If this fault occurs during site deployment, check the MDU hardware and the initial MDU software configuration.
- If this fault occurs during routine maintenance, this fault is unlikely to be caused by the MDU software. In this case, check the MDU hardware. If new users have been added or user configurations have been modified during routine maintenance, check user configurations.

10.2.1.3 Multicast User Is Blocked

Fault Information

After multicast debugging is enabled on the MDU, whenever a user fails to order a video due to blocked user status, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
 2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
 Type: REPORT, Version: V2, Group IP: 224.1.1.2
 Ethernet, src: 00-e0-fc-c4-80-34
 IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
  Warning: the user has been blocked
Debugging information: "Warning: the user has been blocked"
```

Determining the Fault

The status of this user is **block**. This status is queried by running the **display igmp user service-port index** command.

Troubleshooting

Run the **undo igmp user block** command to unblock the user if necessary.



If a user, such as an overdue user, is expected to remain in a multicast group but is forbidden to order videos, run the **igmp user block** command to block this user. The MDU forces this user to go offline in the video being watched and rejects any initiated order requests until the user is unblocked.

10.2.1.4 The User Fails to Pass Bandwidth CAC

Fault Information

After multicast debugging is enabled on the MDU, whenever a user fails to order a video due to a bandwidth connection admission control (CAC) failure, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
 2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
 Type: REPORT, Version: V2, Group IP: 224.1.1.2
 Ethernet, src: 00-e0-fc-c4-80-34
 IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
  Warning: the user fails to pass bandwidth CAC
Debugging information: "Warning: the user fails to pass bandwidth CAC"
```

Determining the Fault

The maximum bandwidth allocated to this user is less than the bandwidth of the video ordered by this user.

To query the maximum bandwidth allocated to this user, run the **display igmp user user-index** command. To query the bandwidth of the video ordered by this user, run the **display igmp program name** command.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- Notify this user of insufficient bandwidth, which leads to inability to order videos.
- Run the **igmp user modify user-index max-bandwidth** command to increase the maximum bandwidth allocated to this user.

10.2.1.5 Number of Specific Videos Ordered Has Reached the Upper Limit

Fault Information

After multicast debugging is enabled on the MDU, whenever a user fails to order a video due to number limitation, the debugging information in the following figure is displayed.

```
huawei(config)#  
*0.367341940 huawei BTV/8/ALL:  
 2015-04-13 18:09:52 service-port index 0 receive an IGMP packet  
  Type: REPORT, Version: V2, Group IP: 224.1.1.2  
  Ethernet, src: 00-e0-fc-c4-80-34  
  IP, src: 10.1.1.11  
huawei(config)#  
*0.367341940 huawei BTV/8/ALL:  
  Warning: the number of the grade program that the user is allowed to watch has reached maximum  
  Debugging information: "Warning: the number of the grade program that the user  
  is allowed to watch has reached maximum"
```

Determining the Fault

The maximum number (**watch limit**) of specific videos that can be ordered by this user is **0**. To query the maximum number, run the **display igmp user extended-attributes user-index** command.

NOTE

- If the value of **watch limit** is **0**, this user is forbidden to watch this type of video. For example, if the value of **HDTV watch limit** is **0**, this user has no rights to watch high definition (HD) videos.
- If the value of **watch limit** is **no-limit**, the maximum number of specific videos that can be ordered by this user is not limited. However, the total number of videos that can be concurrently watched by this user is limited.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- Inform the user that they have no rights to watch this type of video.
- Run the **igmp user watch-limit** command to increase the number of specific videos that can be ordered by this user.

10.2.1.6 Total Number of Ordered Videos Has Reached the Upper Limit

Fault Information

After multicast debugging is enabled on the MDU, whenever a user fails to order a video due to number limitation, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
Type: REPORT, Version: V2, Group IP: 224.1.1.2
Ethernet, src: 00-e0-fc-c4-80-34
IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
Warning: the number of program that the user is allowed to watch has reached maximum
Debugging information: "Warning: the number of program that the user is
allowed to watch has reached maximum"
```

Determining the Fault

The total number of ordered videos has reached the maximum number that can be ordered by this user. To query the two numbers, run the **display igmp user service-port index** command.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- Inform the user that they have no rights to watch more videos.
- Run the **igmp user modify service-port index max-program max-program-num** command to increase the total number of videos that can be ordered by this user.

10.2.1.7 User Has No Rights to Watch a Video

Fault Information

After multicast debugging is enabled on the MDU, whenever a user fails to order a video due to rights limitation, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
Type: REPORT, Version: V2, Group IP: 224.1.1.2
Ethernet, src: 00-e0-fc-c4-80-34
IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
Warning: the user has no right
Debugging information: "Warning: the user has no right"
```

Determining the Fault

To determine whether the failure in ordering videos is caused by rights limitation, run the **display igmp user 10** command. In this command, the index of this user is assumed to be 10.

- If the number of **Bind profiles** is **0**, no rights profile has been bound to this user and no videos can be ordered.
- If the number of **Bind profiles** is **1** or larger, this user can order only permitted videos. In queried results, identify the index (which is assumed to be **1**) and name of the rights profile bound to this user, then, run the **display igmp profile profile-index 1** command to query the rights of this user.
 - If the queried result is **forbidden** or **idle**, this user has no rights to watch this video.
 - If the queried result is **watch** or **preview**, this user has rights to watch this video, which is excluded from the possible offline causes. **preview** right is after a user watches a video for a period of time (for example, a few minutes), the video stops playing, or a blank screen occurs.

 NOTE

Multiple rights profiles can be bound to one user. If these profiles specify different rights for a video, the rights with the highest priority take effect for this user. By default, the rights priorities of **forbidden**, **preview**, **watch**, and **idle** are in descending order. This order can be changed by running the **igmp right-priority** command.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- If this user does not require authentication and can watch all videos, run the **igmp user modify 10 no-auth** command in BTV mode to configure this user to not require authentication. In this command, the index of this user is assumed to be 10.
- If this user requires authentication and can watch only some videos, inform the user that they have no rights to watch this video.
- If this user can only preview the video, inform the user that they can only watch for the permitted duration.
- If this user has viewing rights, modify or replace the rights profile bound to this user.
 - Modifying the rights profile: Run the **igmp profile profile-index 0 program-name PROGRAM-0 watch** to change the viewing rights from **preview** to **watch**.
 - Replacing the rights profile: Run the **undo igmp user bind-profile** command to unbind the original rights profile, then, run the **igmp user bind-profile** command to bind a new rights profile for this user.

10.2.1.8 Match Program Fail

Fault Information

After multicast debugging is enabled on the MDU, whenever a user fails to order a video due to rights limitation, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
```

```
Type: REPORT, Version: V2, Group IP: 224.1.1.2
Ethernet, src: 00-e0-fc-c4-80-34
IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
Warning: match program fail
Debugging information: "Warning: match program fail"
```

Determining the Fault

Possible Cause	Determination Basis
This user is not an M-VLAN member	To query M-VLAN members, run the display igmp multicast-vlan member vlan <i>vlanid</i> command. NOTE A user can watch videos configured in an M-VLAN only if this user is a member in this M-VLAN.
Ordered Video Is Not Contained in the M-VLAN Video List	The video list of the M-VLAN does not contain the ordered video. To query an M-VLAN video list, run the display igmp program vlan command.
No Multicast Uplink Port Has Been Configured in the M-VLAN	No multicast uplink port has been configured in the M-VLAN. To query the uplink port of an M-VLAN, run the display igmp uplink-port all command.

Troubleshooting

Possible Cause	Handling Method
This user is not an M-VLAN member	Use either of the following methods to rectify this fault based on the user's service type: <ul style="list-style-type: none"> Inform the user that they have no rights to watch this video. In M-VLAN mode, run the igmp multicast-vlan member service-port <i>index</i> command to add this user to the M-VLAN.

Possible Cause	Handling Method
Ordered Video Is Not Contained in the M-VLAN Video List	<p>Use either of the following methods to rectify this fault based on the user's service type:</p> <ul style="list-style-type: none"> • If this user has not subscribed to this video, inform the user that they have no rights to watch this type of video. • If this user has subscribed to this video, perform the following operations: <ol style="list-style-type: none"> 1. Run the display igmp config vlan command to query the video mapping mode (Program match mode) supported by the M-VLAN. If the value of Program match mode is enable, this video is a static one and requires configuration before it can be ordered. If the value of Program match mode is disable, this video is a dynamic one and automatically generated when a user orders it. 2. Add this video to the M-VLAN video list. For a static video, run the igmp program add command. For a dynamic video, run the igmp match group command to configure the address range for the M-VLAN video list. Ensure that the IP address of this ordered video is within the address range.
No Multicast Uplink Port Has Been Configured in the M-VLAN	In M-VLAN mode, run the igmp uplink-port command to configure the uplink port on the MDU as the multicast uplink port. Then, all multicast packets in this M-VLAN can be forwarded using this uplink port.

10.2.1.9 IGMP Has Been Incorrectly Configured

Fault Locating Guide

The MDU does not receive the IGMP REPORT packet sent by a user, and all other members in the M-VLAN fail to go online. In this case, the fault may be caused by the disabled status of the IGMP function in this M-VLAN.

Procedure

In M-VLAN mode, run the **display igmp config vlan** command to query the IGMP status (**IGMP mode**) in the M-VLAN.

- If the value of **IGMP mode** is **off**, IGMP is disabled in this M-VLAN. In this case, run the **igmp mode** command in M-VLAN mode to configure the IGMP status to **proxy** or **snooping**.
- If the value of **IGMP mode** is **proxy** or **snooping**, IGMP has been enabled in this M-VLAN, which is excluded from the possible offline causes.

NOTE

If the user terminal does not support multicast management, enable IGMP on the MDU. Otherwise, multicast service provisioning to this user will fail.

10.2.1.10 Subscriber Line or Terminal Is Faulty

Fault Locating Guide

Locate the fault based on symptoms.

- If this user could initially go online and then failed, the MDU software configuration is correct. Pay special attention to hardware, including the user port, user terminal, and physical line between the MDU and the user terminal.
- If this user has never succeeded in going online, check both hardware and MDU data configuration.

Procedure

Step 1 The DSL port fails to activate because the line profile bound to this port has been incorrectly configured.

This fault occurs if both of the following conditions are met:

- The MDU connects to this user using a DSL line.
- The DSL port is in **Activating** or **Deactivated** state. To query the port status, run the **display board frameid/slotid** command.

Bind a proper line profile to this DSL port. For details of the profile configuration, see the configuration of the line profile bound to a functional port.

Step 2 The virtual path identifier (VPI)/virtual channel identifier (VCI) configuration on the MDU is different from that on the modem.

This fault occurs if both of the following conditions are met:

- The MDU connects to this user using a DSL line.

- The VPI/VCI configuration on the MDU is different from that on the modem. To query the VPI/VCI configuration, run the **display service-port port frameid/slotid/portid** command.

Modify the VPI/VCI configuration on the MDU or modem and ensure that the configurations are the same on both of them.

 **NOTE**

To modify the VPI/VCI configuration on the MDU, run the **undo service-port** command to delete the original service port, and then run the **service-port** command to configure a new VPI/VCI.

Step 3 The user port is faulty in hardware.

After this user is connected to another user port, this fault is rectified. Connect this user to another port.

Step 4 User terminal is faulty.

Possible Cause	Determination Basis	Handling Method
The physical line between the MDU and the user terminal is faulty.	After the physical line between the MDU and the user terminal is replaced, this fault is rectified.	Replace this line.
The user terminal is faulty.	The user terminal indicator is faulty. After the user terminal is restarted or replaced, this fault is rectified.	Restart or replace the user terminal.
The set-top box (STB) is faulty.	After the STB is restarted or replaced, this fault is rectified.	Restart or replace the STB.

----End

10.2.2 Blank Screens on the Multicast Service

This section describes how to identify and resolve blank screens on the multicast service for a fiber to the building (FTTB) or fiber to the curb (FTTC) network.

10.2.2.1 Symptoms

Description

After ordering a video, the multicast user experiences a blank screen but not the ordered video.

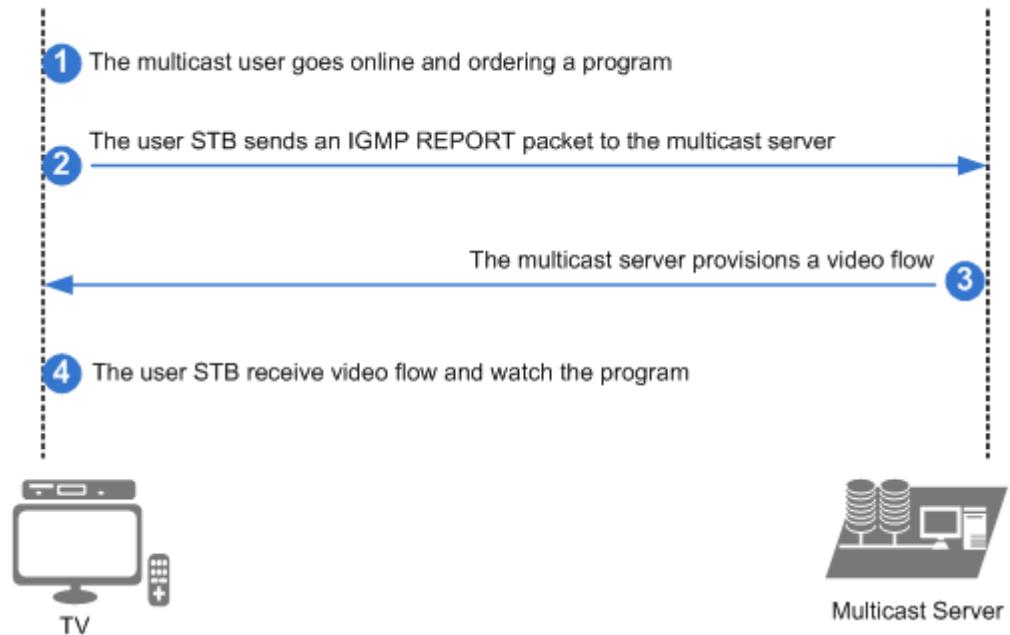
To query the status of a multicast user, run the **display igmp user** command.

The user "State" is **online**.

10.2.2.2 Fault Identification and Demarcation

Overview

The process of ordering a video is as follows:

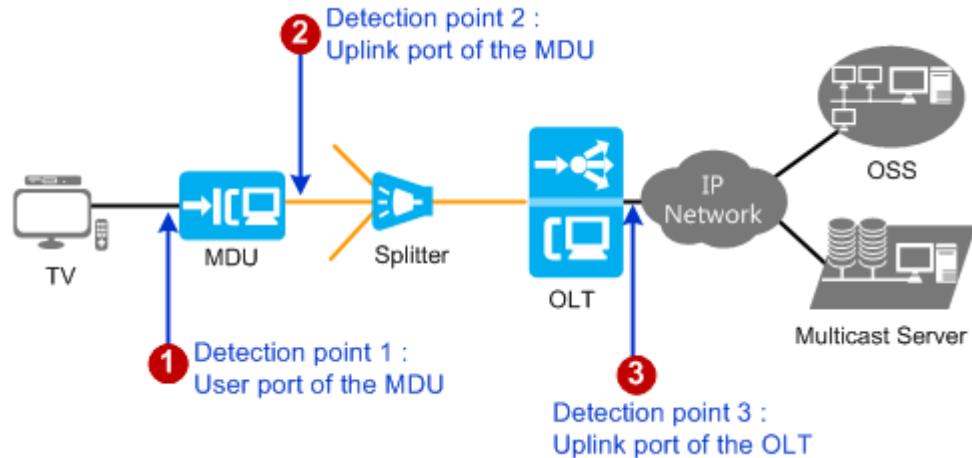


1. The multicast user goes online and ordering a video.
2. The user STB sends an IGMP REPORT packet to the multicast server.
3. Based on the received IGMP REPORT packet, the multicast server provisions a video flow.
4. The network device forward the video flow to the user STB.

Fault Demarcation

When a blank screen occurs on an FTTB or FTTC network, demarcate the fault where the video stream was interrupted, as shown in **Figure 10-3**.

Figure 10-3 Fault demarcation



Detection point	Symptom	Possible Cause
Detection point 1	Multicast streams reach the user port of the MDU	User terminal is faulty.
Detection point 2	Multicast streams reach the upstream port of the MDU but do not reach the user port of the MDU.	<ul style="list-style-type: none"> The remaining multicast bandwidth is lower than the required bandwidth of the ordered program. The number of programs watched by the multicast user reaches the upper limit. The number of programs at a level watched by the multicast user reaches the upper limit. The multicast user does not have the permission to watch the program. The program ordered is not in the MVLAN to which the multicast user belongs. There are too many prejoined static programs, occupying too many bandwidths.
Detection point 3	Multicast streams reach the upstream port of the OLT but do not reach the upstream port of the MDU.	<ul style="list-style-type: none"> The program ordered is not in the MVLAN to which the multicast user belongs. The maximum multicast bandwidth assigned to the PON port is very low.

Detection point	Symptom	Possible Cause
	Multicast streams do not reach the upstream port of the OLT.	<ul style="list-style-type: none">The Host attribute of the video has been incorrectly configured.Multicast server is Faulty.

NOTE

The cause of blank screens may differ from the scenario, and errors may have occurred during deployment or maintenance. Locate the fault based on applicable scenarios.

- If this fault occurs during site deployment, check the MDU hardware and the initial MDU software configuration.
- If this fault occurs during routine maintenance, this fault is unlikely to be caused by the MDU software. In this case, check the MDU hardware. If new users have been added or user configurations have been modified during routine maintenance, check user configurations.

10.2.2.3 Host attribute of multicast video is incorrect

Fault Information

A multicast user orders a video, but no video reaches the multicast uplink port.

Determining the Fault

The video traffic on the multicast uplink port is 0. This indicates that the video stream has not reached the multicast uplink port.

To query the multicast video ordered by a user, run the following command:

```
huawei#display igmp user service-port 500
```

.....

Program name	VLAN	IP/MAC	State	Start time
PROGRAM-0	1	224.1.1.1	watching	2015-03-15 16:02:38+08:00

The preceding terminal display shows that the IP address of the ordered video is 224.1.1.1 and the M-VLAN ID is 1.

To query the real-time video traffic on the multicast uplink port, run the following command:

```
huawei#display multicast flow-statistic vlan 1 ip 224.1.1.1  
Command is being executed. Please wait...  
Multicast flow statistic result: 0(kbps)
```

Troubleshooting

Run the following command to check the **Host attribute** of the ordered video:

```
huawei(config-mvlan1)#display igmp program vlan 1 ip 224.1.1.1
```

```
Program index      : 0
Create mode       : static
Program name      : PROGRAM-0
IP address        : 224.1.1.1
VLAN ID          : 1
Host attribute    : disable
.....
```

NOTE

If the queried result is **disable**, the **Host attribute** of this video is disabled.

- When the M-VLAN works in IGMP proxy mode, the MDU does not send any IGMP packets to the multicast server.
- When the M-VLAN works in IGMP snooping mode:
 - If IGMP report proxy has been enabled on the MDU, the MDU does not send any IGMP report packets to the multicast server.
 - If IGMP leave proxy has been enabled on the MDU, the MDU does not send any IGMP leave packets to the multicast server.

Queried results show that the **Host attribute** of the ordered video is **disable**. In this case, the MDU does not send IGMP packets to the multicast server. As a result, the multicast server does not send the video stream to the multicast uplink port.

Run the **igmp program modify** command to change the **Host attribute** of the ordered video to **enable**.

10.2.2.4 User Has No Rights to Watch a Video

Fault Information

After multicast debugging is enabled, whenever a user fails to order a video, the video stops playing, or a blank screen occurs due to rights limitation, the debugging information in the following figure is displayed.

```
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
Type: REPORT, Version: V2, Group IP: 224.1.1.2
Ethernet, src: 00-e0-fc-c4-80-34
IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
Warning: the user has no right
Debugging information: "Warning: the user has no right"
```

Determining the Fault

To determine whether the failure in ordering videos is caused by rights limitation, run the **display igmp user 10** command. In this command, the index of this user is assumed to be 10.

- If the number of **Bind profiles** is **0**, no rights profile has been bound to this user and no videos can be ordered.
- If the number of **Bind profiles** is **1** or larger, this user can order only permitted videos. In queried results, identify the index (which is assumed to be **1**) and name of the rights profile bound to this user, then, run the **display igmp profile profile-index 1** command to query the rights of this user.

- If the queried result is **forbidden** or **idle**, this user has no rights to watch this video.
- If the queried result is **watch** or **preview**, this user has rights to watch this video, which is excluded from the possible offline causes. **preview** right is after a user watches a video for a period of time (for example, a few minutes), the video stops playing, or a blank screen occurs.

 NOTE

Multiple rights profiles can be bound to one user. If these profiles specify different rights for a video, the rights with the highest priority take effect for this user. By default, the rights priorities of **forbidden**, **preview**, **watch**, and **idle** are in descending order. This order can be changed by running the **igmp right-priority** command.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- If this user does not require authentication and can watch all videos, run the **igmp user modify service-port 10 no-auth** command in BTV mode to configure this user to not require authentication. In this command, the index of this user is assumed to be 10.
- If this user requires authentication and can watch only some videos, inform the user that they have no rights to watch this video.
- If this user can only preview the video, inform the user that they can only watch for the permitted duration.
- If this user has viewing rights, modify or replace the rights profile bound to this user.
 - Modifying the rights profile: Run the **igmp profile profile-index 0 program-name PROGRAM-0 watch** to change the viewing rights from **preview** to **watch**.
 - Replacing the rights profile: Run the **undo igmp user bind-profile** command to unbind the original rights profile, then, run the **igmp user bind-profile** command to bind a new rights profile for this user.

10.2.2.5 The User Fails to Pass Bandwidth CAC

Fault Information

After multicast debugging is enabled on the MDU, whenever a user fails to order a video due to a bandwidth connection admission control (CAC) failure, the debugging information in the following figure is displayed.

```
huawei(config)#  
*0.367341940 huawei BTV/8/ALL:  
2015-04-13 18:09:52 service-port index 0 receive an IGMP packet  
Type: REPORT, Version: V2, Group IP: 224.1.1.2  
Ethernet, src: 00-e0-fc-c4-80-34  
IP, src: 10.1.1.11  
huawei(config)#  
*0.367341940 huawei BTV/8/ALL:  
Warning: the user fails to pass bandwidth CAC  
Debugging information: "Warning: the user fails to pass bandwidth CAC"
```

Determining the Fault

The maximum bandwidth allocated to this user is less than the bandwidth of the video ordered by this user.

To query the maximum bandwidth allocated to this user, run the **display igmp user service-port index** command. To query the bandwidth of the video ordered by this user, run the **display igmp program name** command.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- Notify this user of insufficient bandwidth, which leads to inability to order videos.
- Run the **igmp user modify service-port index max-bandwidth** command to increase the maximum bandwidth allocated to this user.

10.2.2.6 Number of Specific Videos Ordered Has Reached the Upper Limit

Fault Information

After multicast debugging is enabled on the MDU, whenever a user fails to order a video due to number limitation, the debugging information in the following figure is displayed.

```
huawei(config)#  
*0.367341940 huawei BTV/8/ALL:  
 2015-04-13 18:09:52 service-port index 0 receive an IGMP packet  
  Type: REPORT, Version: V2, Group IP: 224.1.1.2  
  Ethernet, src: 00-e0-fc-c4-80-34  
  IP, src: 10.1.1.11  
huawei(config)#  
*0.367341940 huawei BTV/8/ALL:  
  Warning: the number of the grade program that the user is allowed to watch has reached maximum  
  Debugging information: "Warning: the number of the grade program that the user  
  is allowed to watch has reached maximum"
```

Determining the Fault

The maximum number (**watch limit**) of specific videos that can be ordered by this user is **0**. To query the maximum number, run the **display igmp user extended-attributes user-index** command.



- If the value of **watch limit** is **0**, this user is forbidden to watch this type of video. For example, if the value of **HDTV watch limit** is **0**, this user has no rights to watch high definition (HD) videos.
- If the value of **watch limit** is **no-limit**, the maximum number of specific videos that can be ordered by this user is not limited. However, the total number of videos that can be concurrently watched by this user is limited.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- Inform the user that they have no rights to watch this type of video.
- Run the **igmp user watch-limit** command to increase the number of specific videos that can be ordered by this user.

10.2.2.7 Total Number of Ordered Videos Has Reached the Upper Limit

Fault Information

After multicast debugging is enabled on the MDU, whenever a user fails to order a video due to number limitation, the debugging information in the following figure is displayed.

```
huawei(config)#  
*0.367341940 huawei BTV/8/ALL:  
 2015-04-13 18:09:52 service-port index 0 receive an IGMP packet  
  Type: REPORT, Version: V2, Group IP: 224.1.1.2  
  Ethernet, src: 00-e0-fc-c4-80-34  
  IP, src: 10.1.1.11  
huawei(config)#  
*0.367341940 huawei BTV/8/ALL:  
  Warning: the number of program that the user is allowed to watch has reached maximum  
  Debugging information: "Warning: the number of program that the user is  
  allowed to watch has reached maximum"
```

Determining the Fault

The total number of ordered videos has reached the maximum number that can be ordered by this user. To query the two numbers, run the **display igmp user service-port index** command.

Troubleshooting

Use either of the following methods to rectify this fault based on the user's service type:

- Inform the user that they have no rights to watch more videos.
- Run the **igmp user modify service-port index max-program max-program-num** command to increase the total number of videos that can be ordered by this user.

10.2.2.8 Match Program Fail

Fault Information

After multicast debugging is enabled on the MDU, whenever a user fails to order a video due to rights limitation, the debugging information in the following figure is displayed.

```
huawei(config)#  
*0.367341940 huawei BTV/8/ALL:  
 2015-04-13 18:09:52 service-port index 0 receive an IGMP packet
```

```
Type: REPORT, Version: V2, Group IP: 224.1.1.2
Ethernet, src: 00-e0-fc-c4-80-34
IP, src: 10.1.1.11
huawei(config)#
*0.367341940 huawei BTV/8/ALL:
Warning: match program fail
Debugging information: "Warning: match program fail"
```

Determining the Fault

Possible Cause	Determination Basis
This user is not an M-VLAN member	To query M-VLAN members, run the display igmp multicast-vlan member vlanid command. NOTE A user can watch videos configured in an M-VLAN only if this user is a member in this M-VLAN.
Ordered Video Is Not Contained in the M-VLAN Video List	The video list of the M-VLAN does not contain the ordered video. To query an M-VLAN video list, run the display igmp program vlan command.
No Multicast Uplink Port Has Been Configured in the M-VLAN	No multicast uplink port has been configured in the M-VLAN. To query the uplink port of an M-VLAN, run the display igmp uplink-port all command.

Troubleshooting

Possible Cause	Handling Method
This user is not an M-VLAN member	Use either of the following methods to rectify this fault based on the user's service type: <ul style="list-style-type: none">• Inform the user that they have no rights to watch this video.• In M-VLAN mode, run the igmp multicast-vlan member service-port index command to add this user to the M-VLAN.

Possible Cause	Handling Method
Ordered Video Is Not Contained in the M-VLAN Video List	<p>Use either of the following methods to rectify this fault based on the user's service type:</p> <ul style="list-style-type: none"> If this user has not subscribed to this video, inform the user that they have no rights to watch this type of video. If this user has subscribed to this video, perform the following operations: <ol style="list-style-type: none"> Run the display igmp config vlan command to query the video mapping mode (Program match mode) supported by the M-VLAN. If the value of Program match mode is enable, this video is a static one and requires configuration before it can be ordered. If the value of Program match mode is disable, this video is a dynamic one and automatically generated when a user orders it. Add this video to the M-VLAN video list. For a static video, run the igmp program add command. For a dynamic video, run the igmp match group command to configure the address range for the M-VLAN video list. Ensure that the IP address of this ordered video is within the address range.
No Multicast Uplink Port Has Been Configured in the M-VLAN	In M-VLAN mode, run the igmp uplink-port command to configure the uplink port on the MDU as the multicast uplink port. Then, all multicast packets in this M-VLAN can be forwarded using this uplink port.

10.2.2.9 Prejoined Videos Use an Excessively High Bandwidth

Fault Information

A blank screen occurs only in some ordered videos.

Determining the Fault

Video prejoin has been enabled for all videos. To query the prejoin status of all videos, run the **display igmp program all** command.

```
huawei(config-btv)#display igmp program all
```

Index	Create	IP	Program	User	VLAN	Prejoin	Priority
Flag	Address	name	num	ID			

```
0 S 224.1.1.1 PROGRAM-0 0 2 enable 7
1 S 224.1.1.2 PROGRAM-1 0 2 enable 7
2 S 224.1.1.3 PROGRAM-2 0 2 enable 7
3 S 224.1.1.4 PROGRAM-3 0 2 enable 7
```

Total: 4 program(s) (Static/Dynamic: 4/0)

The bandwidth used by prejoined static videos is so high that it reaches the maximum downstream bandwidth allocated to the PON port connected to the affected MDU. As a result, no more video can be ordered due to an insufficient bandwidth.

Perform the following operations on the OLT to query the maximum downstream bandwidth allocated to a PON port:

1. Run the **display igmp config global** command to query the status of bandwidth management, which should be **enable**.
2. Run the **display igmp bandwidth port** command to query the maximum downstream bandwidth allocated to the PON port.

Troubleshooting

Although the video prejoin function implements rapid video ordering, prejoined videos may use an excessively high bandwidth. Rectify the fault based on service scenarios.

Service Scenario	Handling Method
The video prejoin function is required for rapid video ordering.	Run the igmp bandwidth port command on the OLT to increase the maximum downstream bandwidth allocated to the PON port.
The video prejoin function is not required for rapid video ordering.	Run the igmp program modify command on the OLT to disable video prejoin.

NOTE

The status of video prejoin for all videos can be changed in any M-VLAN. However, the status cannot be changed for a video that is being played.

10.2.2.10 Maximum Downstream Bandwidth Allocated to a PON Port Is Excessively Low

Fault Information

Videos can be ordered properly at working hours. However, a blank screen occurs when videos are ordered during traffic rush hours at night.

Determining the Fault

The remaining bandwidth of the PON port connected to the affected MDU is less than the bandwidth required by the ordered video. As a result, this video fails to order due to an insufficient bandwidth.

Perform the following operations on the OLT to query the remaining bandwidth of a PON port:

1. Run the **display igmp config global** command to query the status of bandwidth management, which should be **enable**.
2. Run the **display igmp bandwidth port** command to query the maximum downstream bandwidth allocated to the PON port and the used bandwidth of this port.
3. Use the following formula to calculate the remaining bandwidth of the PON port: Remaining bandwidth = Maximum downstream bandwidth allocated to the PON port - Used bandwidth of this port

Troubleshooting

Run the **igmp bandwidth port** command on the OLT to increase the maximum downstream bandwidth allocated to the PON port.

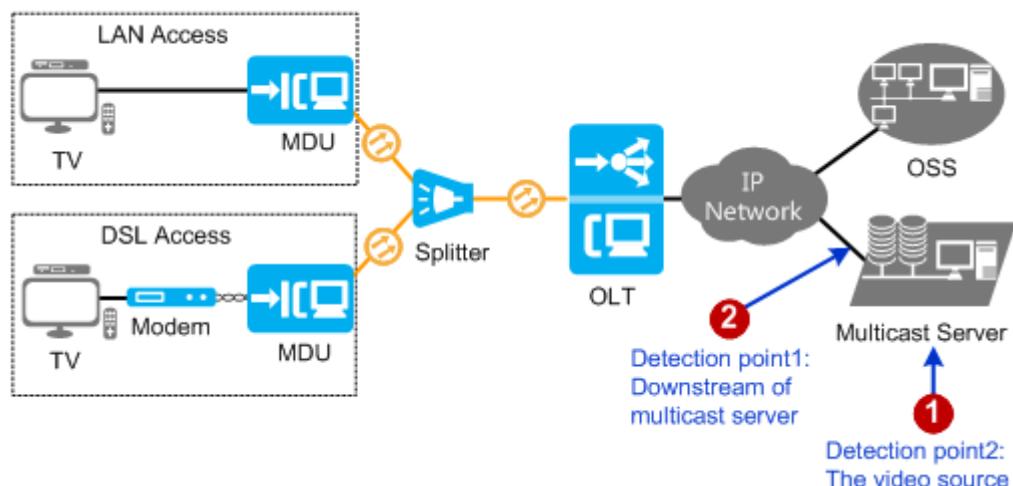
10.2.2.11 Poor Video Source Quality

Fault Information

Video stops or a blank screen occurs for all users connected to a multicast server.

Determining the Fault

If all users connected to the multicast server are affected, the fault occurs on the multicast server. The method of determining the fault is shown in the following figure.



Detection Point	Determination Basis
Detection point 1: video source	<p>View the video on the screen of the multicast server.</p> <ul style="list-style-type: none"> • If the video is functional, the video source is excluded from the possible blank screen causes. • If the video stops or a blank screen occurs, the media file of the video source is incorrect.
Detection point 2: outbound port on the multicast server	<p>Capture packets on the outbound port of the multicast server and restore the video from the packets. Alternatively, order a video on the outbound port.</p> <ul style="list-style-type: none"> • If the video is functional, the video source is excluded from the possible blank screen causes. • If the video stops or a blank screen occurs, the fault occurs on the multicast server. <ul style="list-style-type: none"> – The multicast server is faulty. – An error occurs in video codec. <p>NOTE</p> <p>Capture packets may involve obtaining the personal information, such as the IP address, MAC address, the personal data of users and the content of users' communications (the product does not save, parse, or process such information). Huawei alone is unable to collect or save the personal data of users and the content of users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the personal data of users and the content of users' communications are fully protected when the personal data and the content are being used and saved.</p>

Troubleshooting

Fault Point	Handling Method
Media file of the video source is incorrect.	Verify that parameter settings in the file comply with service requirements.
The multicast server is faulty.	<p>Check and rectify the following faults on the multicast server:</p> <ul style="list-style-type: none"> • The load or CPU usage is excessively high, or the available memory is insufficient. • The number of users connected by the multicast server has reached the upper limit. • An alarm affecting services has been generated. • The outbound port is faulty. • Data configuration is incorrect.

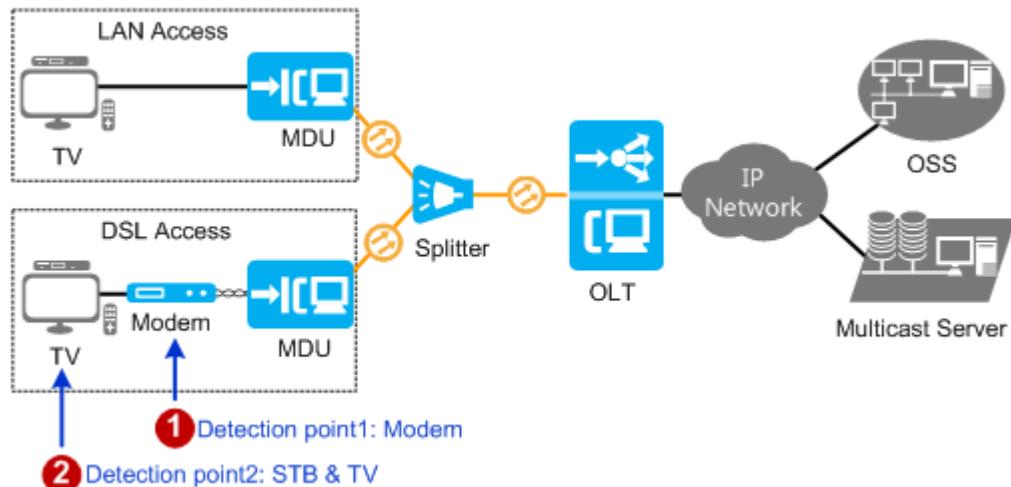
10.2.2.12 User Terminal Is Faulty

Fault Information

The ordered video stream has reached the user port. However, an artifact occurs for this user.

Confirm the Fault

The ordered video stream has reached the user port. However, an artifact occurs for this user. In this case, the user terminal may be faulty.



Detection Point	Determination Basis
Detection point 1: Modem	The modem indicator is faulty. After the modem is restarted or replaced, this fault is rectified.
Detection point 2: STB and TV	<ul style="list-style-type: none">After the STB is restarted or replaced, this fault is rectified.After the TV video cable is connected to a video input device, such as a digital video disc (DVD) recorder or a video recorder, this fault persists.

To query the multicast video ordered by a user, run the following command:

```
huawei#display igmp user service-port 500
```

```
User          : 0/1/0/500
State         : online
-----
Program name  VLAN IP/MAC      State    Start time
----- 
PROGRAM-0     1   224.1.1.1    watching  2015-03-15
                           16:02:38+08:00
```

The preceding terminal display shows that the IP address of the ordered video is 224.1.1.1 and the M-VLAN ID is 1.

To query real-time video traffic on the multicast uplink port, run the following command:

```
huawei#display multicast flow-statistic vlan 1 ip 224.1.1.1
Command is being executed. Please wait...
Multicast flow statistic result: 4096(kbps)
```

The preceding terminal display shows that the video traffic on the multicast uplink port is 4096 kbit/s, which is the same as the traffic of the ordered video. This indicates that the video stream has reached the multicast uplink port.

To query the traffic collected on the service port of the multicast user, run the **display statistics service-port 500** command. In this command, parameter **Number of downstream bytes** specifies the video traffic collected on the user terminal, which is the same as the traffic of the ordered video. This indicates that the video stream has reached the user terminal.

Troubleshooting

Possible Cause	Handling Method
The modem is faulty.	Restart or replace the modem.
The STB is faulty.	Restart or replace the STB.
The TV is faulty.	Replace the TV.

10.2.3 Multicast Video Artifacts and Intermittent Video Stops

This section describes how to identify and resolve the appearance of multicast video artifacts and intermittent video stops that occur on a fiber to the building (FTTB) or fiber to the curb (FTTC) network.

10.2.3.1 Symptoms

Multicast Video Artifacts

Artifacts appear on the screen during the display of a multicast video if one or multiple of the following cases continuously occur: pixelation, stripes, stains, color blocks, position reversal, video jitter, or image distortion, as shown in [Figure 10-4](#).

Figure 10-4 Example of multicast video artifacts



Intermittent Multicast Video Stops

Intermittent multicast video stops occur when the display of a multicast video is not smooth or stops for a long period of time (for example, a few minutes) for video loading, as shown in [Figure 10-5](#).

Figure 10-5 Example of intermittent multicast video stops



10.2.3.2 Fault Identification and Demarcation

Overview

In IPTV applications, video data packets (UDP packets) are classified as multicast packets and unicast packets.

- For multicast packets, video data is duplicated on a multi-dwelling unit (MDU), and packets are forwarded based on multicast forwarding entry settings on the optical line terminal (OLT).

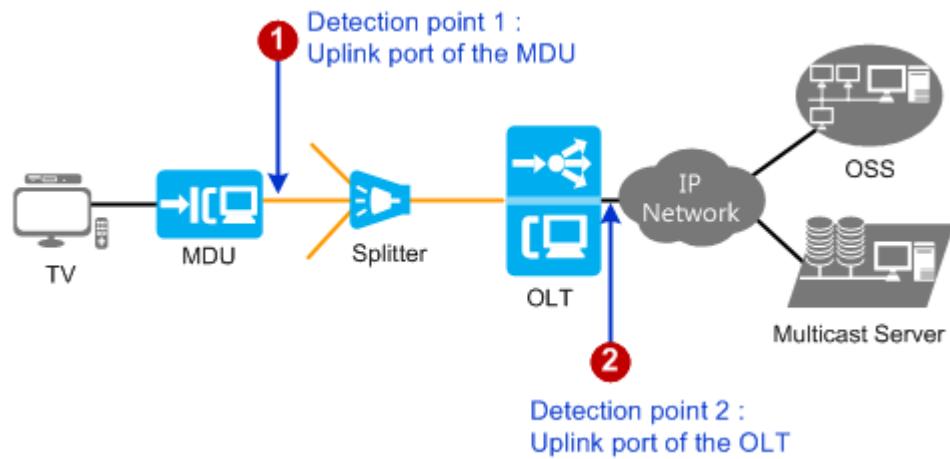
- For unicast packets, video data is duplicated on the broadband remote access server (BRAS), and packets are forwarded using the same flow as that for forwarding Internet access service packets.

If packet loss occurs between an IPTV set-top box (STB) and the multicast server, the appearance of artifacts or intermittent video stops occur after the STB restores video data, regardless of whether the video data is carried in multicast or unicast packets.

Fault Demarcation

If multicast video artifacts appear or intermittent video stops occur on an FTTB or FTTC network, identify the location where packet loss has occurred in demarcate the fault, as shown in [Figure 10-6](#).

Figure 10-6 Fault demarcation



Detection Point	Symptom	Possible Cause
Detection point 1	Packet loss does not occur on the MDU uplink port	<ul style="list-style-type: none"> User bandwidth is insufficient. User terminal is faulty.
Detection point 1	Packet loss does not occur on the OLT uplink port, but packet loss occurs on the MDU uplink port	Poor ODN lines quality.
	Packet loss occurs on the OLT uplink port	<ul style="list-style-type: none"> Poor video source quality. Poor OLT's upper-Layer network quality.

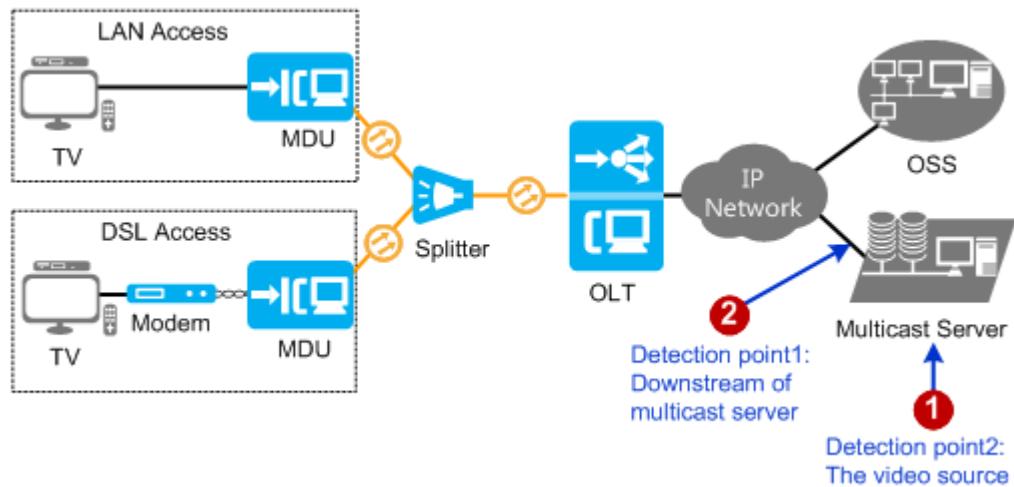
10.2.3.3 Poor Video Source Quality

Fault Information

Video artifact occurs for all users connected to a multicast server.

Determining the Fault

If all users connected to the multicast server are affected, the fault occurs on the multicast server. The method of determining the fault is shown in the following figure.



Detection Point	Determination Basis
Detection point 1: video source	<p>View the video on the screen of the multicast server.</p> <ul style="list-style-type: none">• If the video is functional, the video source is excluded from the possible artifact causes.• If the video artifact occurs, the media file of the video source is incorrect.

Detection Point	Determination Basis
Detection point 2: outbound port on the multicast server	<p>Capture packets on the outbound port of the multicast server and restore the video from the packets. Alternatively, order a video on the outbound port.</p> <ul style="list-style-type: none"> • If the video is functional, the video source is excluded from the possible artifact causes. • If the video artifact occurs, the fault occurs on the multicast server. <ul style="list-style-type: none"> – The multicast server is faulty. – An error occurs in video codec. <p>NOTE</p> <p>Capture packets may involve obtaining the personal information, such as the IP address, MAC address, the personal data of users and the content of users' communications (the product does not save, parse, or process such information). Huawei alone is unable to collect or save the personal data of users and the content of users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the personal data of users and the content of users' communications are fully protected when the personal data and the content are being used and saved.</p>

Troubleshooting

Fault Point	Handling Method
Media file of the video source is incorrect.	Verify that parameter settings in the file comply with service requirements.
The multicast server is faulty.	<p>Check and rectify the following faults on the multicast server:</p> <ul style="list-style-type: none"> • The load or CPU usage is excessively high, or the available memory is insufficient. • The number of users connected by the multicast server has reached the upper limit. • An alarm affecting services has been generated. • The outbound port is faulty. • Data configuration is incorrect.

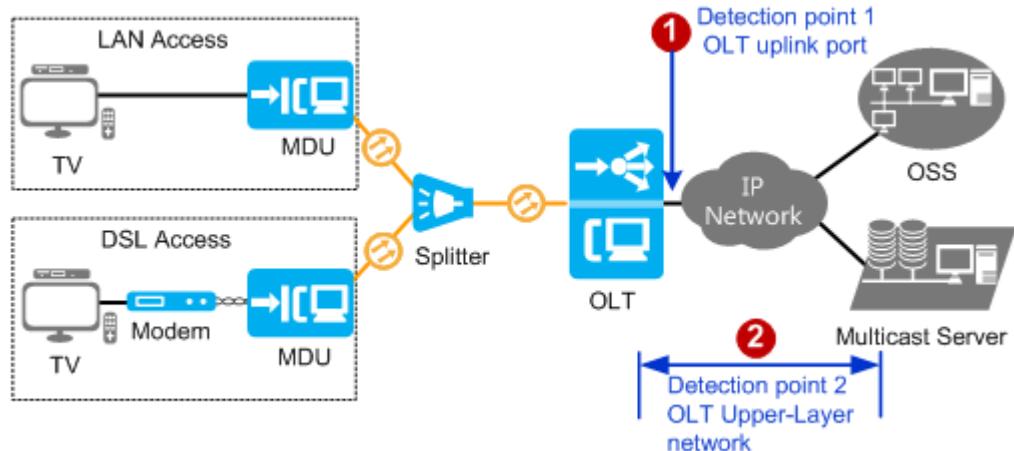
10.2.3.4 Poor OLT's Upper-Layer Network Quality

Fault Information

The ordered video stream has reached the OLT uplink port. However, packets have been lost.

Fault Locating Guide

The guide to locate an issue caused by poor OLT's upper-layer network quality.



Detection Point	Determination Basis
Detection point 1: OLT uplink port	<ul style="list-style-type: none">The uplink port state is abnormal.The status of the optical module installed in the uplink port is abnormal.
Detection point 2: OLT upper-layer network	Packets have been lost before the video stream reaches the uplink port on the OLT.

Procedure

Step 1 Check whether the optical module installed in the uplink port on the OLT is functional.

1. Check whether the uplink port is functional.

An OLT equipped with an ETH board for upstream transmission is used as an example. Run the **display port state all** command to query the status of the optical module installed in the uplink port.

The value of the **Optic Status** parameter specifies the status of the optical module.

- **absence**: indicates that the optical module is not securely installed.
- **abnormal**: indicates that the optical module is faulty.
- **normal**: indicates that the optical module is securely installed.

2. Run the **display port ddm-info** command to query the diagnosis information about the optical module.

```
huawei(config-if-eth-0/19)#display port ddm-info 0
Temperature(C)          : 38.375000
Supply voltage(V)        : 3.304000
TX bias current(mA)     : 16.541125
TX power(dBm)           : -6.623598
RX power(dBm)           : -6.292528
```

Both TX and RX optical power is generally -5 dBm. If the queried value is significantly different from this value, the optical path is unreachable. In this case, you must check the optical path.

Step 2 Check line quality on the upper-layer network.

Start a **multicast emulation test** on the OLT. After the test is complete, run the **display multicast flow-statistic vlan 3 ip 224.1.1.1** command to query the real-time traffic parameter **Multicast flow statistic result** of the multicast video. The multicast VLAN (M-VLAN) and IP address of the video are assumed to be 3 and 224.1.1.1, respectively. Then, perform operations listed in the following table based on queried results.

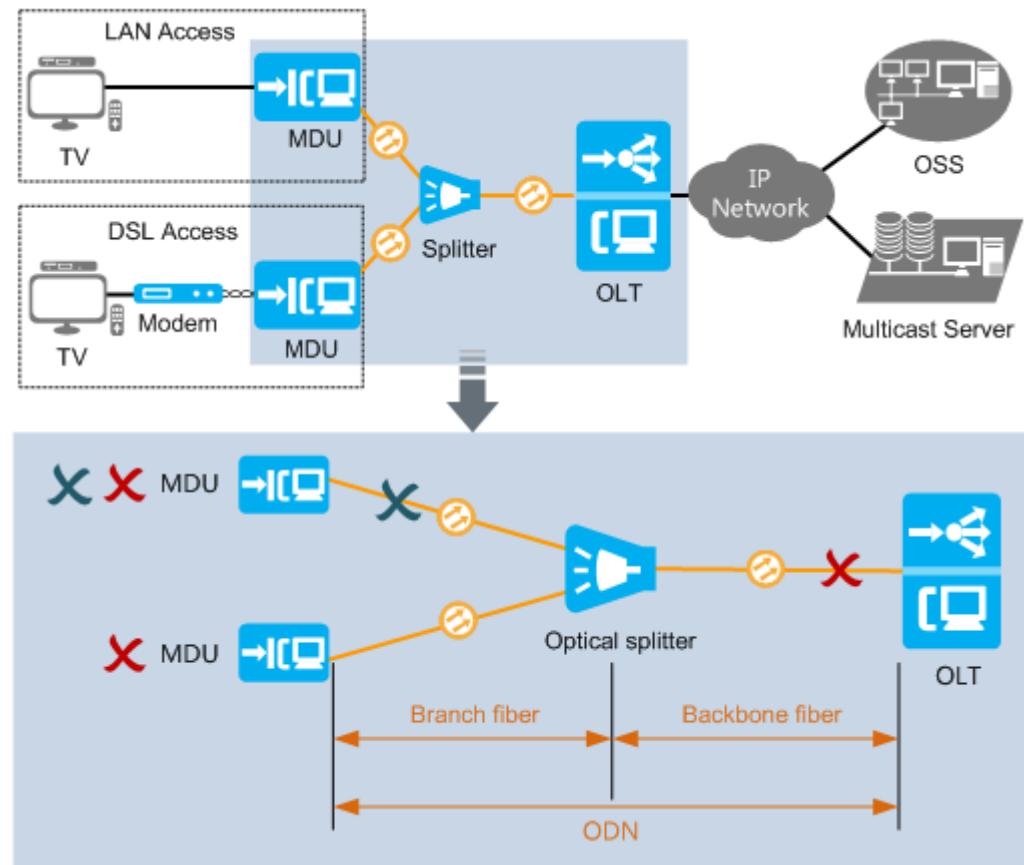
Queried Result	Handling Method
The real-time traffic of the multicast video is approximately the same as the rate of the video stream.	The video stream has reached the uplink port on the OLT properly. In this case, packets are not lost on the upper-layer network.
The real-time traffic of the multicast video is significantly less than the rate of the video stream.	<p>Packets have been lost before the video stream reaches the uplink port on the OLT. In this case, the line quality of the OLT's upper-layer network must be poor.</p> <ul style="list-style-type: none">• Check whether the optical fiber is securely connected to the uplink port and whether the fiber connector is clean.• Connect the optical fiber to the uplink port again, or replace this optical fiber.• Check upper-layer devices, such as the switch, router.

----End

10.2.3.5 Poor ODN Line Quality

Fault Locating Guide

The network between a PON port on an OLT and MDUs is shown in the following figure.



In this figure:

- Poor feeder fiber quality prevents service provisioning on all MDUs connected to the PON port.
- Poor branch fiber quality prevents service provisioning on one MDU.

Troubleshooting Guide

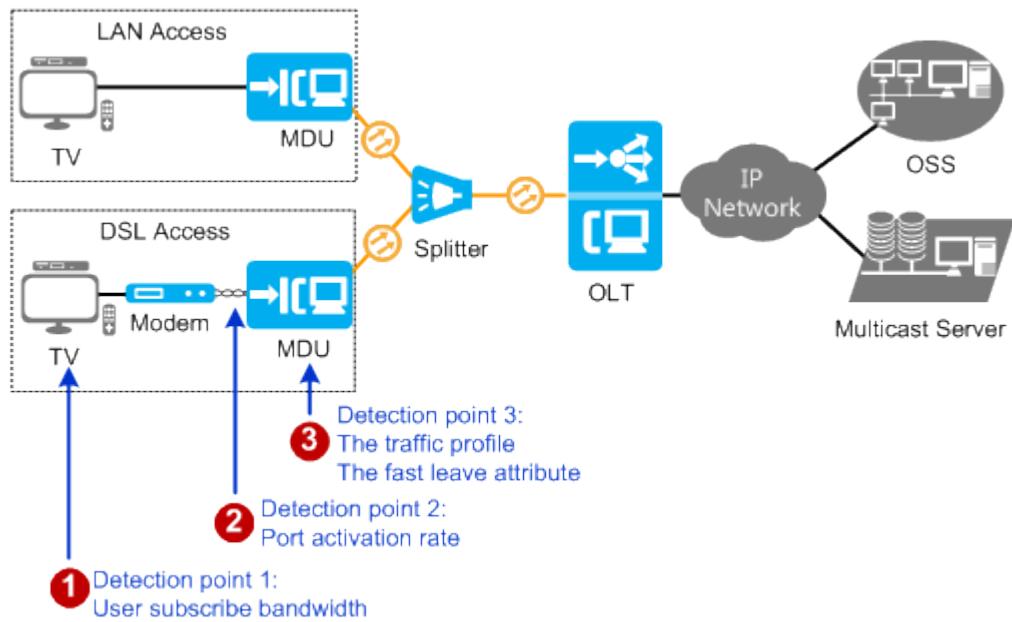
Please refer to [**<Methods of Locating and Troubleshooting Common ODN Faults>**](#).

10.2.3.6 User Bandwidth Is Insufficient

Fault Locating Guide

If a user port carries other services, such as Internet access, in addition to multicast, the bandwidth of all services on this user port must be less than or equal to the target rate. Otherwise, artifacts may appear due to insufficient multicast bandwidth.

The guide to locate an issue caused by an insufficient user bandwidth.



Detection Point	Determination Basis
Detection point 1: User subscribe bandwidth	The subscribed user bandwidth is too low to support the multicast service.
Detection point 2: Port activation rate	The port activation rate is less than the subscribed user bandwidth.
Detection point 3: • The traffic profile • The fast leave attribute	<ul style="list-style-type: none"> The traffic profile bound to the multicast service is incorrect. The function of quick leave is disable.

Procedure

Step 1 Check the subscribed user bandwidth.

If the subscribed user bandwidth is too low to support the multicast service, artifacts are caused by insufficient user bandwidth.

Use either of the following methods to rectify this fault based on the user's service type:

- Notify this user of insufficient bandwidth, which leads to inability to order videos.
- Increase the bandwidth allocated to this user.

NOTE

If a user port carries other services, such as Internet access, in addition to multicast, the bandwidth of all services on this user port must be less than or equal to the target rate. Otherwise, artifacts may appear due to insufficient multicast bandwidth.

Step 2 In xDSL mode, run the **display line operation** command to query the port activation rate.

If the port activation rate is less than the subscribed user bandwidth:

- The subscriber line is in poor condition.
- The subscriber line is being interfered with, decreasing the port activation rate.

Step 3 Check whether the traffic profile bound to the MDU is correct.

Run the **display service-port** command on the MDU to query the index of the RX traffic for the multicast service flow. Then, run the **display traffic table ip** command to query the peak information rate (PIR) of the traffic profile bound to the multicast service flow.

If the service port carries other service flows in addition to the multicast service flow, the bandwidth of all services on this service port must be less than or equal to PIR.

 **NOTE**

Common and high definition (HD) videos require different bandwidths. Empirical values are as follows:

- Bandwidth required by common videos: < 5 Mbit/s
- Bandwidth required by HD videos: > 12 Mbit/s

Change the traffic profile bound to the multicast service flow based on site requirements.

- If a proper traffic profile is available, run the **service-port 100 outbound traffic-table index 6** command on the MDU to bind the new traffic profile to the multicast service flow. The indexes of the multicast service flow and the new traffic profile are assumed to be 100 and 6, respectively.
- If no proper traffic profile is available, run the **traffic table ip** command on the MDU to create a desired traffic profile. Bind the new traffic profile to the multicast service flow.

Step 4 Check the configured user attribute.

If multicast video artifacts appear only when videos are switched, the maximum bandwidth of this user must be higher than the downstream line rate, and the fast leave function is not enabled.

Determination Basis	Handling Method
Run the display igmp user service-port index command to query the fast leave attribute (quick leave).	If the value of quick leave is disable , change the attribute based on the application scenario of this user. <ul style="list-style-type: none">• If this user connects to multiple VoD terminals, change the attribute to mac-based.• If this user connects to only one VoD terminal, change the attribute to immediate.

Determination Basis	Handling Method
Run the display igmp user service-port index command to query the maximum bandwidth of the video (User MaxBandWidth).	If the value of User MaxBandWidth is greater than the downstream line rate, artifacts appear due to insufficient line bandwidth. Run the igmp user modify service-port index max-bandwidth command to change the maximum bandwidth for this user to be lower than the line rate.

----End

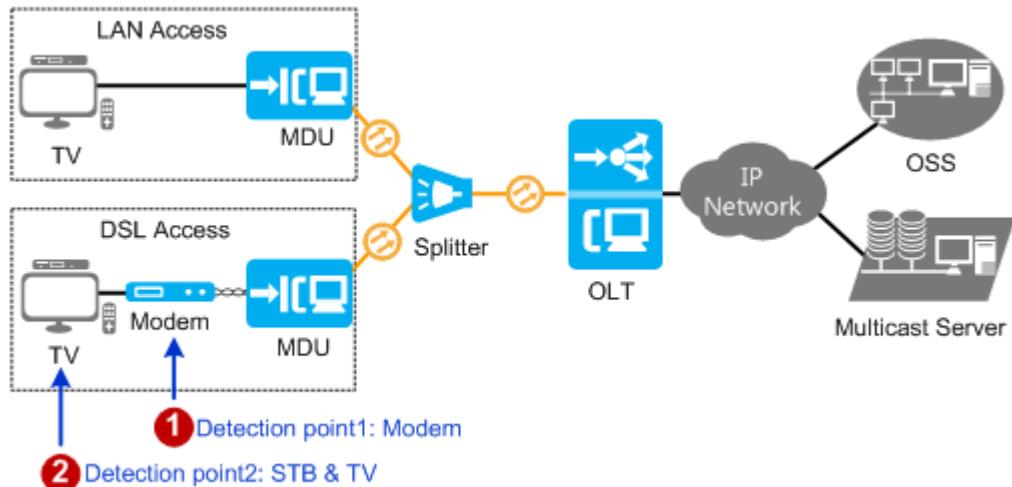
10.2.3.7 User Terminal Is Faulty

Fault Information

The ordered video stream has reached the user port. However, an artifact occurs for this user.

Confirm the Fault

The ordered video stream has reached the user port. However, an artifact occurs for this user. In this case, the user terminal may be faulty.



Detection Point	Determination Basis
Detection point 1: Modem	The modem indicator is faulty. After the modem is restarted or replaced, this fault is rectified.

Detection Point	Determination Basis
Detection point 2: STB and TV	<ul style="list-style-type: none"> After the STB is restarted or replaced, this fault is rectified. After the TV video cable is connected to a video input device, such as a digital video disc (DVD) recorder or a video recorder, this fault persists.

To query the multicast video ordered by a user, run the following command:

```
huawei#display igmp user service-port 500
```

User	: 0/1/0/500			
State	: online			
.....				
Program name	VLAN	IP/MAC	State	Start time
PROGRAM-0	1	224.1.1.1	watching	2015-03-15 16:02:38+08:00

The preceding terminal display shows that the IP address of the ordered video is 224.1.1.1 and the M-VLAN ID is 1.

To query real-time video traffic on the multicast uplink port, run the following command:

```
huawei#display multicast flow-statistic vlan 1 ip 224.1.1.1
```

Command is being executed. Please wait...
Multicast flow statistic result: 4096(kbps)

The preceding terminal display shows that the video traffic on the multicast uplink port is 4096 kbit/s, which is the same as the traffic of the ordered video. This indicates that the video stream has reached the multicast uplink port.

To query the traffic collected on the service port of the multicast user, run the **display statistics service-port 500** command. In this command, parameter **Number of downstream bytes** specifies the video traffic collected on the user port, which is the same as the traffic of the ordered video. This indicates that the video stream has reached the user port.

Troubleshooting

Possible Cause	Handling Method
The modem is faulty.	Restart or replace the modem.
The STB is faulty.	Restart or replace the STB.
The TV is faulty.	Replace the TV.

10.3 Troubleshooting the Voice Service

This topic describes how to troubleshoot common faults in the voice service, including the following faults: no tone after offhook, busy tone after offhook, one-

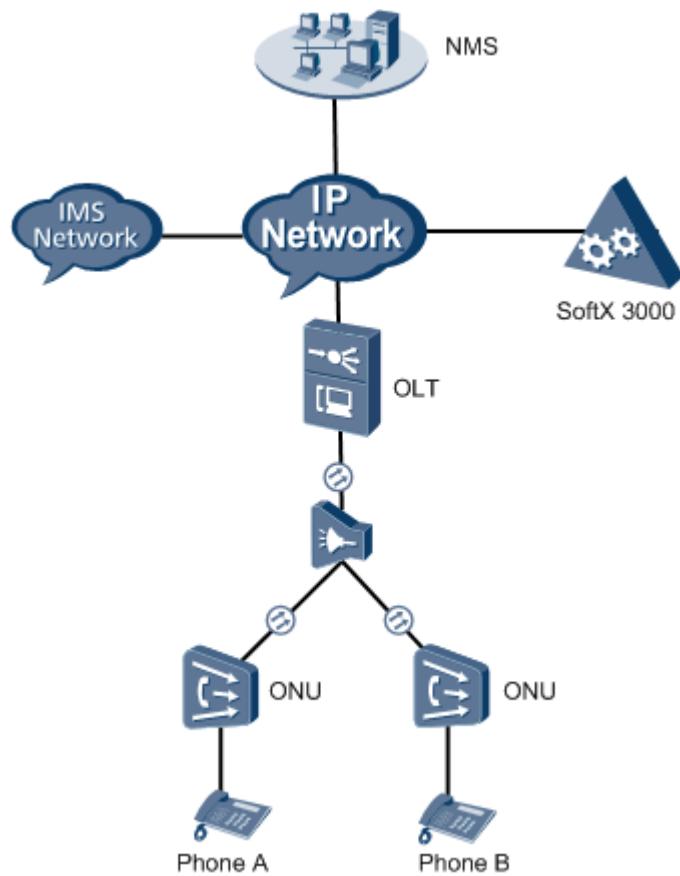
way audio in communication, noise in communication, poor voice service in communication, and failure to dial certain phone numbers.

Prerequisites

- The ONU and the OLT must communicate with each other normally. If a fault occurs in communication between the ONU and the OLT, all the services of the ONU may be interrupted. If an ONU transmits data upstream to an OLT in PON mode, troubleshoot the fault first by referring to the methods described in [6 GPON ONU Abnormal State](#).
- Different ONUs support different functions and commands. In troubleshooting the voice service, consider the MA562x as an example.

Context

In an FTTx network, voice subscribers access the ONU, and the ONU works together with the upper-layer softswitch or an IMS network to achieve the VoIP service. After being encapsulated by the ONU, voice packets are forwarded to the NGN network through the OLT. The following figure shows a network of the FTTx voice service.



 NOTE

Voice signaling tracing and voice VBD fault diagnosis may be used in voice service troubleshooting.

Based on your requirements, signaling tracing and VBD fault diagnosis may obtain some contents of users' communications

(integrity communication contents are not obtained and user information will not be disclosed)

for the purpose of safeguarding network operations and protecting services.

Huawei alone is unable to collect or save the content of users' communications.

You must comply with the laws and regulations of the countries concerned for using the functions.

You are obligated to take considerable measures to ensure that the content of users' communications is fully protected when the content is being used and saved.

10.3.1 No Tone When Offhook

Once removed from the hook, if a phone set lacks a dial tone, there is no tone when offhook.

10.3.1.1 Fault Identification and Demarcation

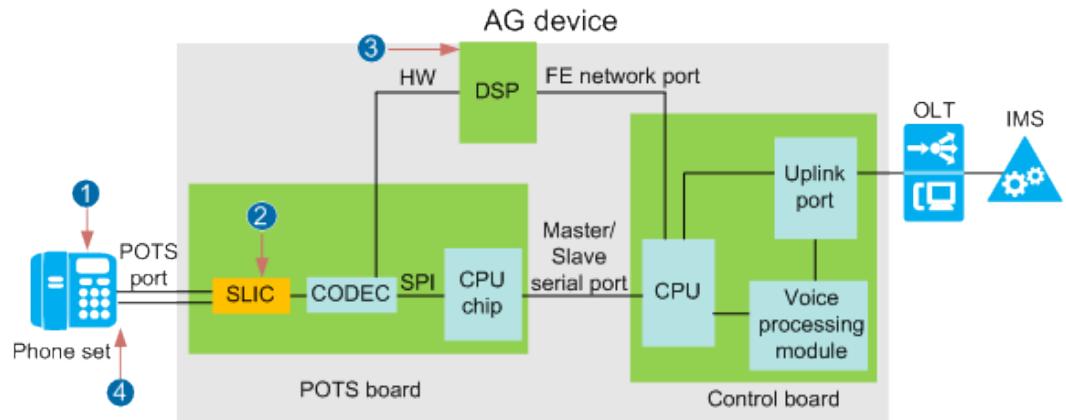
Overview

Generally, a user will hear a dial tone (beep tone) after taking the phone off the hook, letting the user know that they can start dialing a number. After the first digit is dialed, the dial tone stops.

Dial tone playing varies depending on the protocol that is used on the access gateway (AG) device.

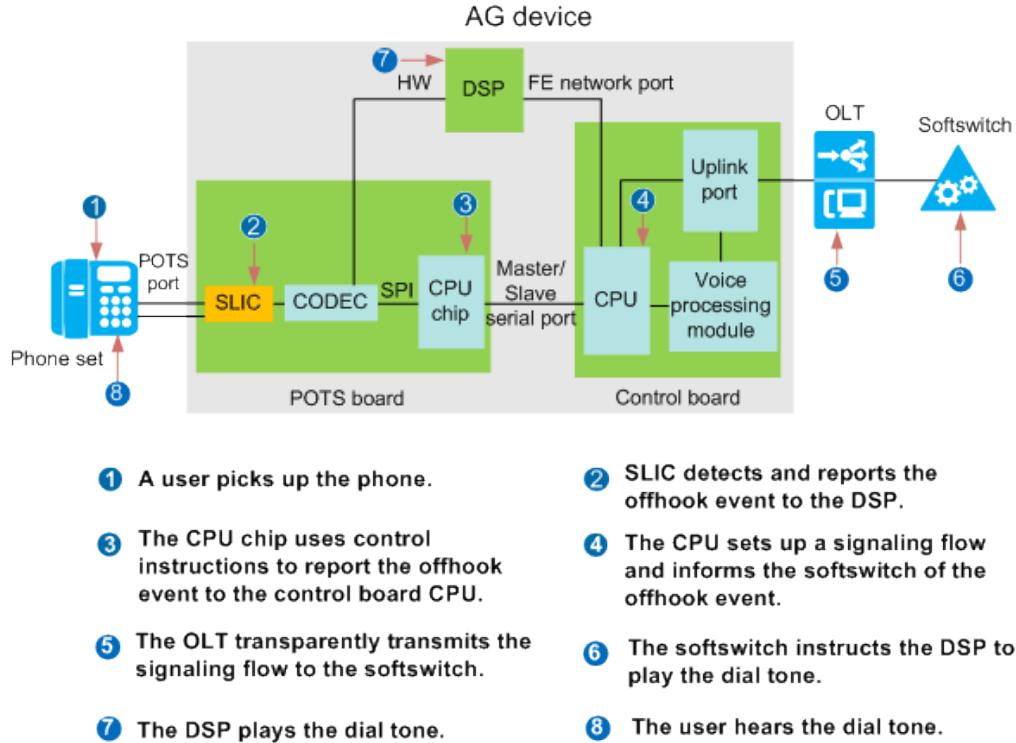
- If the Simple Internet Protocol (SIP) is used, the subscriber line interface circuit (SLIC) chip of the AG device detects the offhook event and reports it to the DSP daughter board, and the DSP daughter board plays the dial tone for the user without reporting this event to the IP multimedia subsystem (IMS). [Figure 10-7](#) shows the process of playing the dial tone on a fiber to the building (FTTB) or fiber to the curb (FTTC) network with SIP enabled.
- If H.248 is used, the SLIC chip detects the offhook event and reports it to the softswitch, and the softswitch instructs the DSP daughter board to play the dial tone for the user. [Figure 10-8](#) shows the process of playing the dial tone on an FTTB or FTTC network with H.248 enabled.

Figure 10-7 Demonstration of dial tone playing if SIP is used



- Note:**
After the user dials the first digit, the SLIC chip detects and reports the dialing event to the DSP daughter board. Then, the DSP daughter board stops playing the dial tone.

Figure 10-8 Demonstration of dial tone playing if H.248 enabled



Note:

After the user dials the first digit, the SLIC chip detects and reports the dialing event to CPU chip. Then, the CPU chip uses control instructions to report the dialing event to the control board CPU. The control board CPU sets up a signaling flow and informs the softswitch of the first digit dialing. Then, the softswitch instructs the DSP daughter board to stop playing the dial tone.

Fault Demarcation

On an FTTB or FTTC network, an optical network unit (ONU) functions as an AG device and connects to phone sets. The optical line terminal (OLT), which is the upper-layer device of the ONU, only forwards the signaling packets sent from the ONU or IMS/softswitch. If there is no tone after a phone set is offhook, demarcate the fault based on the protocol that is used for the ONU.

- If SIP is used, the dial tone is played by the DSP daughter board of the ONU. Therefore, the fault must have occurred between the phone set and the ONU. In this case, check the phone set and the ONU, as shown in [Figure 10-9](#).

Figure 10-9 Fault demarcation if SIP is used

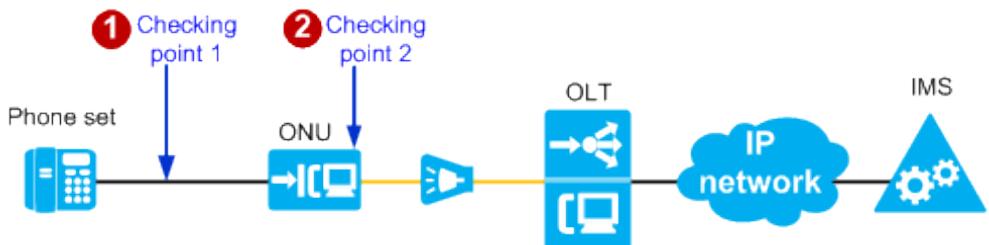


Table 10-1 Fault demarcation description

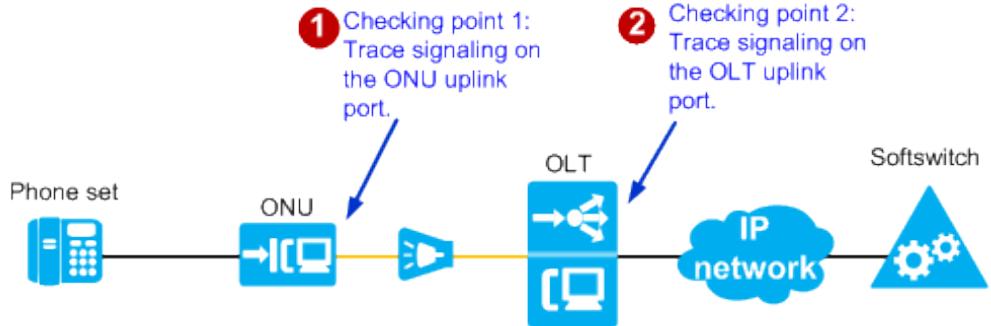
Checking Point	Affected Scope	Checking Method	Determination Basis	Possible Cause
1	Line connected between the phone set and the ONU	Perform a loop line test on the POTS port.	The test result is not Normal .	<ul style="list-style-type: none">• The phone set is faulty.• The line connected between the phone set and the ONU is faulty.
2	POTS port	Perform a circuit test on the POTS port.	The test result contains a parameter with the value Abnormal .	The POTS port is faulty.
		Query the service management status (CTPAdmState) of the POTS port.	The queried result is not StartSvc .	There is a service management malfunction on the POTS port.
	POTS board	Query the POTS board status.	The board status is not Normal .	<ul style="list-style-type: none">• There is a POTS board malfunction.• For board-inserted devices, the POTS board is not securely installed in the ONU.• The POTS board hardware is faulty.• The slot housing the POTS board is faulty.

Checking Point	Affected Scope	Checking Method	Determination Basis	Possible Cause
	DSP daughter board	<ul style="list-style-type: none"> Check whether a voice file has been loaded to the daughter board. Query available channel resources on the DSP daughter board. 	<ul style="list-style-type: none"> No voice file has been loaded to the DSP daughter board. No channel resources are available on the DSP daughter board. 	<ul style="list-style-type: none"> No voice file has been loaded to the DSP daughter board. The DSP daughter board is faulty.
	Media gateway (MG) interface	Query the MG interface status.	The interface status is not Normal .	<ul style="list-style-type: none"> There is an MG interface malfunction. Data has been incorrectly configured on the MG interface or Data hasn't been configured on the VLAN three layer interface.

- If H.248 is used, the dial tone is played by the DSP daughter board of the ONU only after the DSP daughter board receives instructions from the softswitch to play the tone. Therefore, the fault must have occurred between the phone set and the softswitch. In this case, trace signaling to identify the fault location.

 **NOTE**

Based on your requirements, signaling tracing may obtain some contents of users' communications (integrity communication contents are not obtained and user information will not be disclosed) for the purpose of safeguarding network operations and protecting services. Huawei alone is unable to collect or save the content of users' communications. You must comply with the laws and regulations of the countries concerned for using the signaling tracing feature. You are obligated to take considerable measures to ensure that the content of users' communications is fully protected when the content is being used and saved.

Figure 10-10 Fault demarcation if H.248 is used**Table 10-2** Fault demarcation description

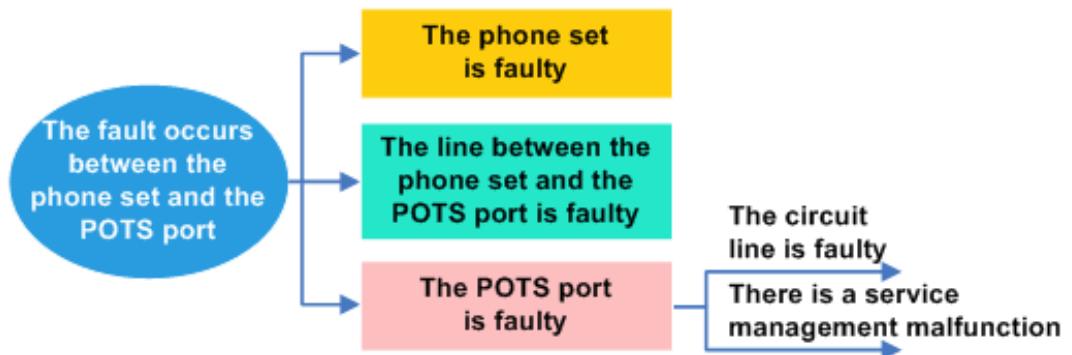
Checking Point	Checking Method	Determination Basis	Possible Cause
1	Trace signaling.	No offhook event (al/of) is detected on the ONU uplink port.	The fault has occurred between the phone set and the ONU. To rectify this fault, see the checking point 1 of Table 10-1 .
2	Trace signaling.	No offhook event (al/of) is detected on the OLT uplink port.	Packets were lost between the ONU and the OLT.
		An offhook event (al/of) has been detected on the OLT uplink port.	Packets were lost on the OLT's upper-layer network.

10.3.1.2 Fault Occurs Between the Phone Set and the POTS Port

Fault Locating Guide

If there is no tone only on certain POTS ports of an ONU when the phone sets connected to these ports are offhook, locate the fault following the guide in [Figure 10-11](#).

Figure 10-11 Fault locating guide



Procedure

Step 1 Check whether the phone set is faulty.

If the fault is rectified after the phone set is replaced, the fault must have been caused by the replaced phone set.

Step 2 Check whether the line between the phone set and the POTS port of ONU is faulty.

Run the **pots loop-line-test** command on the ONU to perform a loop line test for the line. The following terminal display is used as an example:

```

huawei(config-test)#pots loop-line-test 0/2/1
huawei(config-test)#
Testing port: 0/2/1
Telno : -
-----
Test conclusion : AB all break off or no phone connected \\Test result
-----
Line state          AB all break off or no phone connected
Line length
      Line A 0 m
      Line B 0 m
PPA                No PPA between A,B line
Termination type   Invalid
-----
Test parameter item      Value      Validity
-----
Primary test result parameter:
A->ground AC voltage      0.000 V  Valid
B->ground AC voltage      0.000 V  Valid
A->B AC voltage           0.000 V  Valid
A->ground AC Frequency    0     Hz  Invalid
B->ground AC Frequency    0     Hz  Invalid
A->B AC Frequency         0     Hz  Invalid
A->ground DC voltage      0.140 V  Valid
B->ground DC voltage      0.130 V  Valid
A->B DC voltage           0.013 V  Valid
A->ground insulation resistance 4.771 MΩ  Valid
B->ground insulation resistance 6.091 MΩ  Valid
A->B insulation resistance(Low voltage) 10.000 MΩ  Valid
B->A insulation resistance(Low voltage) 10.000 MΩ  Valid
A->B insulation resistance(High voltage) 0     Ω  Invalid
B->A insulation resistance(High voltage) -     Not support
A->ground capacitance      0     nF  Valid
A->ground capacitance      0     nF  Valid
A->B capacitance(Low voltage) 0     nF  Valid
A->B capacitance(High voltage) 0     nF  Invalid
-----
Secondary test result parameter:
  
```

A->ground conductance	1.070	uS	Valid
B->ground conductance	0.857	uS	Valid
A->B conductance(Low voltage)	0.000	uS	Valid
A->B conductance(High voltage)	-		Not support
A->ground susceptance	1.014	uS	Valid
B->ground susceptance	-3.093	uS	Valid
A->B susceptance(Low voltage)	-0.027	uS	Valid
A->B susceptance(High voltage)	-		Not support
A->ground DC current	0	uA	Valid
B->ground DC current	0	uA	Valid
A->B DC current	0	uA	Valid
B->A DC current	0	uA	Valid
A->ground AC current	0	uA	Valid
B->ground AC current	0	uA	Valid
A->B AC current	0	uA	Valid
B->A AC current	0	uA	Valid
<hr/>			
Test auxiliary parameter:			
Test frequency for admittance	-		Not support
Resistance to test the abnormal voltage	-		Not support
Max. voltage to conduct the signature	-		Not support
A->ground max. voltage	-2.647	V	Valid
A->ground min. voltage	-48.520	V	Valid
B->ground max. voltage	-2.626	V	Valid
B->ground min. voltage	-48.640	V	Valid
A->B max. voltage	47.040	V	Valid
A->B min. voltage	-46.870	V	Valid
A->ground max. current	-21	uA	Valid
A->ground min. current	-76	uA	Valid
B->ground max. current	130	uA	Valid
B->ground min. current	74	uA	Valid
A->B max. positive current	112	uA	Valid
A->B max. negative current	57	uA	Valid
<hr/>			

Typical test results and handling methods are as follows:

- If the test result is **Normal**, both the line and the phone set are functional.
- If the test result is **Phone not connected**, the phone set is faulty, or the line is insecurely connected between the phone set and the POTS port. In this case, rectify the phone set fault, or securely connect the line between the phone set and the POTS port.
- If the test result is related to a line fault, such as **B line grounding**, the line is faulty. In this case, handle the fault based on the test result. For example, **B line grounding** indicates that wire B may be damaged. In this case, replace the line.

For more information about test results and handling methods, see **ONU POTS User Loop Line Test**.

Step 3 Check whether the POTS port of ONU is faulty.

1. Run the **pots circuit-test** command on the ONU to perform a circuit test for the POTS port. If the value of at least one parameter is **Abnormal**, the POTS port is faulty. In this case, connect the phone set to a functional POTS port.

The following terminal display is used as an example:

```
huawei(config-test)#pots circuit-test mgid 0 terminalid 1
```

```
huawei(config-test)#
Testing port: 0/2/1
```

```
Telno : -
```

```
MGid : 0
```

```
Terminalid : A1
```

Test item	Result

Digital Voltage:	Abnormal
Low Battery:	Normal
High Battery:	Normal
Positive Battery:	Normal
Loop current:	Normal
Feeder voltage:	Abnormal
Ringing current voltage:	Normal
Ringing current frequency:	Normal
VAG:	Normal
VBG:	Normal

2. Run the **display pstn state** command to query the service management status (**CTPAdmState**) of the POTS port. If the value of **CTPAdmState** is not **StartSvc**, there is a service management malfunction on the POTS port.

Status	Description	Operation
LBlock or RBlock	Indicates that services are interrupted on this port.	Run the undo endservice command to restart services on the POTS port.
-	Indicates that no user has been configured on this port.	Run the sippstnuser add (SIP) or mgpstnuser add (H.248) command to configure a user on the POTS port.

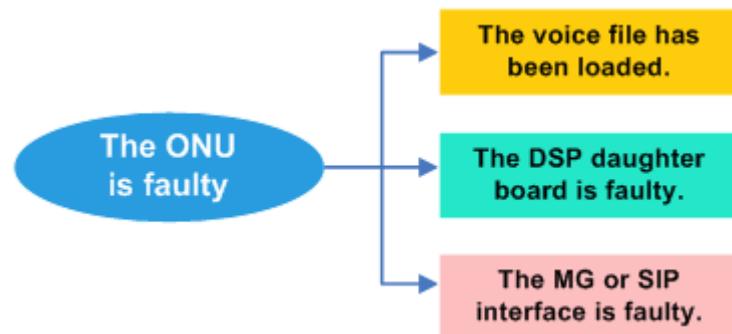
----End

10.3.1.3 ONU Is Faulty

Fault Locating Guide

If there is no tone on all POTS ports of an ONU when the phone sets connected to these ports are offhook, locate the fault following the guide in [Figure 10-12](#).

Figure 10-12 Fault locating guide



Procedure

Step 1 Run the **display version frameid/slotid** command to check whether a voice file has been loaded to the DSP daughter board.

If it has not been loaded, run the **load voice** command to load the file. Then, reset the POTS board. The following terminal display is used as an example:

Step 2 Run the **display dsp state frameid/slotid/subbid** command to check whether the daughter board is functional.

```
huawei(config)#narrow resource
huawei(config-narrow-resource)#display dsp state
```

If the queried result is "Failure: frame 0 slot does not have dsp resource", the DSP daughter board is faulty and needs to be replaced.

 **NOTE**

If the device is an integrated device, please replace the whole one.

Step 3 Check whether the MG or SIP interface is functional.

- If H.248 is used, run the **display if-h248 all** command to query the status (**State**) of the MG interface.

```
huawei>display if-h248 all
```

MGID	Trans State	MGPort MGIP	MGCPort MGCIP/DomainName
0	UDP Normal	2944 10.10.10.2	2944 10.10.10.10

State	Description	Operation
- Local Closed - Remote Closed - Graceful Closed	The MG interface has been disabled.	Run the reset command to reset the MG interface.
Wait ack	The MG interface fails to register with the media gateway controller (MGC).	Run the display if-h248 attribute mgid command to check whether MG interface configurations are the same as those on the MGC. More specifically, check whether the values of the parameters Protocol , MGC PORT , MGC IP , and MGC Domain Name configured on the MG interface are the same as those configured on the MGC. If at least one item is different, run the if-h248 attribute command to configure the MG interface again.

- If SIP is used, run the **display if-sip all** command to query the status (**State**) of the SIP interface.

```
huawei>display if-sip all
```

MGID	0
Transfer Mode	UDP
State	Normal
Signalling IP	10.10.10.1
Signalling Port	5068
Primary Proxy IP 1/DomainName	10.10.10.2
Primary Proxy Port	5060
Primary Proxy State	Up
Secondary Proxy IP 1/DomainName	10.10.10.3
Secondary Proxy Port	5061

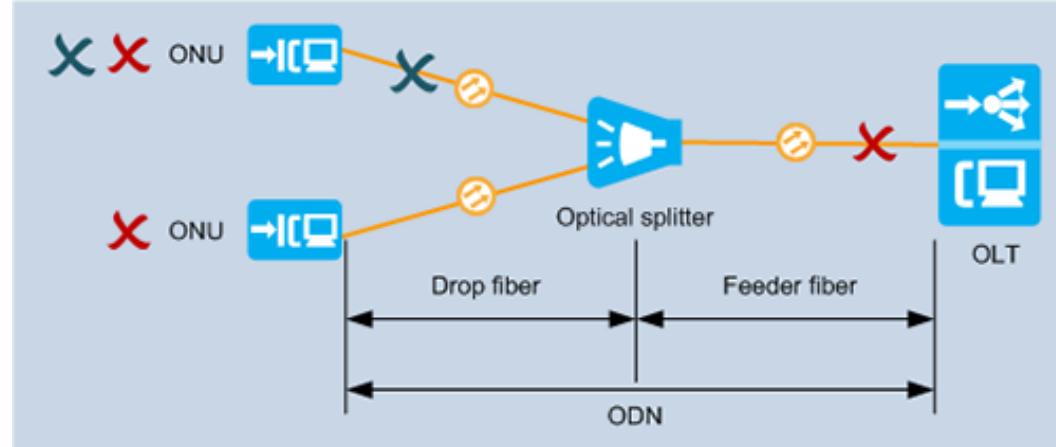
Secondary Proxy State		Up
Current Proxy		Primary Proxy
State	Description	Operation
Not start	The SIP interface has been disabled.	Run the reset command to reset the SIP interface.
Fault	The SIP interface fails to register with the IMS.	Run the display if-sip attribute command to check whether SIP interface configurations are the same as those on the IMS. More specifically, check whether the values of the parameters Protocol , Primary Proxy IP 1 , Primary Proxy Port , and Home Domain Name configured on the SIP interface are the same as those configured on the IMS. If at least one item is different, run the if-sip attribute basic command to configure the SIP interface again.

----End

10.3.1.4 ODN Fiber Quality Is Poor

Fault Locating Guide

The network between a PON port on an OLT and ONUs is shown in the following figure.



In the preceding figure,

- Poor feeder fiber quality prevents service provisioning on all ONUs connected to the PON port.
- Poor branch fiber quality prevents service provisioning on one ONU.

Troubleshooting

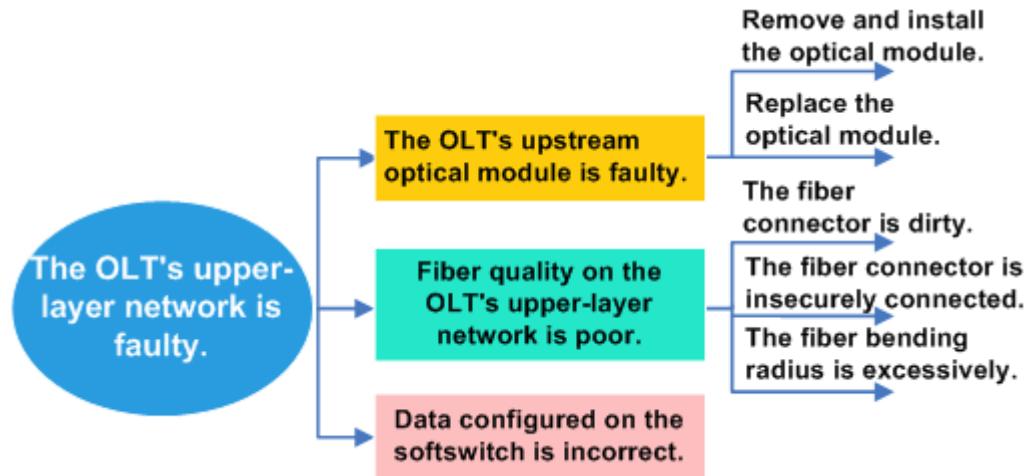
See [5.6 Methods of Locating and Troubleshooting Common ODN Faults](#).

10.3.1.5 OLT's Upper-Layer Network Is Faulty

Fault Locating Guide

If there is no tone on POTS ports of all ONUs connected to an OLT when the phone sets connected to these ports are offhook, locate the fault following the guide in [Figure 10-13](#).

Figure 10-13 Fault locating guide



Procedure

Step 1 Check whether the optical module installed on the uplink port of the OLT is functional.

1. Check whether the uplink port is functional.

An OLT equipped with an ETH board for upstream transmission is used as an example here. Run the **display port state all** command to query the uplink port status.

The value of the **Optic Status** parameter specifies the optical module status.

- **absence**: indicates that the optical module is not securely installed.
- **abnormal**: indicates that the optical module is faulty.
- **mismatch**: indicates that the optical module does not match the uplink port.
- **normal**: indicates that the optical module is securely installed.

2. Run the **display port ddm-info** command to query diagnosis information about the optical module.

Both TX and RX optical power is generally -5 dBm. If the queried value is significantly different from this value, the optical path is unreachable and needs to be checked.

Step 2 Check upper-layer network quality.

Trace signaling after the user picks up the phone. Then, check whether the offhook event (al/of) is reported by the OLT to the softswitch. If the softswitch does not issue a dial tone event (cg/dt) to the OLT, possible causes are as follows:

 NOTE

Based on your requirements, signaling tracing may obtain some contents of users' communications (integrity communication contents are not obtained and user information will not be disclosed) for the purpose of safeguarding network operations and protecting services. Huawei alone is unable to collect or save the content of users' communications. You must comply with the laws and regulations of the countries concerned for using the signaling tracing feature. You are obligated to take considerable measures to ensure that the content of users' communications is fully protected when the content is being used and saved.

1. Fiber quality on the OLT's upper-layer network is so poor that packet loss has occurred. In this case, perform the following operations:
 - Check whether the optical fiber is securely connected to the PON port and whether the connector is clean.
 - Connect the optical fiber to the PON port again. Alternatively, replace it.
2. Data configured on the softswitch is different from the planned data. In this case, contact softswitch personnel to modify the data configuration to comply with the data plan.

----End

10.3.2 Busy Tone When Offhook

If a phone sounds a busy tone each time it is offhook, a fault has occurred.

10.3.2.1 Fault Identification and Demarcation

Overview

Generally, a user will hear a dial tone (beep tone) after taking the phone off the hook, letting the user know that they can start dialing a number. The user will hear a busy tone played by the DSP daughter board in one of the following scenarios:

- The called party is busy.
- The called party hangs up the phone.
- The called party does not answer the call. After a period of time, the DSP daughter board stops the ringing tone and sounds the busy tone.
- The user does not dial a number after picking up the phone for a period of time.

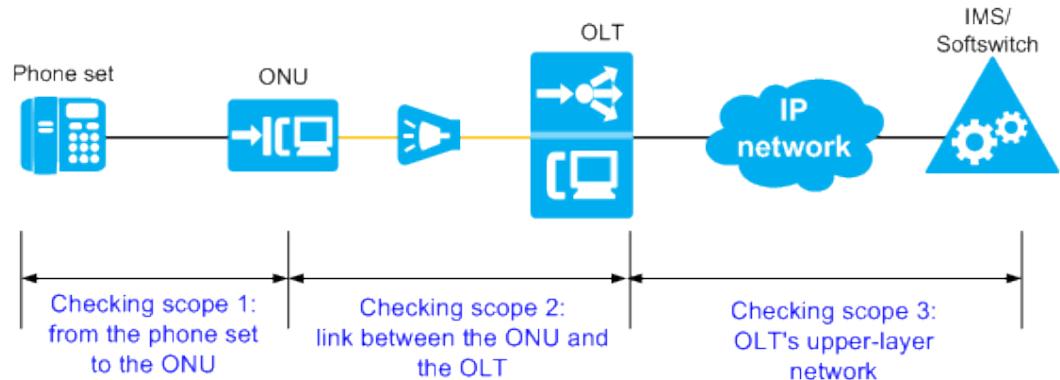
If an offhook phone is not affected by any of the preceding, a fault has occurred. In such a case, the busy tone may be caused by:

- Incorrect user data configuration
 - No user data has been configured on the POTS port.
 - No user data has been configured on the IP multimedia subsystem (IMS) or softswitch.
 - The user data configured on the POTS port is different from that configured on the IMS or softswitch.
- Insufficient available DSP resources
- Faulty link between the phone set and the IMS/softswitch

Fault Demarcation

On an FTTB or FTTC network, an optical network unit (ONU) functions as an access gateway (AG) device and connects to phone sets. The optical line terminal (OLT), which is the upper-layer device of the ONU, only transparently transmits the packets sent from the ONU or IMS/softswitch. If an offhook tone always sounds a busy tone, demarcate the fault between the phone set and the IMS/softswitch segment by segment.

Figure 10-14 Fault demarcation



Checking Point	Affected Scope	Possible Cause
1	Certain POTS ports on the ONU	<ul style="list-style-type: none">The phone sets connected to the POTS ports are faulty.The loop lines connected to the POTS ports are faulty.No user data has been configured on the POTS ports.The POTS ports have been blocked remotely.The POTS ports fail to register with the IMS or softswitch.Available DSP resources are insufficient.
	All ports on a POTS board of the ONU	The POTS board is faulty.
	All ports configured on the MG or SIP interface of the ONU	<ul style="list-style-type: none">There is the MG or SIP interface malfunction.Data has been incorrectly configured on the MG or SIP interface.
2	All POTS ports connected to one PON port on the OLT	Packets were lost between the ONU and the OLT.

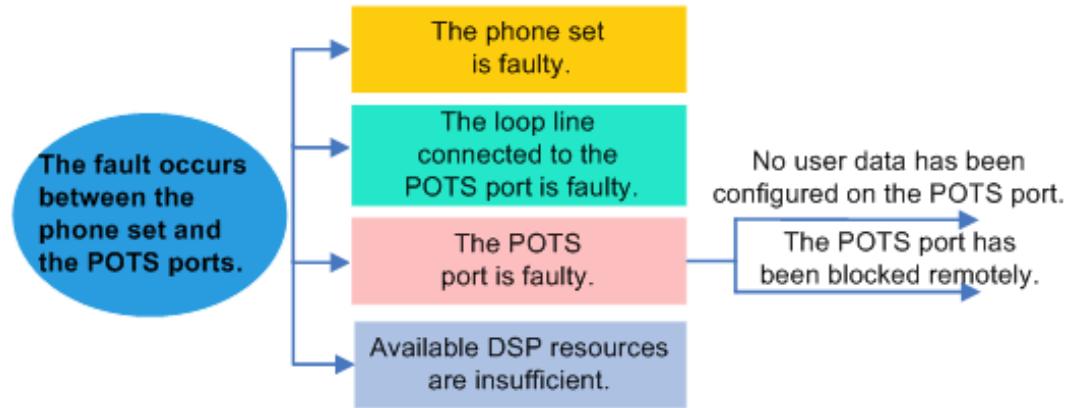
Checking Point	Affected Scope	Possible Cause
3	All ports on the OLT	<ul style="list-style-type: none"> Packets were lost on the OLT's upper-layer network. User data has been incorrectly configured on the IMS or softswitch.

10.3.2.2 Fault Occurs Between the Phone Set and the POTS Port

Fault Locating Guide

If only the phone sets connected to some POTS ports of an ONU sound a busy tone, locate the fault following the guide in [Figure 10-15](#).

Figure 10-15 Fault locating guide



Procedure

Step 1 Check whether the phone set is faulty.

If the fault is rectified after the phone set is replaced, the fault must have been caused by the replaced phone set.

Step 2 Check whether the line between the phone set and the POTS port of ONU is faulty.

Run the **pots loop-line-test** command on the ONU to perform a loop line test for the line. The following terminal display is used as an example:

```
huawei(config-test)#pots loop-line-test 0/2/1
huawei(config-test)#
Testing port: 0/2/1
Telno : -
-----
Test conclusion : AB all break off or no phone connected \\Test result
-----
Line state          AB all break off or no phone connected
Line length        Line A 0 m
                           Line B 0 m
```

PPA	No PPA between A,B line		
Termination type	Invalid		
Test parameter item	Value	Validity	
Primary test result parameter:			
A->ground AC voltage	0.000	V	Valid
B->ground AC voltage	0.000	V	Valid
A->B AC voltage	0.000	V	Valid
A->ground AC Frequency	0	Hz	Invalid
B->ground AC Frequency	0	Hz	Invalid
A->B AC Frequency	0	Hz	Invalid
A->ground DC voltage	0.140	V	Valid
B->ground DC voltage	0.130	V	Valid
A->B DC voltage	0.013	V	Valid
A->ground insulation resistance	4.771	MΩ	Valid
B->ground insulation resistance	6.091	MΩ	Valid
A->B insulation resistance(Low voltage)	10.000	MΩ	Valid
B->A insulation resistance(Low voltage)	10.000	MΩ	Valid
A->B insulation resistance(High voltage)	0	Ω	Invalid
B->A insulation resistance(High voltage)	-		Not support
A->ground capacitance	0	nF	Valid
A->ground capacitance	0	nF	Valid
A->B capacitance(Low voltage)	0	nF	Valid
A->B capacitance(High voltage)	0	nF	Invalid
Secondary test result parameter:			
A->ground conductance	1.070	uS	Valid
B->ground conductance	0.857	uS	Valid
A->B conductance(Low voltage)	0.000	uS	Valid
A->B conductance(High voltage)	-		Not support
A->ground susceptance	1.014	uS	Valid
B->ground susceptance	-3.093	uS	Valid
A->B susceptance(Low voltage)	-0.027	uS	Valid
A->B susceptance(High voltage)	-		Not support
A->ground DC current	0	uA	Valid
B->ground DC current	0	uA	Valid
A->B DC current	0	uA	Valid
B->A DC current	0	uA	Valid
A->ground AC current	0	uA	Valid
B->ground AC current	0	uA	Valid
A->B AC current	0	uA	Valid
B->A AC current	0	uA	Valid
Test auxiliary parameter:			
Test frequency for admittance	-		Not support
Resistance to test the abnormal voltage	-		Not support
Max. voltage to conduct the signature	-		Not support
A->ground max. voltage	-2.647	V	Valid
A->ground min. voltage	-48.520	V	Valid
B->ground max. voltage	-2.626	V	Valid
B->ground min. voltage	-48.640	V	Valid
A->B max. voltage	47.040	V	Valid
A->B min. voltage	-46.870	V	Valid
A->ground max. current	-21	uA	Valid
A->ground min. current	-76	uA	Valid
B->ground max. current	130	uA	Valid
B->ground min. current	74	uA	Valid
A->B max. positive current	112	uA	Valid
A->B max. negative current	57	uA	Valid

Typical test results and handling methods are as follows:

- If the test result is **Normal**, both the line and the phone set are functional.
- If the test result is **Phone not connected**, the phone set is faulty, or the line is insecurely connected between the phone set and the POTS port. In this case,

rectify the phone set fault, or securely connect the line between the phone set and the POTS port.

- If the test result is related to a line fault, such as **B line grounding**, the line is faulty. In this case, handle the fault based on the test result. For example, **B line grounding** indicates that wire B may be damaged. In this case, replace the line.

For more information about test results and handling methods, see **ONU POTS User Loop Line Test**.

Step 3 Check whether the POTS port of ONU is faulty.

1. Check whether user data has been configured on the POTS port.

Run the **display pstn state** command to query the service running status (**CTPSrvState**) and service management status (**CTPAdmState**) of the POTS port. If both parameter values are empty (-), no user data has been configured on the POTS port. In this case, run the **mgpstnuser add** (H.248) or **sippstnuser add** (SIP) command to configure user data on the POTS port.

2. Check whether the POTS port has been blocked remotely.

Run the **display pstn state** command to query the service management status (**CTPAdmState**) of the POTS port. If the queried value is **RBlock**, the POTS port has been blocked remotely. Possible causes are as follows:

- The user data configured on the POTS port is different from that configured on the IMS or softswitch. To check whether the configured user data is the same on both ends, run the **display mgpstnuser** (H.248) or **display sippstnuser** (SIP) command. If they are different, run the **mgpstnuser modify** (H.248) or **sippstnuser modify** (SIP) command to modify the user data configuration on the POTS port.
- No user data has been configured on the IMS or softswitch. In this case, configure the user data on the IMS or softswitch.
- The POTS port fails to register with the IMS or softswitch. In this case, run the **undo endservice** command to unblock the POTS port so that it can automatically register with the IMS or softswitch again.

Step 4 Check whether available DSP resources of ONU are insufficient.

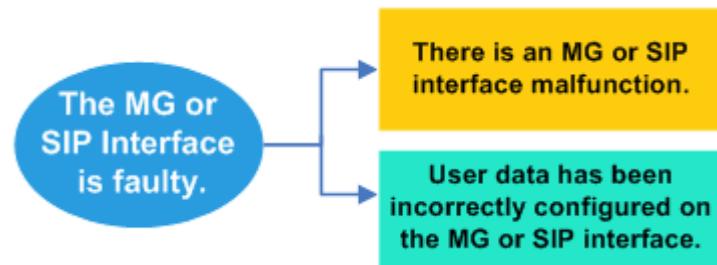
Check whether there is an event of **0x38100003 DSP resources allocated to voice services are insufficient** on the ONU. If there is, available DSP resources are insufficient and need to be expanded.

----End

10.3.2.3 MG or SIP Interface Is Faulty

Fault Locating Guide

If all phone sets connected to the POTS ports configured on the MG or SIP interface of an ONU sound a busy tone, the MG or SIP interface is faulty. This leads to a communication interruption between the MG interface and the softswitch or between the SIP interface and the IMS. Locate the fault following the guide in [Figure 10-16](#).

Figure 10-16 Fault locating guide**NOTE**

Troubleshooting may require the MG or SIP interface to restart, which interrupts user services on the interface. To prevent user service interruptions, make sure that there are no ongoing user services on the MG or SIP interface before restarting it.

Procedure

- Step 1** Check whether the MG or SIP interface is functional.

Table 10-3 Methods of handling an MG or SIP interface malfunction

Protocol Type	Determination Basis	Handling Method
H.248	The MG interface status queried by running the display if-h248 all command is not Normal .	Run the reset coldstart command to reset the MG interface. After users automatically re-register with the MG interface, run the display ptn state command in global config mode to query the service management status (CTPAdmState) of the POTS ports configured on the MG interface. Verify that the parameter value is StartSvc .
SIP	The SIP interface status queried by running the display if-sip all command is not Normal .	Run the reset command to reset the SIP interface. After users automatically re-register with the SIP interface, run the display ptn state command in global config mode to query the service management status (CTPAdmState) of the POTS ports configured on the SIP interface. Verify that the parameter value is StartSvc .

- Step 2** Check whether the user data configured on the MG/SIP interface is the same as that configured on the softswitch/IMS.

Table 10-4 Methods of handling an MG or SIP interface malfunction

Protocol Type	Determination Basis	Handling Method
H.248	<p>MG interface configurations queried by running the display if-h248 attribute command are different from those configured on the media gateway controller (MGC). The MG interface configurations involve the Protocol, MGC PORT, MGC IP, and MGC Domain Name parameters.</p> <p>A 502 error message was detected in the H.248 signaling traced on the MGC.</p> <p>NOTE</p> <ul style="list-style-type: none">• A 502 error message indicates that a termination is invalid. The termination can be a Real-Time Transport Protocol (RTP) termination or a physical termination. If a 502 error message is detected in the H.248 signaling traced on the MGC, the termination ID format configured on the MG is different from that configured on the MGC.• Based on your requirements, signaling tracing may obtain some contents of users' communications (integrity communication contents are not obtained and user information will not be disclosed) for the purpose of safeguarding network operations and protecting services. Huawei alone is unable to collect or save the content of users' communications. You must comply with the laws and regulations of the countries concerned for using the signaling tracing feature. You are obligated to take considerable measures to ensure that the content of users' communications is fully protected when the content is being used and saved.	<p>Run the if-h248 attribute command to modify MG interface configurations to the same as those configured on the MGC. Then, run the reset coldstart command to reset the MG interface.</p> <ol style="list-style-type: none">1. Run the tid-template modify command on the ONU to change the termination ID format on the MG to be the same as that on the MGC.2. Run the reset coldstart command on the ONU to reset the MG interface. Users automatically re-register with the MG interface.

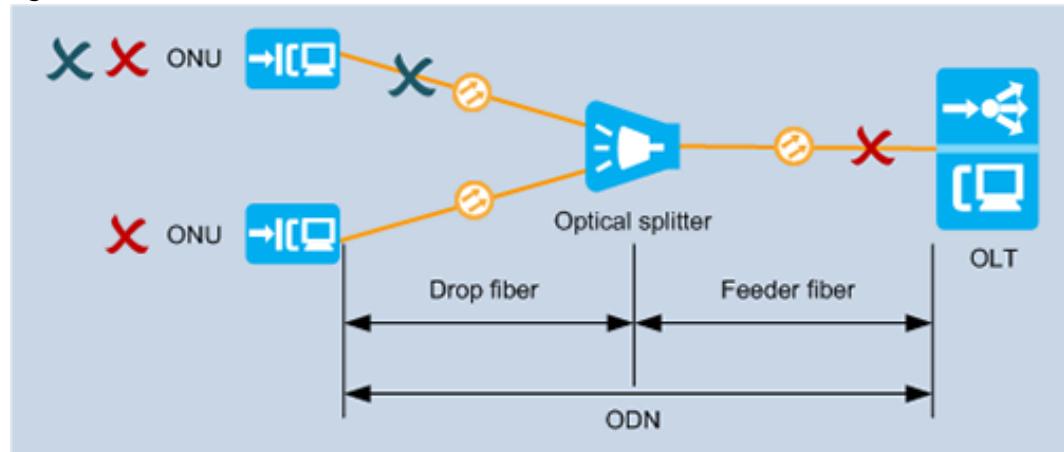
Protocol Type	Determination Basis	Handling Method
SIP	SIP interface configurations queried by running the display if-sip attribute command are different from those configured on the IMS. The SIP interface configurations involve the Protocol , Primary Proxy IP 1 , Primary Proxy Port , and Home Domain Name parameters.	Run the if-sip attribute basic command to modify SIP interface configurations to the same as those configured on the IMS. Then, run the reset command to reset the SIP interface.

----End

10.3.2.4 ODN Fiber Quality Is Poor

Fault Locating Guide

The network between a PON port on an OLT and ONUs is shown in the following figure.



In the preceding figure,

- Poor feeder fiber quality prevents service provisioning on all ONUs connected to the PON port.
- Poor branch fiber quality prevents service provisioning on one ONU.

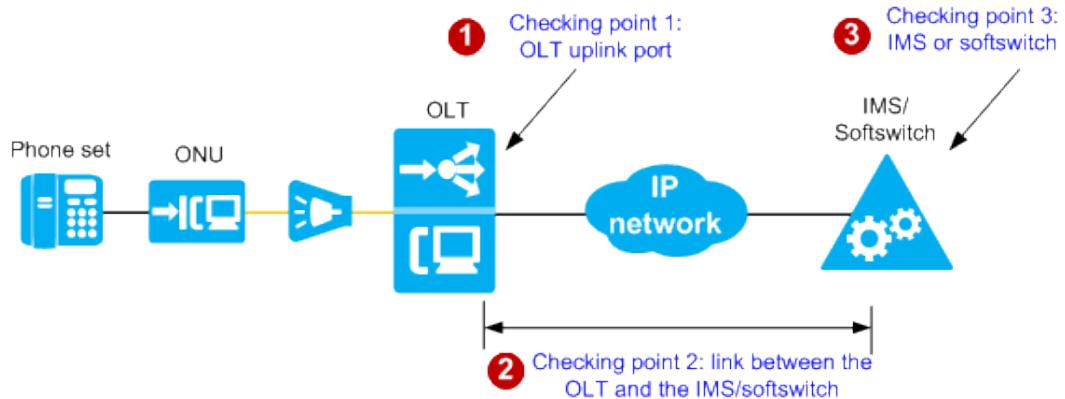
Troubleshooting

See [5.6 Methods of Locating and Troubleshooting Common ODN Faults](#).

10.3.2.5 OLT's Upper-Layer Network Is Faulty

Fault Locating Guide

If all phone sets connected to an OLT sound a busy tone, the OLT's upper-layer network is faulty. Locate the fault following the guide in [Figure 10-17](#).

Figure 10-17 Fault locating guide

Checking Point	Affected Scope	Determination Basis
1	OLT uplink port	<ul style="list-style-type: none">• There is an uplink port malfunction.• There is an optical module malfunction on the uplink port.
2	Link between the OLT and the IMS or softswitch	Packets were lost on the link.
3	IMS or softswitch	User data has been incorrectly configured on the IMS or softswitch.

Procedure

Step 1 Check whether the optical module installed on the uplink port of the OLT is functional.

1. Check whether the uplink port is functional.

An OLT equipped with an ETH board for upstream transmission is used as an example here. Run the **display port state all** command to query the uplink port status.

The value of the **Optic Status** parameter specifies the optical module status.

- **absence**: indicates that the optical module is not securely installed.
- **abnormal**: indicates that the optical module is faulty.
- **mismatch**: indicates that the optical module does not match the uplink port.
- **normal**: indicates that the optical module is securely installed.

2. Run the **display port ddm-info** command to query diagnosis information about the optical module.

Both TX and RX optical power is generally -5 dBm. If the queried value is significantly different from this value, the optical path is unreachable and needs to be checked.

Step 2 Check fiber quality on the upper-layer network.

Ping the network IP from the OLT. If packets are lost, perform the following operations:

- Check whether the optical fiber is securely connected to the PON port and whether the connector is clean.
- Connect the optical fiber to the PON port again. Alternatively, replace it.

Step 3 Check whether the user data configured on the IMS or softswitch is correct.

If no user data has been configured on the IMS or softswitch, or the configured data is different from the planned data, contact the IMS or softswitch personnel to configure or modify the data to be the same as the planned data.

----End

10.3.3 One-Way Audio During Communication

One-way audio is a voice service fault where a call is successfully established between the calling party and the called party, but neither party can hear the other party's voice after the call is established.

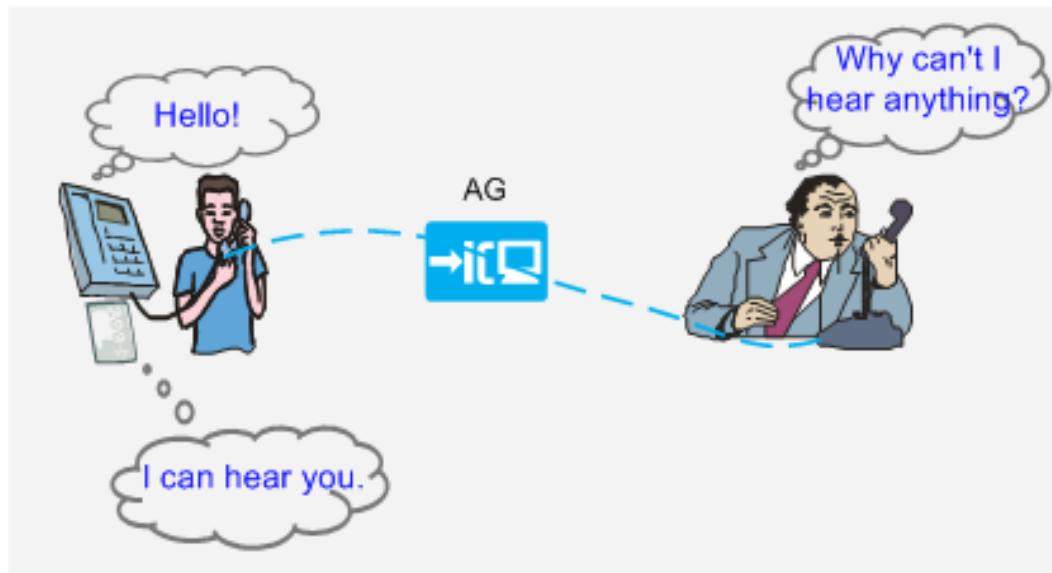
10.3.3.1 Symptoms

Description

After the calling party picks up the phone and dials a number, the called party hears the ringing and picks up the phone. If either of the following cases occurs, there is one-way audio during communication:

- The calling party can hear the called party's voice, but the called party can hear nothing, or only an echo.
- The called party can hear the calling party's voice, but the calling party can hear nothing, or only an echo.

Figure 10-18 Demonstration of one-way audio



10.3.3.2 Fault Identification and Demarcation

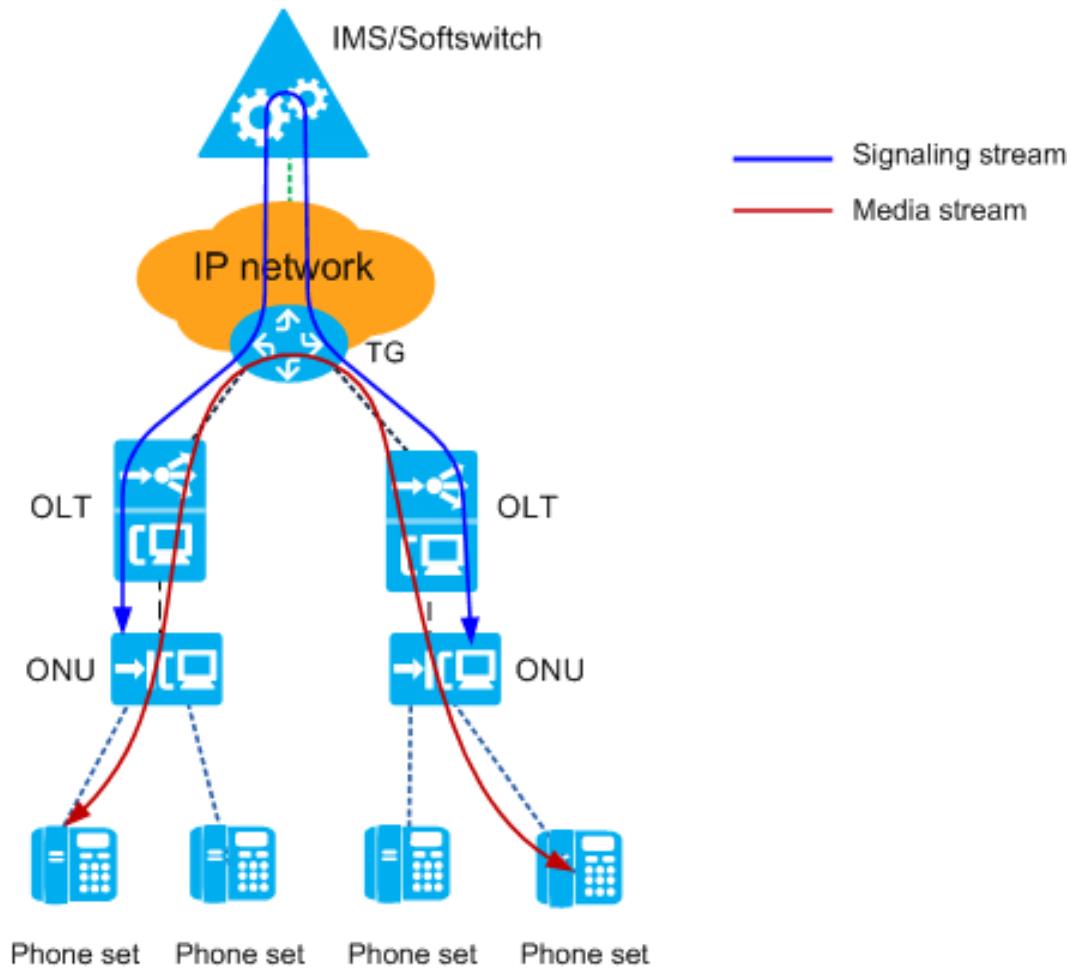
Overview

Voice communication involves signaling stream and media stream.

- A signaling stream is used to establish and control a call between two phone sets.
- A media stream carries communication content.

Figure 10-19 shows the transmission of a signaling stream and media stream.

Figure 10-19 Transmission of a signaling stream and media stream

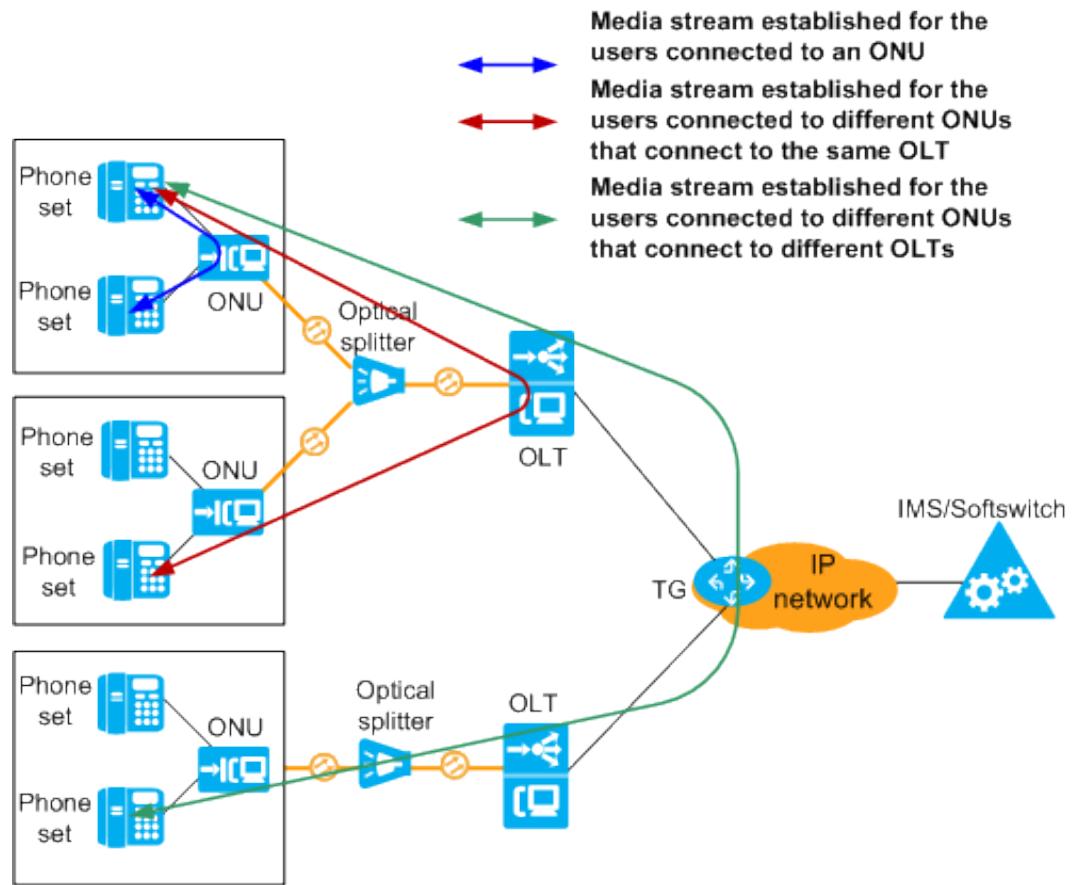


When one-way audio occurs, both number dialing and ringing are functional, which indicates that the signaling stream is functional. In most cases, the fault is caused by incorrect routing configurations on the optical network units (ONUs) connected to the phone sets or on the IP network.

Fault Demarcation

If one-way audio occurs, have the affected user dial the number of a non-affected user and identify possible fault causes, as shown in **Figure 10-20**.

Figure 10-20 Fault demarcation



Determination Basis	Possible Cause
Calls fail to be established between the users connected to an ONU.	<p>The ONU configuration is incorrect.</p> <ul style="list-style-type: none"> • The media gateway (MG) IP address of the ONU is incorrect. • The ONU routing configuration is incorrect. • The ONU access control list (ACL) configuration is incorrect.
<ul style="list-style-type: none"> • Calls can be established between the users connected to an ONU. • Calls fail to be established between the users connected to different ONUs that connect to the same optical line terminal (OLT). 	The OLT ACL configuration is incorrect.

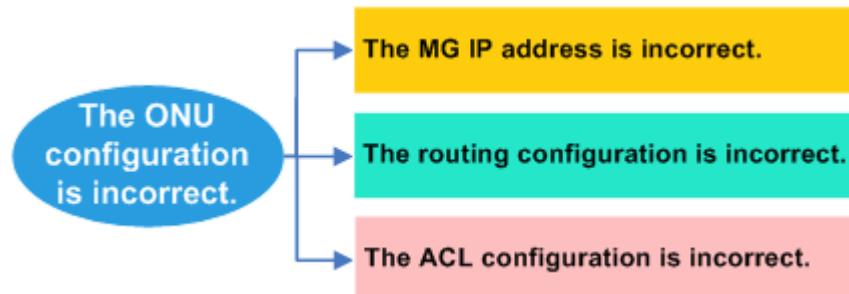
Determination Basis	Possible Cause
<ul style="list-style-type: none">Calls can be established between the users connected to an ONU.Calls can be established between the users connected to different ONUs that connect to the same OLT.Calls fail to be established between the users connected to different ONUs that connect to different OLTs.	<p>The OLT's upper-layer network is faulty.</p> <ul style="list-style-type: none">The ACL configuration of the IP network router, which functions as a trunk gateway (TG), is incorrect.The IP multimedia subsystem (IMS)/softswitch configuration is incorrect.

10.3.3.3 ONU Configuration Is Incorrect

Fault Locating Guide

If calls fail to be established between the users connected to an ONU, locate the fault following the guide in [Figure 10-21](#).

Figure 10-21 Fault locating guide



Procedure

Step 1 Run the **display ip address media** command on the ONU to check whether the MG IP address of the ONU is correct.

If the MG IP address is incorrect, run the **ip address media gateway** command to correct it.

Step 2 Run the **display ip routing-table** command on the ONU to check the IP routing configuration.

In the queried result, check whether the destination IP address of the ONU is contained in the IP network segment allocated by the TG. If it is out of the IP network segment, run the **ip route-static** command on the ONU to add a static route between the ONU and the TG. In this way, the TG can be pinged from the ONU.

Step 3 Run the **display acl all** command on the ONU to check the ACL configuration.

In the queried result, check whether there is an ACL rule filtering out downstream or upstream media streams. If there is, run the **undo rule** command on the ONU to cancel the ACL rule.

 **NOTE**

An ACL rule that has been issued to a port cannot be deleted. If such a rule must be deleted, run the **undo packet-filter** command on the ONU to cancel the ACL rule issuing.

----End

10.3.3.4 OLT ACL Configuration Is Incorrect

Procedure

If calls can be established between the users connected to an ONU, but fail to be established between the users connected to different ONUs that connect to the same OLT, the OLT ACL configuration is incorrect.

Run the **display acl all** command on the OLT to check whether there is an ACL rule filtering out downstream or upstream media streams. If there is, run the **undo rule** command on the OLT to cancel the ACL rule.

 **NOTE**

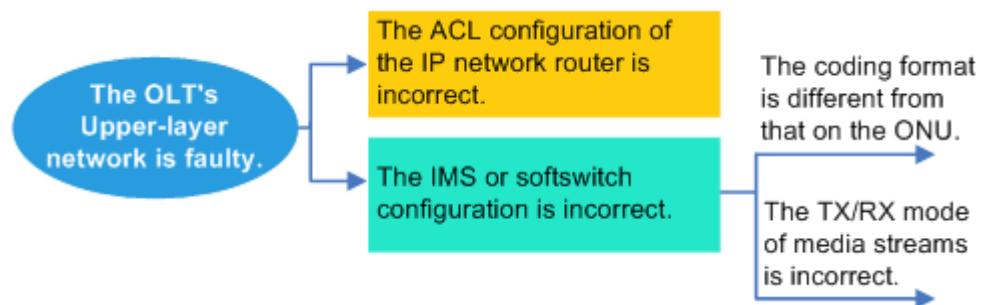
An ACL rule that has been issued to a port cannot be deleted. If such a rule must be deleted, run the **undo packet-filter** command on the OLT to cancel the ACL rule issuing.

10.3.3.5 OLT's Upper-Layer Network Is Faulty

Fault Locating Guide

If calls can be established between the users connected to an OLT, but fail to be established between the users connected to different OLTs, locate the fault following the guide in [Figure 10-22](#).

Figure 10-22 Fault locating guide



Procedure

Step 1 Check whether the ACL configuration of the IP network router is correct.

Check whether a UDP port number-based ACL has been configured on the IP network router. The ACL limits the UDP port range so that the UDP port range of

the IP network router is different from that of ONU media streams. If the ACL has been configured, cancel it on the IP network router.

Step 2 Check whether the IMS or softswitch configuration is correct.

Capture signaling packets on OLT uplink ports. Then, perform the following operations:

1. Check whether the preferential coding format supported by the IMS or softswitch is the same as that configured on the ONU. If they are different, contact the IMS or softswitch personnel to change the coding priority so that the preferential coding format contained in signaling packets is the same as that configured on the ONU.
2. Check whether the TX/RX mode of media streams is **sendrecv**. If it is not, contact the IMS or softswitch personnel to change the mode to **sendrecv**.

 **NOTE**

- In signaling packets, if the TX/RX mode of local media streams is **Sendonly** or **Inactive**, local users' media streams can only be sent, or neither received nor sent. In this case, local user ports do not process received media packets.
- In signaling packets, if the TX/RX mode of remote media streams is **Sendonly** or **Inactive**, remote users' media streams can only be sent, or neither received nor sent. In this case, remote user ports do not receive media packets.

----End

10.3.4 Noise Interference During Communication

There is noise interference during communication if a phone set is receiving strong current noises or broadcast noises during a call. This does not include the background noises of both the calling party and the called party.

10.3.4.1 Fault Identification and Demarcation

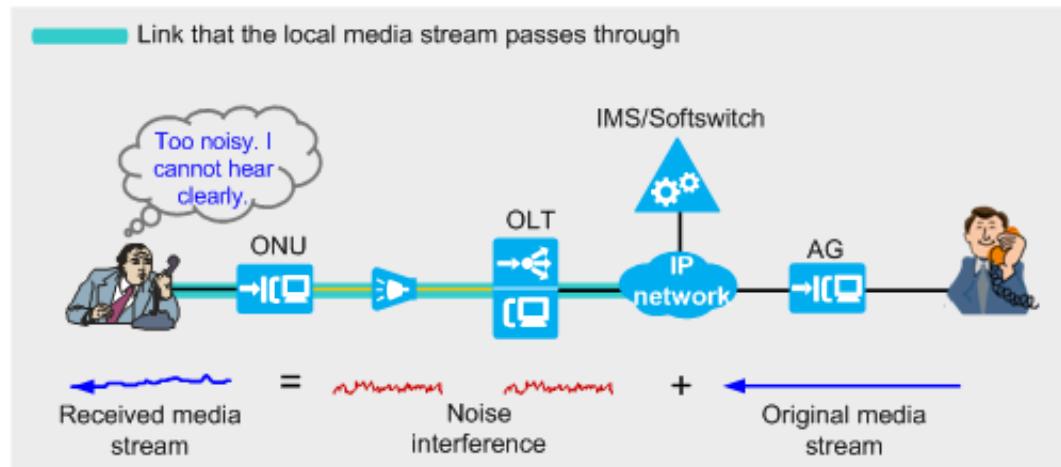
Overview

In voice communication, content is carried over media streams. If speakers experience noise interference during communication, there must be a fault affecting the link where the media stream passes through. Noise interference may be caused by:

- External electromagnetic interference (EMI)
- Power source or grounding
- Line fault

[Figure 10-23](#) shows how noise interference occurs.

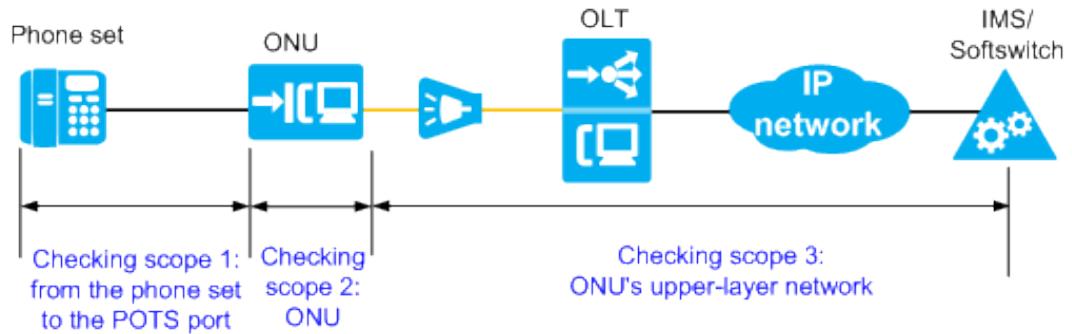
Figure 10-23 How noise interference occurs



Fault Demarcation

If noise interference occurs during communication, demarcate the fault segment by segment, as shown in [Figure 10-24](#).

Figure 10-24 Fault demarcation



Checking Scope	Fault Location	Possible Cause
1	Some ports on an ONU	<ul style="list-style-type: none"> The phone set is faulty. The loop line connected to the POTS port is faulty. The loop line connected to the POTS port has been externally interfered with. The configured electrical attributes of the POTS port do not comply with local usage requirements. Neither DSP input nor output gain comply with local usage requirements.

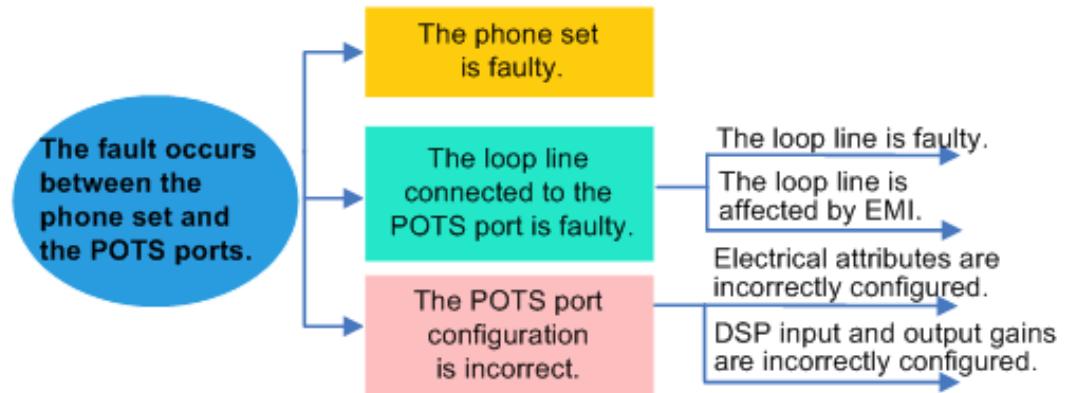
Checking Scope	Fault Location	Possible Cause
2	All ports on an ONU	<ul style="list-style-type: none"> Both the main distribution frame (MDF) and the ONU are insecurely grounded. The ONU is affected by EMI.
3	Ports on different ONUs connected to the same OLT	<ul style="list-style-type: none"> Packets were lost due to poor ODN fiber quality. Packets were lost due to poor fiber quality on the OLT's upper-layer network. The OLT is affected by EMI.

10.3.4.2 Fault Occurs Between the Phone Set and the POTS Port

Fault Locating Guide

If noise interference occurs during calls made or received by some users connected to an ONU, locate the fault following the guide in [Figure 10-25](#).

Figure 10-25 Fault locating guide



Procedure

Step 1 Check whether the phone set is faulty.

If the fault is rectified after the phone set is replaced, the fault must have been caused by the replaced phone set.

Step 2 Check whether the loop line connected to the POTS port of ONU is faulty.

Checking Method	Determination Basis	Handling Method
Run the pots loop-line-test command on the ONU to perform a loop line test for the affected port.	Typical test results are as follows: <ul style="list-style-type: none">If the test result is Normal, both the line and the phone set are functional.If the test result is Phone not connected, the phone set is faulty, or the line is insecurely connected between the phone set and the POTS port.If the test result is related to a line fault, such as B line grounding, the line is faulty. For more information about test results, see ONU POTS User Loop Line Test .	Rectify faults based on test results. For details, see ONU POTS User Loop Line Test .
Use a testing phone set in the equipment room to perform a loop line test.	No noise interference occurs if the phone set connects to the MDF. Therefore, the interference must have been caused by the loop line.	Check the loop line and verify that it is not affected by an EMI source, such as a broadcast transmitter or high-voltage power cable.

Step 3 Run the **display pstnport electric** command on the ONU to query the electrical attributes of the affected port.

- Electrical attributes include the impedance type, current type, TX gain, and RX gain. Check whether the attribute values of the affected port are the same as those of functional ports on the ONU. If at least one value is different, run the **pstnport electric set** command on the ONU to configure the electrical attributes of the affected port again.

 **NOTE**

To configure the electrical attributes of POTS ports in batches, run the **pstnport electric batset** command.

Electrical attribute configurations vary depending on countries and regions. Configured attributes must comply with local usage requirements. Configuring TX and RX gains is used as an example. The TX gain and RX gain of local networks and long-distance networks are generally 0 dB and -7 dB, respectively. In addition, electrical attribute settings must be the same on both interconnected POTS ports.

- Check whether the DSP input gain and output gains of the affected port are the same as those of functional ports on the ONU.

Protocol Type	Determination Basis	Handling Method
H.248	The DSP input and output gains of the affected port queried by running the display mgpstnuser attribute command are different from those of functional ports on the ONU.	Run the mgpstnuser attribute set frameid/slotid/portid dsp-input-gain dsp-input-gain-value dsp-output-gain dsp-output-gain-value command to configure the DSP input and output gains to be the same as those of functional ports.
SIP	The DSP input and output gains of the affected port queried by running the display sippstnuser attribute command are different from those of functional ports on the ONU.	Run the sippstnuser attribute set frameid/slotid/portid dsp-input-gain dsp-input-gain-value dsp-output-gain dsp-output-gain-value command to configure the DSP input and output gains to be the same as those of functional ports.

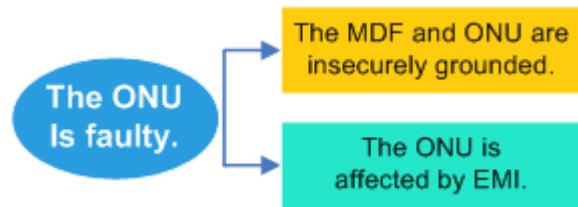
----End

10.3.4.3 ONU Is Faulty

Fault Locating Guide

If noise interference occurs during calls made or received by all users connected to an ONU, locate the fault following the guide in [Figure 10-26](#).

Figure 10-26 Fault locating guide



Procedure

Step 1 Check the equipment room environment, MDF, and ONU, as well as the grounding of the MDF and ONU onsite.

The following requirements are used as an example:

- The ONU grounding complies with national and industrial usage requirements.
- The connection points on both ends of the PGND cable are in reliable electric contact.

Step 2 Eliminate EMI sources so that the ONU is EMI-free.

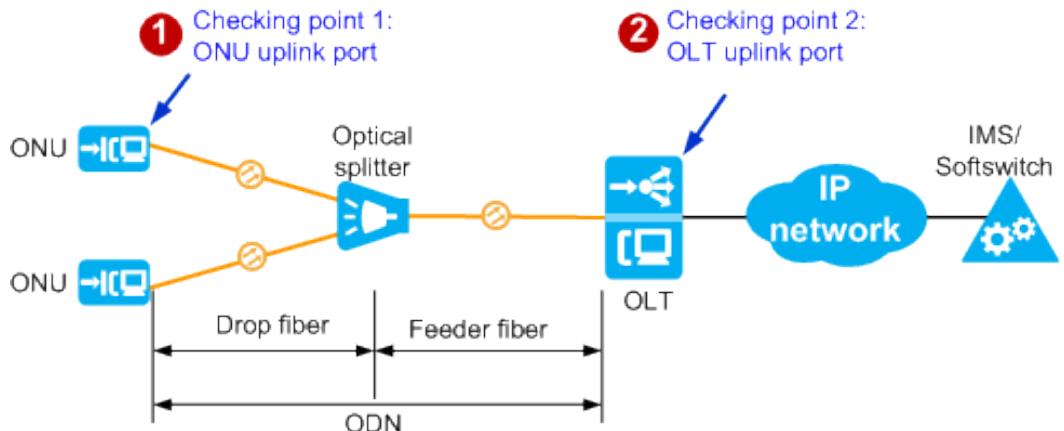
----End

10.3.4.4 ONU's Upper-Layer Network Is Faulty

Determining the Fault

If noise interference occurs during calls made or received by the users connected to different ONUs that connect to the same OLT, the fault must have occurred on the ONUs' upper-layer network. Identify the location where packets were lost to determine the fault, as shown in [Figure 10-27](#).

Figure 10-27 Determining the fault



Determination Basis	Possible Cause
Packets were lost on the ONU uplink port but were not lost on the OLT uplink port.	<p>ODN fiber quality is so poor that packets were lost, leading to noise interference during communication.</p> <p>NOTE User experience varies depending on packet loss scenarios. For example, users will experience noise interference if packets are frequently lost.</p>
Packets were lost on the OLT uplink port.	<p>Fiber quality on the OLT's upper-layer network is so poor that packets were lost, leading to noise interference during communication.</p> <p>NOTE User experience varies depending on packet loss scenarios. For example, users will experience noise interference if packets are frequently lost.</p>
Packets were not lost on both the ONU and OLT uplink ports.	The OLT is affected by EMI.

Procedure

Step 1 Check whether ODN fiber quality is poor.

- Poor feeder fiber quality prevents service provisioning on all ONUs connected to one PON port.
- Poor drop fiber quality prevents service provisioning on one ONU.

For details about troubleshooting, see [5.6 Methods of Locating and Troubleshooting Common ODN Faults](#).

Step 2 Check whether fiber quality on the OLT's upper-layer network is poor.

1. Check whether the OLT's upstream optical module is faulty. An OLT equipped with an ETH board for upstream transmission is used as an example here. Run the **display port ddm-info** command to query diagnosis information about the optical module installed on the uplink port. Both TX and RX optical power is generally -5 dBm. If the queried value is significantly different from this value, the optical path is unreachable and needs to be checked.
2. Check the fiber quality and perform the following operations:
 - Check whether the optical fiber is securely connected to the PON port and whether the connector is clean.
 - Connect the optical fiber to the PON port again. Alternatively, replace it.

Step 3 Check whether the OLT is affected by EMI.

Eliminate EMI sources so that the OLT is EMI-free.

----End

10.3.5 Poor Voice Service During Communication

Poor voice service occurs when a call is established, but one party can only hear the peer party's voice intermittently.

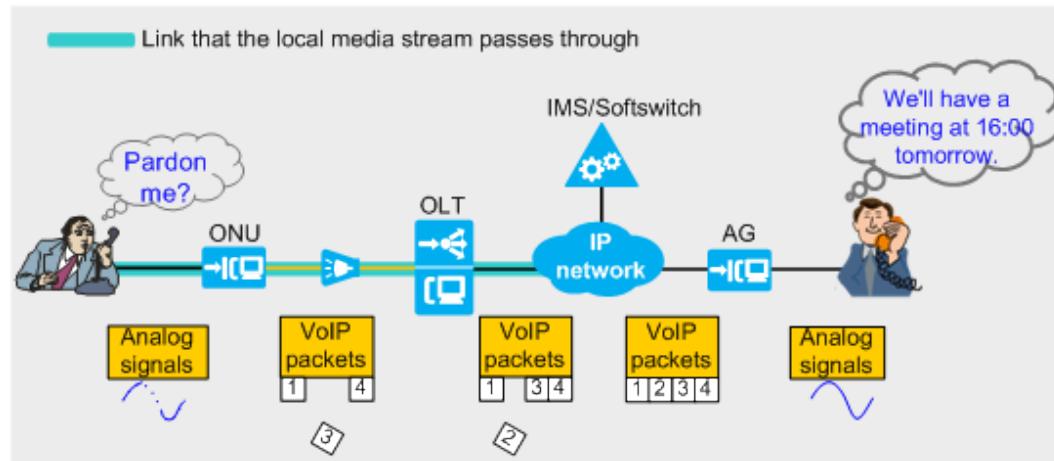
10.3.5.1 Fault Identification and Demarcation

Overview

In voice communication, content is carried over media streams. Therefore, if media packets are lost, the voice service is poor.

On the network shown in [Figure 10-28](#), analog signals are transmitted between the phone set and the ONU, and VoIP packets are transmitted between the ONU and the peer AG device. If packets are lost, some communication content is also lost, leading to voice intermittence. The link that the local media stream passes through carries data exchanged between the phone set and the IP network. Any packet loss that occurs in any segment of the link will lead to poor voice service.

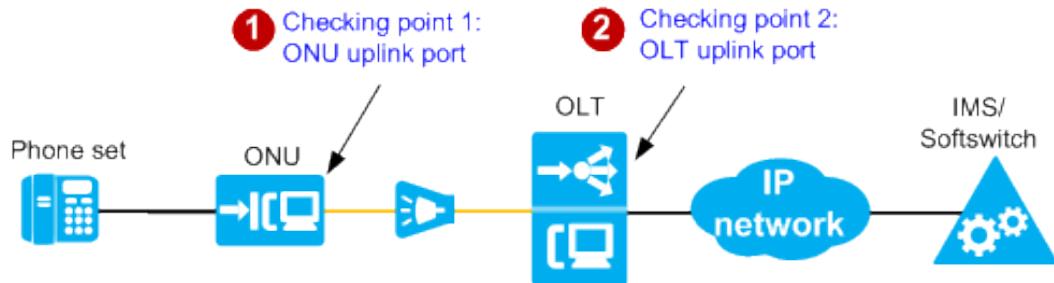
Figure 10-28 Demonstration of poor voice service



Fault Demarcation

If voice service is poor, identify the location where packets were lost to demarcate the fault, as shown in **Figure 10-29**.

Figure 10-29 Fault demarcation



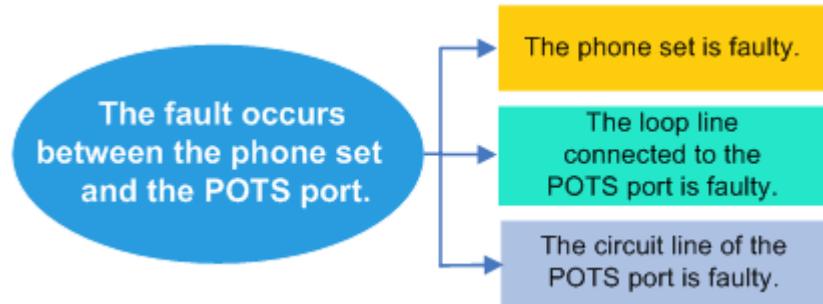
Checking Point	Determination Basis	Possible Cause
1	Packets were lost on the ONU uplink port.	<ul style="list-style-type: none"> The phone set is faulty. The loop line connected to the POTS port is faulty. The circuit line of the POTS port is faulty. The ONU QoS configuration is incorrect.
2	Packets were lost on the ONU uplink port while not on the OLT uplink port.	Packets were lost due to poor ODN fiber quality.
	Packets were lost on the OLT uplink port.	The OLT's upper-layer network is faulty.

10.3.5.2 Fault Occurs Between the Phone Set and the POTS Port

Fault Locating Guide

If voice service is poor during calls made or received by some users connected to an ONU, locate the fault following the guide in [Figure 10-30](#).

Figure 10-30 Fault locating guide



Procedure

Step 1 Check whether the phone set is faulty.

If the fault is rectified after the phone set is replaced, the fault must have been caused by the replaced phone set.

Step 2 Check whether the line between the phone set and the POTS port of ONU is faulty.

Run the **pots loop-line-test** command on the ONU to perform a loop line test for the line. The following terminal display is used as an example:

```
huawei(config-test)#pots loop-line-test 0/2/1
huawei(config-test)#
Testing port: 0/2/1
Telno : -
-----
Test conclusion : AB all break off or no phone connected \\Test result
-----
Line state          AB all break off or no phone connected
Line length
Line A 0 m
Line B 0 m
PPA                No PPA between A,B line
Termination type   Invalid
-----
Test parameter item      Value      Validity
-----
Primary test result parameter:
A->ground AC voltage      0.000 V    Valid
B->ground AC voltage      0.000 V    Valid
A->B AC voltage           0.000 V    Valid
A->ground AC Frequency    0     Hz    Invalid
B->ground AC Frequency    0     Hz    Invalid
A->B AC Frequency         0     Hz    Invalid
A->ground DC voltage      0.140 V    Valid
B->ground DC voltage      0.130 V    Valid
A->B DC voltage           0.013 V    Valid
A->ground insulation resistance 4.771 MΩ  Valid
B->ground insulation resistance 6.091 MΩ  Valid
A->B insulation resistance(Low voltage) 10.000 MΩ  Valid
B->A insulation resistance(Low voltage) 10.000 MΩ  Valid
```

A->B insulation resistance(High voltage)	0	Ω	Invalid
B->A insulation resistance(High voltage)	-		Not support
A->ground capacitance	0	nF	Valid
A->ground capacitance	0	nF	Valid
A->B capacitance(Low voltage)	0	nF	Valid
A->B capacitance(High voltage)	0	nF	Invalid
<hr/>			
Secondary test result parameter:			
A->ground conductance	1.070	uS	Valid
B->ground conductance	0.857	uS	Valid
A->B conductance(Low voltage)	0.000	uS	Valid
A->B conductance(High voltage)	-		Not support
A->ground susceptance	1.014	uS	Valid
B->ground susceptance	-3.093	uS	Valid
A->B susceptance(Low voltage)	-0.027	uS	Valid
A->B susceptance(High voltage)	-		Not support
A->ground DC current	0	uA	Valid
B->ground DC current	0	uA	Valid
A->B DC current	0	uA	Valid
B->A DC current	0	uA	Valid
A->ground AC current	0	uA	Valid
B->ground AC current	0	uA	Valid
A->B AC current	0	uA	Valid
B->A AC current	0	uA	Valid
<hr/>			
Test auxiliary parameter:			
Test frequency for admittance	-		Not support
Resistance to test the abnormal voltage	-		Not support
Max. voltage to conduct the signature	-		Not support
A->ground max. voltage	-2.647	V	Valid
A->ground min. voltage	-48.520	V	Valid
B->ground max. voltage	-2.626	V	Valid
B->ground min. voltage	-48.640	V	Valid
A->B max. voltage	47.040	V	Valid
A->B min. voltage	-46.870	V	Valid
A->ground max. current	-21	uA	Valid
A->ground min. current	-76	uA	Valid
B->ground max. current	130	uA	Valid
B->ground min. current	74	uA	Valid
A->B max. positive current	112	uA	Valid
A->B max. negative current	57	uA	Valid

Typical test results and handling methods are as follows:

- If the test result is **Normal**, both the line and the phone set are functional.
- If the test result is **Phone not connected**, the phone set is faulty, or the line is insecurely connected between the phone set and the POTS port. In this case, rectify the phone set fault, or securely connect the line between the phone set and the POTS port.
- If the test result is related to a line fault, such as **B line grounding**, the line is faulty. In this case, handle the fault based on the test result. For example, **B line grounding** indicates that wire B may be damaged. In this case, replace the line.

For more information about test results and handling methods, see **ONU POTS User Loop Line Test**.

Step 3 Check whether the circuit line of the POTS port of ONU is faulty.

Run the **pots circuit-test** command on the ONU to perform a circuit test for the affected port. If the value of the **Low Battery** or **Loop current** parameter is **Abnormal**, the POTS port is faulty. In this case, connect the phone set to a functional POTS port.

```
huawei(config-test)#pots circuit-test mgid 0 terminalid 1
huawei(config-test)#
Testing port: 0/2/1
Telno      : -
MGid      : 0
Terminalid : A1
-----
Test item          Result
-----
Digital Voltage:   Normal
Low Battery:       Abnormal
High Battery:      Normal
Positive Battery:  Normal
Loop current:      Abnormal
Feeder voltage:    Normal
Ringing current voltage: Normal
Ringing current frequency: Normal
VAG:               Normal
VBG:               Normal
-----
```

----End

10.3.5.3 ONU QoS Configuration Is Incorrect

Fault Locating Guide

If voice service is poor during calls made or received by all users connected to an ONU, the QoS priorities of the voice service have been set too low on the ONU, causing packet loss.

Procedure

Run the **display qos ip** and **display qos vlan** commands on the ONU to query the QoS priorities set for the voice service. If the priorities are set too low, run the **qos ip** and **qos vlan** commands to change the IP and VLAN priorities, respectively, for media and signaling packets to 6.

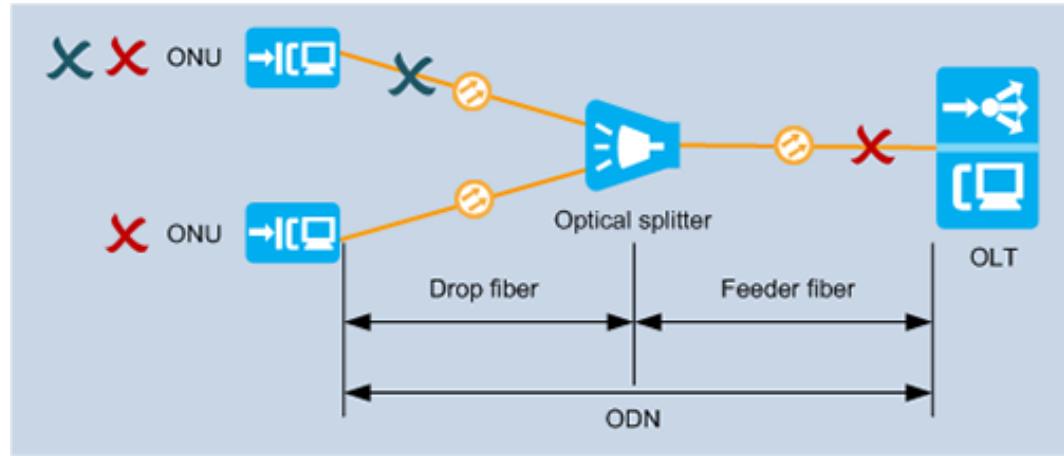
NOTE

- QoS priorities range from 0 to 7. A value of 7 indicates the highest priority. When network congestion occurs, the packets with a low QoS priority are preferentially discarded.
- Voice services have strict QoS requirement on networks. Huawei suggests that customers set the QoS priorities for VoIP packets to 6 on the ONU.

10.3.5.4 ODN Fiber Quality Is Poor

Fault Locating Guide

The network between a PON port on an OLT and ONUs is shown in the following figure.



In the preceding figure,

- Poor feeder fiber quality prevents service provisioning on all ONUs connected to the PON port.
- Poor branch fiber quality prevents service provisioning on one ONU.

Troubleshooting

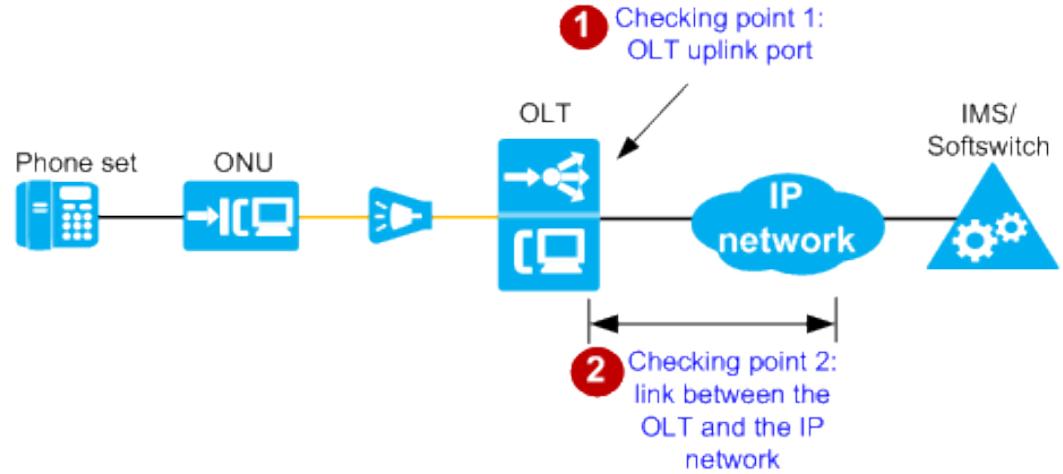
See [5.6 Methods of Locating and Troubleshooting Common ODN Faults](#).

10.3.5.5 OLT's Upper-Layer Network Is Faulty

Fault Locating Guide

If packets were lost on the OLT uplink port, locate the fault following the guide provided in [Figure 10-31](#).

Figure 10-31 Fault locating guide



Checkin g Point	Affected Scope	Determination Basis
1	OLT uplink port	<ul style="list-style-type: none">• There is an uplink port malfunction.• There is an optical module malfunction on the uplink port.
2	Link between the OLT and the IP network	Packets were lost on the link.

Procedure

Step 1 Check whether the optical module installed on the uplink port of the OLT is functional.

1. Check whether the uplink port is functional.

An OLT equipped with an ETH board for upstream transmission is used as an example here. Run the **display port state all** command to query the uplink port status.

The value of the **Optic Status** parameter specifies the optical module status.

- **absence**: indicates that the optical module is not securely installed.
- **abnormal**: indicates that the optical module is faulty.
- **mismatch**: indicates that the optical module does not match the uplink port.
- **normal**: indicates that the optical module is securely installed.

2. Run the **display port ddm-info** command to query diagnosis information about the optical module.

Both TX and RX optical power is generally -5 dBm. If the queried value is significantly different from this value, the optical path is unreachable and needs to be checked.

Step 2 Check fiber quality on the upper-layer network.

Ping the network IP from the OLT. If packets are lost, perform the following operations:

- Check whether the optical fiber is securely connected to the PON port and whether the connector is clean.
- Connect the optical fiber to the PON port again. Alternatively, replace it.

----End

11

Troubleshooting the FTTM Services

If services are interrupted when the device is running, you can troubleshoot faults according to the following troubleshooting procedures.

11.1 Ethernet Access Services

The ONU supports base station data transmission services using Ethernet access.

11.2 Abnormal PoE Power Supply

This section describes how to resolve the issue that a power sourcing equipment (PSE) fails to supply power to a powered device (PD).

11.1 Ethernet Access Services

The ONU supports base station data transmission services using Ethernet access.

Fault Location

Use the following guidelines to locate the fault:

Fault Scope	Possible Causes
Link between the base station and the ONU	<ul style="list-style-type: none">The line between the base station and the ONU is faulty.Port negotiation between the base station and the ONU failed.The data configurations of the ONU are incorrect.
Link between the ONU and the OLT	The line between the ONU and the OLT is faulty.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check whether the line between the ONU and the OLT is faulty.

Run the **display alarm history** command on the OLT to query alarms associated with the line. If an alarm, such as **The distribute fiber is broken or OLT can not receive expected optical signals from GPON ONT(LOSi)** is generated, the line quality is poor. Check whether any of the following is true:

- The transmit power of the upstream PON port on the ONU is wrong.
- The optical distribution network (ODN) plan is wrong. Specifically, the optical split ratio is too large, the reach is too long, or the signal is too attenuated.
- The optical fiber is bent severely.
- The types of the optical fiber connectors do not match each other.
- The optical fiber connector is dirty.

Step 2 Check whether the data configuration of the ONU is correct.

1. Run the **display service-port** command to query the service port configuration. Check whether the VLAN ID and port ID match the data plan.

If the parameters do not match the data plan, perform the following operations to modify them:

- Run the **undo service-port** command to delete the original service port.
- Run the **service-port** command to create a service port according to the data plan.

2. Run the **display port vlan** command to check whether the upstream port has been added to the upstream VLAN.

If the upstream port has not been added to the upstream VLAN, run the **port vlan** command to add it to the upstream VLAN.

Step 3 Check the Ethernet port parameter settings on the base station and the ONU.

- Run the **display port state** command to query the Ethernet port parameter settings on the ONU. The parameters include port auto-negotiation mode and network cable auto-sensing mode.
- Check whether the Ethernet port parameter settings on the ONU match those on the peer video monitor. If they do not match, perform the following operations to modify the settings on the ONU:
 - Run the **auto-neg** command to enable or disable the auto-negotiation mode of the Ethernet port.
 - Run the **duplex** command to set the duplex mode of the Ethernet port.
 - Run the **speed** command to set the Ethernet port rate.
 - Run the **mdi** command to set the network cable auto-sensing mode of the Ethernet port.

Step 4 Check whether the line between the base station and the ONU is functional.

Run the **display port statistics** command at least 10 times to query the Ethernet port statistics every 20 seconds. Check whether **Number of CRC error frames** increases during testing. If it increases, the line is faulty. Check whether any of the following is true:

- The network cable is old or short-circuited.
- The connectors at the end of the network cable are loose or in poor contact.
- The signal is too attenuated because the network cable is too long.

Step 5 Contacting Huawei for Assistance.

Step 6 End.

----End

11.2 Abnormal PoE Power Supply

This section describes how to resolve the issue that a power sourcing equipment (PSE) fails to supply power to a powered device (PD).

Context

The PoE system consists of a PSE and PDs.

- A PSE supplies power to other devices in the PoE system, which is a power source.
- A PD receives power in the PoE system. A PD does not have its own power supply and can work only after being powered by the PSE through an Ethernet port.

Location Method

When a PSE fails to supply power to a PD, use the following guidelines to locate the fault.

1. Check whether the network cable is functional and whether the pin assignments of the network cable are correct.
2. Check whether the distance between the PSE and the PD is excessively long.
3. Check whether the PSE and the PD are grounded.
4. Check whether the PD is a standard PD.
5. Check whether the power supplied by the PSE is lower than PD usage requirements.

Procedure

Step 1 Replace the damaged cable or correct the pin assignments.

- Ensure that the cable electrical specifications comply with enhanced category 5 cable requirements.
- If the PD power is lower than 15 W, the cable loop resistance must be less than 40 ohms. If the PD power is greater than 15 W, the cable loop resistance must be less than 25 ohms.
- Ensure that the pin assignments comply with the following international requirements.
 - For the PSE:

- Signal loop feeding: mode A (alternative A); pin assignments: 1/2 and 3/6
- Idle loop feeding: mode B (alternative B); pin assignments: 4/5 and 7/8
- For the PD:
 - Signal loop feeding: mode A (alternative A); pin assignments: 1/2 and 3/6
 - Idle loop feeding: mode B (alternative A); pin assignments: 4/5 and 7/8

 **NOTE**

Only the pin assignment combinations 1/2 and 3/6 as well as 4/5 and 7/8 can be used, regardless of whether mode A or B is used.

Step 2 The maximum reliable distance between a PSE and a PD is 100 m. Shorten the distance to be less than 100 m.

Step 3 Securely ground the PSE and the PD to prevent the PSE from being interfered with external voltage during detection and maintenance so that the PSE can classify the PDs and stably supply the PDs.

Step 4 Run the **poe legacy** command to enable PD compatibility check.

```
huawei(config-if-eth-0/1)#poe legacy
```

 **NOTE**

According to IEEE 802.3af, the capacitance of a standard PD is less than 150 nF. On the live network, the capacitance of some PDs ranges from 150 nF to 10 uF. The PD compatibility check enables the PSE to support these PDs as standard PDs for classification and power-on.

Step 5 Run the **display poe** command to query PoE status.

```
huawei(config-if-eth-0/1)#display poe
{ all<K>|portid<U><0,3>|powersupply<K> }1

Command:
    display poe 1

-----
Port power switch      :enable
Port power mode        :signal
Port power priority    :low
Port max power(mW)    :30000
Port force-power       :disable
Port poe status        :enable
Port power status      :Powered //Port power status
Port PD class          :4
Port current power(mW) :7008
Port average power(mW) :6806
Port peak power(mW)   :7186
Port current(mA)       :120.849
Port voltage(V)        :57.994
Last power-on fail time :2013-05-26 13:34:56+08:00
Last power-on fail reason:PD detection failure (excessively large resistance)
Last power-off time    :-
Last power-off reason  :-
```

Step 6 Run the **display poe power-on failure info** and **display poe power-off info** commands to query PoE power-on failures and power-off records.

```
huawei(diagnose)%%display poe power-on failure info
{ frameid/slotted/portid<S><Length 1-15> }:0/1/1
Command:
    display poe power-on failure info 0/1/3
-----
sn      time            reason
-----
1       2013-05-24 09:46:25+08:00 invalid PD(resistance too high)
2       2013-05-24 09:46:24+08:00 invalid PD(resistance too high)
3       2013-05-24 09:46:22+08:00 invalid PD(resistance too high)
4       2013-05-24 09:46:21+08:00 invalid PD(resistance too high)
5       2013-05-24 09:46:19+08:00 invalid PD(resistance too high)
6       2013-05-24 09:46:18+08:00 invalid PD(resistance too high)
7       2013-05-24 09:46:17+08:00 invalid PD(resistance too high)
8       2013-05-24 09:46:16+08:00 invalid PD(resistance too high)
9       2013-05-24 09:43:59+08:00 invalid PD(resistance too high)
10      2013-05-24 09:43:58+08:00 invalid PD(resistance too high)

huawei(diagnose)%%display poe power-off info
{ frameid/slotted/portid<S><Length 1-15> }:0/1/1
Command:
    display poe power-off info 0/1/1
-----
sn      time            reason
-----
1       2013-05-26 09:45:57+08:00 port power disabled
```

Rectify the fault based on the power-on failure or power-off causes.

Power-on Failure Cause	Troubleshooting Suggestion
PD detection failure: open circuit	Check lines or replace the PD.
PD detection failure: short circuit	Check lines or replace the PD.
PD detection failure: excessively large capacitance	Check the configuration and enable PD compatibility check.
PD detection failure: excessively large resistance	Replace the PD.
PD classification failure: unknown classification	Enable PD compatibility check, check lines, or replace the PD.
PD classification failure: port overcurrent during classification	Enable PD compatibility check, check lines, or replace the PD.
Greater reference power than the preset power	Adjust the maximum port power or replace the PD with a lower-power PD.
Disabled port power supply	Adjust the priority of port power supply or replace the PD with a lower-power PD.
Insufficient system power	Check the configuration and enable port power supply.
Faulty PoE chip	Replace the PoE chip.
PD disconnection	Check lines or replace the PD.
Port overcurrent	Check lines or replace the PD.

Power-on Failure Cause	Troubleshooting Suggestion
Power-on timeout	Enable PD compatibility check, check lines, or replace the PD.

----End

12

Troubleshooting the D-CCAP Service

OptiCable Distributed-Converged Cable Access Platform (D-CCAP) meets the requirements of triple-play network services over hybrid fiber coaxial (HFC) networks of multiservice operators (MSOs) because of unique advantages of the D-CCAPs, such as high bandwidth and supporting HFC networks. This topic describes how to troubleshoot common faults in Internet access and multicast (IPTV) services in the radio frequency (RF) access mode.

12.1 Service Troubleshooting

Describes how to rectify common faults.

12.2 Fault Cases

This section describes common troubleshooting processes.

12.1 Service Troubleshooting

Describes how to rectify common faults.

12.1.1 NMS Fails to Manage a Device

If the NMS fails to manage the device, it means that the NMS loses control over the ONU.

Location Method

When the NMS fails to manage the ONU, locate the fault according to the following procedure:

1. Check the fault scope.
2. Check whether the ONU can ping the IP address of the NMS server.
3. Check whether NMS parameter configurations of the ONU and the NMS server are correct.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Check whether the same NMS fails to manage other devices, that is, whether the fault occurs in a large scale.
- If the same NMS fails to manage other devices, go to **Step 2**.
 - If the same NMS can manage other devices, go to **Step 4**.
- Step 2** Check whether the NMS version matches the device version.
- If the NMS version matches the device version, go to **Step 4**.
 - If the NMS version does not match the device version, upgrade NMS version or device version so that the NMS version matches the device version. Then, go to **Step 3**.
- Step 3** Check whether the fault is rectified.
- If the fault is rectified, go to **Step 12**.
 - If the fault persists, go to **Step 4**.
- Step 4** Run the **ping** command to ping the IP address of the NMS server.
- If the device can ping the IP address of the NMS server, go to **Step 10**.
 - If the device cannot ping the IP address of the NMS server, go to **Step 5**.
- Step 5** Run the **display ip routing-table** command to check whether there is a route from the ONU to the NMS server.
- If there is a route from the ONU to the NMS server, go to **Step 7**.
 - If there is not a route from the ONU to the NMS server, run the **ip route-static** command to add a static route from the ONU to the NMS server. Then, go to **Step 6**.
- Step 6** Check whether the fault is rectified.
- If the fault is rectified, go to **Step 12**.
 - If the fault persists, go to **Step 7**.
- Step 7** Run the **display arp** command to check on the ONU whether the ARP information about the NMS exists in the ARP mapping table.
- If the ARP information about the NMS exists in the ARP mapping table, go to **Step 10**.
 - If no ARP information about the NMS exists in the ARP mapping table, go to **Step 8**.
- Step 8** Check whether the upper layer device of the ONU learns the MAC address of the L3 interface of the ONU.
- If the upper layer device of the ONU learns the MAC address of the L3 interface of the ONU, go to **Step 10**.
 - If the upper layer device of the ONU does not learn the MAC address of the L3 interface of the ONU, go to **Step 9**.
- Step 9** Check the physical link between the ONU and the upper layer device. Ensure that the communication between the ONU and the upper layer device is normal. Then, check whether the fault is rectified.
- If the fault is rectified, go to **Step 12**.

- If the fault persists, go to **Step 10**.

Step 10 Check NMS parameter configurations of the ONU and the NMS. Make sure that NMS parameter configurations are correct. Then, check whether the fault is rectified.

- If the fault is rectified, go to **Step 12**.
- If the fault persists, go to **Step 11**.

 **NOTE**

The following configurations need to be checked.

- Run the **display snmp-agent sys-info** command to check whether the SNMP version of the device is consistent with that of the NMS. If they are different, run the **snmp-agent sys-info** command to set them to be consistent.
- Run the **display snmp-agent community read** command to check whether the read community name of the device is the same as that of the NMS. If they are inconsistent, run the **snmp-agent community read** command to modify the read community name of the device to be the same as that of the NMS.
- Run the **display snmp-agent community write** command to check whether the write community name of the device is the same as that of the NMS. If they are inconsistent, run the **snmp-agent community write** command to modify the write community name of the device to be the same as that of the NMS.
- Run the **display snmp-agent target-host** command to check whether the IP address of the NMS server is included in the target host list for traps. If the IP address of the NMS server is not included in the target host list for traps, run the **snmp-agent target-host trap-hostname** command to add the NMS server to the target host list for traps.
- Run the **display snmp-agent trap enable** command to check whether traps can be sent to the NMS from the device. If it is **disable**, run the **snmp-agent trap enable** command to enable trap sending from the device to the NMS.
- Run the **display snmp-agent mib-view** command to query whether the configured MIB view contains ISO sub-trees. If no MIB view is configured and it is needed, run the **snmp-agent mib-view** command to configure it.
- (Optional) If SNMPv3 is used, run the **display snmp-agent group** command to check whether the information about an SNMPv3 work group is correct. If the information is incorrect, run the **snmp-agent group** command to configure the correct information.
- (Optional) If SNMPv3 is used, run the **display snmp-agent usm-user** command to check whether the information about an SNMPv3 user is correct. If the information is incorrect, run the **snmp-agent usm-user** command to add or modify the SNMPv3 user.

For detailed configuration method, see the corresponding Command Reference.

Step 11 Contacting Huawei for Assistance.

Step 12 End.

----End

12.1.2 Unexpected Reset of the System

This topic describes how to troubleshoot unexpected reset of the system. When the system is reset unexpectedly, all services carried on the device are interrupted and the device cannot be managed by the network management system (NMS).

Location Method

Use the following guidelines to locate the fault:

1. Check whether the user has issued a command to reset the device.
2. Check whether the power supply for the device is normal.
3. Check whether the device temperature is within the acceptable range.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Run the **display log all** command to check whether the user has issued a command to reset the device.
- If the device is reset following the execution of a reset command, go to [Step 5](#).
 - If no command has been issued to reset the device, go to [Step 2](#).

 **NOTE**

For example, the device displays the following information in the output of the **display log all** command.

```
No. UserName          Domain      IP-Address
343 root              --          192.168.0.10
Time: 2016-12-11 00:00:02+08:00
Cmd: reboot system
```

If the time when the system is unexpectedly reset is the same as the time when the system reset log is recorded, the user has issued a command to reset the system.

- Step 2** Check whether the power supply for the device is normal.

1. Check whether the power supply for the device has been cut off.
 - If the power supply for the device has been cut off, the system reset is caused by the power cutoff. Go to [Step 5](#).
 - If the power supply for the device has always been normal, go to [Step 2.2](#).
2. Check whether the voltage of the device is normal.
 - If the voltage of the device is normal, go to [Step 3](#).
 - If the voltage of the device is too low, the device may be reset. Go to [Step 5](#).

- Step 3** Check whether the device temperature is too high.

- If the device temperature is too high, the system will be automatically reset to protect system components from being burnt out. Go to [Step 5](#).
- If the device temperature is within the range, go to [Step 4](#).

- Step 4** Contacting Huawei for Assistance.

- Step 5** End.

----End

12.1.3 Failure to Automatically Discover a CMC in the Extended Subrack

Under aggregation management, after a coaxial media converter (CMC) in the extended subrack is connected to the OLT, the OLT cannot automatically discover the CMC.

Problem Diagnosis

The following table describes the diagnosis criteria and possible causes based on the fault scope.

Fault Scope	Diagnosis Criterion	Possible Cause
OLT	A single CMC in the extended subrack cannot be automatically discovered.	<ul style="list-style-type: none">• The CMC is not authenticated.• The distance between the CMC and the OLT is beyond the ranging compensation distance range configured on the OLT.• No extended subrack software is configured in the flash memory of the OLT. Agent loading is configured on the host, and the agent loading server is not configured with extended subrack software.
	All CMCs in the extended subrack under the passive optical network (PON) port cannot be automatically discovered.	<ul style="list-style-type: none">• The ONU automatic discovery function is disabled on the PON port.• The laser on the PON port is disabled.• The PON port is faulty.• The pluggable optical module of the PON port is faulty.
	All CMCs in the extended subrack under the board cannot be automatically discovered.	<ul style="list-style-type: none">• The Ethernet board of the extended subrack is connected to the OLT, but the board is not in extended mode.• The board or slot is faulty.

Fault Scope	Diagnosis Criterion	Possible Cause
Optical distribution network (ODN)	5.6.2 ODN-Related Alarms are generated at the PON port, for example, 0x2e11a001 "The backbone fiber is broken or the OLT cannot receive expected optical signals (LOS)".	<p>ODN failures generally occur due to large reflection and attenuation caused by improper design, construction, or optical component selection. For details, see 5.6.1 Common ODN Faults.</p> <ul style="list-style-type: none"> If a single CMC or some CMCs cannot be automatically discovered, the branch fiber or the optical component may be faulty. If all CMCs under the PON port cannot be automatically discovered, the backbone fiber and the optical component may be faulty.
CMC	A single CMC or some CMCs cannot be automatically discovered.	<ul style="list-style-type: none"> The CMC is not powered on. A rogue ONU affects the proper operating of other ONUs. The CMC encounters a hardware fault. The optical module of the CMC is faulty. Authentication information (SN or password) of multiple CMCs conflicts. Therefore, CMCs that are powered on later cannot get online. The pigtail of the CMC is broken or subject to excessive bending. The CMC is incorrectly connected to another PON port.
	The OLT successfully discovers a single CMC or some CMCs in the extended subrack, but the discovery fails later.	<ul style="list-style-type: none"> The CMC is not compatible with the OLT. The package file of the OLT does not contain board software for the CMC. The CMC resets repeatedly because automatic loading fails. The extended subrack does not operate properly because a board in the extended subrack is faulty.

NOTICE

To facilitate fault report, save the results of the following steps.

Optical module parameters in this topic comply with the Class B+ standard. Note that such parameters are slightly different from the parameters complying with the Class C+ standard.

Procedure

- Step 1** If the CMC still cannot be automatically discovered after OLT problems are resolved, proceed to **Step 2**.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
The ONU automatic discovery function is disabled on the PON port.	Run the display port info command to query the information about the PON port. It is found that Autofind is in the Disable state.	Run the port ont-auto-find command to enable the ONU automatic discovery function of the PON port. NOTE By default, the ONU automatic discovery function is disabled on the PON port.
The distance between the CMC and the OLT is beyond the ranging compensation distance range configured on the OLT.	Run the display port info command to query the minimum ranging compensation distance (Min distance) and maximum ranging compensation distance (Max distance) configured for the PON port. It is found that the distance between the CMC and the OLT is beyond the ranging compensation distance range. For example, the length of the optical fiber between the CMC and the OLT is about 25 km, which is beyond the ranging compensation distance range of 0–20 km.	Run the port range command to adjust the minimum and maximum ranging compensation distances, to ensure that the distance between the CMC and the OLT is within the ranging compensation distance range. NOTE <ul style="list-style-type: none">• By default, the ranging compensation distance range of a gigabit-capable passive optical network (GPON) port is 0–20 km.• According to the Class B+ standard, the maximum ranging compensation distance of a GPON port must be less than or equal to 60 km, and the difference between the minimum ranging compensation distance and the maximum ranging compensation distance must be less than or equal to 20 km.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
The laser on the PON port is disabled.	Run the display port info command to query the information about the PON port. It is found that Laser switch is in the Off state.	Run the port portid laser-switch command to enable the laser on the PON port. NOTE By default, the laser on a GPON port is enabled.
The PON port is faulty.	The PON port is faulty if either of the following conditions is met: <ul style="list-style-type: none"> Run the display port state command to query the status of the PON port. Abnormal items are found in the query result. For example, the optical module status (Laser state) is abnormal, or the transmit optical power (TX power) is beyond the normal range. The CMC can be automatically discovered after services are migrated to other ports. 	Replace the optical module or the board.
An incorrect type of optical module is connected to the PON port.	Run the display port state command to query the status of the PON port. If the value of encoding is NRZ , the optical module applies to a GPON port; if the value of encoding is 10B8B , the optical module applies to an EPON port.	Replace the optical module.
The board or slot is faulty.	Run the display board command to check the board status. The board is not in the Normal state.	Run the board reset command to reset the board or insert the board in another slot. If the problem persists, replace the board. NOTE For the detailed procedure, see Service Board Is in the Failed State.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
The Ethernet board of the extended subrack is connected to the OLT, but the board is not in extended mode.	Enter the ETHB board interface mode and run the display network-role command. It is found that the board is not in extended mode.	Enter the Ethernet board interface mode and run the network-role extend-mode command to switch the board to the extended mode.

Step 2 If the CMC still cannot be automatically discovered after ODN problems are resolved, proceed to [Step 3](#).

Possible Cause	Diagnosis Criterion	Troubleshooting Method
<p>The optical fiber connector is not clean.</p> <p>NOTE An unclean optical fiber connector causes large attenuation and abnormal reflection.</p>	<ol style="list-style-type: none"> Measure the backbone and branch fibers by using the optical time domain reflectometer (OTDR). It is found that abnormal reflection and return loss occur. Check the optical fiber connector on site by using the fiber end-face inspector. It is found that the optical fiber connector is not clean. 	Clean the optical fiber connector.
<p>The optical fiber is bent excessively.</p> <p>NOTE Optical attenuation increases when the bending radius is excessively small.</p>	<ol style="list-style-type: none"> Measure the backbone and branch fibers by using the OTDR. It is found that abnormal return loss occurs. Check the optical fiber on site. It is found that the optical fiber is bent excessively. 	Route the optical fiber properly.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
<p>The optical fiber is not securely connected, or different types of optical fiber connectors are interconnected.</p> <p>NOTE Optical attenuation and reflection increase when the optical fiber is not securely connected or different types of optical fiber connectors are interconnected.</p>	<ol style="list-style-type: none"> Measure the backbone and branch fibers by using the OTDR. It is found that abnormal return loss occurs. Check the optical fiber connectors on site. It is found that the optical fiber is not securely connected or the PC connector (blue) and the APC connector (green) are interconnected. 	<ul style="list-style-type: none"> If the optical fiber is not securely connected, reconnect the optical fiber securely. If different types of optical fiber connectors are interconnected, replace the incompatible connector with a compatible one or replace related devices, such as the optical splitter. <p>NOTE If the CATV service is required, it is recommended that you use APC connectors (green) only.</p>
<p>The multi-mode optical fiber is used as the backbone or branch optical fiber.</p> <p>NOTE If the multi-mode optical fiber is used as the backbone or branch optical fiber, the optical signal attenuates quickly and the return loss increases.</p>	<ol style="list-style-type: none"> Measure the backbone and branch fibers by using the OTDR. It is found that optical signals attenuate seriously. Check the optical path on site. It is found that the multi-mode optical fiber is used. The multi-mode optical fiber can be recognized by its physical features such as its color. 	Replace the multi-mode optical fiber with the single-mode optical fiber.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
<p>The optical attenuation of the optical path is excessively small.</p> <p>NOTE</p> <ul style="list-style-type: none"> If the optical attenuation of the optical path is excessively small, the optical power received by the CMC exceeds the overload optical power of the CMC. Such a situation occurs usually in labs, where the OLT and the CMC may be directly connected to each other through a short optical fiber. 	<p>The optical attenuation of the optical path is excessively small if either of the following conditions is met:</p> <ul style="list-style-type: none"> Measure the receive optical power of the CMC by using the optical power meter. It is found that the actual receive optical power of the CMC is greater than -8 dBm. Check the optical path between the OLT and the CMC. It is found that the optical attenuation of the optical path is excessively small. The normal attenuation range is 10–25 dB. 	Add an optical attenuator on the optical path between the OLT and the CMC.
<p>The ODN is not properly planned.</p> <p>NOTE</p> <ul style="list-style-type: none"> The split ratio of the ODN link is not determined by the number of optical network terminals (ONTs) connected but by the split ratio of optical splitters. When an optical splitter is connected to the ODN, attenuation occurs and the split ratio of the optical splitter needs to be calculated. The difference between optical powers of two adjacent CMCs received by the OLT must be less than or equal to 15 dB. 	<p>The ODN does not comply with the ODN link plan or the GPON Class B+ standard.</p> <ul style="list-style-type: none"> Three-level splitting exists in the ODN. The network coverage of the ODN far exceeds 20 km. The split ratio exceeds the specification. For example, a board supports a maximum split ratio of 1:64. If the first-level split ratio is 1:8, the second-level is 1:16, and the actual split ratio is 1:128, this exceeds the specification (1:64). The optical attenuation difference of two optical paths exceeds 15 dB. 	Optimize the ODN to meet Huawei's ODN construction requirements and specifications.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
The optical splitter is faulty, or the connectors on the optical splitter are not clean.	<p>Measure the input and output optical power of the optical splitter by using the optical power meter. It is found that the actual attenuation exceeds the theoretical attenuation.</p> <p>NOTE The faults related to the optical splitter cannot be located by the OTDR because the OTDR cannot penetrate the optical splitter.</p>	Replace the faulty optical splitter or clean the connectors on the optical splitter.
A backbone fiber break occurs.	<ol style="list-style-type: none"> Check the backbone fiber by using the OTDR. It is found that a backbone fiber break occurs. Check the backbone fiber on site. It is found that the backbone fiber is broken or not connected. 	Reconnect the backbone fiber.
A branch fiber break occurs.	<ol style="list-style-type: none"> Check the branch fiber by using the OTDR. It is found that a branch fiber break occurs. Check the branch fiber on site. It is found that the branch fiber is broken or not connected. 	Reconnect the branch fiber.

Step 3 If the CMC still cannot be automatically discovered after CMC problems are resolved, proceed to [Step 4](#).

Possible Cause	Diagnosis Criterion	Troubleshooting Method
The CMC is not powered on.	Check the power supply of the CMC on site. It is found that the power supply of the CMC fails or is turned off.	Restore the power supply of the CMC.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
<p>A rogue ONU affects the proper operating of other ONUs.</p> <p>NOTE If a rogue ONU exists, the ONU that fails to go online may be a normal one and the ONU that goes online may be a rogue one.</p>	<p>A rogue CMC exists if any one of the following conditions is met:</p> <ul style="list-style-type: none"> The OLT generates the alarm 0x2e314021 "There are illegal intrusive rogue ONTs under the port". The OLT generates the alarm 0x2e314022 "The ONT is a rogue ONT". Connect the optical fiber of the OLT PON port to the optical power meter for measurement. If the optical power meter displays the optical power, a continuous-mode ONU or an irregular-mode ONU exists. <p>NOTICE Services are interrupted during optical power measurement. Therefore, it is recommended that you measure the optical power when no service runs on the PON port, for example, during deployment.</p>	Replace the rogue ONU.
The CMC encounters a hardware fault.	<p>The CMC encounters a hardware fault if either of the following conditions is met:</p> <ul style="list-style-type: none"> The indicator of the CMC is off when the CMC is powered on. After the CMC is replaced with a normal one, the new CMC is automatically discovered by the OLT. 	Replace the faulty CMC or the optical module of the CMC.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
The optical module of the CMC is abnormal. For example, the transmit optical power of the optical module is excessively small or the receiver sensitivity is low.	<p>After the CMC is replaced with a normal one, the new CMC is automatically discovered by the OLT.</p> <p>Alternatively, the cause can be identified as follows:</p> <ul style="list-style-type: none"> • Set the optical module of the CMC to the continuous mode, and measure the transmit optical power by using the optical power meter. It is found that the actual transmit optical power is beyond the normal range. • Measure the receive optical power of the CMC by using the optical power meter. It is found that the actual receive optical power is within the normal range. 	Replace the faulty CMC or the optical module of the CMC.
The pigtail of the CMC is broken or subject to excessive bending.	Check the pigtail on site. It is found that the pigtail is broken or subject to excessive bending.	Replace the pigtail of the CMC.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
The CMC is not compatible with the OLT.	<ul style="list-style-type: none"> The R version of the CMC is different from that of the OLT. The CMC does not operate properly. For non-CCKRA and non-CCKRB control boards, if the OLT version is earlier than V800R016C00, the CMC does not operate properly. 	<ol style="list-style-type: none"> Run the sysman centralized-mgmt primary stand-alone command to switch the CMC to the standalone mode. Load the standalone normalization package file to the CMC, to ensure that the R version of the CMC is the same as that of the OLT. Run the sysman centralized-mgmt primary extend-frame command to switch the CMC to the aggregation mode, and connect the CMC to the OLT.
The package file of the OLT does not contain board software for the CMC.	Run the display io-packetfile information command to query the I/O package information of the OLT. The package file does not contain board software for the CMC.	Load the package file of the OLT again and ensure that the package file contains board software for the CMC.
The CMC resets repeatedly because automatic loading fails.	<p>Connect the CMC to the serial port and check the startup information of the CMC. If the CMC attempts to load the board software repeatedly, the OLT does not respond to the automatic loading request.</p> <p>NOTE Local serial port login can be used only locally. The user name and password can be used for authentication. The serial port is enabled by default and is usually used during device deployment. If the serial port is enabled for a long time, security risks may exist. You are advised to run the sysman console disable command to disable the serial port if it is not needed.</p>	<ol style="list-style-type: none"> Check whether the package file of the OLT contains the board software for the CMC. If not, load the correct package file of the OLT. Ensure that the CMC is compatible with the OLT.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
The extended subrack does not operate properly because a board of the CMC in the extended subrack is faulty.	<ul style="list-style-type: none"> • Connect the CMC to the serial port and check the startup information of the CMC. If an error occurs when the CMC attempts to load board software for the extended subrack, and the CMC repeatedly resets, the board in the extended subrack is faulty. <p>NOTE Local serial port login can be used only locally. The user name and password can be used for authentication. The serial port is enabled by default and is usually used during device deployment. If the serial port is enabled for a long time, security risks may exist. You are advised to run the sysman console disable command to disable the serial port if it is not needed.</p> <ul style="list-style-type: none"> • After the CMC is replaced with a normal one, the new CMC is automatically discovered by the OLT. 	Replace the CMC.

Step 4 Contacting Huawei for Assistance.

Step 5 End.

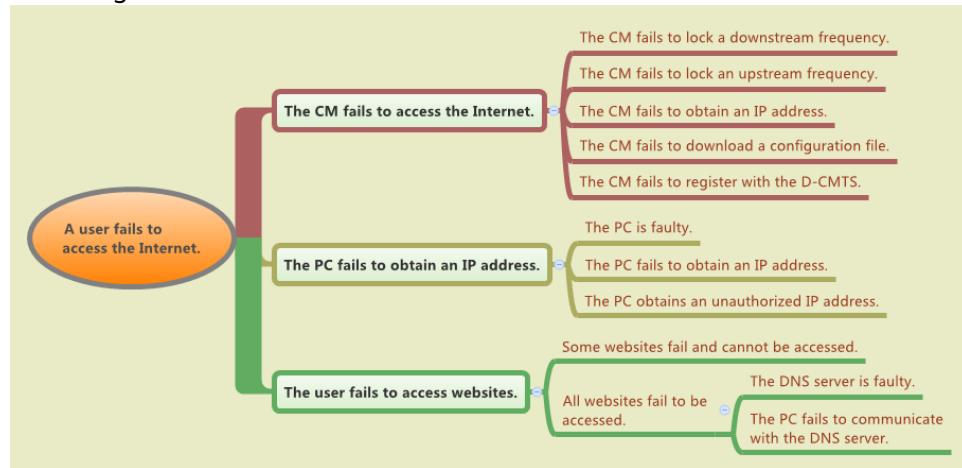
----End

12.1.4 Failure to Access the Internet

If an Internet access failure occurs, users who have permission to access the Internet cannot obtain network resources. For example, the users cannot open web pages.

Location Method

If an Internet access failure occurs, locate the fault using the methods listed in the following table.



NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check for the possible causes on the CM and troubleshoot the faults accordingly. If the user still fails to access the internet, go to [Step 2](#).

Runs the **display cable modem** command to query the state of the CM is offline, go to [12.1.11 Failure to Go Online of a CM](#).

Step 2 Check for the possible causes on the PC and troubleshoot the faults accordingly. If the user still fails to access the internet, go to [Step 3](#).

Possible Causes	Location Analysis	Handling Method
The PC fails to obtain an IP address from the DHCP server.	The PC fails to obtain an IP address (excluding the PCs with static IP addresses).	See 12.1.18 Failure to Obtain an IP Address of a PC .
<ul style="list-style-type: none">The PC is infected with viruses.The Internet Explorer (IE) on the PC is faulty.The PC is slow to respond after running for a long period.	The PC obtains an IP address (excluding the PCs with static IP addresses). The user can access the Internet after replacing the PC.	Use another PC to access the Internet.

Possible Causes	Location Analysis	Handling Method
The PC has obtained an incorrect IP address.	The PC obtains an IP address (excluding the PCs with static IP addresses). The user cannot access the Internet after replacing the PC.	Check whether the IP address is within the accepted IP address range.
The IP address is different from the IP address bound to the CM through SAV.		Run the display cable source-verify bind-ip cm command to query the IP address bound to the CM. Then, check whether this IP address is the same as the IP address of the PC.

Step 3 Use another website for testing.

- If the user can access the Internet, the original website is faulty.
- If the user cannot access the Internet, go to **Step 4**.

Step 4 Check the DNS.

1. Enter the IP address of an existing website in the address bar of IE (format: `http://x.x.x.x`) and check whether the website opens.
 - If the website opens, the fault is on the DNS and the DNS cannot resolve the domain name. Go to **Step 4.2**
 - If the website does not open, go to **Step 5**
2. Check whether the PC can ping the IP address of the DNS.

 **NOTE**

To view the DNS IP address of the PC, do as follows:

1. Choose **Start > Run** from the Windows main menu. In the **Run** dialog box displayed, enter **cmd** and press **Enter**.
2. In the command line interface (CLI) window displayed, run the **ipconfig/all** command to view the DNS IP addresses obtained by the PC, namely, the values of the **DNS Servers** parameter.
 - If the PC can ping the IP address of the DNS, the link between the PC and the DNS is normal and the DNS is faulty. Go to **Step 4.3**
 - If the PC cannot ping the IP address of the DNS, go to **Step 5**
3. Rectify the fault on the DNS. Then, check whether the user can access the Internet.
 - If the user can access the Internet, go to **Step 6**.
 - If the user cannot access the Internet, go to **Step 5**.

Step 5 Contacting Huawei for Assistance.

Step 6 End.

----End

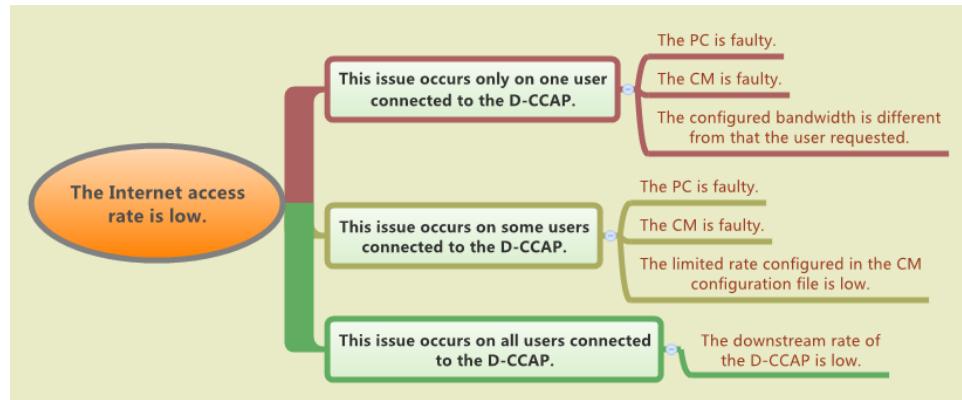
12.1.5 Troubleshooting a Low Internet Access Rate

Low Internet access rate indicates that the attainable rates when users access the Internet are lower than those provided for the users.

Location Method

NOTE

- Determine the service priority of the user and the time range during which the Internet access rate is low. If the service priority of the user is low, the low Internet access rate during peak hours is normal.
- Use well-known rate test websites to test the Internet access rate.



NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check the PC and the CM.

1. Replace the PC and check whether the Internet access rate is normal.
 - If the Internet access rate is normal, the PC is faulty. Check whether the NIC in the PC is faulty, the PC is infected with viruses, the PC responds slowly after running for a long period of time, or the user uses a low-end PC. Rectify any problems you encounter. Then, go to **Step 4**.
 - If the Internet access rate is low, go to **Step 1.2**.
2. Check whether the CM is working properly. Replace the CM and check whether the Internet access rate is normal.
 - If the Internet access rate is normal, the CM is faulty. Then, go to **Step 4**.
 - If the Internet access rate is still low, go to **Step 2**.

Step 2 Check whether the D-CCAP configuration is correct.

Possible Cause	Location Analysis	Handling Method
The bandwidth configured on the D-CCAP is different from that the user requested.	The configured bandwidth is different from that the user requested according to the result obtained by running the display cable service-flow command.	Run the cable service-class command to change the maximum rate for service flows.
The downstream rate of the D-CCAP is low. NOTE This cause may occur only when the MA5633 is used as a standalone NE.	The used bandwidth of the uplink port on the D-CCAP is approaching the maximum permitted DBA bandwidth. <ul style="list-style-type: none"> • Run the display ont info command on the OLT to query the ID of the DBA profile bound to the MA5633. • Run the display DBA-profile command on the OLT to query the bandwidth configured in the DBA profile. • Run the display pon-bandwidth command on the MA5633 to query the real-time traffic on the uplink port. 	<ul style="list-style-type: none"> • Modify the DBA profile on the OLT to allocate a higher bandwidth to the MA5633. • Reduce the number of users connected to the D-CCAP.
The rate limited in the CM configuration file is low.	The service recovers after the CM configuration file is changed on the OSS server to the one without rate limitation or with a higher limited rate.	Change the value of the rate limitation parameter in the CM configuration file.

Step 3 Contacting Huawei for Assistance.

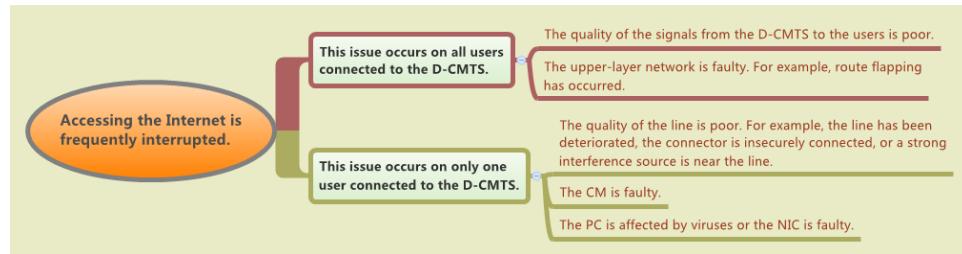
Step 4 End.

----End

12.1.6 Troubleshooting Frequent Interruptions in the Internet Access Service

If frequent interruptions occur in the Internet access service, users frequently fail to access the Internet.

Location Method



NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Check whether all users connect to the D-CCAP frequently fail to access the Internet.
 - If yes:
 - Run the **display cable modem status trace** command to query CM status changes. If the CMs frequently go online and offline, check signal quality segment by segment from the D-CCAP to the user side.
 - Ping a well-known website or the IP address of a server from the D-CCAP for a long period of time. If packet loss frequently occurs, check whether the upper-layer network is functional.
 - If no, go to **Step 2**.
- Step 2** Verify the network between the CM and the D-CCAP.
If users still frequently fail to access the Internet, go to **Step 3**.

Possible Causes	Location Analysis	Handling Method
<ul style="list-style-type: none"> The line quality is poor and therefore there is a large attenuation. The subscriber line is deteriorated. The subscriber line connectors are insecurely connected. There are too many branches on the link and therefore there is a large attenuation. There is a strong source of interference around the line. 	Run the display cable modem 1 remote-detail command to query the remote CM receive power. It is found that CM input signals are abnormal.	Check whether connectors are securely connected, lines are functional, the number of link branches is proper, attenuation is within the normal range, and line connections comply with customer requirements.

Step 3 Verify the network between the PC and the CM.

If users still frequently fail to access the Internet, go to **Step 4**.

Possible Causes	Location Analysis	Handling Method
The user's PC is infected with viruses or has a faulty network interface card (NIC).	The fault is resolved after the PC is replaced.	Use another PC to access the Internet.
<ul style="list-style-type: none"> The line quality is poor. The subscriber line is deteriorated. The subscriber line connectors are insecurely connected. 	The fault is resolved after the cable connecting the PC to the CM is replaced.	Check the subscriber line between the PC and the CM. Verify that the subscriber line is functional, connectors are securely connected, and line quality is good.
The CM is faulty.	The fault is resolved after the CM is replaced.	Replace the CM.

Step 4 Contacting Huawei for Assistance.

Step 5 End.

----End

12.1.7 Pixelated or Frozen Display of a Program

This topic describes how to resolve the problem of pixelated or frozen display of a live program due to poor program quality.

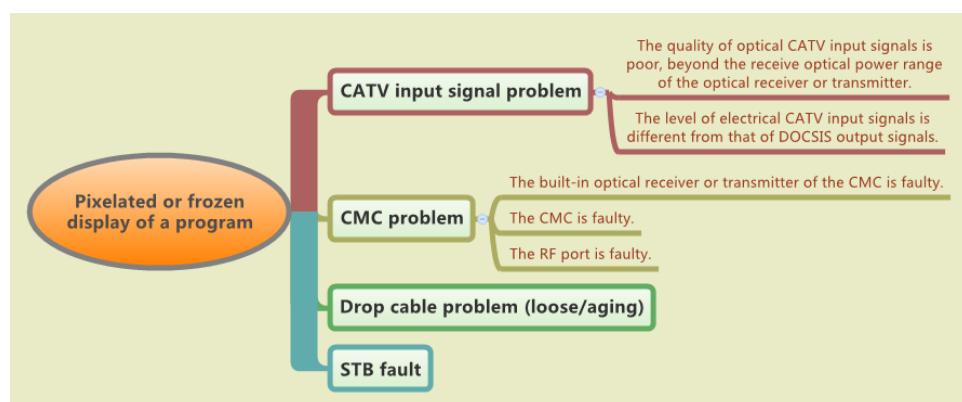
Program Diagnosis

The following 2 live program scenarios are available:

- The upper-layer optical receiver transmits cable TV (CATV) signals to the RF_IN port of the D-CCAP through a coaxial cable. After undergoing frequency mixing with DOCSIS radio frequency (RF) signals, the signals are output through the RF_OUT port. (DOCSIS stands for data over cable service interface specification.)
- CATV signals are transmitted to the built-in optical receiver of the D-CCAP through an optical fiber. The optical receiver performs optical-to-electrical conversion on the signals. After undergoing frequency mixing with DOCSIS RF signals, the signals are output through the RF_OUT port.

The distributed converged cable access platform (D-CCAP) mainly performs frequency mixing. If the quality of a live program is poor, check the input and output signal quality and the line quality.

The following figure shows the problem diagnosis process.



NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check the electrical or optical input signals of the D-CCAP.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
<p>The quality of optical CATV input signals is poor, beyond the receive optical power range of the optical receiver or transmitter.</p> <ul style="list-style-type: none"> ● The upper-layer optical CATV signal transmitter is faulty. ● The CATV signal transmission node is faulty. ● The CATV signal transmission fiber is aging. ● The connector of the optical receiver for CATV signals is loose. 	The indicator of the optical receiver or transmitter indicates an error.	Check the upper-layer optical CATV signal line and ensure that the signals adapt to the receive optical power range of the built-in optical receiver or transmitter of the D-CCAP.
The level of electrical CATV input signals is different from that of DOCSIS output signals.	For a device not configured with the D-CCAP built-in optical receiver or transmitter, the service board of the D-CCAP operates properly, but the CATV service is interrupted.	Ensure that the level of CATV input signals is the same as that of DOCSIS output signals.

Step 2 Check the coaxial media converter (CMC).

Possible Cause	Diagnosis Criterion	Troubleshooting Method
<ul style="list-style-type: none"> ● The built-in optical receiver or transmitter of the CMC is faulty. ● The CMC is faulty. 	All users under the CMC experience pixelated or frozen display when watching a program.	Replace the CMC.
The RF port is faulty.	All users under the RF_OUT port of the CMC experience pixelated or frozen display when watching a program. The problem is resolved after the users are switched to other RF_OUT ports.	<ul style="list-style-type: none"> ● Switch users under the faulty RF port to other RF_OUT ports that function properly. ● Replace the CMC.

Step 3 Check the connection between the TV and the cable modem (CM).

Possible Cause	Diagnosis Criterion	Troubleshooting Method
The drop cable is loose or aging.	A single user experiences pixelated or frozen display.	Measure the signals by using a measuring instrument such as a field strength indicator. Adjust the drop cable to ensure that the signal quality meets the requirements of the set-top box (STB).
The STB is faulty.	The problem is resolved after the STB is replaced.	Replace the STB.

Step 4 Contacting Huawei for Assistance.

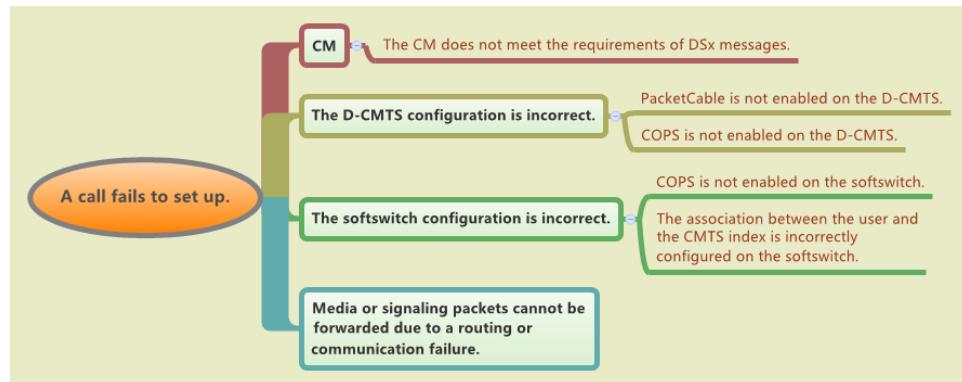
Step 5 End.

----End

12.1.8 Failure to Make a Call

This section describes how to troubleshoot a failure to make a call on cable networks. MSOs can provide the VoIP service on cable networks.

Fault Location



NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Verify the CM is functional.

If the CM is faulty, replace it. If the fault persists, go to **Step 2**.

Step 2 Verify that the D-CCAP is functional.

If the fault persists, go to [Step 3](#).

Possible Cause	Location Analysis	Troubleshooting Method
PacketCable is disabled on the D-CCAP.	The fault does not recur after PacketCable is enabled on the D-CCAP.	<ul style="list-style-type: none"> Run the packetcable 1dotx command to enable PacketCable 1.x. Run the packetcable multimedia command to enable PacketCable Multimedia.
COPS is not configured on the D-CCAP.	The fault does not recur after COPS is configured on the D-CCAP.	<p>After enabling PacketCable 1.x:</p> <ol style="list-style-type: none"> Run the cops pepid command to configure the policy enforcement point (PEP) ID. Run the cops access-list command to configure a COPS access control list (ACL).

NOTE

If COPS is not used on the D-CCAP, you only need to check whether common embedded multimedia terminal adapters (eMTAs) are allowed to dynamically create a media stream.

Step 3 Verify that the softswitch is correctly configured.

If the fault persists, go to [Step 4](#).

Step 4 Verify that the upper-layer device of the D-CCAP is correctly configured if the affected user, regardless of the calling party or the called party, cannot be pinged from the media gateway.

If the fault persists, go to [Step 5](#).

Step 5 Contacting Huawei for Assistance.

Step 6 End.

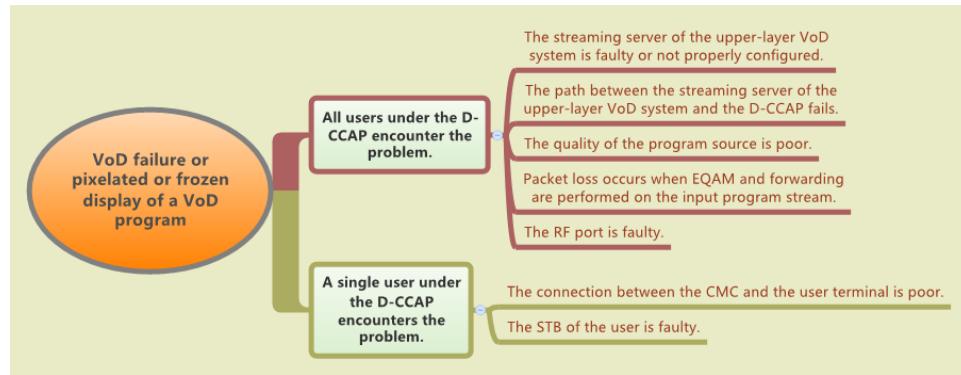
----End

12.1.9 VoD Failure or Pixelated or Frozen Display of a VoD Program

This topic describes how to resolve the problem that the video on demand (VoD) service is unavailable or pixelated or frozen display occurs when users watch a VoD program.

Problem Diagnosis

The following figure shows the problem diagnosis process.



NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 If the problem persists after upper-layer server problems are resolved, proceed to [Step 2](#).

Possible Cause	Diagnosis Criterion	Troubleshooting Method
The streaming server of the upper-layer VoD system is faulty or not properly configured.	<ul style="list-style-type: none">All users watching the program encounter the problem.After a user requests the program, run the display cable eqam video statistics input command to query the program input statistics. No input statistics data is available.Check the streaming server of the VoD system. It is found that the streaming server is faulty or not properly configured.	Verify the configurations of the streaming server of the VoD system. Ensure that the configurations are correct and the streaming server operates properly.
The path between the streaming server of the upper-layer VoD system and the Distributed Converged Cable Access Platform (D-CCAP) fails.	The D-CCAP fails to ping the streaming server of the VoD system.	Check the D-CCAP router and the upper-layer router.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
The quality of the program source is poor.	Users can watch other VoD programs properly.	Replace the program source.

Step 2 If the problem persists after D-CCAP problems are resolved, proceed to **Step 3**.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
Packet loss occurs when Edge Quadrature Amplitude Modulation (EQAM) and forwarding are performed on the input program stream.	<ul style="list-style-type: none"> Run the display cable eqam video statistics output command to query the video program output statistics of the EQAM module of the coaxial media converter (CMC). It is found that packet loss occurs. Connect a stream analyzer to the RF_OUT port of the CMC and check the continuity check (CC) and program clock reference (PCR) statistics. Packet loss and error packets are found. 	Replace the CMC.
The RF port is faulty.	All users under the RF_OUT port of the CMC experience pixelated or frozen display when watching a program. The problem is resolved after the users are switched to other RF_OUT ports.	<ul style="list-style-type: none"> Switch users under the faulty RF port to other RF_OUT ports that function properly. Replace the CMC.

Step 3 If the problem persists after connection problems between the CMC and user terminals are resolved, proceed to **Step 4**.

Possible Cause	Diagnosis Criterion	Troubleshooting Method
<p>The connection between the CMC and the user terminal is poor.</p> <ul style="list-style-type: none"> ● The line quality is poor, causing large attenuation. ● The subscriber line is aging. ● The connector of the subscriber line is loose. ● There are a large number of branch links, causing large attenuation. ● The line is close to a strong interference source. 	Measure the input signal strength of the CM by using a field strength indicator. It is found that the input signal strength is weak.	<ul style="list-style-type: none"> ● Reduce the line attenuation. ● Replace the aging line. ● Reconnect the loose connector. ● Eliminate the interference source.
The set-top box (STB) of the user is faulty.	The problem is resolved after the STB is replaced.	Replace the STB.

Step 4 Contacting Huawei for Assistance.

Step 5 End.

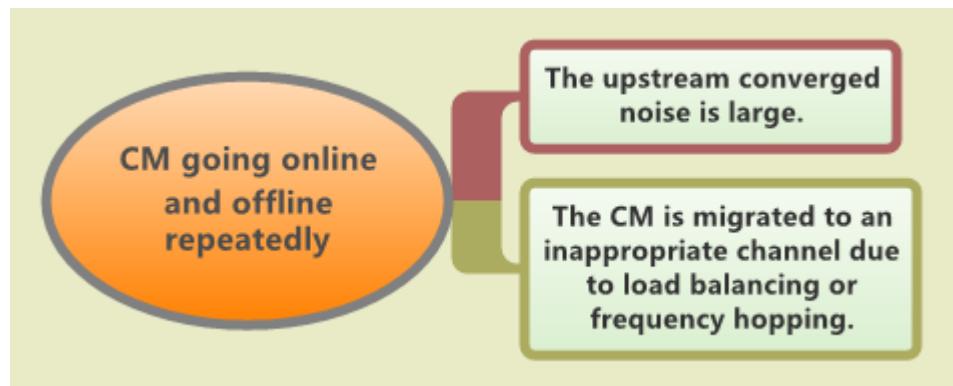
----End

12.1.10 CM Going Online and Offline Repeatedly

This topic describes how to resolve the problem that a cable modem (CM) goes online and offline repeatedly.

Problem Diagnosis

The following figure shows the problem diagnosis process.



NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Resolve the problem based on the following possible causes. If the problem persists, proceed to [Step 2](#).

Possible Cause	Diagnosis Criterion	Troubleshooting Method
The upstream converged noise is large.	Use the detection instrument to test the upstream frequency. Alternatively, run the display cable signal quality frameid/slotid/portid upstream channel-id command to query the signal to noise ratio (SNR) of the upstream channel.	<ul style="list-style-type: none">Increase the upstream attenuation to improve the transmit power of the CM, so as to improve the SNR.Locate the source of noise and eliminate the source.
The CM is migrated to an inappropriate channel due to load balancing or frequency hopping.	The problem is resolved after the CM that goes online and offline repeatedly is forcibly migrated to the specified channel.	<ul style="list-style-type: none">Forcibly migrate the CM that goes online and offline repeatedly to a channel that operates properly. NOTE For example, add all channels and CMs to a restrict load balancing group.Run the cable load-balance disable command to disable load balancing, or run the undo cable upstream channel-id spectrum-group command to disable frequency hopping.

Step 2 Contacting Huawei for Assistance.

Step 3 End.

----End

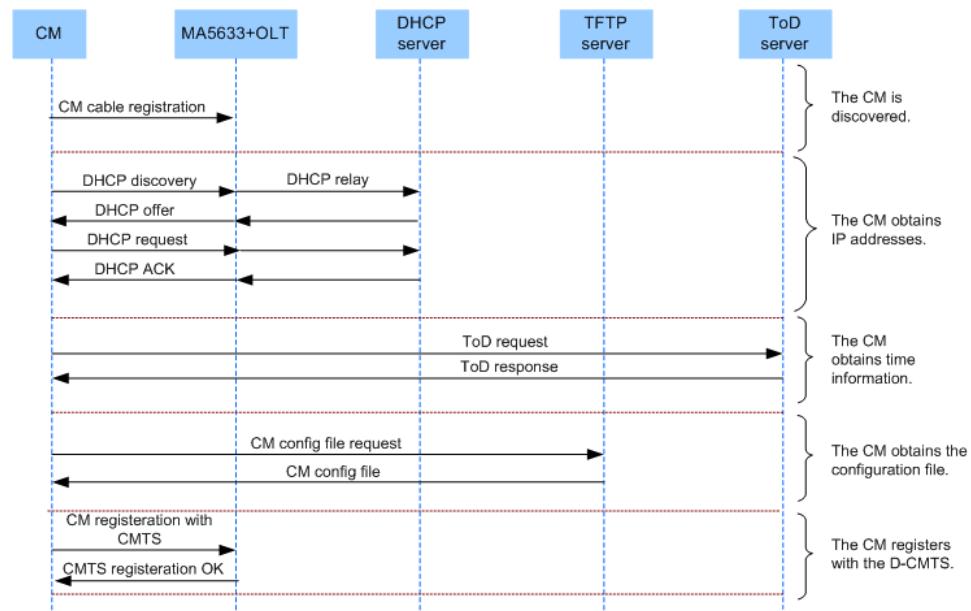
12.1.11 Failure to Go Online of a CM

A CM connects to carriers' hybrid fiber coaxial (HFC) or user networks. If a CM fails to go online, you can run the **display cable modem status trace** command on a D-CCAP to query the CM status. Based on the status, you can determine whether the CM is functional.

Context

Figure 12-1 shows the CM registration process.

Figure 12-1 CM registration process



DHCP server: provides the IP, gateway, TFTP server, and ToD server addresses for a CM.

TFTP server: stores CM configuration files. A CM obtains a configuration file from the TFTP server.

ToD server: provides the date and time for a CM. After obtaining this information, the CM reports event logs with accurate date and time information. This facilitates device management.

The following table describes the CM registration process.

Stage	Procedure	Remarks
The CM is discovered.	<p>The CM sets up the temporary connection with the D-CCAP.</p> <ol style="list-style-type: none"> 1. The CM is powered on. 2. The CM selects upstream channels, scans downstream channels, and locks the main downstream channel. The CM transmits all packets over the upstream and downstream channels. 3. The CM starts ranging and enters the automatic discovery stage. The D-CCAP creates a temporary service flow for the CM. 	None
The CM obtains its IP address and the IP addresses of the TFTP and ToD servers.	<ol style="list-style-type: none"> 1. The CM initiates a DHCP request. 2. The D-CCAP service module captures the DHCP packet, adds the MAC address and physical port number of the CM to the DHCP Option 82 field in the packet, performs DHCP relay, and forwards the DHCP packet to the DHCP server through an uplink port. 3. The DHCP server checks CM configurations according to the MAC address of the CM, allocates an IP address to the CM, and uses the DHCP Option 82 field to send the CM configuration file name and the IP addresses of the TFTP and ToD servers to the D-CCAP. 4. The D-CCAP service module captures the DHCP response packet and learns the mapping between the MAC address of the CM and the configuration file name. This information is subsequently used when the CM requests the configuration file from the TFTP server. 	None

Stage	Procedure	Remarks
The CM obtains time information.	<ol style="list-style-type: none"> 1. The CM initiates a ToD request. 2. The ToD server responds and the CM obtains the date and time information. 	Based on the date and time information obtained by the CM, users can manage devices and obtain device running information.
The CM obtains the configuration file.	<ol style="list-style-type: none"> 1. The CM requests the configuration file from the TFTP server according to the configuration file name contained in the DHCP Option 82 field. 2. The TFTP server sends the configuration file to the CM in TFTP mode. 	A CM configuration file defines service flows, quality of service (QoS), and security policies. After the CM obtains a configuration file, it initiates a registration request to the D-CCAP.

Stage	Procedure	Remarks
The CM registers with the D-CCAP.	<ol style="list-style-type: none">After the CM parses the configuration file, it initiates a registration request to the D-CCAP. The registration request is in the type-length-value (TLV) format and contains service flow parameters.The D-CCAP performs a message integrity check (MIC) on the CM registration request to prevent the CM from modifying the configuration file without authorization. For details about the MIC,The D-CCAP performs an X.509 certificate authentication on the CM. For details about the authentication.The D-CCAP checks service parameter settings and resources. It allocates service flow resources to the CM according to the parameter settings in the CM configuration file only if the service parameter settings comply with the configuration file and the remaining service resources meet the resource request requirement. In addition, the D-CCAP maps the service flow resources to DOCSIS service flows.The CM successfully registers with the D-CCAP. CM service flows can be forwarded.	None

A CM can provide services only after it goes online. The CM status can be queried by running the **display cable modem status trace** command.

 **NOTE**

The **display cable modem status trace** command must be executed in diagnose mode. In privilege or global config mode, before running the **display cable modem status trace** command, run the **diagnose** command to enter diagnose mode.

The following table lists the mapping between the CM status and the events that trigger CM status changes.

Table 12-1 Mapping between the CM status and the events that trigger CM status changes

CM Status	Triggering Event	Remarks
init	CM initialization (CM_ARRIVAL)	Ranging is started after the CM is powered on.
start DHCP	DHCP request initiated by a CM (CM_DHCP_DISCOVERY)	None
DHCP offer	DHCP offer received from the DHCP server (CM_DHCP_OFFER)	None
DHCP request	DHCP request received from the CM (CM_DHCP_REQUEST)	None
DHCP complete	DHCP request is complete (CM_DHCP_ACK)	After a DHCP request, the DHCP server allocates an IP address to the CM, and uses the DHCP option 66 field to send the configuration file name, uses DHCP option 67 field to send the IP addresses of the TFTP and ToD servers to the D-CCAP.
register	CM registration request (CM_REGREQ)	The CM sends a registration request to the D-CCAP.
online	Successful CM registration (Register success)	The CM registers successfully and can transmit and receive services normally.
offline	CM going offline (CM_DEPATURE)	The CM is disconnected or powered off.

CM Status	Triggering Event	Remarks
reject	<ul style="list-style-type: none"> • CM_MALLOC_DYN_DATA_FAIL: Applying for dynamic data fails. • CM_ARRIVAL_MALLOC_SERVICE_FAI L: Applying for a service stream in automatic discovery phase fails. • CM_READ_DYN_DATA_FAIL: Reading dynamic data fails. • CM_AUTHREG_FAIL: The CM authentication fails. • Register fail: Requesting for CM registration fails. • CM_REGISTER_BOARD_CHECK_FAI: The board check fails when the CM starts registration. • CM_REGISTER_MIC_CHECK_FAIL: The MIC check fails when the CM starts registration. • CM_REGISTER_MALLOC_SERVICE_F AIL: Applying for a service stream fails in CM registration. 	If a CM fails to be authenticated, it cannot connect to the D-CCAP.

If a CM is not online for a long period of time (for example, several minutes), locate faults according to the CM status.

Location Method

Fault Scope	Location Analysis	Possible Causes
Physical lines	An insecurely connected connector causes a downstream frequency locking failure.	The connector is insecurely connected to an RF line.
	Use an instrument to measure the upstream spectrum, or log in to the D-CCAP and run the display cable signal quality command to query the upstream signal-to-noise ratio (SNR).	The upstream aggregation noises are excessively loud.

Fault Scope	Location Analysis	Possible Causes
	The level of the signals received on RF ports that is measured using an instrument is different from the theoretical value in line design.	The uplink attenuation is excessively large or small.
Radio frequency (RF) lines	The CM is in the offline state.	<ul style="list-style-type: none"> • The CM is not powered on. • Line noises are excessively loud. • The channel frequency is incorrect.
	The CM is in the init state.	The CM exchanges data with the D-CCAP. However, the CM ranging fails due to RF line faults.
System configuration	The CM remains in the start DHCP state.	<ul style="list-style-type: none"> • The D-CCAP does not receive the DHCP discover packet sent from the CM due to a CM fault. As a result, the DHCP process cannot be complete. • Obtain DHCP packets on the D-CCAP and check the DHCP server configuration if one of the following cases occurs: <ul style="list-style-type: none"> - The DHCP server can receive the DHCP discover packet sent from the CM but does not reply a DHCP offer packet. - After replying a DHCP offer packet to the CM, the D-CCAP does not receive a DHCP request packet sent from the CM. - The DHCP server can receive the DHCP request packet sent from the CM but does not reply a DHCP ACK packet. • The D-CCAP fails to communicate with the DHCP server. Specifically, the D-CCAP fails to ping the DHCP server.

Fault Scope	Location Analysis	Possible Causes
	The CM remains in the DHCP complete state.	<ul style="list-style-type: none"> After the DHCP is complete, the CM does not send an ARP query packet to the TFTP server. The CM fails to obtain a configuration file due to a TFTP server fault, the disconnection from the OLT to the TFTP server, or the incorrect TFTP server configuration.
	The CM remains in the register state.	The CM obtains an incorrect configuration file.
	The CM remains in the reject state.	<ul style="list-style-type: none"> The CM fails to be authenticated. (CM_AUTHREG_FAIL) The CM message integrity check (MIC) fails. (CM_REGISTER_MIC_CHECK_FAIL) The D-CCAP does not support the class of service (CoS) parameter setting in the CM configuration file. As a result, no service flow can be created. (CM_REGISTER_MALLOC_SERVICE_FAIL)
	The CM can go online only during non-peak hours.	Planned IP resources are insufficient.

NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check for the possible causes on the physical lines and troubleshoot the faults accordingly. If the failure to go online after that, proceed to =>[Step 2](#)

Possible Causes	Location Analysis	Handling Method
The connector is insecurely connected to an RF line.	An insecurely connected connector causes a downstream frequency locking failure.	Securely connect the connector to the RF line.
The upstream aggregation noises are excessively loud.	Use an instrument to measure the upstream spectrum, or log in to the D-CCAP and run the display cable signal quality command to query the upstream signal-to-noise ratio (SNR).	Add the upstream attenuation to improve the CM transmit power and SNR.
The uplink attenuation is excessively large or small.	The level of the signals received on RF ports that is measured using an instrument is different from the theoretical value in line design.	The level of the signals received on RF ports is adjusted.

Step 2 Check for the possible causes on the RF lines and troubleshoot the faults accordingly. If the failure to go online after that, proceed to =>[Step 3](#)

Possible Causes	Location Analysis	Handling Method
<ul style="list-style-type: none"> The CM is not powered on. Line noises are excessively loud. The channel frequency is incorrect. 	The CM is in the offline state.	<ul style="list-style-type: none"> Power on the CM. Cancel line noises. Adjust the center frequency for the channel.
The CM exchanges data with the D-CCAP. However, the CM ranging fails due to RF line faults.	The CM is in the init state.	

Step 3 Check for the possible causes on the system configuration and troubleshoot the faults accordingly. If the failure to go online after that, proceed to =>[Step 4](#)

Possible Causes	Location Analysis	Handling Method
<ul style="list-style-type: none"> ● The D-CCAP does not receive the DHCP discover packet sent from the CM due to a CM fault. As a result, the DHCP process cannot be complete. ● Obtain DHCP packets on the D-CCAP and check the DHCP server configuration if one of the following cases occurs: <ul style="list-style-type: none"> - The DHCP server can receive the DHCP discover packet sent from the CM but does not reply a DHCP offer packet. - After replying a DHCP offer packet to the CM, the D-CCAP does not receive a DHCP request packet sent from the CM. - The DHCP server can receive the DHCP request packet sent from the CM but does not reply a DHCP ACK packet. ● The D-CCAP fails to communicate with the DHCP server. Specifically, the D-CCAP fails to ping the DHCP server. 	The CM remains in the start DHCP state.	See 12.1.14 CM Fails to Obtain an IP Address

Possible Causes	Location Analysis	Handling Method
<ul style="list-style-type: none"> After the DHCP is complete, the CM does not send an ARP query packet to the TFTP server. The CM fails to obtain a configuration file due to a TFTP server fault, the disconnection from the OLT to the TFTP server, or the incorrect TFTP server configuration. 	The CM remains in the DHCP complete state.	
The CM obtains an incorrect configuration file.	The CM remains in the register state.	-
<ul style="list-style-type: none"> The CM fails to be authenticated. (CM_AUTHREG_FAIL) The CM message integrity check (MIC) fails. (CM_REGISTER_MIC_CHECK_FAIL) The D-CCAP does not support the class of service (CoS) parameter setting in the CM configuration file. As a result, no service flow can be created. (CM_REGISTER_MALL_OC_SERVICE_FAIL) 	The CM remains in the reject state.	See 12.1.17 CM Remains in the Reject State
Planned IP resources are insufficient.	The CM can go online only during non-peak hours.	Reallocate IP resources.

Step 4 Contacting Huawei for Assistance.

Step 5 End.

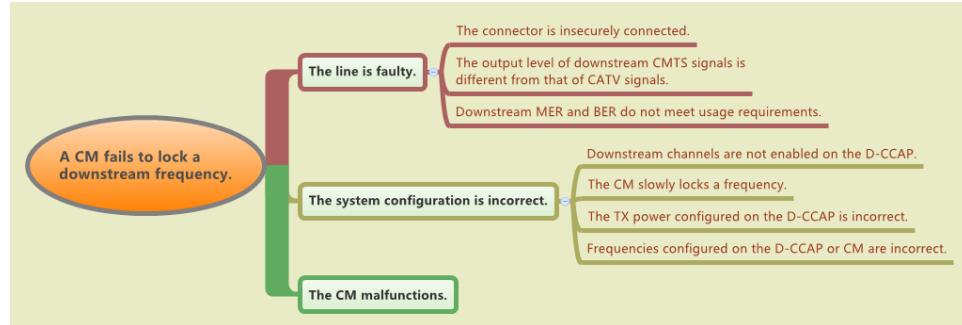
----End

12.1.12 Failure to Lock a Downstream Frequency of a CM

If a CM fails to lock a downstream frequency, the Receive indicator on the CM panel consistently blinks and cannot be steady on.

Location Method

If a CM fails to lock a downstream frequency, locate and troubleshoot the fault using the methods listed in the following table.



NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

- Step 1** Check for the possible causes on the physical lines and connect the RF line securely. If the CM still fails to lock a downstream frequency, go to **Step 2**.
- Step 2** Check for the possible causes on the RF lines and troubleshoot the faults accordingly. If the CM still fails to lock a downstream frequency, go to **Step 3**.

Possible Cause	Location Analysis	Handling Method
The downstream output level does not meet usage requirements.	The downstream signal output level of the D-CCAP device is different from the CATV signal level.	<p>Check the D-CCAP device downstream signal output level and the CATV signal level. Verify that the D-CCAP device downstream signal output level is the same as the theoretical value in line design.</p> <p>NOTE When calculating the level, check whether line equalization has been implemented on the output of the optical receiver. If the line equalization has been implemented, the D-CCAP device signal level should be the same as the equalized CATV signal level of the frequency.</p>
The downstream MER and BER do not meet usage requirements.	The downstream MER measured using an instrument is less than 35 dB and the BER is not 0. (The downstream MER must be at least 35 dB and the BER must be 0.)	<ol style="list-style-type: none"> Configure the testing frequency, modulation mode, and code rate on the instrument to be the same as the configured values. Measure the downstream MER and BER. In the 256 QAM modulation, the downstream MER must be greater than 35 dB and the BER must be 0 after FEC.

Step 3 Check for the possible causes on the system configuration and troubleshoot the faults accordingly. If the CM still fails to lock a downstream frequency, go to [Step 4](#).

Possible Cause	Location Analysis	Handling Method
No D-CCAP device downstream channel has been enabled.	Run the display cable downstream all config command to query enabled downstream channels. It is found that no downstream channel has been enabled.	Run the cable downstream command to configure a center frequency and enable a downstream channel.
The CM takes a long time to lock a frequency.	Log in to the CM management web page. It is found that the CM consistently scans downstream frequencies.	Log in to the CM management web page. Manually change the start CM downstream frequency to the same as that configured on the D-CCAP device. Then, restart the CM.
None	<ul style="list-style-type: none">Run the display cable downstream command to query the D-CCAP device frequency and transmit power. It is found that the configurations do not meet customer requirements.Query the CM frequency. It is found that the CM frequency is different from the D-CCAP device frequency.	<ul style="list-style-type: none">Change the D-CCAP device transmit power to comply with customer requirements.Change the D-CCAP device and CM frequency to comply with customer requirements.

Step 4 If the CM still fails to lock a downstream frequency after replace the CM, go to [Step 5](#).

Step 5 Contacting Huawei for Assistance.

Step 6 End.

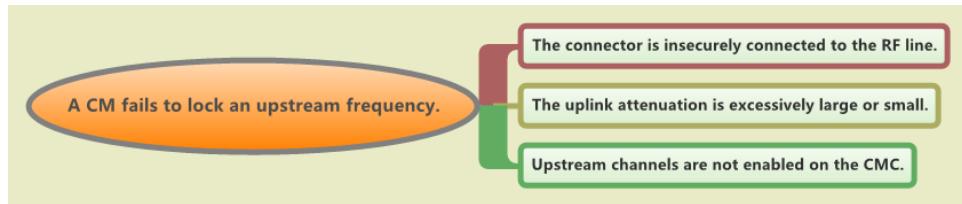
----End

12.1.13 Failure to Lock an Upstream Frequency of a CM

If a CM fails to lock an upstream frequency, the Send indicator on the CM panel consistently blinks and cannot be steady on.

Location Method

If a CM fails to lock an upstream frequency, locate and troubleshoot the fault using the methods listed in the following table.



NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Check for the possible causes on the physical lines and connect the RF line securely. Check whether cables are properly connected to the RF_IN and RF_OUT ports. If the CM still fails to lock an upstream frequency, proceed to **Step 2**.

Step 2 Check for the possible causes on the RF liens and troubleshoot the faults accordingly. If the CM still fails to lock an upstream frequency, proceed to **Step 3**.

Use an instrument to send single-frequency signals from the CM and measure the level of the signals received on RF ports. Then, check whether the signal level is the same as the theoretical value in line design. If the signal level is excessively large or small, detect line faults.

NOTE

The CM causes an 8 dB attenuation. Therefore, the line attenuation from the CM to the D-CCAP is recommended to be 40 dB at most.

Step 3 Check for the possible causes on the system configuration and troubleshoot the faults accordingly. If the CM still fails to lock an upstream frequency, proceed to **Step 4**.

Run the **display cable upstream all config** command to query enabled upstream channels. It is found that no upstream channel has been enabled. Run the **cable upstream** command to configure a center frequency and enable an upstream channel.

Step 4 Contacting Huawei for Assistance.

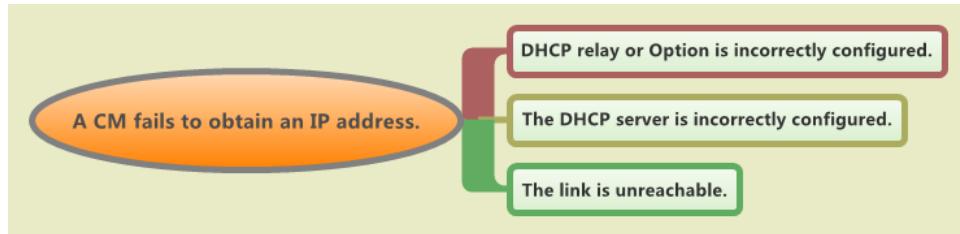
Step 5 End.

----End

12.1.14 CM Fails to Obtain an IP Address

If a CM fails to obtain an IP address, it remains in the IP address obtaining state and cannot go online.

Location Method



When a CM fails to obtain an IP address, perform the following steps to locate the fault:

Procedure

- Step 1** Run the **display dhcp l2 statistics** or **display dhcp l3 statistics** command on the D-CCAP to query the statistics of the DHCP packets received or forwarded by the D-CCAP.
 1. If the number of received DHCP packets is different from that of forwarded ones, check DHCP relay settings.
 2. If the packet statistics on the OLT and the CMC are different, the route is unreachable from the OLT to the CMC.
 - Step 2** Run the **debugging dhcp l3** command to enable debugging on the D-CCAP, run the **terminal debugging** command to enable the terminal to output debugging information, and run the **terminal monitor** command to query the DHCP packets sent by the CM. Then, analyze the displayed information. If the packets are discarded by the D-CCAP, identify the cause based on the displayed information.
 - Step 3** Obtain DHCP packets on the DHCP server. Check the DHCP discovery packets received by the DHCP server.
 1. Check whether the information, such as Option 60, Option 82, and relay configuration, carried in the DHCP packets is correct.
 2. Check whether the RID format in the DHCP Option 82 field on the D-CCAP is the same as that on the DHCP server. If they are different, check the DHCP relay configuration on the D-CCAP.
 - Step 4** If the DHCP server does not receive any DHCP discovery packets, check whether the DHCP server can be pinged from the D-CCAP. If the DHCP server cannot be pinged, check VLAN, VLAN interface, and route configurations.
 - Step 5** Check DHCP configuration and DHCP packets from the D-CCAP to the Layer 3 switch segment by segment.
- End

12.1.15 CM Fails to Download a Configuration File

If a CM fails to download a configuration file, it remains in the DHCP-C state, which indicates that the CM has obtained a dynamic IP address and is downloading a configuration file.

Possible Causes

The TFTP server configuration is incorrect. For example, the name of the configuration file is incorrect or the configuration file is unavailable.

When a CM fails to download a configuration file, perform the following steps to locate the fault:

Procedure

- Step 1** After obtaining an IP address, the CM uses the times packet to calibrate the system time and starts TFTP downloading. In this case, obtain packets on the TFTP server. After detecting the **file not found** information, check whether the **bootfile name** and **tftp server name** settings are correct on the DHCP server.

 NOTE

TFTP has security risks due to protocol restrictions, and can be used only in a secure environment.

- Step 2** Check whether the IP and directory configurations of the TFTP server are correct.

1. If the configuration file is statically configured, disable **File Manager Primary** and **File Manager Secondary** in **incognito configuration** of the service provisioning service when the TFTP server is available for configuration file downloading.
2. If the configuration file is dynamically generated, enable **File Manager Primary** and **File Manager Secondary**.

----End

12.1.16 CM Fails to Register with the D-CCAP

If a CM fails to register with the D-CCAP, it cannot go online. In this case, the CM repeatedly downloads a configuration file and obtains IP address from the DHCP server.

Possible Causes

- The configuration file is incorrect.
- The configuration file does not match the CM.

Procedure

Replace the configuration file for the CM.

12.1.17 CM Remains in the Reject State

If a CM remains in the reject state, it fails to be authenticated by the D-CCAP and cannot communicate with the D-CCAP.

Possible Causes

The reject type of the CM can be used to identify the failure cause.

- rej-m: The MIC check fails.
- rej-pt: BPI+ authentication fails.
- rej-o: Other reasons cause the failure.

Procedure

- Step 1** Run the **display certificate** command to query certificates on the D-CCAP. Then, check whether the BPI+ certificate is correct.
- Step 2** Check whether the CM configuration file is correct.
- Step 3** Check whether the version of the DOCSIS standard that the CM complies with is correct.
- Step 4** Check whether the number of service flows that have been created on the D-CCAP has reached the maximum number.

----End

12.1.18 Failure to Obtain an IP Address of a PC

If a PC fails to obtain an IP address, the PC connected to an online CM cannot obtain an IP address from a DHCP server.

Location Method and Procedure

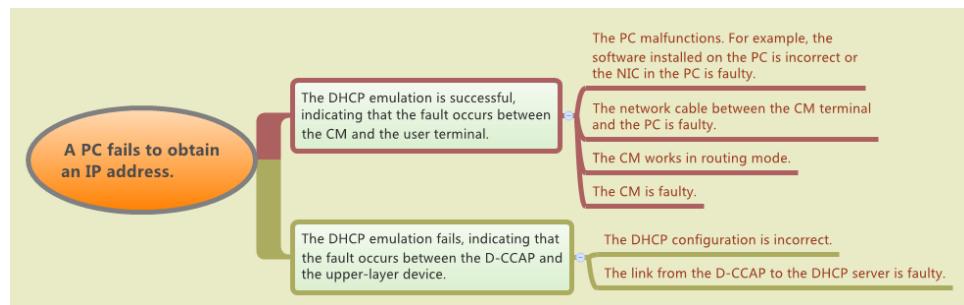
If a PC fails to obtain an IP address, perform a DHCP emulation test on the CM. Specifically, apply to the DHCP server for an IP address on the CM. This facilitates fault location.

- In global config mode, run the **simulate dhcp start cm mac-address [option60 option60]** command to start a DHCP emulation test.

NOTE

In the preceding command, *option60* is the DHCP domain name of the PC queried by running the **display dhcp domain** command.

- Run the **display simulation dhcp** command to query the test result.



NOTICE

To facilitate fault report, save the results of the following steps.

Procedure

Step 1 Verify that the link between the PC and the CM is functional.

If the fault persists, go to [Step 2](#).

Possible Cause	Location Analysis	Handling Method
<ul style="list-style-type: none">The software is incorrectly installed on the PC.The network interface card (NIC) in the PC is faulty.The PC is affected by viruses.	The fault does not recur after the PC is replaced.	Check whether the software is correctly installed on the PC and the NIC in the PC is functional.
The network cable between the CM terminal and the PC is faulty.	The fault does not recur after the cable is replaced.	Ensure that the network cable is securely connected.
The CM works in routing mode.	The fault does not recur after the working mode of the CM is corrected.	Modify the MC to work in bridging mode.
The CM terminal is faulty.	The fault does not recur after the CM terminal is replaced.	Replace the CM.

Step 2 Verify that the link between the D-CCAP and the upper-layer device is functional.

If the fault persists, go to [Step 3](#).

Possible Cause	Location Analysis	Handling Method
The DHCP configuration is incorrect.	The DHCP server can be pinged from the D-CCAP.	Check the DHCP configuration.
The link between the D-CCAP and the DHCP server is faulty.	The DHCP server cannot be pinged from the D-CCAP.	Check the routing configuration.

Step 3 Contacting Huawei for Assistance.

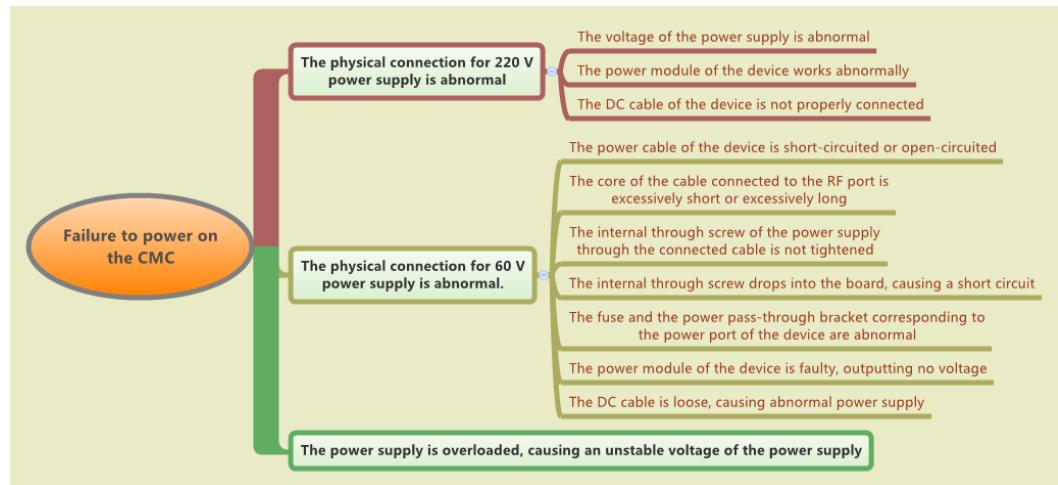
Step 4 End.

----End

12.1.19 Failure to Power on the CMC

The CMC cannot be powered on after the power supply is turned on. The power indicator (PWR) is not steady on.

Location Method



Procedure

Step 1 In the 220 V power supply scenario:

1. Check whether the 220 V power supply voltage is normal (normal voltage range: 100 V to 240 V). For example, check whether the supply voltage is too high or too low.
2. Check whether the power supply module is normal. You can check the voltage at the 220 V input point, and then check the voltage at the 24 V and the 12 V output points. If the input voltage is normal but no power is output, the power supply module is faulty.
3. Check whether the DC cable of the device DC is loose. If the DC cable is loose, connect it properly.

Step 2 In the 60 V power supply scenario:

1. Check whether the 60 V power supply voltage is normal (normal voltage range: 35 V to 90 V). For example, check whether the supply voltage is too high or too low.
2. Check whether the power cable is short-circuited or open-circuited.
3. Check whether the pin of the F connector or KS connector on the RF OUT port is too long or too short. According to the product specifications, the total length from the pin end to the shell edge must be within 27 mm and 29 mm, including the pin length and the length of the invisible part installed inside the shell for thread matching.
4. Check whether the internal through screw is tightened.
5. Check whether the internal through screw drops into the device, causing a short circuit.
6. Check whether the fuse and the power pass-through bracket corresponding to the power port of the device are abnormal
7. Check whether the power supply module is normal. You can check the voltage at the 60 V input point, and then check the voltage at the 24 V and the 12 V output points. If the input voltage is normal but no power is output, the power supply module is faulty.

8. Check whether the DC cable of the device DC is loose. If the DC cable is loose, connect it properly.

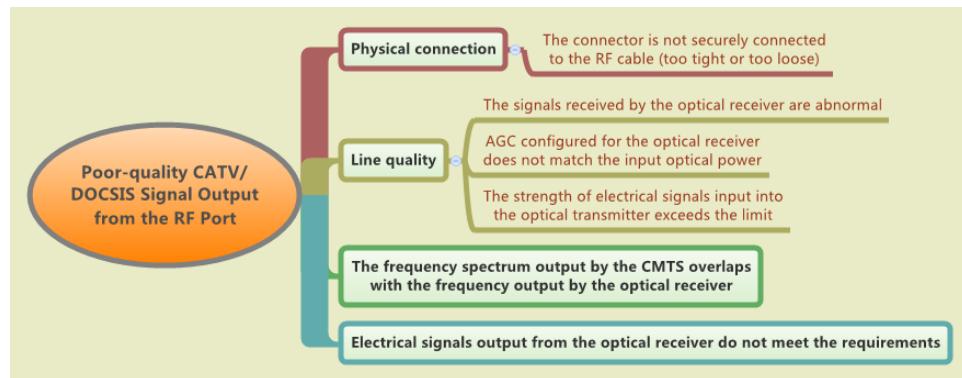
Step 3 If the fault persists even after the troubleshooting measures described in this document have been taken, contacting Huawei for Assistance.

----End

12.1.20 Poor-quality CATV/DOCSIS Signal Output from the RF Port

A field strength meter is used to test the RF OUT port, and it is found that the quality of CATV/DOCSIS signals is poor, and one or more indicators such as MER, BER, and level cannot meet the output requirements of the device.

Location Method



Procedure

Step 1 Check whether the connector is securely connected to the RF cable.

If the connector is not securely connected (excessively tight or excessively loose), the output CATV or DOCSIS signals may be abnormal. As a result, indicators such as level, MBR, and BER are abnormal.

Step 2 Check the optical power of the optical receiver.

Run the **config** command to enter global config mode and run the **interface optical-receiver** command to enter optical receiver mode. Then, run the **display option-receive run info** command to query the optical power of the optical receiver. You can locate optical power abnormalities by checking the following items:

- Whether the APC or UPC connectors on the optical path are matched.
- Whether the attenuation is normal.
- Whether the optical fiber is broken.
- Whether the fiber coiling diameter is greater than 10 cm.

Step 3 Check whether the frequency spectra of DOCSIS and CATVT signals overlap.

Through the steps below, check whether the frequency spectra of DOCSIS and CATVT signals overlap.

- Run the **display current-configuration** command to query the output frequency of DOCSIS signals.

- Use a field strength meter to measure the output frequency of the CATV signals.

Step 4 Check the indicators of the electrical signals output by the optical receiver.

- Ensure that the level difference of the CATV analog signals and DOCSIS signals output by the optical receiver is 6–10 dB, the levels of the CATV digital signals and DOCSIS signals are consistent, and the maximum level of the CATV digital signals does not exceed the limit.
- Test the level of signals at the test point of the optical receiver, and ensure that MER and BER are not deteriorated. If MER and BER are deteriorated, check the upper-level circuit, and check whether the electrical signals input into the corresponding optical transmitter are abnormal.

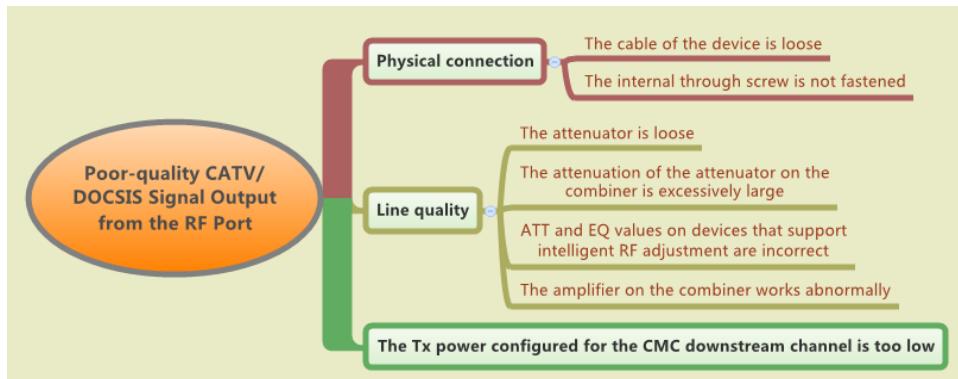
Step 5 If the fault persists even after the troubleshooting measures described in this document have been taken, contacting Huawei for Assistance.

----End

12.1.21 Low-power-level CATV/DOCSIS Signal Output from the RF Port

CATV/DOCSIS signals are output at low power level from the RF OUT port.

Location Method



Procedure

Step 1 Check the physical connection.

- Check whether the connection of the DOCSIS signal link is normal according to the following signal flow direction:
MA5633 board -> RF cable -> connection end of the combiner -> attenuation on the combiner -> internal through screw on the combiner -> connector of the RF OUT port
- Check whether the connection of the CATV signal link is normal according to the following signal flow direction:
EQ and ATT on the optical receiver or transmitter (optional) -> cable connecting the optical receiver or transmitter and combiner -> connection end of the combiner -> attenuation on the combiner -> internal through screw on the combiner -> connector of the RF OUT port

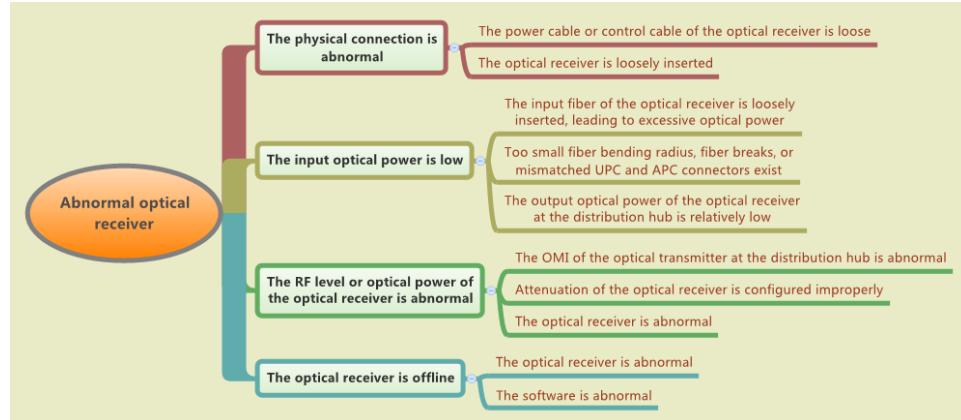
- Step 2** Check whether the specifications of EQ, ATT, and other brackets meet the customer's power level output requirements. Ensure that the attenuation bracket is securely installed.
- Step 3** For devices that support intelligent RF adjustment, run the **display cable rf-power frameid downstream** or **display cable rf-power frameid upstream** command to check whether the ATT and EQ configuration on the combiner is correct. Run the **display cable rf-power-monitor frameid downstream status** command to query the output power level detected by the tuner inside the MA5633, or use a signal tester to check whether the output power level is correct.
- Step 4** Check the amplifier status.
Check the power at both input point and output point of the amplifier. Then, check whether the power difference is the same as the amplifier gain, which is generally 20 dB (varies depending on different combiner types).
- Step 5** Run the **display cable downstream** to check whether the Tx power configured for the CMC downstream channel is too low.
- Step 6** Check the power level of signals output from the optical receiver or transmitter.
Use the field strength indicator to measure the power level at the output point of the optical receiver or transmitter, or measure the power level of output signals combined with CATV signals in the combiner. Then check whether the measured output power level is the same as the configured value.
- Step 7** If the fault persists even after the troubleshooting measures described in this document have been taken, contacting Huawei for Assistance.

----End

12.1.22 Abnormal Optical Receiver

When the optical receiver is abnormal, the device generates the corresponding alarm.

Locating Method



Procedure

- Step 1** Check whether the optical receiver or cable is properly installed and ensure that there are no loose cable or optical receiver.

Step 2 Check the optical receiver status.

Run the **display optical-receiver run info** command to query the optical receiver status. Check whether there are alarms related to abnormal optical signals, RF signals, or optical power and ensure that the RF function of the optical receiver is enabled and attenuation of the optical receiver is correctly configured.

Step 3 Check the offline optical receiver.

If the optical receiver is offline in the **display optical-node** command output, power off and restart the device. If the fault persists, the optical receiver is faulty. In this case, replace the CMC.

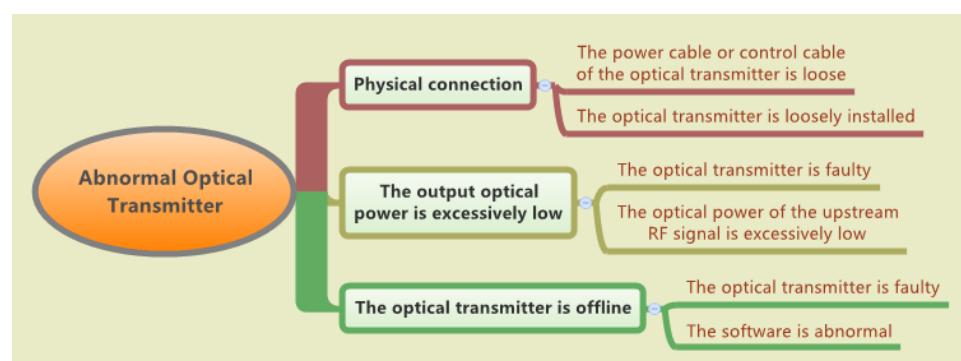
Step 4 If the fault persists even after the troubleshooting measures described in this document have been taken, contacting Huawei for Assistance.

----End

12.1.23 Abnormal Optical Transmitter

When the optical transmitter is abnormal, the device generates the corresponding alarm.

Location Method



Procedure

Step 1 Check whether the optical transmitter or cable is properly installed and ensure that there are no loose cable or optical transmitter.

Step 2 Check the optical transmitter status.

Run the **display optical-transmitter run info** command to query the optical transmitter status. Check whether there are alarms related to abnormal optical signals, optical power, or bias current.

Step 3 Check the offline optical transmitter.

If the optical transmitter is offline in the **display optical-node** command output, power off and restart the device. If the fault persists, the optical transmitter is faulty. In this case, replace the CMC.

Step 4 If the fault persists even after the troubleshooting measures described in this document have been taken, contacting Huawei for Assistance.

----End

12.2 Fault Cases

This section describes common troubleshooting processes.

12.2.1 Failure to Provision Services Due to a Bug in the ARP Packet Interaction Mechanism

A CM of a model connected to an MA5633. Due to a bug in the ARP packet interaction mechanism, the CM could not provide broadband and VoD services after going online.

Cause Analysis

1. When CM 1 went online, the DHCP server allocated IP address A to CM 1 and the OLT generated ARP entry **IPA---CM1**.
2. When CM 1 went offline, the ARP entry was not aged on the OLT and the DHCP server added IP address A to the IP address pool.
3. When CM 3 went online, the DHCP server allocated IP address A to CM 3 and the OLT generated ARP entry **IPA---CM1**. As a result, an error occurred in ARP packet interaction when CM 3 went online and services on CM 3 failed.
4. After a CM goes online in dialup mode, it should use a gratuitous ARP packet to advertise its ARP entry. In this way, the OLT can update the ARP entry from **IPA---CM1** to **IPA---CM3** when receiving this gratuitous ARP packet. Based on the analysis, this affected CM did not report a gratuitous ARP packet after going online. As a result, the ARP entry on the OLT was not updated and downstream packets that were expected to send to this CM were forwarded in an incorrect direction. That was why this fault occurred.

Solution

- Modify the OLT configuration as follows:
 - a. Run the **arp aging-mode control** command to change the ARP aging mode from the forwarding plane to the control plane.
 - b. Run the **arp aging-time** command to change the ARP aging time to a smaller value based on the number of ARP entries on the OLT.

NOTE

Value 5 is recommended. This configuration significantly reduces the probabilities that this fault occurs. If such a fault occurs, services are interrupted for at most 5 minutes.

- Fix the bug in the CM by modifying service activities performed by the CM. Specifically, after obtaining an IP address, the CM sends a gratuitous ARP packet to adjacent devices, informing them of ARP entry updating.

12.2.2 Interrupted Program Playing Because IGMP Proxy Was Not Enabled

A program was interrupted 5 minutes after it was played. The program playing automatically recovered in 1 minute. The cause of this fault was that IGMP proxy was not enabled on the D-CCAP.

Cause Analysis

The affected CM did not comply with the DOCSIS standard.

- Functioning as the querier of CPEs, the CM did not send IGMP query packets to CPEs.
- The CM did not forward the join packets sent by the CPEs to the D-CCAP.

Solution

Run the **igmp mode proxy** command to enable IGMP proxy on the D-CCAP. Then, run the **igmp query-offline-user enable** command to allow the D-CCAP to send general query packets in offline mode to CPEs.

12.2.3 Failure to Upgrade a CMC Due to Incorrect TFTP Tool Configuration

A CMC was upgraded using the TFTP tool. During data loading, the file failed to transfer.

Cause Analysis



TFTP has security risks due to protocol restrictions. SFTP is recommended.

The timeout time configured on the TFTP tool was excessively short. As a result, the TFTP transmission was interrupted when the timeout time expired.

Solution

Replace the TFTP tool or prolong the timeout time configured on the TFTP tool.

12.2.4 Low Internet Access Rates Due to Excessively Low Output SNRs of CMs

The Internet access rates were low on some CMs connected to a D-CCAP because of the excessively low SNRs of the CMs.

Cause Analysis

Based on the SNRs measured on the CMs, the downstream SNRs of the CMs of a model were excessively low. Generally, the downstream MER should be higher than 35 dB.

Solution

Replace the affected CMs with the ones of another model to rectify this fault.

12.2.5 Frequent CM Online and Offline Due to a CM Fault

A CM frequently went online and offline due to a CM fault.

Cause Analysis

Based on data statistics collected on the CM, the CM went online and then offline every period of time. In addition, some periodic ranging requests were lost.

Possible causes of this fault are as follows:

- The CM was faulty.
- The interference on the line was strong.

Solution

Replace this affected CM with another one and the new CM is functional. Therefore, the line is functional and the fault is caused by the original CM. Replace this CM to rectify this fault.

13 Glossary

Numerics

1+1 backup	A backup method in which two components mirror each other. If the active component goes down, the standby component takes over services from the active component to ensure that the system service is not interrupted.
1000BASE-T	An Ethernet specification that uses the twisted pair cable with the transmission speed as 1000 Mbit/s and the transmission distance as 100 meters.
24-hour alarm threshold	The number of times (greater than the set threshold) an alarm is generated within 24 hours. When the threshold is set to 0, the alarm function is disabled.
3DES	See Triple Data Encryption Standard .
3G	See Third Generation .
3GPP	3rd Generation Partnership Project
802.11n	A wireless transmission standard released after 802.11a/b/g by Wi-Fi Alliance. As a new member to the 802.11 protocol family, 802.11n supports the 2.4 GHz and 5 GHz frequency bands and provides a higher bandwidth (300 Mbit/s, much higher than the 54 Mbit/s provided by 802.11a/g) for WLAN access users. In addition, 802.11n supports the MIMO technology, which provides two methods of increasing the communication rate: by increasing the bandwidth and by improving the channel usage.
802.1Q in 802.1Q (QinQ)	A VLAN feature that allows the equipment to add a VLAN tag to a tagged frame. The implementation of QinQ is to add a public VLAN tag to a frame with a private VLAN tag to allow the frame with double VLAN tags to be transmitted over the service provider's backbone network based on the public VLAN tag. This provides a layer 2 VPN tunnel for customers and enables transparent transmission of packets over private VLANs.

802.1X	An access control and authentication protocol based on the client/server mode. It can prevent unauthorized users/equipment from accessing the LAN/WLAN through an access port. After a client (STA) is associated with an AP, the 802.1X authentication result determines whether the STA can use the wireless services provided by the AP. If the STA passes the authentication, the STA can access the resources in the WLAN. If the STA fails to pass the authentication, the STA cannot access the resources in the WLAN.
802.1ag MAC ping	A network administration utility similar to ping. 802.1ag MAC ping works by sending test packets and waiting for a reply to test whether the destination device is reachable. 802.1ag MAC ping is initiated by a MEP and destined for a MEP or MIP at the same maintenance level within any MA.
802.1ag MAC trace	A network diagnostic tool similar to traceroute or tracert. 802.1ag MAC trace works by sending test packets and waiting for a reply to test the path between the local device and the destination device and to locate faults. 802.1ag MAC trace is initiated by a MEP and destined for a MEP or MIP at the same maintenance level within any MA.
A	
A3	algorithm A3
A5	See algorithm A5 .
AA	anycast addressing
AAA	See Authentication, Authorization and Accounting .
AAA server	The remote server that provides authentication, authorization, accounting, and value-added services for the dialed-in users.
AAL	See ATM Adaptation Layer .
AAL5	ATM Adaptation Layer Type 5
AC	access category
ACB	access barred signal
ACH	associated channel header
ACK	See acknowledgement .
ACL	See Access Control List .
ACL group	A group for ACL rules. One ACL group needs to be set up before the ACL rules are configured. The ACL group is mainly used to determine the type of the ACL rule, the match sequence, and the step length.
ACM	See address complete message .

ACR	allowed cell rate
ACS	See Application Control Server .
AD	active directory
ADC	Analogue-to-Digital Converter
ADD	automatic device detection
ADI	address incomplete signal
ADM	add/drop multiplexer
ADMC	automatically detected and manually cleared
ADN	See abbreviated dialing number .
ADSL	See asymmetric digital subscriber line .
ADSL Port information Protocol (APP)	A protocol that is used to control and maintain the line-capturing device, for example, control the STAM, ETAM, and so on.
ADSL2+	asymmetric digital subscriber line 2 plus
AES	See Advanced Encryption Standard .
AF	adaptation function
AFE	analog front end
AFI	address family identifier
AH	See Authentication Header .
AID	access identifier
AIS	alarm indication signal
ALG	See application level gateway .
ALS	See automatic laser shutdown .
AM	See adaptive modulation .
AMB	active main board
AMC	automatic modulation control
AMI	See alternate mark inversion .
AMR	automatic meter reading system
AN	access node
ANC	answer signal, charge
ANCP	See Access Node Control Protocol .
AND	See ATAE Networking Daemon .
ANI	See automatic number identification .

AOC	See access overload class .
AOE	ATM over Ethernet
AP	access preamble
APC	automatic phase changer
APD	See avalanche photodiode .
API	See application programming interface .
APP	See ADSL Port information Protocol .
APS	automatic protection switching
AR	alternative route
ARL	average rotational latency
ARP	See Address Resolution Protocol .
AS	application server
ASA	average speed of answer
ASBR	See autonomous system boundary router .
ASCII	American Standard Code for Information Interchange
ASE	amplified spontaneous emission
ASIC	See application-specific integrated circuit .
ASL	analog subscriber line
ASM	See any-source multicast .
ASN	abstract syntax notation
ASP	active server page
ATAE Networking Daemon (AND)	The AND helps rectify switch board chip faults, network cable faults, STP use failures, standby link faults, and network faults that occur because bond network adapters monitor links by using the ARP, improving network reliability.
ATAG	autonomously generated correlation tag
ATM Adaptation Layer (AAL)	An interface between higher-layer protocols and Asynchronous Transfer Mode (ATM). The AAL provides a conversion function to and from ATM for various types of information, including voice, video, and data.
ATM switch	A switch that transmits cells over an Asynchronous Transfer Mode (ATM) network. It receives an incoming cell from an ATM endpoint or another ATM switch, analyzes and updates the cell header information, and switches the cell to an output interface towards the destination.

ATM/Ethernet emulation	Emulation of the ATM/Ethernet service in a network which is neither an ATM network nor an Ethernet network.
ATTNDR	See attainable net data rate .
ATU	ADSL terminal unit
ATU-C	ADSL transceiver unit-central office end
ATU-R	ADSL transceiver unit-remote terminal end
AV	antivirus
AVP	See attribute-value pair .
AVS	Audio Video Coding Standard
AWG	arrayed waveguide grating
Access Control List (ACL)	A list of entities, together with their access rights, which are authorized to access a resource.
Access Node Control Protocol (ANCP)	An IP-based protocol that operates between the access node (AN) and the network access server (NAS), over a DSL access and aggregation network.
Address Resolution Protocol (ARP)	An Internet Protocol used to map IP addresses to MAC addresses. The ARP protocol enables hosts and routers to determine link layer addresses through ARP requests and responses. The address resolution is a process by which the host converts the target IP address into a target MAC address before transmitting a frame. The basic function of ARP is to use the target equipment's IP address to query its MAC address.
Advanced Encryption Standard (AES)	The AES algorithm is a symmetric grouped password algorithm and one of the most popular symmetric key encryption algorithms released by the U.S. National Institute of Standards and Technology (NIST) on November 26, 2001. It is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). It supersedes the Data Encryption Standard (DES). AES adopts a symmetric-key algorithm for both encrypting and decrypting the data, where the block size is 128 bits and the key size is 128 bits, 192 bits, or 256 bits.
Ah	ampere hour
Allow	A header field, which gives a list of request types that can all be supported by the proxy server.
AoC	advice of charge
Application Control Server (ACS)	A subsystem of the Media Entertainment Middleware (MEM), used for providing a service control interface for the Electronic Program Guide (EPG) server.

Authentication Header (AH)	A protocol that provides connectionless integrity, data origin authentication, and anti-replay protection for IP data.
Authentication, Authorization and Accounting (AAA)	A security architecture for distributed systems. Enables control over which users are allowed access to which services and how much resources they can use.
abbreviated dialing number (ADN)	The short number used for the feature that permits the calling party to dial the destination telephone number in fewer than normal digits.
access level	The level of users, programs, data, or processes classified according to the resources or resource groups that are authorized to access in the information system.
access list	A list of the resources that can be accessed. For example, the specification list that describes users, programs, or processes and the levels they can access.
access overload class (AOC)	An indication of access load control. The access load control is exerted at 16 levels and each MS is allocated an access load control level. When accessing the networking, each MS continuously monitors the load on the Um interface based on its access load control level. In this way, higher-priority MSs preferentially access the network in some specific scenarios. For example, AOCs 0 to 9 indicate common MSs; AOC 10 indicates a test MS; and AOC 11 indicates a VIP MS.
access port	A switch port used to connect to user hosts. The access port can connect to only the access link. On an access port, all the untagged incoming packets are attached with the same tag through the PVID whereas tagged packets are discarded. If the PVID of a packet is not set, the packet is also discarded.
access security	The security of the measures taken to authenticate a user's access to the system.
accumulation	The sum of the service usage, consumption, and recharge fees of a subscriber.
acknowledgement (ACK)	A response sent by a receiver to indicate reception of information. Acknowledgements may be implemented at any level, including the physical level (using voltage on one or more wires to coordinate a transfer), link level (indicating transmission across a single hardware link), or higher levels.
action type	An operation that does not move principal amounts between accounts. An action is typically an activity that affects the state of an identity, informs identity, or enables identity's engagement.
active link	A link in the link aggregation group, which is connected to the active interface.

active service	A service that a carrier performs to retain customers, for example, customer retaining, customer return visit, customer care, customer investigation, or information releasing.
active/standby backup	A backup mechanism in which the same two systems are deployed to improve the reliability.
actual user	An individual or organization that actually uses the services provided by the carriers.
adaptive modulation (AM)	A technology that is used to automatically adjust the modulation mode according to the channel quality. When the channel quality is favorable, the equipment uses a high-efficiency modulation mode to improve the transmission efficiency and the spectrum utilization of the system. When the channel quality is degraded, the equipment uses the low-efficiency modulation mode to improve the anti-interference capability of the link that carries high-priority services.
additional bandwidth	The sum of the non-assured bandwidth plus the best-effort bandwidth.
additional system ID	A system ID assigned by the network manager. Each additional system ID can generate up to 256 additional or extended LSP fragments.
address complete message (ACM)	A message defined in ISUP and BICC. An ACM message is sent after all address analysis signals are received by the called side.
administrator	A user who has authority to access all EMLCore product management domains. This user has access to the entire network and all management functions.
advance payment	A fee that is paid by a customer in advance when the customer is not in arrears.
advertiser	A manufacturer, service company, retailer, or supplier who advertises their products or services.
aggregated link	Multiple signaling link sets between two nodes.
air duct	A ventilation duct in a chassis to change the direction of air flow and reduce air pressure loss. With the air duct, the chassis uses fans to draw air in through the front and exhaust air through the rear.
alarm ID	The one and only alarm identifier consisting of four bytes. Each alarm has an ID. Generally, allocate the alarm ID according to the alarm category and alarm module.
alarm box	A device that reflects the status of an alarm in visual-audio mode. The alarm box notifies you of the alarm generation and alarm severity after it is connected to the Signaling Network Manager server or client and the related parameters are set.

alarm cause	The root cause of an alarm. A single fault or defect may lead to the generation of multiple alarms. Through a process of alarm correlation analysis, the root alarm cause can be identified.
alarm correlation rule	The rule for processing correlated alarms (for example, alarm 1 and alarm 2) under certain conditions. The following conditions are supported: (1) Alarm 1 and alarm 2 occur on the same object. (2) Alarm 1 occurs in the upstream service end of alarm 2. (3) Alarm 1 occurs at the peer service end of alarm 2. The following actions are supported: (1) Alarm 1 masks alarm 2. (2) The level of alarm 2 is raised. The alarm correlation rule is the basis for alarm correlation analysis, which affects the result of alarm correlation analysis. Exercise caution when setting the alarm correlation rule.
alarm masking	A method to mask alarms for the alarm management purpose. Alarms that are masked are not displayed on the NMS or the NMS does not monitor unimportant alarms.
alarm notification	When an error occurs, the performance measurement system sends performance alarms to the destination (for example, a file and/or fault management system) designated by users.
alarm output	Node or other signals that are sent by an alarm controller to peripheral devices when an alarm is reported.
alarm service	A service wherein the managed device sends the unrequested messages to the log host to report its emergent and important events. If you want a router to actively send trap messages to the log host, you need to configure the alarm service on the router.
alarm source	A device that generates an alarm. To automatically report alarms, the ECC system can receive alarms from multiple alarm sources such as smoke detectors and alarming hosts.
alarm suppression	A method to suppress alarms for the alarm management purpose. Alarms that are suppressed are no longer reported from NEs.
algorithm A5 (A5)	Ciphering algorithms specified in the GSM specification: The A5 ciphering algorithms consist of the A5/0, A5/1, A5/2, A5/3, A5/4, A5/5, A5/6, and A5/7 algorithms.
alternate mark inversion (AMI)	A synchronous clock encoding technique which uses bipolar pulses to represent logical 1 values.

analog signal	A signal in which information is represented with a continuously variable physical quantity, such as voltage. Because of this constant changing of the wave shape with regard to its passing a given point in time or space, an analog signal might have a virtually indefinite number of states or values. This contrasts with a digital signal that is expressed as a square wave and therefore has a very limited number of discrete states. Analog signals, with complicated structures and narrow bandwidth, are vulnerable to external interference.
any-source multicast (ASM)	A multicast service mode. In ASM mode, any sender can become the multicast source to send information to a multicast group address. After joining the multicast group identified by this address, multiple receivers can receive all the information sent to this multicast group.
application level gateway (ALG)	An ALG consists of a security component that augments a firewall or NAT employed in a computer network. It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, BitTorrent, SIP, RTSP, file transfer in IM applications etc. In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.
application programming interface (API)	An application programming interface is a particular set of rules and specifications that are used for communication between software programs.
application-specific integrated circuit (ASIC)	A special type of chip that starts out as a nonspecific collection of logic gates. Late in the manufacturing process, a layer is added to connect the gates for a specific function. By changing the pattern of connections, the manufacturer can make the chip suitable for many needs.
assignment	A process in which radio resources are requested, modified, released and re-established during a call setup.
associated mode	A mode in which signaling messages are exchanged between two signaling points over direct signaling links.

asymmetric digital subscriber line (ADSL)	A technology for transmitting digital information at a high bandwidth on existing phone lines to homes and businesses. Unlike regular dialup phone service, ADSL provides continuously-available, "always on" connection. ADSL is asymmetric in that it uses most of the channel to transmit downstream to the user and only a small part to receive information from the user. ADSL simultaneously accommodates analog (voice) information on the same line. ADSL is generally offered at downstream data rates from 512 kbit/s to about 6 Mbit/s.
asynchronous mode	A mode in which different systems send BFD control packets to each other periodically. If one system fails to receive the BFD control packets sent from the peer end within the detection period, the system reports that the session is down.
attainable net data rate (ATTNDR)	A capacity metric of the ADSL communication channel. It is also referred to as the Maximum Attainable Bit Rate (MABR) in ADSL standards.
attendant	A person who provides service enquiry and assistance for group members. In the VPN service, an attendant may be a group member or someone from the carrier's party.
attenuator	A device used to increase the attenuation of an Optical Fiber Link. Generally used to ensure that the signal at the receive end is not too strong.
attribute-value pair (AVP)	An information element that includes a header and is used to encapsulate protocol-specific data (for example, routing information) as well as authentication, authorization or accounting information. The Diameter protocol consists of a header followed by one or more AVPs.
authentication scheme	A method for implementing user authentication. Users in different domains corresponds with different authentication schemes. The system can be configured with 32 authentication schemes at most.
authentication server	An entity that provides an Authentication Service to an Authenticator. This service determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the Authenticator.
automatic bandwidth adjustment	Traffic Engineering needs to dynamically assign network resources without interrupting services when the environment changes. Because users do not know how many services are transmitted through the network provided by the service provider and will to pay for the used bandwidth, the service provider needs to support the following functions using MPLS TE automatic bandwidth adjustment: 1) Setting up the traffic Engineering tunnel CR-LSP 2) Dynamically adjusting the CR-LSP bandwidth when services increase

automatic laser shutdown (ALS)	A technique (procedure) to automatically shutdown the output power of laser transmitters and optical amplifiers to avoid exposure to hazardous levels.
automatic login	A login mode in which user name and password are not required when you double-click the host icon, when the client disconnects from the host, or when you start the client. The system automatically logs in to the host with the latest user name and password that are used to log in to the host successfully. The automatic login mode is classified into double-click login mode and automatic link mode.
automatic number identification (ANI)	An SS7 feature in which a series of digits, either analog or digital, are included in the call, identifying the telephone number of the calling device.
autonomous system boundary router (ASBR)	A router that exchanges routing information with other autonomous system boundary routers.
availability	A capability of providing services at any time. The probability of this capability is called availability.
avalanche photodiode (APD)	A semiconductor photodetector with integral detection and amplification stages. Electrons generated at a p/n junction are accelerated in a region where they free an avalanche of other electrons. APDs can detect faint signals but require higher voltages than other semiconductor electronics.

B

B-ISDN	See broadband integrated services digital network .
B-VLAN	backbone virtual local area network
BAC	biometric access control
BAM	back administration module
BAS	See broadband access server .
BASE	A kind of bus or plane used to load software, transmit alarms and maintain information exchange.
BAT	bearer association transport
BC	boundary clock
BCH	See broadcast channel .
BCM	basic call management
BDI	See backward defect indication .

BDI packet	A packet used to notify the upstream LSR of the failure event which has occurred on the downstream LSR through the reverse LSP. The BDI packet can be used in the 1:1/N protective switchover service.
BE	See best effort .
BER	See basic encoding rule .
BFD	See Bidirectional Forwarding Detection .
BGP	Border Gateway Protocol
BHCA	See busy hour call attempts .
BIOS	See basic input/output system .
BIP	See bit interleaved parity .
BIS	See Business Interface Server .
BITS	See building integrated timing supply .
BMS	business management system
BOM	bill of materials
BOOTP	See Bootstrap Protocol .
BPDU	See bridge protocol data unit .
BPON	See broadband passive optical network .
BR	border router
BRA	See basic rate access .
BRAS	See broadband remote access server .
BRI	basic rate interface
BSC	binary synchronous communication
BSP	board support package
BSS	Business Support System
BTS	base transceiver station
BTV	broadcast TV
BYE	A SIP request that indicates session ending.
Bidirectional Forwarding Detection (BFD)	A fast and independent hello protocol that delivers millisecond-level link failure detection and provides carrier-class availability. After sessions are established between neighboring systems, the systems can periodically send BFD packets to each other. If one system fails to receive a BFD packet within the negotiated period, the system regards that the bidirectional link fails and instructs the upper layer protocol to take actions to recover the faulty link.

Bootstrap Protocol (BOOTP)	A TCP/IP protocol that enables a network device to discover certain startup information, such as its IP address.
Business Interface Server (BIS)	The BIS provides interfaces for policy subscription, log query, and user management, and these interfaces can be invoked by third-party systems, for example, the portal of customers.
backbone network	A network that forms the central interconnection for a connected network. The communication backbone for a country is WAN. The backbone network is an important architectural element for building enterprise networks. It provides a path for the exchange of information between different LANs or subnetworks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Generally, the backbone network's capacity is greater than the networks connected to it.
backup center	A mechanism in which interfaces on a device back up each other and the status of each interface is traced. If an interface is Down, the backup center provides a backup interface to take over.
backup link	A link that is used to improve link reliability in link aggregation. A backup link is in inactive state and changes to active state only when the current active interface fails.
backup task	A process of backing up data based on backup policies.
backward defect indication (BDI)	A function that the sink node of a LSP, when detecting a defect, uses to inform the upstream end of the LSP of a downstream defect along the return path.
bandwidth protection	A mechanism ensuring that the bypass tunnel reserves sufficient bandwidth to protect the traffic of the protected tunnel.
baseband	A form of modulation in which the information is applied directly onto the physical transmission medium.
basic encoding rule (BER)	A rule in the syntax structure of the ASN.1, which describes how data is represented during transmission.
basic input/output system (BIOS)	Firmware stored on the computer motherboard that contains basic input/output control programs, power-on self test (POST) programs, bootstraps, and system setting information. The BIOS provides hardware setting and control functions for the computer.
basic rate access (BRA)	An ISDN interface typically used by smaller sites and customers. This interface consists of a single 16 kbit/s data (or "D") channel plus two bearer (or "B") channels for voice and/or data. Also known as Basic Rate Access, or BRI.

bearer control	A lower-layer capability that enables bearer services to provide signaling transmission capability between subscriber access points (subscriber/network interface). Briefly, it is the function of setup release of the bearer plane.
best effort (BE)	A traditional IP packet transport service. In this service, the diagrams are forwarded following the sequence of the time they reach. All diagrams share the bandwidth of the network and routers. The amount of resource that a diagram can use depends of the time it reaches. BE service does not ensure any improvement in delay time, jitter, packet loss ratio, and high reliability.
best-effort service	A unitary and simple service model. Without being approved, but after notifying the network, the application can send any number of packets at any time. The network tries its best to send the packets, but delay and reliability cannot be ensured. Best-Effort is the default service model of the Internet. It can be applied to various networks, such as FTP and E-Mail. It is implemented through the First In First-Out (FIFO) queue.
bidirectional isolation	A method of isolating two interfaces from each other. For example, if isolation from interface B is configured on interface A and isolation from interface A is configured on interface B, interface A and interface B cannot forward packets to each other.
bidirectional protection switching	A switching that occurs in both directions for a unidirectional fault (of the trail, subnetwork connection, and so on), including the affected and unaffected directions.
binding authentication	An authentication mode in which the BRAS creates a user name and a password for the user according to the location of the user.
bit interleaved parity (BIP)	A method of error monitoring. With even parity, the transmitting equipment generates an X-bit code over a specified portion of the signal in such a manner that the first bit of the code provides even parity over the first bit of all X-bit sequences in the covered portion of the signal, the second bit provides even parity over the second bit of all X-bit sequences within the specified portion, and so forth. Even parity is generated by setting the BIP-X bits so that an even number of 1s exist in each monitored partition of the signal. A monitored partition comprises all bits in the same bit position within the X-bit sequences in the covered portion of the signal. The covered portion includes the BIP-X.
bit/s	See bits per second .
bits per second (bit/s)	A rate at which the individual bits are transmitted through a communication link or circuit. Its unit can be bit/s, kbit/s, and Mbit/s.

blacklist	A method of filtering packets based on their source IP addresses. Compared with ACL, the match condition for the black list is much simpler. Therefore, the black list can filter packets at a higher speed and can effectively screen the packet sent from the specific IP address.
blacklist and whitelist	A method used by the system to determine whether to connect a call based on the preset restriction relation between the home group of the calling party and the home group of the called party.
bridge protocol data unit (BPDU)	Data messages exchanged across switches within an extended LAN that uses a spanning tree protocol (STP) topology. BPDU packets contain information on ports, addresses, priorities, and costs, and they ensure that the data reaches its intended destination. BPDU messages are exchanged across bridges to detect loops in a network topology. These loops are then removed by shutting down selected bridge interfaces and placing redundant switch ports in a backup, or blocked, state.
broadband access server (BAS)	A server that provides features such as user access, connection management, address allocation and authentication, authorization, and accounting. It can also provide features of a router, such as effective route management and high forwarding performance, and supports a wide range of services.
broadband integrated services digital network (B-ISDN)	A standard defined by the ITU-T to handle high-bandwidth applications, such as voice. It currently uses the ATM technology to transmit data over SONNET-based circuits at 155 to 622 Mbit/s or higher speed.
broadband passive optical network (BPON)	One-to-many broadband optical transmission system. B-PONs can transparently transport any type of data, for example voice, video, IP data, and so on. The B-PON is able to carry data regardless of the type of data link frame.
broadband remote access server (BRAS)	A new type of access gateway for broadband networks. As a bridge between backbone networks and broadband access networks, BRAS provides methods for fundamental access and manages the broadband access network. It is deployed at the edge of network to provide broadband access services, convergence, and forwarding of multiple services, meeting the demands for transmission capacity and bandwidth utilization of different users. BRAS is a core device for the broadband users' access to a broadband network.
broadcast channel (BCH)	A code channel in a Forward CDMA Channel used for transmission of control information and pages from a base station to a mobile station.

broadcast domain	A group of network stations that receives broadcast packets originating from any device within the group. The broadcast domain also refers to the set of ports between which a device forwards a multicast, broadcast, or unknown destination frame.
broadcast message	A message sent to a specified type of systems.
broadcast service	A unidirectional service from one service source to multiple service sinks.
building integrated timing supply (BITS)	In the situation of multiple synchronous nodes or communication devices, one can use a device to set up a clock system on the hinge of telecom network to connect the synchronous network as a whole, and provide satisfactory synchronous base signals to the building integrated device. This device is called BITS.
built-in WDM	A function which integrates some simple WDM systems into products that belong to the OSN series. That is, the OSN products can add or drop several wavelengths directly.
busbar	An electrical conductor that makes a common connection between several circuits.
busy hour call attempts (BHCA)	The number of call attempts during the busiest hour of the day. BHCA cover successful calls and unsuccessful call attempts.
C	
C interface	An interface between the mobile switching center (MSC) and the home location register (HLR). The C interface adopts the Mobile Application Part (MAP) protocol. When a call is set up to a mobile station (MS) or a short message (SM) is sent to the MS, the MSC or gateway mobile switching center (GMSC) queries the location, status, and subscription information of the roaming subscriber in the HLR over the C interface. Based on the mobile station roaming number (MSRN) of the called MS, the MSC then determines the route of the call or SM.
C3	See CloudCube .
CA	See call agent .
CAB	converged address book
CAC	See connection admission control .
CAM	content addressable memory
CANCEL	A SIP request that indicates incomplete requests must be canceled. It has no effect on acknowledged requests (meaning the final responses to the requests have been received).

CAPEX	capital expenditure
CAPS	See call attempts per second .
CAPWAP	See Control and Provisioning of Wireless Access Points .
CAR	committed access rate
CAS	column address select
CAT	See Charge Audit Tool .
CATV	cable TV
CBC	See cell broadcast center .
CBR	See condition-based routing .
CBS	central battery signaling telephony
CBU	See cellular backhaul unit .
CC	ceramic capacitor
CCC	circuit cross connect
CCFE	call control functional entity
CCITT	Consultative Committee of International Telegraph and Telephone
CCM	continuity check message
CCM termination	CCMs are generated and also terminated by MEPs. A MEP forwards received CCMs at a higher level but drops CCMs at a lower level or at the same level. In this manner, CCMs from a low-level MD are confined within the bounds of the MD.
CCR	See call completion rate .
CCS	common capability set
CD	compact disc
CD-ROM	compact disc read-only memory
CDC	countdown counter
CDE	common desktop environment
CDMA	See Code Division Multiple Access .
CDMA2000	A 3G technology developed by Qualcomm of the US. Technology competitive with WCDMA, upgraded from CDMA1, and developed by the GSM community as a worldwide standard for 3G mobile.
CDP	customized dialing plan
CDR	See call detail record .
CE	channel element

CE1	channelized E1
CEP	See complex event processing .
CES	See circuit emulation service .
CF	compact flash
CFB	See call forwarding on mobile subscriber busy .
CFM	connectivity fault management
CFNR	See call forwarding no reply .
CFR	cell fill rate
CFU	See Call Forwarding - Unconditional .
CHAP	See Challenge Handshake Authentication Protocol .
CID	call instance data
CIDR	See classless inter-domain routing .
CIF	Common Intermediate Format
CIR	cab integrated radio
CISPR	International Special Committee on Radio Interference
CIST	See Common and Internal Spanning Tree .
CLEI	common language equipment identification
CLI	command-line interface
CLIP	See calling line identification presentation .
CLIR	See calling line identification restriction .
CLK	clock card
CLNP	connectionless network protocol
CMC	core network management component
CMM	chassis management module
CMP	See Content Management Protocol .
CMS	See content management system .
CN	call notification
CO	Central Office
CODEC	coder/decoder
COM	component object model
CON	conference calling
CONF	conference calling function

COPS	Common Open Policy Service
CORBA	See Common Object Request Broker Architecture .
COS	chip operating system
CP	crypto period
CPCS	common part convergence sublayer
CPE	See customer-premises equipment .
CPLD	complex programmable logic device
CPU	See Central Processing Unit .
CQT	cable quality tester
CR	carriage return
CR-LDP	Constraint-based Routed Label Distribution Protocol
CR-LSP	constraint-based routed label switched path
CR-LSP backup	End-to-end path protection that provides the protection to the whole LSP. On the same tunnel, the path that backs up the master LSP is the backup path. When the ingress finds that the master LSP is unavailable, it switches the traffic to the backup path. After the master LSP recovers, it switches the traffic back to protect the master path. There are hot backup and common backup.
CRC	See cyclic redundancy check .
CRD	call rerouting distribution
CRL	See certificate revocation list .
CRM	customer relationship management
CS	circuit service
CSA	Canadian Standards Association
CSCF	See call session control function .
CSCP	See class selector code point .
CSES	consecutive severely errored second
CSF	Client Signal Fail
CSG	closed subscriber group
CSMA/CD	See carrier sense multiple access with collision detection .
CSNP	See complete sequence numbers protocol data unit .
CSP	certified spare parts
CSPF	Constrained Shortest Path First

CSS	cascading style sheet
CST	See common spanning tree .
CSV	See comma separated values .
CT	class type
CT1	channelized T1
CTC	common transmit clock
CTD	cell and time distribution
CTL	certificate trust list
CTR	counter mode
CU	See Configuration Utility .
CUG	See closed user group .
CV	connectivity verification
CV packet	A type of packet that is generated at the frequency of 1/s on the source end LSR of an LSP, and is terminated on the destination end LSR of the LSP. A CV packet is transmitted from the source end LSR to the destination LSR along the LSP. A CV packet contains the unique identifier (TTSI) of the LSP so that all types of abnormalities on the path can be detected.
CVC	code verification certificate
CW	See continuous wave .
CWDM	See coarse wavelength division multiplexing .
Call Forwarding - Unconditional (CFU)	A service that allows all the calls to a registered user to be forwarded to a preset phone number irrespective of the status of this user.
Central Processing Unit (CPU)	The computational and control unit of a computer. The CPU is the device that interprets and executes instructions. The CPU has the ability to fetch, decode, and execute instructions and to transfer information to and from other resources over the computer's main data-transfer path, the bus.
Challenge Handshake Authentication Protocol (CHAP)	A password-based authentication protocol that uses a challenge to verify that a user has access rights to a system. A hash of the supplied password with the challenge is sent for comparison so the cleartext password is never sent over the connection.
Charge Audit Tool (CAT)	The CAT is developed to ensure the security and veracity of the charging audit system. It also provides support for BSS solutions to ensure the system security in the efficient and reliable ways.

CloudCube (C3)	Also called C3. Huawei cloud platform that supports heterogeneous virtualization and heterogeneous device integration and provides various types of cloud services. C3 provides cloud computing IaaS and PaaS solutions.
CoS	class of service
Code Division Multiple Access (CDMA)	A communication scheme that uses frequency expansion technology to form different code sequences. When the CDMA scheme is used, subscribers with different addresses can use different code sequences for multi-address connection.
Common Object Request Broker Architecture (CORBA)	A specification developed by the Object Management Group in 1992 in which pieces of programs (objects) communicate with other objects in other programs, even if the two programs are written in different programming languages and are running on different platforms. A program makes its request for objects through an object request broker, or ORB, and therefore does not need to know the structure of the program from which the object comes. CORBA is designed to work in object-oriented environments.
Common and Internal Spanning Tree (CIST)	The single spanning tree jointly calculated by STP and RSTP, the logical connectivity using MST bridges and regions, and MSTP. The CIST ensures that all LANs in the bridged local area network are simply and fully connected.
Configuration Utility (CU)	A system configuration and management interface.
Contact	A header field used in the INVITE request, ACK request, REGISTER request, successful response, call progress response and redirection response. Its value shows the address that is used to communicate with users through subsequent messages.
Content Management Protocol (CMP)	Self-defined protocol between the Portal and the MM, used for content publishing.
Control and Provisioning of Wireless Access Points (CAPWAP)	A protocol that defines how communication is implemented between an access point (AP) and an access controller (AC) and provides a universal encapsulation and transmission mechanism for the interoperation between the AP and the AC.
cable aperture	A hole which is used for cable routing in a cabinet.
call ID	The unique ID that the system allocates to a call.
call agent (CA)	An external call control unit for controlling telephony gateways. A CA provides signaling and call processing functions.

call attempts per second (CAPS)	The number of call attempts in a second. Both successful and failed calls are taken into account.
call completion rate (CCR)	In a measurement period, the ratio of the number of connected calls to the total number of call attempts. Calculation formula: Call completion rate = Number of connected calls / Total number of call attempts x 100%
call control	A set of functions used to process a call, including establishing, supervising, maintaining, connecting, and releasing calls, and provide service features.
call detail record (CDR)	A record unit used to create billing records. A CDR contains details such as the called and calling parties, originating switch, terminating switch, call length, and time of day.
call forwarding no reply (CFNR)	A service that allows an incoming call to be forwarded to a third party when a mobile subscriber does not answer the call before the timer times out.
call forwarding on mobile subscriber busy (CFB)	A service that permits a called mobile subscriber to have the network send all incoming calls addressed to the called mobile subscriber's directory number to the registered number when the called mobile subscriber is busy. Based on the time of call forwarding, the service is classified into Network Determined User Busy (NDUB) or User Determined User Busy (UDUB).
call out	To make a call to objects outside a customer service center in a way such as voice, short message, email, fax, or chat.
call routing	A SIP signaling process for joining a meeting. The eCCAS server routes an incoming call to the specified server.
call session control function (CSCF)	The core component of the IMS network. It performs the functions such as registration, authentication, session control, service triggering, topology hiding, QoS control, NAT traversal, and security management.
call transfer service	A service that allows any party in a call to transfer the call to a third-party and then exit from the call.
call waiting service	When there is a call to a user that is already in conversation, the user hears a prompt. In this case, the user can answer this call or neglect it. If the user answers this call, the user can switch between the two conversations.
callback	A call mode in which both ends of the communication participate in the call. One end is called the Client, while the other end is called the Server. The Client initiates a call, and the Server decides whether to callback or not. If a callback is needed, the Server tears down the connection and then initiates a call to the Client.

calling line identification presentation (CLIP)	A supplementary service that allows the number of the calling party to be presented to the called party.
calling line identification restriction (CLIR)	A supplementary service that prevents the number of the calling party from being presented to the called party.
carrier sense multiple access with collision detection (CSMA/CD)	Carrier sense multiple access with collision detection (CSMA/CD) is a computer networking access method in which: a carrier sensing scheme is used. A transmitting data station that detects another signal while transmitting a frame, stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to send that frame again.
cell broadcast center (CBC)	A functional entity within the mobile network that is responsible for the generation of cell broadcast information.
cellular backhaul unit (CBU)	A network access unit used for access base transceiver stations. It provides Ethernet, IP, and TDM services; has multiple Ethernet and 1PPS+ToD interfaces and optionally E1 interfaces. It is mainly applicable to backhaul in mobile base transceiver stations.
centralized forwarding	Forwarding of OMC packets, H.248 packets and SIGTRAN packets through one IP interface. It can save IP address resources and avoid a complex network.
certificate	The certificate, also called the digital certificate, establishes the association between the user identity and user public key. The certificate is issued by the third-party authority, and provides identity authentication for the communications parties.
certificate chain	The identity of a public key certificate should be authenticated by the CA of the upper level. The process for authenticating a public key becomes an iterative process. As a result, a certificate chain is formed, which ends at the root certificate.
certificate revocation list (CRL)	[Data Security] A time-stamped list of certificates, signed by the issuing Certification Authority, that have been revoked by that CA. The CRL is made available to entities that need to rely on a certificate for authentication.

channel	A telecommunication path of a specific capacity and/or speed between two or more locations in a network. The channel can be established through wire, radio (microwave), fiber, or any combination of the three. The amount of information transmitted per second in a channel is the information transmission speed, expressed in bits per second. For example, b/s (100 bit/s), kb/s (103 bit/s), Mb/s (106 bit/s), Gb/s (109 bit/s), and Tb/s (1012 bit/s).
channel adjustment	A mechanism that achieves the following effects for WLAN: Every AP is assigned an optimal channel, with minimum interference to and from neighboring channels; APs are free from interference sources such as radar and microwave ovens with the help of real-time channel detection. In a WLAN, channels are scarce resources, and non-overlapping channels over which every AP works are very limited. In addition, a large number of possible interference sources, such as radars and microwave ovens, may exist within the operating frequency band of WLAN. Such interference sources will interfere with the normal operating of APs. Dynamic channel adjustment allows for continuous communications and provides reliable transmission over the wireless network.
circuit emulation service (CES)	A function with which the E1/T1 data can be transmitted through ATM networks. At the transmission end, the interface module packs timeslot data into ATM cells. These ATM cells are sent to the reception end through the ATM network. At the reception end, the interface module re-assigns the data in these ATM cells to E1/T1 timeslots. The CES technology guarantees that the data in E1/T1 timeslots can be recovered to the original sequence at the reception end.
claim	To transfer a trouble ticket from the trouble ticket pool to the operator's to-do area, after the system dispatches trouble tickets to a department or role. A claimed trouble ticket can be processed only by the operator who claims it.
class selector code point (CSCP)	Bits 0 to 2 in DSCP are class selector code point (CSCP) and they indicate a specific type of DSCP.
classifier	A set of matching criteria. It consists of classifier priority and protocol-related criteria (such as the IP address) for mapping data packets.
classless inter-domain routing (CIDR)	A routing mode in which IP addresses and masks are used to indicate network address and subnetwork address. Through CIDR, routers can flexibly aggregate routes. This reduces the size of the routing table.
clock filtering	Selection of a best time sample from a specified peer as for the same peer for the local clock.
clock offset	Time offset between the local clock and the reference clock.

clock tracing	The method of keeping the time on each node synchronized with a clock source in the network.
closed user group (CUG)	A service that enables subscribers, connected to a PLMN and possibly also other networks, to form Closed User Groups (CUGs) to and from which access is restricted. A specific user may be a member of one or more CUGs. Members of a specific CUG can communicate among each other but not, in general, with users outside the group. This service is applicable to all the telecom services except emergency calls and SMS.
clutter	The overall volume of advertising messages within an individual TV program or a single issue of a magazine.
coarse wavelength division multiplexing (CWDM)	A signal transmission technology that multiplexes widely-spaced optical channels into the same fiber. CWDM spaces wavelengths at a distance of several nm. CWDM does not support optical amplifiers and is applied in short-distance chain networking.
codec negotiation	A process in which the core network, access network, and media gateway (MGW) coordinate to implement transcoding. Transcoding is required when terminals supporting different audio codec types want to communicate with each other. During the transcoding, these audio codec types are decoded and then coded, deteriorating voice quality. To reduce the number of transcoding times and improve voice quality, codec negotiation is introduced.
comma separated values (CSV)	A CSV file is a text file that stores data, generally used as an electronic table or by the database software.
command script	A text file that records a batch of MML commands for a single NE or multiple NEs of the same type.
commission	A fee paid by a carrier to a dealer based on the service traffic, customer expenditure, and service quality of the dealer.
common spanning tree (CST)	A single spanning tree that connects all the MST regions in a network. Every MST region is considered as a switch; therefore, the CST can be considered as their spanning tree generated with STP/RSTP.
comparison analysis	A multidimensional analysis method. In this method, a special mathematical model is used to compare multidimensional analysis results according to a dimension member. In normal cases, the indexes of two hierarchies are compared from a same dimension, and the results are displayed as rates. For example, the result of the comparison between the number of new customers in March 2003 with that in February 2003 is 115%.

complete sequence numbers protocol data unit (CSNP)	A unit that contains brief information about the local LSDB and is used to synchronize the LSDBs of neighbors. CSNPs are sent and resolved at different levels.
complex event processing (CEP)	Evolution mode of the traditional SOA architecture, used in the scenarios that involve a great number of events and complex events.
compromise	A violation of the security policy of a system or an organization such that unauthorized disclosure or modification of sensitive information occurs.
condition-based routing (CBR)	A routing mode that provides an intelligent peak time resource management tool. The CBR occurs subject to a condition being met, or a 'flag' state being raised.
conference	An IP multimedia session that has two or more participants. Each conference has a focus and can be identified uniquely.
confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities or processes.
configuration script	A collection of the command lines in a data file according to which the variable values of a template are assigned. The configuration script can be either a complete script or a script snippet.
congestion management	A flow control measure to solve the problem of network resource competition. When the network congestion occurs, it places packets into the queue for buffer and determines the packet forwarding order.
connection admission control (CAC)	A control process in which the network takes actions in the call set-up phase (or call re-negotiation phase) to determine which connection request is admitted.
connection point	A reference point where the output of a trail termination source or a connection is bound to the input of another connection, or where the output of a connection is bound to the input of a trail termination sink or another connection. The connection point is characterized by the information which passes across it. A bidirectional connection point is formed by the association of a contradirectional pair.
consistency check	A function that is used to check the consistency of service data and resource data between two softswitches that have the dual homing relation. This ensures the consistency of service data and resource data between the softswitches.
constraint-based routed LSP	An LSP set up on the basis of certain constraints. Unlike a common LSP, the creation of a CR-LSP depends on route information and other conditions, such as the specified bandwidth, selected path, and QoS parameters.

content management system (CMS)	Software that serves as the intermediate system between the CP and subscribers' value chain or subscribers' value network to publish and manage media content.
continuous wave (CW)	An electromagnetic wave of constant amplitude and frequency.
control flow	A flow defined according to service requirements, which is a basic unit operated in the system. A control flow comprises tasks and events. Tasks are cascaded through events. Arranges tasks and controls the task execution flow. Data is not transmitted between tasks in a control flow.
core layer	A layer that functions as the backbone of high speed switching for networks and provides high speed forwarding communications. It has a backbone transmission structure that provides high reliability, high throughput, and low delay. The core layer devices must have a good redundancy, error tolerance, manageability, adaptability, and they support dual-system hot backup or load balancing technologies. In a real network, the core layer includes the IP/MPLS backbone network consisting of NPEs and backbone routers.
correlation analysis	A function of the network management system. This function is used to analyze reported alarms comprehensively and effectively with rule-based correlation analysis technologies, which helps to reduce network storms and enables the maintenance personnel to quickly locate faults.
counteract	To reduce the effect of a transaction. For example, to counteract a payment of 100 dollars is to add a payment record of 100 dollars.
countermeasure	A control, method, technique, or procedure that is put into place to prevent a threat agent from exploiting a vulnerability. A countermeasure is put into place to mitigate risk. Also called a safeguard or control.
credit	Reduction of assets and costs, as well as an increase in liabilities, equity, and income.
cross-connection	The connection of channels between the tributary board and the line board, or between line boards inside the NE. Network services are realized through the cross-connections of NEs.
crosstalk coupling	The cross coupling between speech communications channels or their component parts.
crystal oscillator	An oscillator that produces electrical oscillations at a frequency determined by the physical characteristics of a piezoelectric quartz crystal.
customer service	A service provided for customers before, during, and after a purchase. Customer services include customer registration, consultation, SMS notifications, and bill printing and delivery.

customer-premises equipment (CPE)	Customer-premises equipment or customer-provided equipment (CPE) is any terminal and associated equipment located at a subscriber's premises and connected with a carrier's telecommunication channel at the demarcation point ("demarc"). The demarc is a point established in a building or complex to separate customer equipment from the equipment located in either the distribution infrastructure or central office of the communications service provider. CPE generally refers to devices such as telephones, routers, network switches, residential gateways (RG), set-top boxes, fixed mobile convergence products, home networking adapters and Internet access gateways that enable consumers to access communications service providers' services and distribute them around their house via a local area network (LAN).
cutover	The process of migrating the data of an application system to another application system, which then provides services.
cyclic redundancy check (CRC)	A mathematical checksum that can be used to detect data corruption in transmitted frames. The CRC is a linear hash function, and should not be used for data security assurance.
D	
D channel	A signaling channel used to carry messages on the initialization and termination of a session, caller identification, call forwarding, and call negotiation in ISDN. D is short for data.
D-V	distance vector routing algorithm
DB	database
DBA	dynamic bandwidth assignment
DBG	See database gateway .
DC	direct current
DCN	See data communication network .
DD	database description
DDF	data decryption field
DDI	See direct dialing in .
DDM	difference in depth of modulation
DDN	See digital data network .
DDR	dial-on-demand routing
DEC	An operand in COPS. It is used for the PDP to send a decision to the PEP as the response of a request.
DEI	device emulation interrupt

DELT	dual-ended loop test
DES	See Data Encryption Standard .
DF	dielectric film
DFB	distribution feedback laser
DH	See Diffie-Hellman .
DHCP	See Dynamic Host Configuration Protocol .
DHCP option	A field in Dynamic Host Configuration Protocol (DHCP) messages to contain additional information.
DHCP proxy	A program that relays the DHCP request of a user to the DHCP/BOOTP server, which then allocates an IP address to the user.
DIP	Dynamic Inspection Protocol
DIP switch	dual in-line package switch
DLCI	See data link connection identifier .
DLM	See dynamic line management .
DM	differential mode
DMM	distributed message manager
DMR	See digital media renderer .
DMS	database managed space
DMT	See discrete multi-tone .
DMTI	See desired Min Tx interval .
DMZ	See demilitarized zone .
DN	directory number
DND	See do not disturb .
DNS	See domain name service .
DNS client	A device that sends a request to the DNS server and waits for a response.
DNS server	A device that can provide domain name resolution for the client on the network
DO	digital output
DOCSIS	Data Over Cable Service Interface Specification
DOD	See direct outward dialing .
DOM	document object model

DOPRA	See Distributed Object-oriented Programmable Real-time Architecture .
DP	See detection point .
DPM	dual processor module
DPN	digital path not provided signal
DR	dielectric resonator
DRQ	disengage request
DS node	A DS-compliant node, which is subdivided into DS boundary node and ID interior node.
DS-TE	See DiffServ-aware Traffic Engineering .
DSA	directory system agent
DSC	data source control
DSCP	See differentiated services code point .
DSL	See digital subscriber line .
DSLAM	See digital subscriber line access multiplexer .
DSM	digital storage media
DSP	digital signal processing
DSR	data set ready
DSS	door status switch
DSS1	Digital Subscriber Signaling No. 1
DST	daylight saving time
DT	decay time
DTE	See data terminal equipment .
DTMF	See dual tone multiple frequency .
DTS	digital test sequence
DU	downstream unsolicited
DUP	Data User Part
DV	See digital vehicle .
DVB	See digital video broadcasting .
DWDM	See dense wavelength division multiplexing .
Data Encryption Standard (DES)	A specification for encryption of computer data developed by IBM and adopted by the U.S. government as a standard in 1976. DES uses a 56-bit key.

Diameter	A protocol that is developed by the Internet Engineering Task Force (IETF) and provides authentication, authorization, and accounting (AAA) services for access technologies.
DiffServ	See differentiated service .
DiffServ-aware Traffic Engineering (DS-TE)	A technology used to optimize and subdivide network transmission resources, classify traffic, and specify the proportion of each flow to the link bandwidth.
Diffie-Hellman (DH)	A public algorithm of key. Two communication parties can obtain the keys by exchanging some data instead of transmitting the key across the link.
Distributed Object-oriented Programmable Real-time Architecture (DOPRA)	An OS-layer, middleware-level, highly-tailorable, component-based, open software platform. It helps to accommodate the difference of upper-layer OS, hardware, network, and system scale.
DoD	downstream on demand
DoS	denial of service
DoS attack	See denial-of-service attack .
Dynamic Host Configuration Protocol (DHCP)	A client-server networking protocol. A DHCP server provides configuration parameters specific to the DHCP client host requesting information the host requires to participate on the Internet network. DHCP also provides a mechanism for allocating IP addresses to hosts.
damping	A technique for preventing overshoot (exceeding the desired limit) in the response of a circuit or device.
data VLAN	A virtual local area network (VLAN) that transmits only data packets.
data access	Accessing the data stored in a physical database.
data communication network (DCN)	A communication network used in a TMN or between TMNs to support the data communication function.
data file	In bulk copy operations, the file that transfers data from the bulk copy out operation to the bulk copy in operation. In databases, data files hold the data stored in the database. Every database has at least one primary data file, and can optionally have multiple secondary data files to hold data that does not fit on the primary data file.
data integrity	The accuracy of data and its conformity to its expected value, especially after being transmitted or processed.

data link connection identifier (DLCI)	An identifier for an individual user's information stream as well as the connection between terminal equipment and the user equipment.
data terminal equipment (DTE)	A user device composing the UNI. The DTE accesses the data network through the DCE equipment (for example, a modem) and usually uses the clock signals produced by DCE.
database gateway (DBG)	A functional entity that provides services at the Data Base Management System (DBMS) interface layer. The DBG implements communication between the physical database and the DRU or DSU.
deactivation	An operation that disables a postpaid subscriber to use different telecommunications services provided by a carrier. After being deactivated, a subscriber account enters the Disable state.
deadlock	A failure or inability to proceed due to two programs or devices both requiring a response from the other before you complete an operation.
dealer	A commercial organization that handles various communication businesses with authorization from a carrier to obtain profits.
demilitarized zone (DMZ)	A buffer area between an insecure system and the secure system and is used to solve the problem that the external network cannot access the internal network equipped with a firewall. The DMZ is located between the internal network and the external network. In the DMZ, some public server facilities, such as the enterprise Web server and FTP server, can be located. The DMZ effectively protects the internal network.
demodulation	In communications, the means by which a modem converts data from modulated carrier frequencies (waves that have been modified in such a way that variations in amplitude and frequency represent meaningful information) over a telephone line. Data is converted to the digital form needed by a computer to which the modem is attached, with as little distortion as possible.
denial-of-service attack (DoS attack)	The attack that denies the services. The attacker sends a lot of request packets to a target server. The request packets take up too much resource of the target server, so that the target server cannot respond to the normal request of authorized users.
dense wavelength division multiplexing (DWDM)	The technology that utilizes the characteristics of broad bandwidth and low attenuation of single mode optical fiber, employs multiple wavelengths with specific frequency spacing as carriers, and allows multiple channels to transmit simultaneously in the same fiber.

deregistration	An operation of deregistering a subscriber. After being deregistered, a subscriber cannot use the products and services that are provided by the carrier.
designated port	A port defined in the STP protocol. On each switch that runs the STP protocol, the traffic from the root bridge is forwarded to the designated port. The subnet connected to the STP switch receives the data traffic from the root bridge. All the ports on the root bridge are designated ports. On each subnet, there is only one designated port. When a network topology is stable, only the root port and the designated port forward traffic. Other non-designated ports are in the blocking state, and they receive STP packets, but does not forward user traffic.
desired Min Tx interval (DMTI)	The minimum interval that the local system would like to use when transmitting BFD control packets.
destination route	An information mapping table that stores information such as the destination address, match length of the destination address, and message type. It is the information source for routers to route messages based on the matched destination address.
detection point (DP)	In the intelligent network, the service switching point (SSP) defines a series of relatively stable states for all the calls. A DP refers to a transition point at which a call changes from one state to another.
detection sensitivity	The capability for a detector to respond to an exception.
detour LSP	An LSP that is used to re-route traffic around a point of failure in one-to-one backup mode.
device upgrade	A function used to load the software for multiple devices on a site for upgrading the device. This reduces the daily workload of the maintenance engineer and facilitates the management of the device software version.
device version	Versions of the devices of the same type but different manufacturers and specifications.
dial tone test	A test that is performed to locate the fault on a port on the narrowband switch. The most common faults that may occur on a port of the narrowband switch are the power feeding fault and the dial tone fault. Therefore, currently, the dial tone test is used to test only these two faults.
differentiated service (DiffServ)	An IETF standard that defines a mechanism for controlling and forwarding traffic in a differentiated manner based on CoS settings to handle network congestion.

differentiated services code point (DSCP)	According to the QoS classification standard of the Differentiated Service (Diff-Serv), the type of services (ToS) field in the IP header consists of six most significant bits and two currently unused bits, which are used to form codes for priority marking. Differentiated services code point (DSCP) is the six most important bits in the ToS. It is the combination of IP precedence and types of service. The DSCP value is used to ensure that routers supporting only IP precedence can be used because the DSCP value is compatible with IP precedence. Each DSCP maps a per-hop behavior (PHB). Therefore, terminal devices can identify traffic using the DSCP value.
digital data network (DDN)	A data transmission network that is designed to transmit data on digital channels (such as the fiber channel, digital microwave channel, or satellite channel).
digital media renderer (DMR)	A consumer electronics device. It can receive data media streams from a computer through a fixed or wireless home network.
digital modulation	A method that controls the changes in amplitude, phase, and frequency of the carrier based on the changes in the baseband digital signal. In this manner, the information can be transmitted by the carrier.
digital network	A telecommunication network where information is first converted into distinct electronic pulses and then transmitted to a digital bit stream.
digital signal	A signal in which information is represented by a limited number of discrete states (for example, high and low voltages) rather than by fluctuating levels in a continuous stream, as in an analog signal. In the pulse code modulation (PCM) technology, the 8 kHz sampling frequency is used and a byte contains 8 bits in length. Therefore, a digital signal is also referred to as a byte-based code stream. Digital signals, with simple structures and broad bandwidth, are easy to shape or regenerate, and are not easily affected by external interference.
digital signature	A message signed with a sender's private key that can be verified by anyone who has access to the sender's public key. Digital signature gives the receiver the reason to believe the message was sent by the claimed sender. A proper implementation of digital signature is computing a message digest for the message sent from the sender to the receiver, and then signing the message digest. The result is called digital signature and is sent to the receiver together with the original message.
digital subscriber line (DSL)	A technology for providing digital connections over the copper wire or the local telephone network. DSL performs data communication over the POTS lines without affecting the POTS service.

digital subscriber line access multiplexer (DSLAM)	A network device, usually situated in the main office of a telephone company, that receives signals from multiple customer Digital Subscriber Line (DSL) connections and uses multiplexing techniques to put these signals on a high-speed backbone line.
digital vehicle (DV)	A new vehicle management mode that uses GIS and GPS technologies to build a system for providing information about vehicle management.
digital video broadcasting (DVB)	A suite of internationally accepted open standards for digital television. DVB standards are maintained by the DVB Project, an international industry consortium with more than 300 members, and they are published by a Joint Technical Committee (JTC) of European Telecommunications Standards Institute (ETSI), European Committee for Electrotechnical Standardization (CENELEC) and European Broadcasting Union (EBU).
direct dialing in (DDI)	A service that allows an intra-office user to be connected through the PSTN long number of this user. The call does not need to be transferred to this user through the automatic switchboard.
direct outward dialing (DOD)	A facility of a PABX that allows internal users to make outgoing calls without operator intervention.
direct route	In this mode of load balancing, after processing a client request forwarded by the SLB, a real server returns the request processing result to the client through a direct route without being forwarded by the SLB.
discrete multi-tone (DMT)	A modulation mode of the asymmetric digital subscriber line (ADSL), which uses the frequency division multiplex technology to divide the frequency band in use into multiple subchannels to carry data independently. ITU-T defines the maximum number of bits that each subchannel can carry. In each subchannel, data can be modulated and transmitted independently and the ADSL based on the DMT technology has a strong anti-noise capability. The transmission capability of the ADSL based on the DMT technology is related to the following factors: frequency response (line attenuation), line noise, noise margin, transmit power, preset maximum number of bits that each subfrequency band can carry.
dispatch system	A system for dispatching and allocating resources.
distribute	To move resources from the Data Warehouse to resource use departments.
do not disturb (DND)	A service that allows the calling party to hear the busy tone or an announcement indicating that the called party has registered with the do not disturb service. A user that does not want to answer calls can use this service. After subscribing to this service, the user can still make calls.

domain name service (DNS)	A hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participants. The DNS distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain.
dormant state	The state of the data service DCR entity in which no dedicated logical channels are maintained, the service option is disconnected, but the Link Layer connection for the data service instance between the IWF and the MS is maintained.
download	To obtain data from an upper-layer device or the server.
downstream	In an access network, the direction of transmission toward the subscriber end of the link. A direction of message forwarding within a transaction that refers to the direction that requests flow from the user agent client to user agent server.
dual tone multiple frequency (DTMF)	Multi-frequency signaling technology for telephone systems. According to this technology, standard set combinations of two specific voice band frequencies, one from a group of four low frequencies and the other from a group of four high frequencies, are used.
dynamic data	The data that changes in real time during the running of a program.
dynamic line management (DLM)	A method of adjusting the maximum transmit power of a single line to achieve the best transmit power and reduce the crosstalk between lines.
dynamic range	The ratio between the greatest signal power that can be transmitted over a multichannel analogue transmission system without exceeding distortion or other performance limits, and the least signal power that can be utilized without exceeding noise, error rate or other performance limits.
dynamic service data	The core data that guarantees normal operation of a system. The data can be generated from the database during system initialization upon system resetting, or generated through the related configuration command. The data can be modified only during the first configuration operation and during smoothing. The data can change during the system running, but the change is small, such as data change in the case of a board failure.
dynamic service flow	A mechanism in which traffic flows are established and resources are occupied only when service data transmission is required. After a call is complete, the occupied resources are released immediately. Therefore, compared with the mechanism of provisioned service flows, the mechanism of dynamic service flows is more efficient at resource allocation.

E

E-LAN	See Ethernet local area network .
E-Line	See Ethernet line .
E-NNI	external network-network interface
E-Tree	See Ethernet-tree .
E1	An European standard for high-speed data transmission at 2.048 Mbit/s. It provides thirty-two 64 kbit/s channels. A time division multiplexing frame is divided in to 32 timeslots numbered from 0 to 31. Timeslot 0 is reserved for frame synchronization, and timeslot 16 is reserved for signaling transmission. The rest 30 timeslots are use as speech channels. Each timeslot sends or receives an 8-bit data per second. Each frame sends or receives 256-bit data per second. 8000 frames will be sent or received per second. Therefore the line data rate is 2.048 Mbit/s.
E2E	end to end
EAPoL	Extensible Authentication Protocol over LAN
EBGP	External Border Gateway Protocol
EBS	See excess burst size .
EC	See enterprise customer .
ECC	See error checking and correction .
ECM	entitlement control message
EEC	Ethernet Electric Interface PMC Card
EF	elementary function
EFC	Ethernet Fiber Interface PMC Card
EFM	Ethernet in the First Mile
EFM OAM	Ethernet in the first mile OAM
EFS	error-free second
EGP	See Exterior Gateway Protocol .
EIGRP	Enhanced Interior Gateway Routing Protocol
EM	element management
EMC	See electromagnetic compatibility .
EMF	element management framework
EMI	external machine interface
EMM	entitlement management message
EMP	emergency management port

EMS	See enhanced messaging service .
EMU	See environment monitoring unit .
EN	end node
EOC	embedded operations channel
EP	elementary procedure
EPFD	equivalent power flux-density
EPLD	See erasable programmable logic device .
EPON	See Ethernet passive optical network .
ERP	effective radiated power
ERPS	Ethernet ring protection switching
ES	edge server
ESC	See electric supervisory channel .
ESL	See extended signaling link .
ESN	See equipment serial number .
ESP	See Encapsulating Security Payload .
ET	event trigger
ETC	See Establish Temporary Connection .
ETH-CC	Ethernet continuity check
ETH-LB	Ethernet loopback
ETH-LT	Ethernet link trace
ETS	European Telecommunication Standards
ETSI	See European Telecommunications Standards Institute .
EUI	extended user interface server
EVC	Electronic Voucher Center
EXP	See experimental bits .

Encapsulating Security Payload (ESP)	A key protocol in the IP Security (IPsec) architecture. ESP adopts encryption and authentication mechanisms. It is used in transport mode or tunnel mode to authenticate the source of IP packets, and ensure data integrity, anti-replay, and confidentiality. ESP provides data confidentiality and integrity by encrypting the data to be protected and placing the encrypted data in the data part of the IP ESP. Based on security requirements of subscribers, this mechanism can be used to encrypt either a transport-layer segment or an IP data packet. A transport-layer segment includes Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), and Internet Group Management Protocol (IGMP).
Establish Temporary Connection (ETC)	A request for connecting to the tone playback and digit collection resource on an advanced intelligent peripheral (ATP).
Ethernet line (E-Line)	A type of Ethernet service that is based on a point-to-point EVC (Ethernet virtual connection).
Ethernet local area network (E-LAN)	A type of Ethernet service that is based on a multipoint-to-multipoint EVC (Ethernet virtual connection).
Ethernet passive optical network (EPON)	An Ethernet Passive Optical Network (EPON) is a passive optical network based on Ethernet. It is a new generation broadband access technology that uses a point-to-multipoint structure and passive fiber transmission. It supports upstream/downstream symmetrical rates of 1.25 Gbit/s and a reach distance of up to 20 km. In the downstream direction, the bandwidth is shared based on encrypted broadcast transmission for different users. In the upstream direction, the bandwidth is shared based on TDM. EPON meets the requirements for high bandwidth.
Ethernet-tree (E-Tree)	An Ethernet service type that is based on a Point-to-multipoint Ethernet virtual connection.
European Telecommunications Standards Institute (ETSI)	ETSI is a multinational standardization body with regulatory and standardization authority over much of Europe. GSM standardization took place under the auspices of ETSI.
Expires	A header field of the SIP message. It specifies the duration after which the message or message content expires.
Extensible Markup Language (XML)	A specification developed by the World Wide Web Consortium (W3C). XML is a pared-down version of Standard Generalized Markup Language (SGML), designed especially for Web files. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.

Exterior Gateway Protocol (EGP)	A protocol for exchanging routing information between two neighboring gateway hosts (each with its own router) in a network of autonomous systems.
eNodeB	E-UTRAN NodeB
eSFP	enhanced small form-factor pluggable
electric supervisory channel (ESC)	A technology that implements communication among all the nodes and transmission of monitoring data in an optical transmission network. The monitoring data of ESC is introduced into DCC service overhead and is transmitted with service signals.
electromagnetic compatibility (EMC)	A condition which prevails when telecommunications equipment is performing its individually designed function in a common electromagnetic environment without causing or suffering unacceptable degradation due to unintentional electromagnetic interference to or from other equipment in the same environment.
emergency channel	The emergency channel refers to that the Service Manager allows unauthorized terminal hosts to access network resources in the post-authentication domain. The emergency channel is enabled only when serious faults occur in the Service Controller, so that network communications remain normal during such faults. The emergency channel automatically disables itself after faults are rectified.
emergency maintenance	A type of measure taken to quickly rectify an emergency fault to recover the proper running of the related system or device and to reduce losses.
emulation call	A Graphical User Interface (GUI) mode used to stimulate a call flow and display the table-querying information, key information (including parameters), and CDR information in the form of packets. Subscribers can identify configuration errors by analyzing the packets.
encryption	A function used to convert data so as to protect the content from unauthorized use.
end-to-end security	The security protection during transmission of the three types of information streams sent from the data source to the destination network. The information streams are the media stream, control stream, and management stream. The end-to-end security includes the access control, discrimination, non-repudiation, data confidentiality, communication security, data integrity, availability, and privacy.
enhanced messaging service (EMS)	An application-level extension to SMS for mobile phones available on GSM, TDMA, and CDMA networks. To be specific, EMS messages contain special text formatting (such as bold or italic), animations, pictures, icons, sound effects, and special ring tones.

enterprise customer (EC)	A target customer of industry applications.
environment monitoring unit (EMU)	A unit that uses sensors to monitor the temperature, humidity, smoke, and intrusion in the environment in real time. The environment can be automatically monitored according to the preset value and alarms are automatically generated when the preset threshold is exceeded.
equipment serial number (ESN)	A string of characters that identify a piece of equipment and ensures correct allocation of a license file to the specified equipment. It is also called "equipment fingerprint".
erasable programmable logic device (EPLD)	A logic array device which can be used to implement the required functions by programming the array. In addition, a user can modify and program the array repeatedly until the program meets the requirement.
error checking and correction (ECC)	A technique used for detecting and correcting errors by adding check bits to the source bits. If the source data has eight bits, five check bits are required to perform error checking and correction. When the data bits are doubled every time, one more check bit is required. Compared with the parity check, the ECC can not only detect but also correct errors. This improves the reliability of data storage. This technique can be used in the ECC memory to improve the security and reliability of the memory.
error packet	The packets with received messages not translated or translated incorrectly.
error tolerance	The ability of a system or component to continue normal operation despite the presence of erroneous inputs.
event level	An attribute of an event, which is used to help decide whether the event needs to be logged and an alarm to be reported. Currently, there are three event levels: 1) major: send alarms when recording logs; 2) minor: only record logs but not send alarms; 3) ignore: ignore the event. Such an event does not require logging or alarm reporting.
excess burst size (EBS)	A parameter related to traffic. In the single rate three color marker (srTCM) mode, traffic control is achieved by token buckets C and E. The excess burst size parameter defines the capacity of token bucket E, that is, the maximum burst IP packet size when the information is transferred at the committed information rate. This parameter must be greater than 0 but should be not less than the maximum length of an IP packet to be forwarded.
execution time	The time, measured in clock ticks (pluses of the internal timer of a computer), required by a microprocessor to decode and carry out an instruction after it is fetched from memory.
experimental bits (EXP)	A field in the MPLS packet header, three bits long. This field is always used to identify the CoS of the MPLS packet.

extended ID	The number of the subnet to which an NE belongs, used to identify different network segments in a wide area network (WAN). Together, the ID and extended ID form the physical ID of the NE.
extended signaling link (ESL)	A type of link that is responsible for transmitting the Abis timeslot dynamic connection message.
extract	To read the data required by the destination system from the source system.
F	
F interface	An interface between the mobile switching center (MSC) and the equipment identity register (EIR). The F interface is used for data exchange between the MSC and the EIR to authenticate the international mobile station equipment identity (IMEI) of a mobile station (MS) and prevent unauthorized access. It is a standard protocol interface and adopts the Mobile Application Part (MAP) protocol.
FA	foreign agent
FAT	flexible access termination
FBB	fixed broadband
FC	See Fibre Channel .
FCB	fan control board
FCC	See Flow Control Center .
FCS	frame check sequence
FD	See frequency diversity .
FDA	See first deliver attempt .
FDB	flash database
FDD	See frequency division duplex .
FDDI	See fiber distributed data interface .
FDI	See forward defect indication .
FDI packet	See forward defect indication packet .
FDM	fiber data management
FE	fast Ethernet
FE port	See fast Ethernet port .
FEBE	Far-End Block Error
FEC	See forwarding equivalence class .

FEM	finite element method
FER	See frame error rate .
FF	fixed filtering
FFD	fast failure detection
FFD packet	A path failure detection method independent from CV. Different from a CV packet, the frequency for generating FFD packets is configurable to satisfy different service requirements. By default, the frequency is 20/s. An FFD packet contains information the same as that in a CV packet. The destination end LSR processes FFD packets in the same way for processing CV packets.
FH	frame header
FIB	See forwarding information base .
FID	function identification
FIFO	first in first out queuing
FIN	fixed intelligent network
FM	feature management
FMC	See fixed mobile convergence .
FP	See fax peripheral .
FPGA	See field programmable gate array .
FPS	See fast protection switching .
FR	See frame relay .
FRR	See fast reroute .
FRU	See field replaceable unit .
FSM	finite state machine
FT	fault tolerance
FTN	FEC to NHLFE
FTP	File Transfer Protocol
FTPS	See File Transfer Protocol server .
FTTB	See fiber to the building .
FTTC	See fiber to the curb .
FTTH	See fiber to the home .
FTU	fan transit unit
Fabric	A kind of bus/plane used to exchange system service data.

Fax over IP (FoIP)	A technique for facsimile (fax) transmission over the Internet or other IP-based packet network, rather than over the traditional public switched telephone network (PSTN). FoIP typically involves a fax gateway, which not only serves as a physical gate bet
Fibre Channel (FC)	A high-speed transport technology used to build SANs. FC is primarily used for transporting SCSI traffic from servers to disk arrays, but it can also be used on networks carrying ATM and IP traffic. FC supports single-mode and multi-mode fiber connections, and can run on twisted-pair copper wires and coaxial cables. FC provides both connection-oriented and connectionless services.
File Transfer Protocol server (FTPS)	A file server that uses the File Transfer Protocol (FTP) to permit users to upload or download files through the Internet or any other TCP/IP network.
Flow Control Center (FCC)	A core management control module of the Short Message Center (SMC). The FCC can improve the flow distribution processing capacity of the system and enhance its redundancy capability.
FoIP	See Fax over IP .
facility backup	A local repair method in which a bypass tunnel is used to protect one or more protected LSPs that traverse the PLR, the resource being protected, and the Merge Point in that order.
fairness	A feature in which for any link specified in a ring network, the source node is provided with certain bandwidth capacities if the data packets transmitted by the source node are constrained by the fairness algorithm.
fan module	A module that consists of fans and fan boards and dissipates heat for the system.
fast Ethernet port (FE port)	The port that provides a rate of 100 Mbit/s.
fast protection switching (FPS)	A type of pseudo wire automatic protection switching (PW APS). When the working PW is faulty, the source transmits services to the protection PW and the sink receives the services from the protection PW. FPS generally works with the interworking function (IWF) to provide end-to-end protection for services.
fast reroute (FRR)	A technology which provides a temporary protection of link availability when part of a network fails. The protocol enables the creation of a standby route or path for an active route or path. When the active route is unavailable, the traffic on the active route can be switched to the standby route. When the active route is recovered, the traffic can be switched back to the active route. FRR is categorized into IP FRR, VPN FRR, and TE FRR.

fault	A failure to operate correctly. A fault does not include failures caused by preventative maintenance, insufficient external resources, or intentional settings.
fault alarm	A type of alarm caused by hardware and/or software faults, for example, board failure, or by the exception that occurs in major functions. After handling, a fault alarm can be cleared, upon which the NE reports a recovery alarm. Fault alarms are of higher severity than event alarms.
fault detection	The process of determining that a fault has occurred.
fax peripheral (FP)	An intelligent peripheral that provides the fax sending, fax receiving, and fax storing and transferring functions.
fiber distributed data interface (FDDI)	A standard developed by the American National Standards Institute (ANSI) for high-speed fiber-optic LANs. FDDI provides specifications for transmission rates of 100 megabits per second on token ring networks.
fiber to the building (FTTB)	A fiber-based networking scenario. There are two types of FTTB scenarios: multi-dwelling unit (MDU) and business buildings. Each scenario includes the following service types: FTTB to the MDU and FTTB to the business buildings.
fiber to the curb (FTTC)	A fiber-based networking scenario. The FTTC scenario provides the following services: asymmetric broadband services (such as digital broadcast service, VOD, file download, and online gaming), symmetric broadband services (such as content broadcast, email, file exchange, distance education, and distance medical care), POTS, ISDN, and xDSL backhaul services.
fiber to the home (FTTH)	A fiber-based networking scenario. The FTTH scenario provides the following services: asymmetric broadband services (digital broadcast service, VoD, file download, and online gaming), symmetric broadband services (content broadcast, email, file exchange, distance education, and distance medical care), POTS, and ISDN services.
field programmable gate array (FPGA)	A semi-customized circuit that is used in the Application Specific Integrated Circuit (ASIC) field and developed based on programmable components. FPGA remedies many of the deficiencies of customized circuits, and allows the use of many more gate arrays.
field replaceable unit (FRU)	A unit or component of a system that is designed to be replaced in the field, i.e., without returning the system to a factory or repair depot. Field replaceable units may either be customer-replaceable or their replacement may require trained service personnel.

filler panel	A piece of board to cover blank slots to keep the cabinet or shelf away from dust, to keep proper airflow inside the cabinet or shelf, to keep proper airflow inside the frame, to beautify the frame appearance, and to screen electromagnetic.
firmware	Low-level software for booting and operating an intelligent device. Firmware generally resides in read-only memory (ROM) on the device.
first deliver attempt (FDA)	A mode in which the Router attempts to deliver a short message (SM) only once. If the Router fails to deliver the SM, the Router forwards the SM to the short message center (SMC) for delivery. In the FDA mode, the Router does not store any SMs.
fit AP	See fit access point .
fit access point (fit AP)	An AP that is configured and managed by and works under an AC. An AC manages fit APs by using the CAPWAP protocol. Certain real-time operations of real-time frame exchange and MAC address management are implemented on the fit AP, while the authentication, security management, and mobile functions are implemented by the AC.
fixed mobile convergence (FMC)	Communication service provided based on the combination of fixed-line and wireless technologies. Service providing, access technologies, and terminal devices on an FMC network are independent from each other. The same service can be obtained from various access networks. Subscribers from different access networks can obtain and use the same service.
flooding threshold	The ratio of the changed bandwidth to the reservable bandwidth of the link where no flooding occurs. A flooding threshold is set to avoid consuming excessive resources due to flooding that is caused by the change in the link bandwidth.
flow	A sequence of packets or E2E service data having similar characteristics, such as source and sink device, destination IP address, and traffic size.
flush	A process of writing data in a Memtable to a SSTable.
forced switching	The action of switching traffic signals between a working channel and protection channel. The switching occurs even if the channel to which traffic is being switched is faulty or an equal or higher priority switching command is in effect.
forward defect indication (FDI)	A packet generated and traced forward to the sink node of the LSP by the node that first detects defects. It includes fields to indicate the nature of the defect and its location. Its primary purpose is to suppress alarms being raised at affected higher level client LSPs and (in turn) their client layers.

forward defect indication packet (FDI packet)	A packet that responds to the detected failure event. It is used to suppress alarms of the upper layer network where failure has occurred.
forwarding equivalence class (FEC)	A class-based forwarding technology that classifies the packets with the same forwarding mode. Packets with the same FEC are processed similarly on an MPLS network. The division of FECs is flexible, and can be a combination of the source address, destination address, source port, destination port, protocol type, and VPN.
forwarding information base (FIB)	A table that provides information for network hardware (bridges and routers) for them to forward data packets to other networks. The information contained in a routing table differs according to whether it is used by a bridge or a router. A bridge relies on both the source (originating) and destination addresses to determine where and how to forward a packet.
frame error rate (FER)	The number of received frames that contain an error in the frame payload divided by the total number of transmitted frames in one direction of a single connection.
frame relay (FR)	A packet-switching protocol used for WANs. Frame relay transmits variable-length packets at up to 2 Mbit/s over predetermined, set paths known as PVCs (permanent virtual circuits). It is a variant of X.25 but sacrifices X.25's error detection for the sake of speed.
free-run mode	An operating condition of a clock, the output signal of which is strongly influenced by the oscillating element and not controlled by servo phase-locking techniques. In this mode the clock has never had a network reference input, or the clock has lost external reference and has no access to stored data, that could be acquired from a previously connected external reference. Free-run begins when the clock output no longer reflects the influence of a connected external reference, or transition from it. Free-run terminates when the clock output has achieved lock to an external reference.
frequency diversity (FD)	The signal is transmitted using several frequency channels or spread over a wide spectrum that is affected by frequency-selective fading.
frequency division duplex (FDD)	An application in which channels are divided by frequency. In an FDD system, the uplink and downlink use different frequencies. Downlink data is sent through bursts. Both uplink and downlink transmission use frames with fixed time length.

full mesh topology	A topology in which any two devices are connected, and there is a link between any two devices. Such a network provides a higher redundancy, and the deployment cost is very high although it prevents the single-point failure on links.
fuse	A safety device that protects an electric circuit from excessive current, consisting of or containing a metal element that melts when current exceeds a specific amperage, thereby opening the circuit.
G	
G.711	Audio codec standard (A-law or U-law) that uses pulse code modulation (PCM). Its data rate is 64 kbit/s.
G.722	Audio codec standard that uses adaptive differential pulse-code modulation (ADPCM). Its data rate is 48 kbit/s, 56 kbit/s, or 64 kbit/s.
G.728	Audio codec standard that uses low-delay code excited linear prediction (LD-CELP). Its data rate is 16 kbit/s.
GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GEM	GPON encapsulation mode/method
GGSN	See gateway GPRS support node .
GIP	GARP information propagation
GMII	gigabit media independent interface
GMP	Group Map Protocol
GMRP	GARP Multicast Registration Protocol
GMSC	See gateway mobile switching center .
GMT	Greenwich Mean Time
GPS	See Global Positioning System .
GR	See graceful restart .
GR helper	A neighbor of a GR restarter. The GR helper must support GR.
GR restarter	A node that is restarted by the administrator or in case of failures. The GR restarter must support GR.
GRE	See Generic Routing Encapsulation .
GRQ	general request message
GSM	See global system for mobile communications .
GSMP	See General Switch Management Protocol .

GTSM	Generalized TTL Security Mechanism
GUI	graphical user interface
GVRP	GARP VLAN registration protocol
General Switch Management Protocol (GSMP)	A general purpose protocol developed by Ipsilon Networks to control an ATM switch. GSMP allows a controller to establish and release connections across the switch; add and delete leaves on a point-to-multipoint connection; manage switch ports; request configuration information; request statistics. It also allows the switch to inform the controller of asynchronous events such as a link going down.
Generic Routing Encapsulation (GRE)	A mechanism for encapsulating any network layer protocol over any other network. GRE is used for encapsulating IP datagrams tunneled through the Internet. GRE serves as a Layer 3 tunneling protocol and provides a tunnel for transparently transmitting data packets.
Global Positioning System (GPS)	A global navigation satellite system that provides reliable positioning, navigation, and timing services to users worldwide.
gateway GPRS support node (GGSN)	A functional entity that provides packet data services. It is in charge of the routing and encapsulation of the packet data between the General Packet Radio Service (GPRS) or Universal Mobile Telecommunications System (UMTS) network and the external PDN.
gateway mobile switching center (GMSC)	A type of Mobile Switching Center (MSC), which requests the routing information about a called subscriber and performs interconnection and settlement between networks.
global system for mobile communications (GSM)	The second-generation mobile networking standard defined by the European Telecommunications Standards Institute (ETSI). It is aimed at designing a standard for global mobile phone networks. GSM consists of three main parts: mobile switching subsystem (MSS), base station subsystem (BSS), and mobile station (MS).
goods	Entities provided by a carrier to customers in promotions or as rewards.
graceful restart (GR)	In IETF, protocols related to Internet Protocol/Multiprotocol Label Switching (IP/MPLS) such as Open Shortest Path First (OSPF), Intermediate System-Intermediate System (IS-IS), Border Gateway Protocol (BGP), Label Distribution Protocol (LDP), and Resource Reservation Protocol (RSVP) are extended to ensure that the forwarding is not interrupted when the system is restarted. This reduces the flapping of the protocols at the control plane when the system performs an active/standby switchover. This series of standards is called graceful restart.

granularity	The extent to which a system is broken down into small parts, either the system itself or its description or observation. It is the extent to which a larger entity is subdivided. If a system has more granularity for you to choose, that is, there are more granules in the system for you to choose, then you can customize the system more flexibly.
granularity period	The time interval between two successive collections of performance data. The granularity period is also called measurement period in Huawei MML speculation. The unit of granularity period is minute, such as one minute, five minutes, ten minutes, 15 minutes, 30 minutes, 60 minutes and 1440 minutes.
graph	A graph is used to process data in a specific way. To be specific, a graph is used to read data from the source system, filter, calculate, group, and summarize the data, process data inconsistency if any, and delete invalid data to obtain data that meets requirements of the target system, and then load the data to the target system. Components, ports, and lines are connected to each other to form a graph, which contains transformations and jobs.
group attribute	The administrator classifies users into groups according to a certain attribute or certain attributes. In this way, operations such as policy configuration and report query can be performed on a group of users.
guide trough	A trough on the expansion bolt; or the guiding component that is installed on the rack, cabinet, or chassis, supporting slide of the shelf or the rack.
H	
H-VPN	See hierarchy VPN .
H.248	A media gateway control protocol used for communications between the media gateway controller (MGC) and the media gateway (MGW) in the detached gateway architecture so that the MGC can control the MGW. In Universal Mobile Telecommunications System (UMTS) networks, the interface between the MGC and the MGW is the Mc interface and the 3GPP defines specific usage of H.248 over the Mc interface.
H.261	A video codec standard for video conferences at px64 kbit/s. Two formats are available, including CIF and QCIF.
H.264	Compared with H.263, H.264 can provide the same-quality video at half of the bit rate, with strong error resilience characteristics.
HA	See high availability .
HA system	high availability system
HC	high capacity

HD	high definition
HDB3	See High Density Bipolar of Order 3 .
HDSL	high-speed digital subscriber line
HDTV	See high-definition television .
HEC	See header error control .
HEX	heat exchanger
HFC	See high-level foundation classes .
HGU	HLR general unit
HMAC	See hash-based message authentication code .
HO	See head office .
HP	higher order path
HQoS	See hierarchical quality of service .
HRC	hypothetical reference circuit
HSI	high speed Internet
HSRP	Hot Standby Router Protocol
HSS	See home subscriber server .
HTTP	See Hypertext Transfer Protocol .
HTTPS	See Hypertext Transfer Protocol Secure .
HVPLS	hierarchical virtual private LAN service
HWTACACS	See Huawei Terminal Access Controller Access Control System .
HWTACACS accounting	An accounting mode in which the BRAS sends accounting packets to the HWTACACS server, which then performs accounting on users.
HWTACACS authentication	An authentication mode in which the BRAS sends the user name and password to the HWTACACS server by using the HWTACACS protocol. The HWTACACS server authenticates the user, and then returns the result to the BRAS.
High Density Bipolar of Order 3 (HDB3)	A code used for baseband transmissions between telecommunications devices. The HDB3 code has the following feature: high capability of clock extraction, no direct current component, error-checking capability, and a maximum of three consecutive zeros.

Huawei Terminal Access Controller Access Control System (HWTACACS)	A security protocol with enhanced functions on the base of TACACS (RFC1492). Similar to the RADIUS protocol, HWTACACS implements multiple subscriber AAA functions through communications with the HWTACACS server in the client/server mode.
Hypertext Transfer Protocol (HTTP)	An application-layer protocol used for communications between web servers and browsers or other programs. HTTP adopts the request-response mode. A client sends a request to the server. The request consists of two parts: request header and MIME-like message. The request header contains request method, uniform resource locator (URL), and protocol version. The MIME-like message contains request modifiers, client information, and possible body content. Upon receiving the request, the server responds with a status line. The status line includes the message's protocol version, a success or error code, and a MIME-like message, which contains server information, entity meta-information, and possible entity-body content. For details about HTTP, see RFC2616. The protocol used to carry requests from a browser to a Web server and to transport pages from Web servers back to the requesting browser. Although HTTP is almost universally used on the Web, it is not an especially secure protocol. Hypertext Transfer Protocol (HTTP) - a networking protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.
Hypertext Transfer Protocol Secure (HTTPS)	An HTTP protocol that runs on top of transport layer security (TLS) and Secure Sockets Layer (SSL) for secured transactions. It is used to establish a reliable channel for encrypted communication and secure identification of a network web server. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security, or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.
handshake message	A series of signals acknowledging that communication or the transfer of information can take place between computers or other devices.
hang up	A call processing mode used by an attendant to end the conversation with a user.
hardware loopback	A connection mode in which a fiber jumper is used to connect the input optical interface of a board to the output optical interface of the board to achieve signal loopback.

hash-based message authentication code (HMAC)	In cryptography, a keyed-hash message authentication code (HMAC) is a specific type of message authentication code (MAC) involving a cryptographic hash function (hence the 'H') in combination with a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message. Any cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key.
head office (HO)	The top level organization for an organization hierarchy.
headend	The headend receives TV signals from satellites and the terrestrial, and encodes, transcodes, and encapsulates the signals into message formats that can be transmitted through the IP network.
header error control (HEC)	A field within the ATM frame whose purpose is to correct any single bit error in the cell Header and also to detect any multi-bit errors. It actually performs a CRC check in the first four header bits and also at the receiving end.
hello packet	The commonest packet which is periodically sent by a router to its neighbors. It contains information about the DR, Backup Designated Router (BDR), known neighbors and timer values.
heterogeneous IP-interworking	A PWE3 service mode used to implement interworking between two networks that have different link types.
hierarchical quality of service (HQoS)	A type of QoS that controls the traffic of users and performs the scheduling according to the priority of user services. HQoS has an advanced traffic statistics function, and the administrator can monitor the usage of bandwidth of each service. Hence, the bandwidth can be allocated reasonably through traffic analysis.
hierarchy VPN (H-VPN)	An L3VPN networking type. Using the hierarchy technology, H-VPN distributes PE functions such as user access and router management to multiple PEs to enhance network scalability.
high availability (HA)	A scheme in which two modules operate in active/standby mode to achieve high availability. When the active module fails, the standby module automatically takes over the system functions of the active module.

high-definition television (HDTV)	High-definition television (HDTV) is a television system providing an image resolution that is substantially higher than that of standard-definition television. HDTV may be transmitted in various formats: 1080p: 1920×1080p: 2,073,600 pixels (~2.07 megapixels) per frame 1080i: 1920×1080i: 1,036,800 pixels (~1.04 MP) per field or 2,073,600 pixels (~2.07 MP) per frame Some countries also use a non-standard CEA resolution, such as 1440×1080i: 777,600 pixels (~0.78 MP) per field or 1,555,200 pixels (~1.56 MP) per frame 720p: 1280×720p: 921,600 pixels (~0.92 MP) per frame The letter "p" here stands for progressive scan, while "i" indicates interlaced.
high-level foundation classes (HFC)	A group of encapsulated function databases provided by the iStar. You can use the provided functions to accelerate script editing.
hold priority	The priority of the tunnel for holding resources, ranging from 0 (indicates the highest priority) to 7. It is used to determine whether the resources occupied by the tunnel can be preempted by other tunnels.
home domain	The administration realm that maintains the mapping between users and accounts.
home subscriber server (HSS)	The central database in an IP multimedia subsystem (IMS) network. The database stores information about all IMS subscribers, including subscriber IDs, security context, routing information, and subscribed services. The HSS also provides a management interface for carriers and subscribers to customize and modify the subscription data. It is similar to the home location register (HLR) in the Global System for Mobile communications (GSM).
hop count	The simplest routing metric in which each link has a cost of 1. This function counts the number of times a packet must be forwarded.
I	
I-SPF	incremental shortest path first
I/O	input/output
IAD	See integrated access device .
IANA	See Internet Assigned Numbers Authority .
IAS	See integrated access software .
IBGP	Internal Border Gateway Protocol
IBMS	See Integrated Business Management System .
IC	See integrated circuit .
ICC	See ITU carrier code .

ICMP	See Internet Control Message Protocol .
ICMP attack	The attacks against the ICMP protocol.
ICMPv6	See Internet Control Message Protocol version 6 .
ICP	IMA Control Protocol
ICT	in-circuit test
IDP	See initial domain part .
IE	signaling information element
IEEE	See Institute of Electrical and Electronics Engineers .
IETF	Internet Engineering Task Force
IGMP	See Internet Group Management Protocol .
IGP	See Interior Gateway Protocol .
IISP	interim interswitch signaling protocol
ILM	incoming label map
IM	See instant messaging .
IMA frame	A control unit in the IMA protocol. It is a logical frame defined as M consecutive cells, numbered 0 to M-1, transmitted on each of the N links in an IMA group.
IMAP	Internet Message Access Protocol
IMC	See intelligent metric collector .
IMM	integrated management module
IMPI	See IP multimedia private identity .
IMS	IP multimedia subsystem
IN	intelligent network
INFO	A SIP request. It transmits interaction information in a call.
INVITE	A SIP request that is used to initiate a session or invite a user to join a session. The session contains the caller ID, callee ID, routing information, security information, and SDP information.
IOS	intelligent optimum sample
IP Header Compression (IPHC)	A host-to-host protocol that is used on the IP network to compress such real-time multimedia services as voice and video. To reduce the consumption of valid bandwidth, IPHC can be used on links to compress TCP/IP and IP/UDT/RTP packet headers.

IP address	A 32-bit (4-byte) binary number that uniquely identifies a host connected to the Internet. An IP address is expressed in dotted decimal notation, consisting of the decimal values of its 4 bytes, separated with periods; for example, 192.168.1.1. The first three bytes of the IP address identify the network to which the host is connected, and the last byte identifies the host itself.
IP address unnumbered	A mechanism in which an interface that is not configured with an IP address can borrow the IP address of an interface that is configured with an IP address to save IP address resources.
IP multimedia private identity (IMPI)	A globally unique identity assigned by the home network operator. It may be used within the home network to uniquely identify the subscriber from a network perspective.
IP path	A logical link with virtual bandwidth. The logical link is carried on the physical link in the IP network. IP path is a mechanism for performing access control on transmission resources.
IP spoofing	The act of inserting a false sender IP address into an Internet transmission in order to gain unauthorized access to a computer system.
IP subnet	A special submap used to identify an IP network segment. It is displayed as the submap icon in the topological view.
IP telecommunications network (IPTN)	Global end-to-end controllable QoS solution for the entire network. It guarantees the end-to-end QoS through such measures as reasonable network planning and area-based resource reservation. It also rejects service requirements in advance that cannot be satisfied to avoid network congestion.
IPC	interprocess communication
IPHC	See IP Header Compression .
IPMB	Intelligent Platform Management Bus
IPTN	See IP telecommunications network .
IPTS	intelligent public telephone service
IPTV	See Internet Protocol television .
IPX	Internet Packet Exchange
IPoA	IP over ATM
IPoE	Internet Protocol over Ethernet
IPoEoA	IP over Ethernet over ATM
IPsec	See Internet Protocol Security .
IPv4	See Internet Protocol version 4 .

IPv6	See Internet Protocol version 6 .
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISDN	Integrated Services Digital Network
ISDN Q.921-User Adaptation Layer (IUA)	A layer that provides transport of signaling messages between the signaling gateway (SG) and the media gateway controller (MGC), including transporting Q.921/Q.931 boundary primitives, communication between layer management modules, and management of active associations.
ISP	See Internet service provider .
IST	internal spanning tree
IT	information technology
ITC	independent transmit clock
ITE	information technology equipment
ITU	See International Telecommunication Union .
ITU carrier code (ICC)	A code assigned to a network operator/service provider, maintained by the ITU-T Telecommunication Standardization Bureau (TSB).
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
IUA	See ISDN Q.921-User Adaptation Layer (IUA)
InARP	Inverse Address Resolution Protocol
Institute of Electrical and Electronics Engineers (IEEE)	A professional association of electrical and electronics engineers based in the United States, but with membership from numerous other countries. The IEEE focuses on electrical, electronics, and computer engineering, and produces many important technology standards.
Integrated Business Management System (IBMS)	Business management platform of the PTT service. It provides a data synchronization interface for the BOSS so that enterprise administrators and members can perform operations such as registration, deregistration, modification, and query.
Interior Gateway Protocol (IGP)	A routing protocol that is used within an autonomous system. The IGP runs in small-sized and medium-sized networks. The IGPs are RIP, IGRP, EIGRP, OSPF, and IS-IS.
International Telecommunication Union (ITU)	A United Nations agency, one of the most important and influential recommendation bodies, responsible for recommending standards for telecommunication (ITU-T) and radio networks (ITU-R).

Internet Assigned Numbers Authority (IANA)	A department operated by the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the NIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP suite, including autonomous system numbers.
Internet Control Message Protocol (ICMP)	A network layer protocol that provides message control and error reporting between a host server and an Internet gateway.
Internet Control Message Protocol version 6 (ICMPv6)	A basic protocol of IPv6 and generates error messages and informational messages used by IPv6 nodes to report errors and information generated during packet processing.
Internet Group Management Protocol (IGMP)	One of the TCP/IP protocols for managing the membership of Internet Protocol multicast groups. It is used by IP hosts and adjacent multicast routers to establish and maintain multicast group memberships.
Internet Protocol Security (IPsec)	A protocol family defined by the Internet Engineering Task Force (IETF). By authenticating and encrypting each IP packet of a data stream, this protocol family provides high quality, interoperable, and cryptology-based security for IP packets.
Internet Protocol television (IPTV)	A system that provides TV services over the IP network. In the IPTV system, media streams from satellites, terrestrial, and studios are converted by the encoder to the media streams applicable to the IP network. Then the media streams are transmitted to the terminal layer on the IP network. Media content is displayed on a TV set after media streams are processed by specified receiving devices (for example, an STB).
Internet Protocol version 4 (IPv4)	The current version of the Internet Protocol (IP). IPv4 utilizes a 32bit address which is assigned to hosts. An address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods and may range from 0.0.0.0 through to 255.255.255.255. Each IPv4 address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork.
Internet Protocol version 6 (IPv6)	An update version of IPv4, which is designed by the Internet Engineering Task Force (IETF) and is also called IP Next Generation (IPng). It is a new version of the Internet Protocol. The difference between IPv6 and IPv4 is that an IPv4 address has 32 bits while an IPv6 address has 128 bits.
Internet service provider (ISP)	An organization that offers users access to the Internet and related services.

in-service upgrade	An upgrade mode in which services are not interrupted or the interruption time is acceptable for terminal users when a software is upgraded.
information channel	A channel used for information output. A user can classify, limit, and manage information through this channel.
information security	Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.
initial domain part (IDP)	The part which is standardized by ISO, and specifies the format and permissions for assigning the rest of the address.
insertion loss	The loss of power that results from inserting a component, such as a connector, coupler, or splice, into a previously continuous path.
instant hotline	A service that allows the calls to a registered user to be forwarded immediately to a preset phone number (hotline number).
instant messaging (IM)	A form of real-time communication between two or more people based on typed text. The text is conveyed via devices connected over a network such as the Internet.
integrated access device (IAD)	An access node that can simultaneously deliver Class 5 switch voice services, packet voice services, and data services (through LAN ports) over a single WAN link. IADs provide a common platform that enables service providers to deliver voice and data over a single access network, reducing the cost of co-located equipment in the Telco central office and allowing service providers to minimize transport spans.
integrated access software (IAS)	The software used to approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.
integrated circuit (IC)	A combination of inseparable associated circuit elements that are formed in place and interconnected on or within a single base material to perform a microcircuit function.
intelligent metric collector (IMC)	A service provided by the C3 to collect and process data and save the data to a database. It generates and monitors service reports.
inter-office line cut	The cutting of the phone line out of the office, for example, wire A is cut, wire B is cut, or wires A and B are cut.
intercept	To stop an incoming call that is being processed by an agent when a Quality Control (QC) inspector listens to the call so that the inspector processes the call.
interface status	The running status of an interface, which can be normal, blocked, disabled, or not learning MAC address.

internal call	An operation that a service agent performs to call another service agent in the customer service center.
internal links	The links between web pages of the same website.
intra-office line cut	The cutting of the phone line in the office, for example, wire A is cut, wire B is cut, or wires A and B are cut.
J	
jitter transfer	The physical relationship between jitter applied at the input port and the jitter appearing at the output port.
K	
knowledge base	A repository of knowledge about a domain represented in machine-processable form, which may be rules (in which case the knowledge base may be considered as a rule base), facts, or other representations.
L	
L2F	See Layer Two Forwarding Protocol .
L2TP	Layer 2 Tunneling Protocol
L2TP network server (LNS)	A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP access concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunneled from the remote system by the LAC.
L2VPN	Layer 2 virtual private network
L3VPN	Layer 3 virtual private network
LA	line amplifier
LAC	link access control
LACP	See Link Aggregation Control Protocol .
LACPDU	Link Aggregation Control Protocol data unit
LAG	See link aggregation group .
LAN	See local area network .
LAPB	Link Access Procedure Balanced
LATN	See line attenuation .
LB	local battery
LBM	See loopback message .
LBR	See loopback reply .
LC	Lucent connector

LCK	See locked signal function .
LCP	Link Control Protocol
LCS	See location service .
LCT	local craft terminal
LE	See local exchange .
LER	See label edge router .
LFIB	label forwarding information base
LI	length indicator
LIC	large-scale integrated circuit
LIU	logical interface unit
LLC	low layer compatibility
LLDP	See Link Layer Discovery Protocol .
LLDP agent	An entity that manages LLDP operations for an interface.
LLDP local system MIB	A database that stores information about the local station, including the chassis ID, port ID, system name, system description, port description, system capabilities, and management address.
LLDP management address	An address used by the NMS to identify a device and implement network management. This facilitates the layout of the network topology and network management with a clear view of the topology status. The LLDP management address is carried in the management address Type-Length-Value (TLV) field in an LLDP frame to be transmitted to neighbor stations.
LLDP remote system MIB	A database that stores information about adjacent stations, including the chassis ID, port ID, system name, system description, port description, system capabilities, and management address.
LLDP trap	The trap message that the device sends to the NMS for updating the topology when the LLDP local system MIB or the LLDP remote system MIB changes.
LLDPDU	See Link Layer Discovery Protocol data unit .
LLID	local loopback ID
LM	See loss measurement .
LNS	See L2TP network server .
LOC	loss of clock
LOG	call logging
LOM	loss of multiframe

LOP	loss of pointer
LOS	See loss of signal .
LOSW	loss of sync failure
LP	lower order path
LPC	linear predictive coding
LPR	local primary reference
LPU	line interface processing unit
LR	See loose routing .
LS	logical system
LSA	link-state advertisement
LSAck packet	See link state acknowledgment packet .
LSDB	link state database
LSN	license serial number
LSP	locally significant part
LSP tunnel	An LSP over which traffic is transmitted based on labels that are assigned to FECs on the ingress. The traffic is transparent to the intermediate nodes
LSR	See label switching router .
LSR packet	See link state request packet .
LSU	lone signal unit
LSU packet	See link state update packet .
LT	line termination
LTE	Long Term Evolution
LTM	See linktrace message .
LTR	See linktrace reply .
Layer 2 switching	A data forwarding method. In a LAN, a network bridge or 802.3 Ethernet switch transmits and distributes packet data based on the MAC address. Since the MAC address is at the second layer of the OSI model, this data forwarding method is called Layer 2 switching.
Layer Two Forwarding Protocol (L2F)	A protocol that offers encapsulation of tunnels at higher-level link layer. L2F helps realize the physical separation of the dial-up server and the dial-up protocol connection.

Link Aggregation Control Protocol (LACP)	A dynamic link aggregation protocol that improves the transmission speed and reliability. The two ends of the link send LACP packets to inform each other of their parameters and form a logical aggregation link. After the aggregation link is formed, LACP maintains the link status in real time and dynamically adjusts the ports on the aggregation link upon detecting the failure of a physical port.
Link Layer Discovery Protocol (LLDP)	The Link Layer Discovery Protocol (LLDP) is an L2D protocol defined in IEEE 802.1ab. Using the LLDP, the NMS can rapidly obtain the Layer 2 network topology and changes in topology when the network scales expand.
Link Layer Discovery Protocol data unit (LLDPDU)	The data unit that carries the local device information encapsulated in the data field in an LLDP frame.
label distribution	Packets with the same destination address belong to an FEC. A label out of an MPLS label resource pool is allocated to the FEC. LSRs record the relationship of the label and the FEC. Then, LSRs sends a message and advertises to upstream LSRs about the label and FEC relationship in message. The process is called label distribution.
label edge router (LER)	A device that sits at the edge of an MPLS domain, that uses routing information to assign labels to datagrams and then forwards them into the MPLS domain.
label space	Value range of the label allocated to peers.
label switching router (LSR)	Basic element of an MPLS network. All LSRs support the MPLS protocol. The LSR is composed of two parts: control unit and forwarding unit. The former is responsible for allocating the label, selecting the route, creating the label forwarding table, creating and removing the label switch path; the latter forwards the labels according to groups received in the label forwarding table.
laser	A component that generates directional optical waves of narrow wavelengths. The laser light has better coherence than ordinary light. Semi-conductor lasers provide the light used in a fiber system.
line attenuation (LATN)	The loss of signal power on a signal cable or optical fiber.
line capacity	The distribution capacitance caused by the length of a subscriber cable. In normal situations, the capacitance is proportional to the cable length.
link aggregation group (LAG)	An aggregation that allows one or more links to be aggregated together to form a link aggregation group so that a MAC client can treat the link aggregation group as if it were a single link.

link group	According to some principles, links are divided into the set in the logical term. A set of links is called the link group. The division makes management more convenient.
link protection	Protection provided by the bypass tunnel for the link on the working tunnel. The link is a downstream link adjacent to the point of local repair (PLR). When the PLR fails to provide node protection, the link protection should be provided.
link state acknowledgement packet (LSAck packet)	A packet used for acknowledging the received LSU packets. One packet can acknowledge the receipt of multiple LSAs.
link state request packet (LSR packet)	Packets exchanged for desired LSAs. By exchanging the DD packets, two routers get to know which LSAs of the peer routers are unavailable in the local LSDBs and send LSR packets to the peer routers. The LSR packets contain the digest of the desired LSAs.
link state update packet (LSU packet)	A packet used to send the needed LSAs to the peer router. It contains a collection of multiple LSAs (complete contents).
linktrace message (LTM)	The message sent by the initiator MEP of 802.1ag MAC Trace to the destination MEP. LTM includes the Time to Live (TTL) and the MAC address of the destination MEP2.
linktrace reply (LTR)	For 802.1ag MAC Trace, the destination MEP replies with a response message to the source MEP after the destination MEP receives the LTM, and the response message is called LTR. LTR also includes the TTL that equals the result of the TTL of LTM minus 1.
listening	An operation performed by an inspector to audit the conversation of a service agent in real time.
live TV	Live TV is a service that allows subscribers to view SD and HD quality digital TV broadcast channels in real-time streaming over broadband connection. Unlike traditional broadcast TV, live TV channels support enhanced services such as Time Shift TV (TSTV), Catch-up TV.
load balancing	The distribution of activity across two or more servers or components in order to avoid overloading any one with too many requests or too much traffic.
loading	A process of importing information from the storage device to the memory to facilitate processing (when the information is data) or execution (when the information is program).
local MEP	An MEP of a device on a network enabled with Ethernet CFM.

local area network (LAN)	A network formed by the computers and workstations within the coverage of a few square kilometers or within a single building, featuring high speed and low error rate. Current LANs are generally based on switched Ethernet or Wi-Fi technology and run at 1,000 Mbit/s (that is, 1 Gbit/s).
local authorization	An activity of authorizing users based on user attributes configured on the Broadband Remote Access Server (BRAS).
local control	An optional mobile station feature used to perform manufacturer-specific functions.
local exchange (LE)	An exchange nearest to users or directly connected to user terminals.
local loopback	A type of test equivalent to the line self-loop test of the E1 or T1 interface, used for the chip self-test and E1 or T1 link self-loop test.
local port number	The port number of the local device when the interworking data is configured.
local time	Display time of a local computer, which varies according to the time zone.
location service (LCS)	Basic functions, such as bucket location allocation and query, are provided in the object cloud storage service system to ensure global uniqueness of users' buckets. HTTP-based interfaces are used to manage locations of users' buckets. The location service and DNS are used in combination to provide domain name resolution for unified namespace.
locked signal function (LCK)	A function administratively locks an MEG end point (MEP) at the server layer, informs consequential data traffic interruption to the peer MEP at the client layer, and suppresses the alarm at the client layer.
log server	A subsystem of eLog, used for alarm, report, traffic, device, system, and user management.
logical chip	An integrated circuit that processes information, as opposed to simply storing it. A logic chip is made up of logic circuits.
logical reach	The maximum distance that can be achieved for a particular transmission system, regardless of the optical budget.
loop protection	A function to prevent network loops. In MSTP, the re-selection of the root interface may result in a loop when the topology is changed. The loop protection function can prevent network loop. If the root interface cannot receive the BPDU from the uplink device after the protection function is enabled, the root interface is to be blocked. The previous blocked interface becomes the root interface and enter into the forwarding state if it can receive BPDU; it retains the state of being blocked and cannot forward packets if it cannot receive BPDU. This prevents the occurrence of a network loop.

loopback message (LBM)	The loopback packet sent by the node that supports 802.2ag MAC Ping to the destination node. LBM message carries its own sending time.
loopback reply (LBR)	A response message involved in the 802.1ag MAC Ping function, with which the destination MEP replies to the source MEP after the destination MEP receives the LBM. The LBR carries the sending time of LBM, the receiving time of LBM and the sending time of LBR.
loose routing (LR)	A routing mode in which the Request-URI specifies the final destination address of a short message and the route header field specifies the SIP Proxy that the short message needs to pass by.
loss measurement (LM)	A method used to collect counter values applicable for ingress and egress service frames where the counters maintain a count of transmitted and received data frames between a pair of MEPs.
loss of signal (LOS)	No transitions occurring in the received signal.
M	
M2	See Memory Stick Micro .
M2M	See machine-to-machine .
MA	maintenance association
MAB	MIB access broker
MAC address	A link layer address or physical address. It is six bytes long.
MAC address aging	A function that deletes MAC address entries of a device when no packets are received from this device within a specified time period.
MAC address authentication	An authentication method based on port and MAC address and used to control the network access authority of users. In the MAC address authentication mode, a list of permitted MAC addresses is maintained manually and serves as the criterion for filtering the MAC addresses of STAs. However, the efficiency of this method decreases as the number of STAs increases. Therefore, this method is applicable to scenarios that do not have a high requirement on security, such as the home scenario and small office scenario.
MAC binding	MAC address binding binds fixed IP addresses to MAC addresses.
MAC spoofing	media access control address spoofing
MAC sublayer	See media access control sublayer .
MAP	See Mobile Application Part .

MBB	mobile broadband
MC	metrics coordinator
MCA	multi-channel spectrum analyzer unit
MCC	multichannel controller
MCE	MAC control element
MCID	See multimedia caller identification service .
MCU	See multipoint control unit .
MD	See maintenance domain .
MD5	See message digest algorithm 5 .
MDF	See main distribution frame .
MDI	medium dependent interface
MDT	message distribution
MDU	See multi-dwelling unit .
ME	See managed element .
MEC	method of equivalent currents
MED	See Multi-Exit Discriminator .
MEG	See maintenance entity group .
MEL	maintenance entity group level
MELT	See metallic line testing .
MEM	See Media Entertainment Middleware .
MEP	maintenance association end point
MER	message error rate
MF	mediation function
MFC	metalized film capacitor
MG	monitored group
MGC	media gateway controller
MGCF	See media gateway control function .
MGCP	See Media Gateway Control Protocol .
MGW	See media gateway .
MIB	See management information base .
MIC	microwave integrated circuit
MID	message identification

MIN	mobile identification number
MIP	maintenance association intermediate point
MLD	See multicast listener discovery .
MLPPP	Multi-Link Point-to-Point Protocol
MLT	mechanized loop testing
MM	See mobility management .
MME	mobility management entity
MNO	See mobile network operator .
MO	mobile originated
MON	See monitor cluster .
MOS	mean opinion score
MP	multipoint processor
MPLS	See Multiprotocol Label Switching .
MPLS L2VPN	A network that provides the Layer 2 VPN service based on an MPLS network. In this case, on a uniform MPLS network, the carrier is able to provide Layer 2 VPNs of different media types, such as ATM, FR, VLAN, Ethernet, and PPP.
MPLS TE	multiprotocol label switching traffic engineering
MPLS TE FRR	multiprotocol label switching traffic engineering fast reroute
MPLS VPN	See multiprotocol label switching virtual private network .
MPU	main processing unit
MRC	maximum ratio combining
MRU	maximum receive unit
MS	multiplex section
MS-PW	See multi-segment pseudo wire .
MSAN	multiservice access node
MSC	mobile switching center
MSDP	See Multicast Source Discovery Protocol .
MSN	multiple subscriber number
MSO	multiple system operator
MSR	multiple service ring
MST	See multiplex section termination .
MST region	See multiple spanning tree region .

MSTI	See multiple spanning tree instance .
MSTP	See Multiple Spanning Tree Protocol .
MT	multicast tunnel
MTA	multifunctional terminal adapter
MTBF	See mean time between failures .
MTI	moving targets indication radar
MTIE	maximum time interval error
MTTR	See Mean Time to Repair .
MTU	See maximum transmission unit .
MUX	See multiplexer .
MVPN	See mobile virtual private network .
MWI	See message waiting indicator .
Map Layer	Each map layer is used to display and work with a specific GIS dataset. A layer represents geographic data in the GIS map, such as a particular theme of data. Example map layers include streams and lakes, terrain, roads, political boundaries, parcels, building footprints, utility lines, and orthophoto imagery.
Mean Time to Repair (MTTR)	The average time that a device will take to recover from a failure.
Media Entertainment Middleware (MEM)	A core component of Hybrid Video Solution. The MEM provides interfaces for the UMS, MDN, and other components.
Media Gateway Control Protocol (MGCP)	A protocol that defines a type of call control structure. It is a standard protocol for handling the signaling and session management needed during a multimedia conference. In the structure defined by MGC, call control is separated from service bearer. Being independent of the Media Gateway (MG), the call control function is processed by the external call control unit, known as Media Gateway Controller (MGC) or Call Agent (CA). The MG needs to execute the command issued by the MGC. By nature, MGCP is a master/slave protocol.
Memory Stick Micro (M2)	Memory Stick Micro is a storage device used in digital products. It features a large capacity and a small size.
MoIP	modem over IP
Mobile Application Part (MAP)	A protocol defines how messages are exchanged between mobile network entities for the purpose of achieving the MS roaming function.

Monitor Link	A port association solution developed as a supplementary to Smart Link.
Mosaic	A Mosaic channel allows subscribers to view multiple channels in thumbnails. Each thumbnail corresponds to a live TV channel. Subscribers can select a thumbnail to watch the channel in full-screen mode.
Multi-Exit Discriminator (MED)	1. An attribute that is equivalent to the metrics used by IGP. It is only exchanged between two adjacent ASs. The AS that receives this attribute does not advertise it to any other ASs. 2. The Multi-Exit Discriminator (MED) is a value assigned to a route based on a metric value.
Multicast Source Discovery Protocol (MSDP)	A protocol that is applicable only to the PIM-SM domain and meaningful only for the Any-Source Multicast (ASM) model. After the MSDP peer relationship is set up between RPs of different PIM-SM domains, multicast source information can be shared between PIM-SM domains, and the inter-domain multicast can be implemented. After the MSDP peer relationship is set up between RPs of the same PIM-SM domain, multicast source information can be shared in the PIM-SM domain, and anycast RP can be implemented.
Multiple Spanning Tree Protocol (MSTP)	A protocol that can be used in a loop network. Using an algorithm, the MSTP blocks redundant paths so that the loop network can be trimmed as a tree network. In this case, the proliferation and endless cycling of packets is avoided in the loop network. The protocol that introduces the mapping between VLANs and multiple spanning trees. This solves the problem that data cannot be normally forwarded in a VLAN because in STP/RSTP, only one spanning tree corresponds to all the VLANs.
Multiprotocol Label Switching (MPLS)	A technology that uses short tags of fixed length to encapsulate packets in different link layers, and provides connection-oriented switching for the network layer on the basis of IP routing and control protocols.
mVPLS	See management virtual private LAN service .
mVRRP	management Virtual Router Redundancy Protocol
mVSI	See management virtual switching instance .
machine-to-machine (M2M)	A mode in which data is transferred from one machine to another. An M2M management platform implements three communication modes: machine-to-machine, machine-to-mobile phone (providing the remote monitoring capability), and mobile phone-to-machine (providing the remote control capability).
mail server	A server that can receive and send mails. In the report system, the mail server can forward reports to the external mail boxes of users.

main distribution frame (MDF)	A device at a central office, on which all local loops are terminated.
main subrack	The subrack located in the center of a star topology where subracks are connected.
maintenance domain (MD)	The network or the part of the network for which connectivity is managed by connectivity fault management (CFM). The devices in a maintenance domain are managed by a single Internet service provider (ISP).
maintenance entity group (MEG)	A MEG consists of MEs that meet the following criteria: 1. Exist within the same management edges. 2. Have the same MEG hierarchy. 3. Belong to the same P2P or P2MP connection.
managed element (ME)	A particular entity or resource in a networked system environment. It can also represent a physical piece of equipment on the network, the components of the device on the network, or parts of the network itself.
management VRRP backup group	A type of VRRP backup group. The only difference between an mVRRP backup group and a common backup VRRP group is that the mVRRP backup group can be bound to common VRRP backup groups and determine the status of these common backup VRRP groups according to the binding.
management information	The information that is used for network management in a transport network.
management information base (MIB)	A type of database used for managing the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network.
management node	A management node consists of multiple document security management(DSM) servers (four at most) in an area. Management nodes are created so that the DSM management center can synchronize the department and account information of areas from each node and then deliver all information to all nodes, thus realizing across-system authorization and roaming access of security documents.
management virtual private LAN service (mVPLS)	A type of VPLS. Unlike the service VPLS, the mVPLS is used to transmit VRRP and BFD packets instead of user packets.
management virtual switching instance (mVSI)	A type of VSI. The mVSI can be bound to the service VSI. When receiving gratuitous ARP or BFD Down packets, the mVSI notifies all the bound service VSIs of clearing MAC address entries and re-learning MAC addresses.

manual backup	A data storage operation in the database by operators, achieved by running BKP DB or using the SQL Server tool.
manual load balancing mode	The most basic mode of link aggregation. In the manual load balancing mode, you must manually create the Eth-Trunk, add member interfaces to the Eth-Trunk, and specify active interfaces. The Link Aggregation Control Protocol Data Units (LACPDUs) are not involved. All the member interfaces forward data and perform load balancing.
manual switching	The action of manually switching traffic signals between a working channel and a protection channel. Manual switching fails if the channel to which traffic is being switched is faulty or an equal or higher priority switching command is in effect.
masquerading	Impersonating another user, usually with the intention of gaining unauthorized access to a system.
master-slave synchronization	In master-slave mode, a designated master clock disseminates its frequency reference to all other slave clocks.
maximum transmission unit (MTU)	The largest packet of data that can be transmitted on a network. MTU size varies, depending on the network—576 bytes on X.25 networks, for example, 1500 bytes on Ethernet, and 17,914 bytes on 16 Mbit/s token ring. Responsibility for determining the size of the MTU lies with the link layer of the network. When packets are transmitted across networks, the path MTU, or PMTU, represents the smallest packet size (the one that all networks can transmit without breaking up the packet) among the networks involved.
mean time between failures (MTBF)	The average time between consecutive failures of a piece of equipment. It is a measure of the reliability of the system.
media access control sublayer (MAC sublayer)	A part of the data link layer that supports topology-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer.
media gateway (MGW)	A logical entity that converts the format of the media of a network to meet the format requirement of another network. It can process audio services, video services and data services, and convert the media format in full duplex mode. In addition, it can play certain audio and video signals, and provide the IVR function and media conference.
media gateway control function (MGCF)	A gateway through which the IMS users communicate with the CS users. All the call control signaling messages from the CS/IMS users are sent to the MGCF. The MGCF implements conversion between ISUP or BICC and SIP and forwards sessions to the IMS. In addition, the MGCF controls the media channels in the IM-MGW.

member	A basic element for forming a dimension according to the hierarchy of each level. Each member represents a data element in a dimension. For example, January 1997 is a typical member of the time dimension.
mesh topology	A network topology consisting of manageable segments in which redundant links are used between important devices. It effectively prevents single-point failures on critical paths.
message digest algorithm 5 (MD5)	A hash function that is used in a variety of security applications to check message integrity. MD5 processes a variable-length message into a fixed-length output of 128 bits. It breaks up an input message into 512-bit blocks (sixteen 32-bit little-endian integers). After a series of processing, the output consists of four 32-bit words, which are then cascaded into a 128-bit hash number.
message tracing	A way for service debug, fault diagnosis, and fault rectification. Message tracing is used by maintenance personnel to locate problems that occur when users are connected to the service. Message tracing can transfer the state changes of specified users and the protocol processing results to the terminal or server for reference.
message waiting indicator (MWI)	A common feature of telephone networks. It typically involves an audible or visible indication that voicemail messages are waiting, such as playing a special dial tone.
metallic line testing (MELT)	A test solution that is provided by the DSLAM host and integrates the digital multimeter (DMM). The MELT function is integrated in the internal service board and tests the physical characteristics of the copper line for each service port. The test items include the DC voltage, AC voltage, insulation resistance, and capacitance and the test can diagnose a fault on a twisted pair cable.
microwave	The portion of the electromagnetic spectrum with much longer wavelengths than infrared radiation, typically above about 1 mm.
mobile network operator (MNO)	A company that has a network infrastructure, sells large network capacities, and provides transparent network channels.
mobile virtual private network (MVPN)	A service based on the standard Wireless Intelligent Network (WIN) technology and implemented on the intelligent network (IN). The MVPN is a logical private network provided for some enterprises or groups on the basis of the CDMA network, GSM network, or PSTN network. These enterprises and groups can provide services for their respective subscribers in the MVPN. The MVPN can provide group customers with a preferential charging rate, facilitating control over the call charge of groups and subscribers.

mobility management (MM)	A function in the layer 3 of the Open Systems Interconnection (OSI) reference model which carries out registration and authentication for the mobile station.
module number	A customized number used to uniquely identify a processing unit. The active process and standby process share the same module number.
monitor cluster (MON)	A multi-node cluster that monitors the status and performs data synchronization.
monitored object	A physical or a logical network entity monitored in a centralized network monitoring task. A monitored object can be a physical object such as a board or a subrack. It can also be a logical object such as a cell.
mounting ear	A piece of angle plate on a rack. The mounting ear has holes that can be used to fix network elements or components.
multi-dwelling unit (MDU)	A network access unit used for multi-dwelling units. It provides Ethernet and IP services and optionally VoIP or CATV services; has multiple broadband interfaces on the user side and optionally POTS ports or CATV RF ports. It is mainly applicable to FTTB, FTTC, or FTTCab networks.
multi-homed host	A TCP/IP host that has connections to two or more physical networks.
multi-hop	In the IP network, one hop means that a packet arrives at the destination with a route forwarding. Single-hop means that a packet arrives at the destination with the route forwarding that occurs only once. Multi-hop means that a packet arrives at the destination with the route forwarding that occurs several times.
multi-segment pseudo wire (MS-PW)	A collection of multiple adjacent PW segments. Each PW segment is a point-to-point PW. The use of MS-PWs to bear services saves tunnel resources and can transport services over different networks.
multi-tenant	A software architecture technology. It enables multiple tenants to use the same system or software while separating their data.
multicast listener discovery (MLD)	A protocol used by an IPv6 router to discover the multicast listeners on their directly connected network segments, and to set up and maintain member relationships. On IPv6 networks, after MLD is configured on the receiver hosts and the multicast router to which the hosts are directly connected, the hosts can dynamically join related groups and the multicast router can manage members on the local network.

multicast routing protocol	A protocol used to set up and maintain multicast routes, and to correctly and effectively forward multicast packets. The multicast route is used to set up a loop-free transmission path from the source to multiple receivers, that is, the multicast distribution tree.
multimedia caller identification service (MCID)	A kind of multimedia service based on the IP multimedia subsystem (IMS). A user of the MCID service subscribes to some multimedia resources and uses them as the MCIDs. When the user calls another user, the terminal of the called user plays the MCIDs. The MCIDs can be audio files or video files.
multimedia session	A combination of multimedia senders and receivers. It contains data streams between senders and receivers.
multiple spanning tree instance (MSTI)	A type of spanning trees calculated by MSTP within an MST Region, to provide a simply and fully connected active topology for frames classified as belonging to a VLAN that is mapped to the MSTI by the MST Configuration. A VLAN cannot be assigned to multiple MSTIs.
multiple spanning tree region (MST region)	A region that consists of switches that support the MSTP in the LAN and links among them. Switches physically and directly connected and configured with the same MST region attributes belong to the same MST region.
multiplex section termination (MST)	A function that generates the multiplex section overhead (MSOH) during the formation of an SDH frame signal and that terminates the MSOH in the reverse direction.
multiplexer (MUX)	Equipment that combines a number of tributary channels onto a fewer number of aggregate bearer channels, the relationship between the tributary and aggregate channels being fixed.
multipoint control unit (MCU)	A unit consisting of two parts, namely, Multipoint Controller (MC) and Multipoint Processor (MP). The MC is responsible for internal control and call management, and the MP is responsible for handling media streams.
multiprotocol label switching virtual private network (MPLS VPN)	An Internet Protocol (IP) virtual private network (VPN) based on the multiprotocol label switching (MPLS) technology. It applies the MPLS technology for network routers and switches, simplifies the routing mode of core routers, and combines traditional routing technology and label switching technology. It can be used to construct the broadband Intranet and Extranet to meet various service requirements.

N

NA	numerical aperture
NAB	network address book

NACK	See negative acknowledgement .
NAPT	Network Address and Port Translation
NAS	network access server
NB	normal burst
NBI	See northbound interface .
NBMA	non-broadcast multiple access
NC	See NTP client .
NCP	Network Control Protocol
NCS	Network-Based Call Signaling Protocol
ND	See neighbor discovery .
NDC	national destination code
NDP	See Neighbor Discovery Protocol .
NE	network element
NE Explorer	The main operation interface, which is used to manage the telecommunication equipment. In the NE Explorer, a user can query, manage, and maintain NEs, boards, and ports.
NE user (NU)	A user with the identity for operation and maintenance on an NE through the login to the LMT.
NEBS	Network Equipment Building System
NET	See network entity title .
NEXT	near-end cross talk
NHLFE	next hop label forwarding entry
NHRP	next hop resolution protocol
NIT	network interface tap
NLP	normal link pulse
NLRI	network layer reachability information
NNHOP	next-next hop
NNI	network node interface
NO	See network optimization .
NOTIFY	A SIP request transferring notices about any change in an event.
NP	See network processor .
NPE	network provider edge
NPU	network process unit

NQA	network quality analysis
NR	nature rubber
NRZ	non-return to zero
NS	network system
NSAP	See network service access point .
NSF	non-stop forwarding
NT	See node table .
NT1	See network termination 1 .
NT2	See network termination 2 .
NTC	See network traffic collector .
NTP	Network Time Protocol
NTP client (NC)	A bottom-level device in the time synchronization network. An NTP client obtains time from its upper-level NTP server without providing the time synchronization service. Compared with the top-level NTP server, the intermediate NTP server sometimes is called an NTP client.
NU	See NE user .
NVOD	See Near Video on Demand .
Near Video on Demand (NVOD)	The Near Video on Demand (NVOD) service enables carriers to create a channel that consists of content stored on a media server.
Neighbor Discovery Protocol (NDP)	A protocol that is used to discover the information of the neighboring Huawei device that is connected with the local device.
NetBIOS	Network Basic Input/Output System
negative acknowledgement (NACK)	The notification sent by a network device to another network device. It indicates that the network device fails to understand the message or implement a request operation.
neighbor discovery (ND)	Neighbor discovery, which is used during the forwarding of IPv6 packets for duplicate address detection, neighbor address resolution, and neighbor reachability detection. Additionally, ND is a set of protocols and processes for host address configuration. In ND, different ICMPv6 messages are used for router discovery and neighbor discovery.
network chip	A timeslot exchange chip for time division multiplexing (TDM). The exchange uses the network chip to set up a voice channel between any two internal users.

network entity title (NET)	Network layer information of an IS itself. It excludes the transport layer information (SEL = 0) and can be regarded as a special network service access point (NSAP).
network jitter	A sound adjustment method. A higher network jitter contributes to a better connectivity of sounds. In a conference, the lip movements and voice of a speaker may not be synchronous. To solve this problem, users can adjust the network jitter value.
network layer	Layer 3 of the seven-layer OSI model of computer networking. The network layer provides routing and addressing so that two terminal systems are interconnected. In addition, the network layer provides congestion control and traffic control. In the TCP/IP protocol suite, the functions of the network layer are specified and implemented by IP protocols. Therefore, the network layer is also called IP layer.
network license	A unified license management mode in the help of a unified license management server.
network optimization (NO)	Network adjustment and optimization based on the system operating data that is obtained from the performance statistics or drive test during the network operation process.
network processor (NP)	An integrated circuit which has a feature set specifically targeted at the networking application domain. Network Processors are typically software programmable devices and would have generic characteristics similar to general purpose CPUs that are commonly used in many different types of equipment and products.
network service	In an NFV system, an NS consists of multiple VNFs, network links, and physical network functions.
network service access point (NSAP)	A network address defined by ISO, at which the OSI Network Service is made available to a Network service user by the Network service provider.
network termination 1 (NT1)	A type of terminal device that provides U-interface and S/T interface, used to connect the ISDN terminals and ISDN exchange equipment. It mainly performs code switch between the U-interface and the S/T interface, such as the code switch between the 2B1Q and the AMI in Chinese standards. The NT1 mostly work at only the physical layer, without software intelligence; the devices, however, support functions of line maintenance and performance monitoring, and ensure the clock synchronization between the ISDN terminals and the network.
network termination 2 (NT2)	A type of intelligent terminal device. The common NT2 includes terminal control devices such as the private automatic branch exchanges and the LAN routers that support the ISDN functions.

network traffic collector (NTC)	Application running in Unix or Windows, which is responsible for receiving and processing UDP packets from the NTE (Network Traffic Exporter). Then it sends statistical data to the NTA for further analysis.
node table (NT)	A table that stores information such as the block record size, reference accounts of block data, and index locations of block data links in the file allocation table.
nominal value	Electrical parameters and heat, mechanical, and environmental data specified by the manufacturing entity for specifying the conditions under which SCR, rectifying diodes, stacks, devices, or equipment can work well.
non-real-time polling service (nrtPS)	A type of QoS service defined in IEEE 802.16. It is used to support non-real-time, size-variable, and regular services, such as FTP, which requires large bandwidth.
northbound interface (NBI)	An interface that connects to the upper-layer device to provision services and report alarms and performance statistics.
nrtPS	See non-real-time polling service .
number conversion	A procedure for changing user numbers. Attributes such as the address, number, and user type are used as indexes for adding, deleting, and replacing a number.
number segment	A number of consecutive IMSIs or MSISDNs.
O	
OAM	See operation, administration and maintenance .
OAMPDU	operation, administration and maintenance protocol data unit
OAN	optical access network
OC-3	optical carrier level 3
ODF	optical distribution frame
ODN	optical distribution network
OE	office equipment
OID	object identifier
OIF	See Optical Internetworking Forum .
OLC	overload control
OLR	overall loudness rating
OLT	optical line terminal
OM	optical multiplexing

OMA	operation and maintenance agent
OMCC	See optical network terminal management and control channel .
OMCI	optical network terminal management and control interface
OMU	optical multiplexer unit
ONLY	See one number link you .
ONT	See optical network terminal .
ONU	See optical network unit .
OOF	out of frame
OOS	out of service
OP	operator variant algorithm configuration field
OPEX	operating expense
OPM	optical performance monitor
OPTIONS	A message used to query the capability of a server.
OSI	open systems interconnection
OSI reference model	See Open Systems Interconnection reference model .
OSN	optical switch node
OSNR	See optical signal-to-noise ratio .
OSP	optical software platform
OSPF	See Open Shortest Path First .
OSS	operations support system
OTDR	See optical time domain reflectometer .
OTN	optical transport network
OTT	optical tunable transponder
OU	See organization unit .
OUI	organizationally unique identifier
Open Shortest Path First (OSPF)	A link-state, hierarchical interior gateway protocol (IGP) for network routing that uses cost as its routing metric. A link state database is constructed of the network topology, which is identical on all routers in the area.

Open Systems Interconnection reference model (OSI reference model)	An open network architecture model developed by the International Organization for Standardization (ISO) and the ITU-T. This module consists of 7 layers. Each layer has special network functions, such as addressing, flow control, error control, encapsulation, and reliable message transmission. The lowest layer (physical layer) is closest to media technologies. The lower two layers are implemented in hardware and software, and the upper five layers are implemented only in software. The highest layer (application layer) is closest to users. The OSI reference model is a widely used method of understanding network functions.
Optical Internetworking Forum (OIF) offering	A worldwide non-profit organization with membership open to any organization interested in shaping the future of optical internetworking.
offering	An object created by pricing and packing products based on market strategies. Offerings are sold by carriers to customers for revenue.
one number link you (ONLY)	The function provided for enterprises by the mCentrex service that allows one extension number to map multiple terminal numbers. The terminals can ring in sequence or simultaneously.
operation log	A list of information about operation events.
operation set	A collection of operations. Classifying operations into operation sets helps to manage user operation rights. Operations performed by different users have different impacts on system security. Operations with similar impacts are classified into an operation set. Users or user groups entitled to an operation set can perform all the operations in the operation set. The NMS provides some default operation sets. If the default operation sets cannot meet the requirements for right allocation, users can create operation sets as required.
operation, administration and maintenance (OAM)	A set of network management functions that cover fault detection, notification, location, and repair.
operator domain	To facilitate the management of operator authority, you can define domains, assign authority to each domain, and specify operators of each domain. An operator belonging to a domain has the authority of the domain. That is, the operator can manage and maintain the device data corresponding to the authority of the domain.
optical attenuator	A passive device that increases the attenuation in a fiber link. An optical attenuator is used to ensure that the optical power of a signal at the receive end is not excessively high.

optical connector	A component attached to the end of an optical fiber that allows the fiber to connect to another fiber or an optical source.
optical fiber loopback	An operation of directly connecting the Tx and Rx ends of an optical port using an optical fiber in a manual manner, so as to detect whether the local optical port, peer optical port, or optical line is functional. It is usually performed when the all services carried on an optical port are interrupted or an alarm indicating an abnormality is generated on the optical port.
optical network terminal (ONT)	A device that terminates the fiber optical network at the customer premises.
optical network terminal management and control channel (OMCC)	A communication circuit between the OLT and the ONT. It can be an ATM connection or GEM connection. ITU-T Rec. G. 984.3 specifies the PLOAM message for the activation VPI/VCI (ATM mode) or PortID (GEM mode) between the OLT and the ONT. The VPI/VCI or PortID of OMCC is planned by the OLT in the PLOAM message.
optical network unit (ONU)	A form of Access Node that converts optical signals transmitted via fiber to electrical signals that can be transmitted via coaxial cable or twisted pair copper wiring to individual subscribers.
optical signal-to-noise ratio (OSNR)	The ratio of signal power to noise power in a transmission link. OSNR is the most important index for measuring the performance of a DWDM system.
optical switch	A passive component possessing two or more ports that selectively transmits, redirects, or blocks optical power in an optical fiber transmission line.
optical time domain reflectometer (OTDR)	A device that sends a series of short pulses of light down a fiber-optic cable and measures the strength of the return pulses. An OTDR is used to measure fiber length and light loss, and to locate fiber faults.
organization unit (OU)	A container within a domain that provides a facility to classify and differentiate objects in a directory structure such as LDAP.
original file	A file that is associated with the html file displayed in the knowledge base. An original file is also called a primal file. For example, official letter A is delivered. After being converted to the html format, official letter A is represented as file B in the knowledge base. In this case, official letter A is the original file of file B.
originating system	A router that runs the IS-IS protocol.

overcurrent protection	A circuit protection technology. When there is a great volume of traffic on a circuit and the current is stronger than the protection threshold, the circuit is cut off when the circuit protector timer expires.
P	
P-Access-Network-Info	A header field in the SIP message. It transfers access network technologies to the service proxy. The service proxy then optimizes the services for the UA.
P-Asserted-Identity	A header field in the SIP message. The identity of a caller who sends a SIP message can be inserted into the header field. The inserted identity must have been authenticated.
P-CSCF	See proxy-call session control function .
P-Called-Party-ID	A header field in the SIP message. Before being changed, a Request-URI stores the header field in a P-Called-Party-ID during routing and sent together with the request.
P2MP	point-to-multipoint
PA	See planned area .
PABX	private automatic branch exchange
PAD	packet assembler/disassembler
PADR	PPPoE active discovery request
PAM	See pulse amplitude modulation .
PAP	See Password Authentication Protocol .
PAT	pointing acquisition tracking
PBB-TE	provider backbone bridge-traffic engineering
PBO	power back off
PBS	product breakdown structure
PBT	See power boost technology .
PBX	private branch exchange
PC	port controller
PCI	See peripheral component interconnect .
PCM	See pulse code modulation .
PCR	project change request
PCRF	See policy and charging rules function .
PCS	physical coding sublayer
PD	product daemon

PDB	power distribution box
PDF	See policy decision function .
PDH	See plesiochronous digital hierarchy .
PDM	pulse duration modulation
PDP	Policy Decision Point
PDU	packet data unit
PE	See provider edge .
PEM	See power entry module .
PEP	See policy enforcement point .
PER	packed encoding rules
PET	polyester
PG	See paging group .
PHB	See per-hop behavior .
PHP	penultimate hop popping
PHS	packet handling switching
PI	See performance indicator .
PID	program ID
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast - Dense Mode
PIM-SM	Protocol Independent Multicast - Sparse Mode
PITP	Policy Information Transfer Protocol
PKCS	See Public Key Cryptography Standards .
PKT	partition knowledge table
PLC	power line communication
PLL	See phase-locked loop .
PLMN	public land mobile network
PLOAM	physical layer OAM
PLR	See point of local repair .
PM	See port management .
PMA	physical medium attachment
PMBS	See packet mode bearer service .
PMD	polarization mode dispersion

PMS-TC	physical media specific-transmission convergence
PMT	Program Map Table
PMTU	See path maximum transmission unit .
PMU	power monitoring unit
PN	See personal numbering .
POI	point of initiation
PON	passive optical network
POP	See point of presence .
POP3	Post Office Protocol 3
POS	See packet over SDH/SONET .
POST	power on self-test
POTS	See plain old telephone service .
PPM	peak program meter
PPPoA	Point-to-Point Protocol over ATM
PPPoE	Point-to-Point Protocol over Ethernet
PPPoE test	See Point-to-Point Protocol over Ethernet test .
PPPoE+	See Point-to-Point Protocol over Ethernet plus .
PPPoEoA	Point-to-Point Protocol over Ethernet over ATM
PPS	See prepaid service .
PPT	PDH physical terminal
PPTP	See Point-to-Point Tunneling Protocol .
PPV	See Pay Per View .
PQ	See priority queue .
PR	See public relations .
PRA	primary rate access
PRACK	A SIP request that is a reliability message of a temporary response.
PRBS	See pseudo random binary sequence .
PRC	primary reference clock
PRI	Primary Rate Interface
PS	packet switched
PSB	path state block
PSDN	packet switched data network

PSE	Product Support Engineer
PSI	program specific information
PSM	power supply module
PSN	See packet switched network .
PST	Pacific Standard Time
PSTN	See public switched telephone network .
PSW	program status word
PT	payload type
PTI	P-Box test interface
PTM	pulse time modulation
PTN	public telecommunications network
PTP	See point to point .
PTP clock	See Precision Time Protocol clock .
PTT	See push to talk .
PVID	See port VLAN ID .
PVP	See permanent virtual path .
PW template	pseudo-wire template
PWE3	See Pseudowire Emulation Edge-to-Edge .
PWM	pulse-width modulation
PWR	Power Cable
PacketCable 1.0	An E2E structure that provides home IP telephone service, which is known as the digital announcement. The E2E structure is a complete system, including device configuration, call signaling, event message, configuration management, QoS, PSTN cross connection, and security.
Password Authentication Protocol (PAP)	A method of verifying the identity of a user who attempts to log in to a PPP server. This protocol is adopted when a stricter authentication protocol, such as CHAP, cannot take effect, or the user name and password submitted by the user for authentication must be forwarded to other programs without being encrypted.
Pay Per View (PPV)	Pay Per View (PPV) refers to a subscription-based live TV service that allows carriers to charge subscribers for purchasing specific programs they want to watch.
PiP	Picture-in-Picture
PoE	power over Ethernet

Point-to-Point Protocol over Ethernet plus (PPPoE+)	A protocol through which information about the physical location of a user is added into the PPPoE packets in the PPPoE discovery phase. The information helps BRAS to authenticate the user.
Point-to-Point Protocol over Ethernet test (PPPoE test)	A test that is performed to check whether the BTU can be connected upstream to the PPPoE server (BRAS) based on Ethernet in PPPoE mode.
Point-to-Point Tunneling Protocol (PPTP)	A network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across TCP/IP-based data networks.
Precision Time Protocol clock (PTP clock)	A type of high-decision clock defined by the IEEE 1588 V2 standard. The IEEE 1588 V2 standard specifies the precision time protocol (PTP) in a measurement and control system. The PTP protocol ensures clock synchronization precise to sub-microseconds.
Pseudowire Emulation Edge-to-Edge (PWE3)	An end-to-end Layer 2 transmission technology. It emulates the essential attributes of a telecommunication service such as ATM, FR or Ethernet in a packet switched network (PSN). PWE3 also emulates the essential attributes of low speed time division multiplexing (TDM) circuit and SONET/SDH. The simulation approximates to the real situation.
Public Key Cryptography Standards (PKCS)	A group of standards devised and published by RSA Security, including protocols concerning certification request, certificate update, certificate content extension, digital signature format, and digital envelope format.
packet filtering	A process of passing or blocking packets on a network interface based on source and destination addresses, ports, or protocols. It is a way to prevent against undesired intrusion.
packet forwarding capability	Also called interface throughput, the capability of an interface on a device to forward packets. The unit is packet per second (pps). For low-end devices, the packet forwarding capability ranges only from one-figure number to two-figure number kpps, but the high-end devices can reach two-figure numbers or even three-figure number Mpps.
packet mirroring	Mirroring replicates the specified data packets to the monitoring port.
packet mode bearer service (PMBS)	A service in which point-to-point communication users are allowed to use the ITU-T recommended X.25 encoding scheme for communication through ISDN.
packet over SDH/SONET (POS)	A MAN and WAN technology that provides point-to-point data connections. The POS interface uses SDH/SONET as the physical layer protocol, and supports the transport of packet data (such as IP packets) in MAN and WAN.

packet per second (pps)	Packet per second through the network card. Unit of data service bandwidth.
packet switched network (PSN)	A telecommunications network that works in packet switching mode.
packet switching	A network technology in which information is transmitted by means of exchanging packets and the bandwidth of a channel can be shared by multiple connections.
packing case	A case used for packing a board or subrack.
paging group (PG)	A logical group consisting of multiple BSs. In the coverage of a paging group, an SS/MS does not need to set up an air interface link to a specific BS, and the BS can still periodically page this SS/MS and instruct it to perform location update or network re-entry through broadcast messages.
parity check	A method for character level error detection. An extra bit is added to a string of bits, usually a 7-bit ASCII character, so that the total number of bits 1 is odd or even (odd or even parity). Both ends of a data transmission must use the same parity. When the transmitting device frames a character, it counts the numbers of 1s in the frame and attaches the appropriate parity bit. The recipient counts the 1s and, if there is parity error, may ask for the data to be retransmitted.
passive test	A non-intrusive test that does not intrude but only monitors actual services in a network, and obtains test data by analyzing the service stream.
patch area	A memory area used for storing the patch code in each board of NE.
patch loading	During patch loading, the software is written into the Flash boards and the patch area of the board memory from the specified storage area of the OMU board or the BAM of NEs through commands.
path loss	A loss that occurs when RF (Radio Frequency) waves are transmitted through the air. This loss occurs due to atmospheric influences and interaction with objects, which can have a filtering effect on the signal.
path maximum transmission unit (PMTU)	A method of discovering the supported MTU on a specific path by using ICMPv6 Datagram Too Big messages.
peer service	A type of service that is applied in the invoking of distributed services. If a service is connected to other services in the same network element, the other services are the peer services corresponding to the service.

per-hop behavior (PHB)	IETF Diff-Serv workgroup defines forwarding behaviors of network nodes as per-hop behaviors (PHB), such as, traffic scheduling and policing. A device in the network should select the proper PHB behaviors, based on the value of DSCP. At present, the IETF defines four types of PHB. They are class selector (CS), expedited forwarding (EF), assured forwarding (AF), and best-effort (BE).
performance indicator (PI)	An indicator that measures the performance of a project and the quality of a device.
Peripheral component interconnect (PCI)	A standard designed for the bus connecting the computer main board to peripheral devices. The PCI1.0 standard was released by Intel in 1992 and related standards have been released by PCI-SIG since 1993. Peripheral component interconnect (PCI) delivers I/O functionality for computers ranging from servers to workstations, PCs, laptop PCs and mobile devices.
permanent virtual path (PVP)	Virtual path that consists of PVCs.
personal numbering (PN)	A service feature that supports a UPT number that uniquely identifies each UPT user and is used by the caller to reach that UPT user. A UPT user may have more than one UPT number for different applications; however, a UPT user will have only one UPT number per charging account.
phase-locked loop (PLL)	A circuit that consists essentially of a phase detector that compares the frequency of a voltage-controlled oscillator with that of an incoming carrier signal or reference-frequency generator. The output of the phase detector, after passing through a loop filter, is fed back to the voltage-controlled oscillator to keep it exactly in phase with the incoming or reference frequency.
physical resource	A type of resources, which have physical entities, such as mobile phones.
physical subnets	The subnets in the physical topology view or machine topology view.
ping test	A test that is performed to send a data packet to the target IP address (a unique IP address on the device on the network) to check whether the target host exists according to the data packet of the same size returned from the target host.
plain old telephone service (POTS)	The basic telephone service provided through the traditional cabling such as twisted pair cables.
plaintext	In cryptography, the original readable text before it is encrypted.

planned area (PA)	A data area that serves as an off-line workspace where data is synchronized with the current data area before data configuration.
plesiochronous digital hierarchy (PDH)	A multiplexing scheme of bit stuffing and byte interleaving. It multiplexes the minimum rate 64 kbit/s into rates of 2 Mbit/s, 34 Mbit/s, 140 Mbit/s, and 565 Mbit/s.
point of local repair (PLR)	The head-end node of a backup tunnel or a detour tunnel. Services are forwarded to the backup tunnel at this node.
point of presence (POP)	A Point of Presence (POP) is the same entry used by users in adjacent areas to connect to the network. A POP is the minimum unit depending on which the policy for routing requests varies.
point to point (PTP)	A type of service in which data is sent from a single network termination to another network termination.
policy and charging rules function (PCRF)	A functional entity defined in 3GPP to implement dynamic QoS policy control, dynamic service-based charging control, and subscription-information-based authorization control. The PCRF is a combination of the policy decision function (PDF) and charging rule function (CRF).
policy decision function (PDF)	A functional entity used to set policies according to the sessions and related information obtained from the P-CSCF. The PDF is a policy decision point of the SBLP control.
policy enforcement	An operation that is implemented in a WAG to allow only authorized packets to/from a WLAN AN to pass through.
policy enforcement point (PEP)	A client in the policy system of the intra-domain policy management general model defined by the Policy Framework WG of the Internet Engineering Task Force (IETF). The PEP enforces policy decisions made by the policy decision points (PDPs) using Command-Line Interface (CLI), Simple Network Management Protocol (SNMP), and Common Open Policy Service (COPS). For example, it performs QoS policy control for mobile subscribers.
port VLAN ID (PVID)	A default VLAN ID of a port. It is allocated to a data frame if the data frame carries no VLAN tag when reaching the port.
port management (PM)	A function that defines the rules to access the port of a PC, allowing or prohibiting the specified PC to access the specified resources.
port priority	The priority that is used when a port attaches tags to Layer 2 packets. Packets received on ports with higher priorities are forwarded preferentially.
power boost technology (PBT)	A technology that can be used to expand the radio coverage of BTSs.

power control	A process in which the MS or BS uses certain rules to adjust and control the transmit power according to the change in the channel condition and the power of the received signal.
power entry module (PEM)	The module that transfers the external power supply into the power supply for internal use, including AC PEM and DC PEM.
power on	To start up a computer; to begin a cold boot procedure; to turn on the power
pps	See packet per second .
prepaid service (PPS)	A user prepays a service before using it and is charged in real time. When the prepaid amount is used up, the system stops providing the service. The user can use the service again only after recharging.
primary link	A link used in the service running when the production machine works normally, including signaling link and IP network.
primitive	In the hierarchy of signaling system No.7, when the upper layer applies for services from the lower layer or the lower layer transmits services to the upper layer, the data is exchanged between the user and the service provider. The data transmitted between adjacent layers is called primitive.
priority queue (PQ)	An abstract data type in computer programming that supports the following three operations: 1) Adding an element to the queue with a specific priority 2) Removing the element from the queue that has the highest priority, and returning it 3) Finding out the element with highest priority in the queue
private key certificate	The private key file in a key pair, which needs to be used together with a public key. The private key file is used to decrypt the information encrypted by the public key.
process instance	The running instance generated based on a process template, that is, a TT generated based on a process template.
protection service	A specific service that is part of a protection group and is labeled protection.
provider edge (PE)	A device that is located in the backbone network of the MPLS VPN structure. A PE is responsible for managing VPN users, establishing LSPs between PEs, and exchanging routing information between sites of the same VPN. A PE performs the mapping and forwarding of packets between the private network and the public channel. A PE can be a UPE, an SPE, or an NPE.

proxy-call session control function (P-CSCF)	The initial contact point between subscribers and the IMS during service usage. The P-CSCF: Serves as the agent of all SIP signaling and controls routing of calls. Reserves the QoS resources. Compresses the SIP signaling to improve the bandwidth usage of air interfaces. Provides the NAT control to support the NAT penetration in an intranet. Maintains the security union between the subscribers and the IMS to protect the confidentiality and integrity of the signaling between the UEs and the IMS.
pseudo random binary sequence (PRBS)	A sequence that is random in the sense that the value of each element is independent of the values of any of the other elements, similar to a real random sequence.
pseudonode	A virtual node that is used to simulate broadcast network. It is generated by DIS.
public key	A public key is the key known to everyone and is used together with the private key. A public key can encrypt a session key, verify the digital signature, or encrypt data that can be decrypted using a private key. A public key and a private key are a key pair calculated using an algorithm. The public key is open to the public, whereas the private key is confidential. The key pair calculated using this algorithm is unique in the world. If a key in the key pair encrypts a piece of data, the data can only be decrypted by the other key in the key pair.
public key certificate	The digital certificate with a public key. The public key is used to encrypt the data to be transmitted to ensure the security of data transfer. To ensure the correctness of a public key certificate, a digital signature issued by the CA is required.
public relations (PR)	Communication with various sectors of the public to influence their attitudes and opinions in the interest of promoting a person, product or idea.
public switched telephone network (PSTN)	A telecommunications network established to perform telephone services for the public subscribers. Sometimes it is called POTS.
publication	Any material that is published. For example, magazines and newspapers are referred to as publications.
pull-in range	The allowed maximum frequency difference when the VCO (Vector-Controlled Oscillator) frequency is locked after PLL is unlocked.
pulse amplitude modulation (PAM)	Modulation of pulses in which the pulse magnitude varies in accordance with a given function, generally linear, of the value of the modulating signal.

pulse code modulation (PCM) A method of encoding information in a signal by changing the amplitude of pulses. Unlike pulse amplitude modulation (PAM), in which pulse amplitude can change continuously, pulse code modulation limits pulse amplitudes to several predefined values. Because the signal is discrete, or digital, rather than analog, pulse code modulation is more immune to noise than PAM.

push to talk (PTT) A means of instantaneous communication commonly employed in wireless cellular phone services that use a button to switch a device from voice transmission mode to voice reception mode.

Q

QCELP Qualcomm Code Excited Linear Prediction

QPSK See [quadrature phase shift keying](#).

QRS quasi-random signal

QinQ See [802.1Q in 802.1Q](#).

QoS See [quality of service](#).

quadrature phase shift keying (QPSK) A variation of BPSK, and it is also a Double Side Band Suppressed Carrier (DSBSC) modulation scheme, which sends two bits of digital information at a time, called as bigits.

quality of service (QoS) A commonly-used performance indicator of a telecommunication system or channel. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio. It functions to measure the quality of the transmission system and the effectiveness of the services, as well as the capability of a service provider to meet the demands of users.

R

RA routing area

RAB See [radio access bearer](#).

RACS resource and admission control subsystem

RADIUS accounting An accounting mode in which the BRAS sends the accounting packets to the RADIUS server. Then the RADIUS server performs accounting.

RADIUS authentication An authentication mode in which the BRAS sends the user name and the password to the RADIUS server by using the RADIUS protocol. The RADIUS server authenticates the user, and then returns the result to the BRAS.

RAI resource availability indication

RAM See [random access memory](#).

RAN	See radio access network .
RAS	row address select
RB	See radio bearer .
RC	routing controller
RC4	radio configuration 4
RCD	routing control domain
RCP	Remote Copy Protocol
RD	See route distinguisher .
RDI	remote defect indication
RDM	remote deployment manager
RE	radiated emission
RED	See random early detection .
REG	See regenerator .
REI	remote error indication
REQ	An operand in COPS. The PEP uses it to ask for a decision from the PDP. The PEP establishes a client handle that identifies the specific state relating to the PEP itself.
RFC	remote feature control
RFI	radio frequency interference
RG	rating group
RIB	routing information base
RIP	See Routing Information Protocol .
RIPng	Routing Information Protocol next generation
RJ	registered jack
RJ45	registered jack45
RM	See redundancy machine .
RMEP	remote maintenance association end point
RMRI	See required Min Rx interval .
RMS	resource management system
RNC	See radio network controller .
RP	routing performer
RPC	See remote procedure call .
RPF	reference parameter file

RPR	resilient packet ring
RPT	An operand in COPS. The PEP uses it to report the following contents to the PDP: 1. Whether the policy execution is successful or not 2. A state change
RRC	radio resource control
RRPP	See Rapid Ring Protection Protocol .
RS	router solicitation
RS232	See Recommended Standard 232 .
RS422	The specification that defines the electrical characteristics of balanced voltage digital interface circuits. The interface can change to RS232 via the hardware jumper and others are the same as RS232.
RSA	See Rivest-Shamir-Adleman .
RSA algorithm	See Rivest-Shamir-Adleman algorithm .
RSB	reservation state block
RSC	reset circuit signal
RSP	See Remote Serial Protocol .
RST	regenerator section termination
RSTP	See Rapid Spanning Tree Protocol .
RSVP	See Resource Reservation Protocol .
RSVP-TE	See Resource Reservation Protocol-Traffic Engineering .
RT	reverberation time
RTA	registration termination answer
RTCP	See Real-Time Transport Control Protocol .
RTD	See round-trip delay .
RTE	radio test equipment
RTF	radio terminal function
RTN	radio transmission node
RTP	real-time performance
RTR	registration termination request
RTS	request to send
RTSP	Real-Time Streaming Protocol
RTT	round trip time
RTU	See remote test unit .

RUI	See remote user interface .
RX	receive end
RXD	receive data
Rapid Ring Protection Protocol (RRPP)	An Ethernet ring-specific link layer protocol. It cannot only prevent data loop from causing broadcast storm efficiently when the Ethernet ring is complete, but also restore communication channels among nodes on the Ethernet ring rapidly when a link is torn down.
Rapid Spanning Tree Protocol (RSTP)	An evolution of the Spanning Tree Protocol (STP) that provides faster spanning tree convergence after a topology change. The RSTP protocol is backward compatible with the STP protocol.
Rayleigh scattering	A feature of the optical fiber, which occurs on the entire link of the optical fiber. The length of optical fiber on which the Rayleigh scattering occurs is average. Therefore, the discontinuous Rayleigh scattering can be used to detect the exceptions on the optical fiber link.
Real-Time Transport Control Protocol (RTCP)	A protocol used to monitor data delivery. RTCP enables the receiver to detect if there is any packet loss and to compensate for any delay jitter.
Recommended Standard 232 (RS232)	A standard that defines the electrical characteristics, timing, and meaning of signals, and the physical size and pinout of connectors.
Remote Serial Protocol (RSP)	A communication protocol that is based on the ASCII code. Based on this protocol, the GDB host sends a command, and the target returns the execution result or message. The communication is in half-duplex mode, so the sending and receiving is serialized.
Request-URI	A SIP, a SIP URI, or a universal URI (RFC 2396). It specifies the address of a user or a service that is used by a request.
Require	A header field in a SIP message. The UAC uses it to tell the UAS which features the UAS needs to support.
Resource Reservation Protocol (RSVP)	A protocol that reserves resources on every node along a path. RSVP is designed for an integrated services Internet.
Resource Reservation Protocol-Traffic Engineering (RSVP-TE)	An extension to the RSVP protocol for setting up label switched paths (LSPs) in MPLS networks. The RSVP-TE protocol is used to establish and maintain the LSPs by initiating label requests and allocating label binding messages. It also supports LSP rerouting and LSP bandwidth increasing.

Rivest-Shamir-Adleman (RSA)	An asymmetric cryptographic algorithm, which is recommended by Public-Key Cryptography Standards (PKCS) and widely used in electronic commerce. The RSA algorithm is developed based on the fact that it is easy to multiply two large prime numbers but difficult to factoring their product. Therefore their product is used as the encryption key. The RSA algorithm can resist all known password attacks. It has been recommended as the public key encryption standard by International Organization for Standardization (ISO).
Rivest-Shamir-Adleman algorithm (RSA algorithm)	A widely used public/private key algorithm. It is the default cryptographic service provider (CSP) for Microsoft Windows. It was patented by RSA Data Security, Inc., in 1977.
RoHS	restriction of the use of certain hazardous substances
Routing Information Protocol (RIP)	A simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between the source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers and is known to waste bandwidth.
radio access bearer (RAB)	A term used in UMTS to identify the service the AS (Access Stratum) provides to the NAS (Non Access Stratum) for transfer of user data between the UE (User Equipment) and the CN (Core Network).
radio access network (RAN)	The network that provides the connection between CPEs and the CN. It isolates the CN from wireless network.
radio bearer (RB)	The service provided by the Layer 2 for the transfer of user data between UE (User Equipment) and UTRAN (UMTS Terrestrial Radio Access Network).
radio network controller (RNC)	A device in a radio network subsystem that is in charge of controlling the usage and integrity of radio resources.
random access memory (RAM)	Semiconductor-based memory that can be read and written by the CPU or other hardware devices. The storage locations can be accessed in any order.
random early detection (RED)	A packet loss algorithm used in congestion avoidance. It discards the packet according to the specified higher limit and lower limit of a queue so that global TCP synchronization resulting from traditional tail drop can be prevented.
rate limiting	A traffic management technology used to limit the total rate of packet sending on a physical interface or a Tunnel interface. Rate limiting is directly enabled on the interface to control the traffic passing the interface.
re-mark	To change the Differentiated Services Code Point (DSCP) of a packet using a marker based on a traffic control protocol.

re-registration	After the UE registers successfully, the UE initiates a REGISTER request again because the registration times out.
reactivate	To retrieve the original number for a predeactivated subscriber in the reservation period. The reservation period is the period in which a subscriber is in Predeactivated state.
real-time charging	An accounting way that the charging information can be generated, processed, and transmitted in a customized period (such as one second).
real-time polling service (rtPS)	A type of QoS service defined in IEEE 802.16. It is used to support real-time, periodic, and size-variable service streams, such as the MPEG stream. This service requires the BS to provide periodic unicast polling for the SS to meet the real-time needs of the service stream and enable the SS specify the probability of the data to be transmitted. In this service, the SS inhibit competitive requests and piggyback requests. The major service parameters are polling interval, polling jitter, and minimum reserved rate.
real-time query	If the real-time query function is enabled, a user can query data in read-only mode when the standby database applies the data. In this case, the data replication is not affected.
real-time variable bit rate (rt-VBR)	A parameter intended for real-time applications, such as compressed voice over IP (VoIP) and video conferencing. The rt-VBR is characterized by a peak cell rate (PCR), sustained cell rate (SCR), and maximum burst size (MBS). You can expect the source device to transmit in bursts and at a rate that varies with time.
reboot	To start the system again. Programs or data will be reloaded to all boards.
recording system	A device that is used to record a conference. User can play the file recorded as required.
redundancy machine (RM)	A machine that provides the redundancy function for the production machine.
regenerator (REG)	A piece of equipment or device that regenerates electrical signals.
relay	An electronic control device that has a control system and a system to be controlled. The relay of the telepresence system is used to control the power of telepresence equipment and is controlled by the telepresence host.
remind	To prompt a service agent of the next phase to handle a TT when the TT is forwarded to the next phase and is not handled in time.
remote neighbor	If two adjacent devices are not directly connected but through intermediate devices, they are called remote neighbors.

remote notification	With the remote alarm notification function, the remote maintenance personnel are informed of alarms through Emails or short messages.
remote procedure call (RPC)	In distributed computing, a remote procedure call (RPC) is when a computer program causes a procedure (subroutine) to execute in a different address space (commonly on another computer on a shared network), which is coded as if it were a normal (local) procedure call, without the programmer explicitly coding the details for the remote interaction. That is, the programmer writes essentially the same code whether the subroutine is local to the executing program, or remote.[1] This is a form of client-server interaction (caller is client, executor is server), typically implemented via a request-response message-passing system. In the object-oriented programming paradigm, RPC calls are represented by remote method invocation (RMI). The RPC model implies a level of location transparency, namely that calling procedures is largely the same whether it is local or remote, but usually they are not identical, so local calls can be distinguished from remote calls. Remote calls are usually orders of magnitude slower and less reliable than local calls, so distinguishing them is important.
remote test unit (RTU)	A subsystem capable of collecting, pre-processing, and sending data coming from the field sensors to the SCU.
remote user interface (RUI)	A remote user interface is a role defined in the UPnP protocol. It supports the interaction between an RUI client and RUI server through the Remoting Protocol. Specifically, a remote user interface sends and receives control (for example, record, reservation, playing, pause, and stop) commands between an RUI client and the RUI server.
required Min Rx interval (RMRI)	The minimum interval between receiving BFD control packets on the local device.
resource reservation	The process where one or multiple media PDP contexts are created between user devices to transfer media streams.
resource sharing	A physical resource belonging to two or more protection subnetworks.
resume	To restore a subscriber's service. Resumption is the reverse operation of suspension.
rogue ONU	See rogue optical network unit .
rogue optical network unit (rogue ONU)	A rogue ONU that may appear during the running of the PON. This rogue ONU gives out light when it should not give out light, which affects the communication of another ONU or all the ONUs. The rogue ONU is a fatal problem on the TDM PON because it may result in the breakdown of the entire TDM PON system.

root certificate	An unsigned public key certificate or a self-signed certificate that identifies the Root Certificate Authority (CA). A root certificate is part of a public key infrastructure scheme.
round-trip delay (RTD)	The time from first bit/byte of the Ranging-request in the downstream frame till the reception of the Ranging-transmission's last bit/byte. It is used for the calculation of the Equalization-Delay.
route distinguisher (RD)	A 8-byte field in a VPN IPv4 address. An RD and a 4-byte IPv4 address prefix construct a VPN IPv4 address, which is used to differentiate the IPv4 prefixes using the same address space.
rt-VBR	See real-time variable bit rate .
rtPS	See real-time polling service .
rule	Rules define automatic management services or applications. Rules include triggering conditions and execution logic. Triggering conditions refer to the conditions for executing a rule and execution logic refers to a set of actions executed based on the rule.

S

S-CSCF	See serving-call session control function .
S-VLAN	service virtual local area network
S/P	supplier/partner
SA	See source active .
SAAL	Signaling ATM Adaptation Layer
SAC	sales acquisition cost
SAI	service area identifier
SAP	session announcement protocol
SAR	specific absorption rate
SAS	serial attached SCSI
SAToP	Structure-Agnostic Time Division Multiplexing over Packet
SAV	start of active video
SBC	single-board computer
SBU	See single business unit .
SC	square connector
SCC	synchronous common channel
SCN	switched circuit network

SCP	See service control point .
SCTP	See Stream Control Transmission Protocol .
SCU	simple combiner unit
SDH	See synchronous digital hierarchy .
SDI	See serial digital interface .
SDK	software development kit
SDP	See Session Description Protocol .
SDP negotiation	The provide-response mechanism of the SDP, through which two entities negotiate on items such as the media streams to be contained in a session and the coding scheme.
SDSL	symmetric digital subscriber line
SDT	See structured data transfer .
SDTV	See standard-definition television .
SDU	Selection/Distribution Unit
SE	system engineering
SELT	See single-ended loop test .
SELV	safety extra-low voltage
SEP	system extension board
SES	severely errored second
SF	sampling frequency
SFM	See source-filtered multicast .
SFP	See security function policy .
SFTP	See Secure File Transfer Protocol .
SFU	signal filtering unit
SG	See service guide .
SGSN	See serving GPRS support node .
SHA	See secure hash algorithm .
SHDSL	See single-pair high-speed digital subscriber line .
SHDSL.bis	single-pair high-speed digital subscriber line.bis
SHLR	smart home location register
SI	See service integrator .
SID	share information data
SIGTRAN	See Signaling Transport .

SIP URI	It is used for SIP to identify users. A SIP URI includes a user name and a domain name. It can also contain other parameters.
SIP phone	A multimedia terminal device that supports the SIP protocol.
SIPP	Simple Internet Protocol Plus
SL	service loading
SLA	See Service Level Agreement .
SLM	signaling link management
SME	signaling message encryption
SMI	structure of management information
SMTP	See Simple Mail Transfer Protocol .
SMU	See service management unit .
SN	service node
SNAP	Subnetwork Access Protocol
SNML	subnetwork management layer
SNMP	See Simple Network Management Protocol .
SNP	special number presentation
SNR	serial number
SNRM	signal to noise ratio margin
SNS	Social Networking Service
SNTP	See Simple Network Time Protocol .
SO	See security object .
SOHO	See small office and home office .
SONET	See synchronous optical network .
SOP	See standard operating procedure .
SPA	secure password authentication
SPC	stored program control
SPD	security policy database
SPE	See superstratum provider edge .
SPEC	See standard performance evaluation corporation .
SPF	shortest path first
SPI	See Security Parameters Index .
SPL	sound pressure level

SPLC	split charging
SPM	service processing module
SPS	See Service Process Server .
SPT	shortest path tree
SPT switchover	An SPT switchover is applicable only to PIM-SM. When the rate of the Register packet exceeds the threshold, an RP triggers an SPT switchover, sends a Join message to the multicast source, establishes the multicast path from the source to the RP, and informs the DR not to send the Register message. When the packet rate of the RPT exceeds the threshold, DR triggers an SPT switchover, sends a Join message to the multicast source, establishes an SPT from the source to the DR, and switch the multicast data to the SPT.
SPU	service process unit
SQ	See subscriber queue .
SQL	See Structured Query Language .
SR	See strict routing .
SRA	seamless rate adaptation
SRAM	See static random access memory .
SRD	superluminescent LED
SRG	See shared risk group .
SRL	storage replicator log
SRLG	shared risk link group
SRU	SHDSL regenerator unit
SS	streaming server
SSC	secondary synchronization code
SSD	See service support data .
SSH	See Secure Shell .
SSID	service set identifier
SSL	See Secure Sockets Layer .
SSM	scalable systems manager
SSRC	synchronization source
SST	satellite section termination
SSU	synchronization supply unit
ST	See security target .

STB	See set top box .
STD	system target decoder
STM	synchronous transfer mode
STM-1	See Synchronous Transport Module level 1 .
STP	straight-through processing
STS	space time spreading
STU	See storage unit .
STU-C	SHDSL transceiver unit-central office end
STU-R	SHDSL transceiver unit-remote end
SU	service user
SUBSCRIBE	A SIP request. Users or resources use it to start subscription to other resources.
SVC	switched virtual connection
SVP	See service processor .
SYN	See synchronous idle character .
Secure File Transfer Protocol (SFTP)	A network protocol designed to provide secure file transfer over SSH.
Secure Shell (SSH)	SSH is a set of network protocols for securing connections between computers, as well as the utility suite that implements these protocols.
Secure Sockets Layer (SSL)	A security protocol that works at a socket layer. This layer exists between the TCP layer and the application layer to encrypt/decode data and authenticate concerned entities.
Security Parameters Index (SPI)	An identifier for a Security Association, relative to some security protocol. Each security protocol has its own "SPI-space". A (security protocol, SPI) pair may uniquely identify an SA. The uniqueness of the SPI is implementation dependent, but could be based per system, per protocol, or other options. Depending on the DOI, additional information (e.g. host address) may be necessary to identify an SA. The DOI will also determine which SPIs (i.e. initiator's or responder's) are sent during communication.
Service Level Agreement (SLA)	A service contract between a customer and a (SLA) service provider that specifies the forwarding service a customer should receive. A customer may be a user organization (source domain) or another DS domain (upstream domain). A SLA may include traffic conditioning rules which constitute a TCA in whole or in part.

Service Process Server (SPS)	An internal module of the EIE for parsing and running service scripts defined by users.
Session Description Protocol (SDP)	A protocol intended for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation.
Signaling Transport (SIGTRAN)	A protocol stack for the transport of SCN (Switched Circuit Network) signaling protocols (SS7/C7) over an IP network. SIGTRAN is applied to IP network to support the IP interworking between the traditional narrowband telecommunication network PSTN and wideband network.
Simple Mail Transfer Protocol (SMTP)	The TCP/IP protocol which facilitates the transfer of electronic-mail messages, specifies how two systems are to interact, and the format of messages used to control the transfer of electronic mail.
Simple Network Management Protocol (SNMP)	An IETF protocol for monitoring and managing systems and devices in a network. The data being monitored and managed is defined by a MIB. The functions supported by the protocol are the request and retrieval of data, the setting or writing of data, and traps that signal the occurrence of events.
Simple Network Time Protocol (SNTP)	A protocol that is adapted from the Network Time Protocol (NTP) and synchronizes the clocks of computers over the Internet.
Socket Monitor	The Socket Monitor regularly collects information about TCP connections created on service boards. This information helps locate network connection faults.
Stream Control Transmission Protocol (SCTP)	A transport layer protocol used between the SCTP user application and a connectionless packet network. In the SIGTRAN protocol stack, the upper-layer user of SCTP is the adaptation module of the SCN signaling, for example, M2UA and M3UA, and the lower layer of SCTP is the IP network. The SCTP protocol delivers the higher reliability, optimum real-time performance, and multi-homing feature for signaling transmission.
Structured Query Language (SQL)	A programming language widely used for accessing, querying, updating, and managing data in a relational database. It consists of DDL, DML, and DCL.
Synchronous Transport Module level 1 (STM-1)	Synchronous transfer mode at 155 Mbit/s.

sector	A sub-area of a cell. All sectors within one cell are served by the same base station. A radio link within a sector can be identified by a single logical identification belonging to that sector.
secure hash algorithm (SHA)	A technique that computes a 160-bit condensed representation of a message or data file, called a message digest. The SHA is used by the sender and the receiver of a message in computing and verifying a digital signature, for security purposes.
security function policy (SFP)	A security strategy adopted to implement the functions required by the security factors of the security subsystem of the network (SSON).
security header	A part of the secured packet which consists of all security information (for example, counter, key identification, indication of security level, checksum or Digital Signature).
security object (SO)	A main part of the information security. It is not related with the communication mode or terminal. It does not only focus on the security of the information exchange but also provides feasible solutions of security for the user information, including the user identity authentication, user password, and encryption.
security rule	Local information which, given the security services selected specify the underlying security mechanisms to be employed, including all parameters needed for the operation of the mechanism.
security server	A server that manages and authenticates report users and monitors user operations. When the report system adopts the built-in security mode, the security server of the report system is the report server. When the report system adopts the iMAP (FN) mode, the security server of the report system is the security server integrated with the report system.
security service	A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfer.
security specifications	The standards and descriptions about the specification and requirements of security.
security target (ST)	A set of security functional and assurance requirements and specifications to be used as the basis for evaluation of an identified product or system.
selective QinQ	A function that expands the QinQ function. It enables the interfaces to flexibly add an outer tag of different public VLAN IDs to the frames according to the private network VLAN IDs of the frames.
sensitive information	Information that would negatively impact a company if it were lost or disclosed.

serial digital interface (SDI)	A video interface that transmits data in a single channel in sequence.
service addition	A fixed-line network service application type indicating that a subscriber requires a carrier to provide an additional fixed-line network service for the registered address of the subscriber.
service control point (SCP)	A physical entity in the intelligent network that fulfills the following functions: 1. Controlling services 2. Storing subscriber data and service logics 3. Receiving query requests from the service switching point (SSP) and implementing database query to carry out decoding 4. Initiating service logics according to the call events reported by the SSP 5. Setting up intelligent calls by sending call control instructions to the SSP based on service logics
service flow	An MAC-layer-based unidirectional transmission service. It is used to transmit data packets, and is characterized by a set of QoS parameters, such as latency, jitter, and throughput.
service guide (SG)	A server that provides Electronic Program Guide (EPG) for mobile users.
service integrator (SI)	An integrator for customizing and developing services for ECs.
service interaction	An exchange of information, with a common set of participants (subjects) and involves some activity, governed by rules, requiring evidence and generating outcomes.
service level	The level of service quality of an evaluated party in a specified period, determined by an evaluating party.
service management unit (SMU)	Genetic name of all BSC boards except the GBAM server and the GOMU. A unit that manages users, organizations, and rights in the IVS system.
service number	Unique ID of a network function and its related features provided by a carrier.
service package	A combination of typical services, which is provided by a carrier to publicize and expand service brands and attract more subscribers. The carrier provides the packages with discounts for subscribers who can select and use the packages based on their requirements. Subscribers need to pay only the monthly package fee. They do not need to pay the monthly fee or information fee of each service in the package.
service processor (SVP)	A component that provides a system management and control platform, including power modules and fan modules.
service protection	A measure that ensures that services can be received at the receive end.

service recovery	A function used to restore services existing on devices to the network management system for further management and monitoring. Service recovery is also called automatic service discovery.
service support data (SSD)	An identifier that defines data parameters of specific service feature descriptions in the global functional plane.
service synchronization	Before you use the NMS to manage devices, certain services may have been configured manually or through other tools on the device. Using the service synchronization function, you can discover the services that are not added to the NMS to manage and monitor them.
serving GPRS support node (SGSN)	The Serving GPRS Support Node (SGSN) keeps track of the location of an individual MS and performs security functions and access control. The SGSN is connected to the GERAN base station system through the Gb or Iu interface and/or to the UTRAN through the Iu interface. The SGSN also interfaces via the GPRS Service Switching Function with the GSM Service Control Function for optional CAMEL session and cost control service support.
serving-call session control function (S-CSCF)	Service switching center of the IMS network, which receives and processes registration requests from the UE, manages users, controls sessions, switches services, controls services, processes SIP messages, charges users, and sends SIP requests to ASs.
session timer	A mechanism that is used after establishment of the session. It enables the UE to periodically originate REINVITE or UPDATE to ensure that the session is active.
set top box (STB)	A STB is a part of a user's home network. An STB receives the information services such as TV, films, and music programs from content providers through the broadband IP network and displays various programs to users through a TV set.
settlement	A process of allocating the collected service fees that are generated during the cooperation between partners when a telecommunications service involves the communication resources or value-added service resources of multiple partners. The fee allocation is based on the resource usage and agreement that is signed by the partners in advance.
setup priority	The priority of the tunnel with respect to obtaining resources, ranging from 0 (indicates the highest priority) to 7. It is used to determine whether the tunnel can preempt the resources required by other backup tunnels.

shared key authentication	A process in which both the STA and the AP are configured with the same shared key. The process of shared key authentication is as follows: A STA transmits an authentication request to an AP, and the AP randomly generates a "challenge text" (a character string) and transmits it to the STA. The STA then copies the received "challenge text" to a new message, and transmits the message encrypted with the shared key to the AP. Then, the AP decrypts the message by using the shared key, and compares the decrypted character string with the character string that has been provided to the STA. If the character strings are the same, the STA has the same shared key with the AP, that is, the STA passes the shared key authentication; otherwise, the STA fails to pass the shared key authentication.
shared risk group (SRG)	A group of resources that share a common risk component whose failure can cause the failure of all the resources in the group.
short number	A number that an enterprise assigns to its member. Members from the same or different enterprises can call each other by dialing this number to enjoy the call fee discount.
shorted wires between twisted pairs	Shorted wires due to low performance of insulation resistance or short circuit between wires because of damaged insulation layers between twisted pairs.
showtime	The total time when the line is in the up state.
signaling channel	A channel used for transmission of signaling or data synchronization, including: broadcast channel (BCCH), common control channel (CCCH), and dedicated control channel (DCCH)
signaling link	No.7 signaling link, used to connect the signaling points in the SS7 network and to transfer signaling information.
signaling stream	Streams that control calls and bearer.
signaling tracing	An operation performed to trace messages, the connection process of a signaling link on a port, and service processes in real time. The traced messages can be stored automatically for check. The signaling tracing function provides a basis for rectifying faults.
single business unit (SBU)	A network access unit used for individual enterprise users or individual offices. It functions as a broadband access terminal, provides Ethernet, IP, and TDM services and optionally VoIP services; has Ethernet and E1 interfaces and optionally POTS ports. It is mainly applicable to FTTO networks.
single channel	A channel composed of two half-rate sub-timeslots when one sub-timeslot is occupied and the other is idle.

single-ended loop test (SELT)	An automated way of testing a DSL loop from one end of the line, providing operators with a method for efficiently evaluating their loop as part of their daily operational practices.
single-hop	In the IP network, one hop means that a packet arrives at the destination with a route forwarding. Single-hop means that a packet arrives at the destination with the route forwarding that occurs only once. Multi-hop means that a packet arrives at the destination with the route forwarding that occurs several times.
single-pair high-speed digital subscriber line (SHDSL)	A symmetric digital subscriber line technology developed from HDSL, SDSL, and HDSL2, which is defined in ITU-T G. 991.2. The SHDSL port is connected to the user terminal through the plain telephone subscriber line and uses trellis coded pulse amplitude modulation (TC-PAM) technology to transmit high-speed data and provide the broadband access service.
sink	A sink indicates the receive end in the mirror feature. The mirror feature can transmit information displayed on the screen of a device to the screen of a remote device. Here the remote device is the sink.
sleep mode	A power management mode that shuts down all unnecessary computer operations to save energy. Many battery-powered devices, including portable computers, support sleep mode.
slicing	Dividing data into the information units proper for transmission.
small office and home office (SOHO)	SOHO is an acronym for Small Office, Home Office. The term is usually used in referring to small businesses and home based businesses as a market segment. It is also used to describe a type of working environment.
source active (SA)	A type of the MSDP message. An SA message contains multiple groups of (S,G) information or encapsulates a Register message. MSDP peers exchange (S,G) information to share the multicast source information.
source route	An information mapping table that stores information such as the source address, match length of the source address, account used to deliver messages, and remarks about routing information. It is the information source for routers to route messages and deliver accounts according to the matched destination address.
source system	A system that provides data for the destination system. The HUAWEI ETL collects data from the source system.
source tracing	Source IP addresses of packets are obtained based on the contents of captured packets.

source-filtered multicast (SFM)	A type of the multicast service. The SFM extends the functions based on ASM: the upper-layer software checks the source address of the received multicast packet, and permits or prevents the packets from specific multicast sources to pass through. For the receiver, only some multicast sources are valid.
southbound	Toward, to, or in the south.
specified forwarding	A mode in which a foreground service agent forwards a voice call to a specified service agent. If the specified service agent is idle, the call is forwarded to the service agent directly. Otherwise, the call is forwarded to the private queue of the service agent.
standard operating procedure (SOP)	An SOP is a set of written instructions that document a routine or repetitive activity followed by an organization.
standard performance evaluation corporation (SPEC)	The Standard Performance Evaluation Corporation (SPEC) is a non-profit corporation formed to establish, maintain and endorse a standardized set of relevant benchmarks that can be applied to the newest generation of high-performance computers.
standard-definition television (SDTV)	A type of TV that is capable of displaying at least 480 or 576 interlaced active scan lines.
standby power	A unit that powers a device in a standby mode in case of a power outage.
static LACP mode	A link aggregation method of selecting active and inactive interfaces by negotiating aggregation parameters through LACPDUs. In the static LACP mode, LACP determines active and inactive links of the link aggregation group. It is also called the M:N mode, that is, M active links and N backup links. The M:N mode provides higher reliability and load balancing can be implemented among M links.
static data	The data that does not change in real time during the running of a program.
static random access memory (SRAM)	A type of random access memory. Its contents can be saved only if the SRAM is provided with the uninterrupted power supply. Unlike the DRAM, the SRAM does not need to be refreshed repeatedly.
static user	A user with a fixed IP address.
steady on	Pertaining to a state in which an indicator light is always illuminated and no flicker.

stop bit	In asynchronous transmission, a bit that signals the end of a character. In early electromechanical teleprinters, the stop bit provided time for the receiving mechanism to coast back to the idle position and, depending on the mechanism, had a duration of 1, 1.5, or 2 data bits.
storage area	A combination of user data storage nodes. One storage area consists of one or more data centers. In the web disk service, users can select their nearest storage areas for access acceleration.
storage unit (STU)	An abstract definition of backup storage media for storing backup data. The storage unit is connected to the actual storage media used to back up data.
stream index	An index that is used to uniquely identify a media stream. It is stipulated in the H.248 protocol. For details, refer to the H.248 protocol.
stream mode	A mode that identifies the direction of the media stream on a termination. It is stipulated in the H.248 protocol. For details, refer to the H.248 protocol.
streaming media	Streaming media is media continuously streamed over the network. Combining technologies concerning streaming media data collection, compression, encoding, storage, transmission, playback, and network communications, streaming media can provide high-quality playback effects in real time at low bandwidth.
strict routing (SR)	A routing mode in which the Request-URI specifies the next destination address of a short message. Before delivering a short message, each SIP Proxy replaces the Request-URI of the short message with the address specified by the first route header field, which ensures that the short message passes by all required SIP Proxies.
structured data	Data that can be described by numbers or unified data modules. Structured data has a fixed length and format.
structured data transfer (SDT)	The CS procedure for structured data transfer supports any fixed octet-based structure. In particular, it supports 8 kHz-based structures used in circuit-mode services. When the structure size is greater than one octet, the CS procedure uses a pointer to delineate the structure boundaries.
sub-VLAN	A type of VLAN. A sub-VLAN is a member VLAN of an aggregated VLAN.
subscriber queue (SQ)	A virtual queue. Each SQ maps eight types of FQ priority and can be configured with one to eight FQs. Idle queues cannot be used by other SQs. One to eight FQs share the total SQ bandwidth.

superstratum provider edge (SPE)	Core devices that are located within a VPLS full-meshed network. The UPE devices that are connected with the SPE devices are similar to the CE devices. The PWs set up between the UPE devices and the SPE devices serve as the ACs of the SPE devices. The SPE devices must learn the MAC addresses of all the sites on UPE side and those of the UPE interfaces that are connected with the SPE. SPE is sometimes called NPE.
suspended	A state in the subscriber life cycle. A subscriber in this state cannot use any services but can only dial special service numbers.
switch unit	A critical component of the main control unit, which provides the functions of switching, allocation, scheduling, and control for packets between interface boards. Generally, the switch unit uses ASIC chips of high performance to provide line rate forwarding for packets. The switch unit is also called the switch module (or switch network).
switching capacity	The backplane bandwidth or switching bandwidth. The switching capacity is the maximum data that can be processed by the interface processor of a switch and the data bus. The backplane bandwidth indicates the overall data switching capability of a switch, in Gbit/s.
synchronous digital hierarchy (SDH)	A transmission scheme that follows ITU-T G.707, G.708, and G.709. SDH defines the transmission features of digital signals, such as frame structure, multiplexing mode, transmission rate level, and interface code. SDH is an important part of ISDN and B-ISDN.
synchronous idle character (SYN)	A character used in synchronous (timed) communications that enables the sending and receiving devices to maintain the same timing. Also called sync character.
synchronous optical network (SONET)	A high-speed network that provides a standard interface for communications carriers to connect networks based on fiber optical cable. SONET is designed to handle multiple data types (voice, video, and so on). It transmits at a base rate of 51.84 Mbit/s, but multiples of this base rate go as high as 2.488 Gbit/s.
system-level configuration	A command or configuration that can take effect in the system view.
T	
T-CONT	transmission container
T1	A North American standard for high-speed data transmission at 1.544Mbps. It provides 24 x 64 kbit/s channels.
TA	See terminal adapter .
TAP	transferred account procedure

TAPS	See Terminal Application Portal System .
TAU	test access unit
TB	Turbo Button
TC-PAM	trellis coded pulse amplitude modulation
TCA	threshold crossing alert
TCI	target cell identifier
TCM	See trellis coded modulation scheme .
TCN	telecommunication network
TCP	See Transmission Control Protocol .
TCP/IP	Transmission Control Protocol/Internet Protocol
TCS	terminating call screening
TD	transmit degrade
TD-SCDMA	See Time Division-Synchronous Code Division Multiple Access .
TDD	time division duplex
TDEV	time deviation
TDM	See time division multiplexing .
TDMA	See Time Division Multiple Access .
TDR	time-dependent routing
TE1	See terminal equipment type 1 .
TE2	See terminal equipment type 2 .
TEC	total electron content
TEDB	See traffic engineering database .
TEI	terminal endpoint identification
TF	transport format
TI	transaction identifier
TIE	See Tensilica Instruction Extension .
TIM	trace identifier mismatch
TKIP	Temporary Key Integrity Protocol
TL1	Transaction Language 1
TLS	Transport Layer Security
TLV	See type-length-value .
TM	topology management

TMN	See telecommunications management network .
TOD	time of day
TOO	See transfer of ownership .
TOP	task oriented practice
TOS	type of service
TP	See topology protection .
TPC	See transmit power control .
TPID	tag protocol identifier
TPS	trust point server
TR	token ring
TS	See transport stream .
TSC	test system controller
TSU	Tunnel Service Unit
TT	trouble ticket
TTL	See time to live .
TTSI	See trail termination source identifier .
TU	tributary unit
TX	transmit
Tc	committed rate measurement interval
Telnet service	Service provided using Telnet. After a user makes a Telnet connection to the router through a terminal, a virtual terminal link is set up for bidirectional communication.
Tensilica Instruction Extension (TIE)	A type of chip-related identification language provided by Tensilica. Users can use this language to customize and expand the core architecture.
Terminal Application Portal System (TAPS)	A system that provides a universal solution for launching services rapidly to user terminals. The TAPS sets up channels between the service platform and user terminals, provides flexible client framework, supports widget applications, and enables quick responses on terminals and compatibility with many terminals.
Third Generation (3G)	The third generation of digital wireless technology, as defined by the International Telecommunications Union (ITU). Third generation technology is expected to deliver data transmission speeds between 144 kbit/s and 2 Mbit/s, compared to the 9.6 kbit/s to 19.2 kbit/s offered by second generation technology.

Time Division Multiple Access (TDMA)	An approach used for allocating a single channel among many users, by dividing the channel into different timeslots during which each user has access to the medium.
Time Division-Synchronous Code Division Multiple Access (TD-SCDMA)	A 3G mobile communications standard found in UMTS mobile telecommunications networks in China as an alternative to W-CDMA. TD-SCDMA integrates technologies of CDMA, TDMA, and FDMA, and makes use of technologies including intelligent antenna, joint detection, low chip rate (LCR), and adaptive power control. With the flexibility of service processing, a TD-SCDMA network can connect to other networks through the RNC.
To header field	One part of the SIP header field. To header field is the first logic receiver that specifies the address that sends the request or address-of-record of the user who initiates the request. The address in this field is either the final receiver or not.
ToS priority	A ToS sub-field (the bits 0 to 2 in the ToS field) in the ToS field of the IP packet header.
Transmission Control Protocol (TCP)	The protocol within TCP/IP that governs the breakup of data messages into packets to be sent using Internet Protocol (IP), and the reassembly and verification of the complete messages from packets received by IP. A connection-oriented, reliable protocol (reliable in the sense of ensuring error-free delivery), TCP corresponds to the transport layer in the ISO/OSI reference model.
Triple Data Encryption Standard (3DES)	In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Because the key size of the original DES cipher was becoming problematically short, Triple DES was designed to provide a relatively simple method of increasing the key size (three 56-bit DES keys) of DES to protect against brute force attacks, without designing a completely new block cipher algorithm.
tail drop	A congestion management mechanism, in which packets arrive later are discarded when the queue is full. This policy of discarding packets may result in network-wide synchronization due to the TCP slow startup mechanism.
task	An application or a service invoked to complete an atomic service. A task may or may not belong to a job. For example, the bill generation task exists independently and does not belong to any jobs.
tax	An amount of money paid by a customer when the customer uses a service provided by a carrier. For example, a customer must pay a consumption tax when purchasing a mobile phone.

telecommunications management network (TMN)	A protocol model defined by ITU-T for managing open systems in a communications network. TMN manages the planning, provisioning, installation, and OAM of equipment, networks, and services.
term	Duration of a subscription.
terminal adapter (TA)	A device that is used to connect non-ISDN terminals. A plain telephone can be connected to the ISDN network with a terminal adapter.
terminal equipment type 1 (TE1)	ISDN-compatible terminal. The digital terminals that can be used in the ISDN network directly.
terminal equipment type 2 (TE2)	ISDN non-compatible terminal, that is, non-ISDN digital terminal, such as the plain PSTN telephone set and fax machine, which can be used in the ISDN network through the TA adaptation.
test point	The base point for the network performance test. A user can select a managed device node in the network management system and manually set the device node to a test point. While setting a device node to a test point, the user needs to select an interface IP address of the device and set that IP address as the test IP address. The IP address of the loopback interface is recommended.
thread	A kernel object created by the OS. Creating a thread involves creating a thread object and allocating resources for the thread.
threat	Any potential danger to information or systems.
till	A mobile phone with active system menus that support the organization's interactions with customers in the system. Typically associated with stores, a till can be used by one or more assistants who have been registered to use it.
time division multiplexing (TDM)	A multiplexing technology. TDM divides the sampling cycle of a channel into time slots (TSn, n is equal to 0, 1, 2, 3...), and the sampling value codes of multiple signals engross time slots in a certain order, forming multiple multiplexing digital signals to be transmitted over one channel.
time to live (TTL)	A specified period of time for best-effort delivery systems to prevent packets from looping endlessly. When writing data into Redis, there may be a point at which data is no longer needed. We can remove the data explicitly with DEL, or if we want to remove an entire key after a specified timeout, we can use what's known as expiration. When we say that a key has a time to live, or that it'll expire at a given time, we mean that Redis will automatically delete the key when its expiration time has arrived.

time zone	A division of the earth's surface, usually extending across 15° of longitude devised such that the standard time is the time at a meridian at the center of the zone.
timeout interval	For process control, the time the server waits, when a command cannot be successfully completed, before canceling the command.
timestamp	The current time of an event that is recorded by a computer. By using mechanisms such as the Network Time Protocol (NTP), a computer maintains accurate current time, calibrated to minute fractions of a second.
token bucket algorithm	The token bucket is a container for tokens. The capacity of a token bucket is limited, and the number of tokens determines the traffic rate of permitted packets. The token bucket polices the traffic. Users place the tokens into the bucket regularly according to the preset rate. If the tokens in the bucket exceed the capacity, no tokens can be put in. Packets can be forwarded when the bucket has tokens, otherwise they cannot be transferred till there are new tokens in the bucket. This scheme adjusts the rate of packet input.
topology	The logical layout of the components of a computer system or network and their interconnections. Topology deals with questions of what components are directly connected to other components from the standpoint of being able to communicate. It does not deal with questions of physical location of components or interconnecting cables. The communication infrastructure that provides Fibre Channel communication among a set of PN_Ports (e.g., a Fabric, an Arbitrated Loop, or a combination of the two).
topology protection (TP)	Frames that are used to quickly detect topology changes and perform protection switching within 50 ms. In addition, the frames can be sent strictly according to the sequence without disorder or repeated sending. TP frames contain the topology information including the east and west span protection states, protection configuration information and whether to allow the jumbo frame pass through.
traceroute	A program that prints the path to a destination. Traceroute sends a sequence of datagrams with the time-to-live (TTL) set to 1,2, and so on, and uses ICMP time exceeded messages that return to determine routers along the path.
traffic	The product of the number of calls made and received and the average duration of each call in a measurement period.
traffic engineering database (TEDB)	A type of database that every router generates after collecting the information about TE of every links in its area. TEDB is the base of forming the dynamic TE path in the MPLS TE network.

traffic filtering	To filter the traffic flowing over a device according to certain filtering policies for specific purposes.
traffic mirroring	A feature that allows the packet to be replicated to the monitor port for network monitoring and fault removal.
traffic policy	A full set of QoS policies formed by association of traffic classification and QoS actions.
trail termination source identifier (TTSI)	A TTSI uniquely identifies an LSP in the network. A TTSI is carried in the connectivity verification (CV) packet for checking the connectivity of a trail. If it matches the TTSI received by the sink point, the trail has no connectivity defect.
transaction	Business between the customer and carrier, such as payment, and account adjustment.
transfer of ownership (TOO)	A process of changing the customer that a subscriber belongs to.
transformation function	A system function or self-defined function used to clear and process the data.
transit node	All the nodes except the master node on an RRPP ring.
transmit power control (TPC)	A technical mechanism used within some networking devices in order to prevent too much unwanted interference between different wireless networks.
transport stream (TS)	A standard format for transmission and storage of audio, video, and Program and System Information Protocol (PSIP) data. A TS packet is 188 bytes in length.
tray	A component that can be installed in a cabinet for holding chassis or other components.
trellis coded modulation scheme (TCM)	A modulation scheme which allows highly efficient transmission of information over band-limited channels such as telephone lines.
triplet	A parameter set used for authenticating whether the Global System for Mobile Communications (GSM) network is legal. The triplet is stored in the HLR. It contains the following parameters: 1. RAND: A pseudo-random number generated by the random number generator and provided to the Mobile Station (MS). The MS uses RAND to calculate SRES and Kc. 2. SRES: A parameter used by the MS for authentication response. It is used by the network to authenticate the MS. SRES is the result generated through the A3 algorithm by using RAND and Ki. Ki and A3 algorithm is the fixed data stored in the Subscriber Identity Module (SIM) card. 3. Kc: A GSM ciphering key generated through the A8 algorithm by using RAND and Ki. Ki and A8 algorithm are the fixed data stored in the SIM card.

trunk line	A transmission channel between two switching centers or nodes. It is used to connect the exchange to the network.
tunnel ID	A group of information, including the token, slot number of an outgoing interface, tunnel type, and location method.
twisted pair cable	A type of cable that consists of two independently insulated wires twisted around one another for the purposes of canceling out electromagnetic interference which can cause crosstalk. The number of twists per meter makes up part of the specifications for a given type of cable. The greater the number of twists is, the more crosstalk is reduced.
type-length-value (TLV)	An encoding type that features high efficiency and expansibility. It is also called Code-Length-Value (CLV). T indicates that different types can be defined through different values. L indicates the total length of the value field. V indicates the actual data of the TLV and is most important. TLV encoding features high expansibility. New TLVs can be added to support new features, which is flexible in describing information loaded in packets.

U

UAC	user agent client
UAS	See user agent server .
UDP	See user datagram protocol .
UDR	user-defined routing
UDT	Unstructured Data Transfer
UGC	user group code
UGS	unsolicited grant service
UID	user identity
UMG	See universal media gateway .
UMTS	See Universal Mobile Telecommunications System .
UNI	See User-to-Network Interface .
UNI mode	A mode where an ATM cell is directly carried on a E1/T1 and the bits of the ATM cell are sequentially mapped to the valid timeslots on the E1/T1.
UPC	See usage parameter control .
UPE	user-end provider edge
URL	See uniform resource locator .
URPF	See unicast reverse path forwarding .
USB	See Universal Serial Bus .

UTC	Coordinated Universal Time
UUS	user-to-user signaling
Universal Mobile Telecommunications System (UMTS)	A 3G mobile technology that will deliver broadband information at speeds up to 2 Mbit/s. Besides voice and data, UMTS will deliver audio and video to wireless devices anywhere in the world through fixed, wireless and satellite systems.
Universal Serial Bus (USB)	A serial bus standard to interface devices. It was designed for computers such as PCs and the Apple Macintosh, but its popularity has prompted it to also become commonplace on video game consoles and PDAs.
User-to-Network Interface (UNI)	The interface between user equipment and private or public network equipment (for example, ATM switches).
unicast reverse path forwarding (URPF)	A feature that helps to prevent network attacks based on spoofed IP source addresses.
uniform resource locator (URL)	An address that uniquely identifies a location on the Internet. A URL is usually preceded by http://, as in http://www.example.com. A URL can contain more details, such as the name of a hypertext page, often with the file name extension .html or .htm.
universal media gateway (UMG)	A type of media gateway responsible for service bearer conversion, interconnection, and service stream format processing. It serves as a core network device in the GSM system and can assist carriers in building a low-cost, profitable, and future-oriented mobile telecommunication network.
unprotected	Pertaining to the transmission of services that are not protected. Unprotected services cannot be switched to the protection channel if the working channel is faulty or the service is interrupted, because protection is not configured.
unstructured data	Unstructured data (or unstructured information) is information that either does not have a pre-defined data model or is not organized in a pre-defined manner. Unstructured information is typically text-heavy, but may contain data such as dates, numbers, and facts as well. This results in irregularities and ambiguities that make it difficult to understand using traditional programs as compared to data stored in fielded form in databases or annotated (semantically tagged) in documents. The phrase unstructured data usually refers to information that doesn't reside in a traditional row-column database. As you might expect, it's the opposite of structured data — the data stored in fields in a database.

uplink traffic	The network traffic transferred out of an internal carrier network. Noticeably, uplink refers to directing traffic away from user-end link nodes.
upper limit	A maximum consumption amount that a carrier sets for a subscriber in a bill cycle. If the consumption amount if a subscriber exceeds the maximum consumption amount, the OCS system deducts only the maximum consumption amount from the account of the subscriber.
upstream	In an access network, the direction that is far from the subscriber end of the link. A direction of message forwarding within a transaction that refers to the direction that responses flow from the user agent server back to the user agent client.
upstream interface	The interface through which the local router receives multicast data. The router or the multicast source that forwards multicast data to the local router is called the upstream router or upstream multicast source. The network segment where the upstream interface resides is called the upstream network segment.
usage parameter control (UPC)	During communications, UPC is implemented to monitor the actual traffic on each virtual circuit that is input to the network. Once the specified parameter is exceeded, measures will be taken to control. NPC is similar to UPC in function. The difference is that the incoming traffic monitoring function is divided into UPC and NPC according to their positions. UPC locates at the user/network interface, while NPC at the network interface.
user agent server (UAS)	An entity for processing SIP requests and generating response messages.
user datagram protocol (UDP)	An Internet protocol that provides connectionless datagram delivery service to applications. UDP over IP adds the ability to address multiple endpoints within a single network node.
user-defined service	The user-defined service refers to the application layer service consisting of the specified protocol and port., including the game and instant messaging services.
user-defined template	A type of customized template. The user-defined template is created by the user and stored in a user-defined folder. A user can view the details about a user-defined template, and create, modify, delete, copy, cut, or paste a user-defined template.
V	
V.24	The physical layer interface specification between DTE and DCE defined by the ITU-T. It complies with EIA/TIA-232.

V.35	The synchronous physical layer protocol defined by the ITU-T. It is used for communication between network access devices and the packet-based network. V.35 is mainly used in America and Europe.
VA	value assurance
VAD	voice activity detector
VAG	virtual access gateway
VAS	See value-added service .
VB	virtual bridge
VBAS	virtual broadband access server
VBD	voice band data
VC	video codec
VCC	See virtual channel connection .
VCCV	virtual circuit connectivity verification
VCI	virtual channel identifier
VCL	virtual channel link
VDC	variable dispersion compensator
VDN	See virtual directory number .
VDSL	very-high-data-rate digital subscriber line
VDSL2	See very-high-speed digital subscriber line 2 .
VE	virtual Ethernet interface
VFS	See virtual file system .
VGMP	VRRP Group Management Protocol
VIP	very important person
VLAN	virtual local area network
VLAN mapping table	One of the properties of the MST region, which describes mappings between VLANs and spanning tree instances.
VLAN switch	A technology that sets up the switching table based on the interface and VLAN. Based on the switching table, the device replaces the incoming VLAN tag of a received packet with the outgoing VLAN tag to implement the point-to-point transmission for Ethernet services.
VLC	variable-length coding
VLL	virtual leased line
VLSM	variable length subnet mask

VM	virtual memory
VMAC address	See virtual MAC address .
VOS	virtual operating system
VP	See virtual path .
VPDN	virtual private dial-up network
VPI	See virtual path identifier .
VPLS	virtual private LAN segment
VPN	virtual private network
VPN instance	An entity that is set up and maintained by PEs for directly-connected sites. Each site has its VPN instance on a PE. A VPN instance is also called the VPN Routing and Forwarding (VRF) table. A PE has multiple forwarding tables, including a public-network routing table and one or multiple VRFs.
VPN-Target	A BGP extended community attribute that is also called Route Target. In BGP/MPLS IP VPN, VPN-Target is used to control VPN routing information. The VPN-Target attribute defines which sites can receive a VPN IPv4 route and the routes from which sites can be received by a PE.
VPRN	Virtual Private Routing Network
VPWS	See virtual private wire service .
VQE	voice quality enhancement
VRF	VPN routing and forwarding
VRP	See Versatile Routing Platform .
VRRP	See Virtual Router Redundancy Protocol .
VS	virtual system
VT	virtual terminal
VTP	VLAN Trunk Protocol
VTU	video transmission unit
VTU-R	VDSL transceiver unit-remote office end
VTY	See virtual type terminal .
Vectoring	Vectoring is a transmission method that employs the coordination of line signals from multiple DSL transceivers for the reduction of crosstalk levels. It resolves the FEXT problem facing VDSL2 lines and increases the performance of multi-pair VDSL2 lines.

Versatile Routing Platform (VRP)	A fruit of Huawei's many years of research and application experience in the field of network. VRP is a network OS incorporating Huawei's proprietary intellectual properties and capable of supporting various network systems of Huawei. It features a powerful IP forwarding engine as its core, and a perfect integration of real time OS technology, equipment and network management technology and various network application technologies through an advanced architectural design. As a scalable platform capable of sustained evolution with open interfaces, it supports a large number of protocols and features with great flexibility. With this platform, you can build an end-end, secure network of high efficiency, great intelligence, and easy manageability. Huawei has obtained a lot of experience in network running through the massive application of its network products and gained sufficient knowledge of various customer requirements. Such experience and knowledge serve as the basis for the design of the VRP so that the platform can adapt to most of the application environments through its support of diverse protocols and features.
Virtual Router Redundancy Protocol (VRRP)	A protocol designed for multicast or broadcast LANs such as an Ethernet. A group of routers (including an active router and several backup routers) in a LAN is regarded as a virtual router, which is called a backup group. The virtual router has its own IP address. The host in the network communicates with other networks through this virtual router. If the active router in the backup group fails, one of the backup routers in this backup group becomes active and provides routing service for the host in the network.
VoIP	See Voice over Internet Protocol .
Voice over Internet Protocol (VoIP)	A value-added service technology for IP calls. The VoIP service is a new IP telecom service. It can run on fixed and mobile networks and support flexible access points. Fees for VoIP subscribers are relatively low. Calls between VoIP subscribers who belong to the same carrier are free of charge.
value-added service (VAS)	A service provided by carriers and service providers (SPs) together for subscribers based on voice, data, images, SMS messages, and so on. Communication network technologies, computer technologies, and Internet technologies are used to provide value-added services.
version file	Includes the version software, patches, licenses, configuration data, and logs.
very-high-speed digital subscriber line 2 (VDSL2)	An extension of the VDSL technology, which complies with ITU G.993.2, supports multiple spectrum profiles and encapsulation modes, and provides short-distance and high-speed access solutions to the next-generation FTTx access service.

virtual MAC address (VMAC address)	The source MAC address that is allocated to an access device. When transmitting user packets, the access device replaces the source MAC address of the user packets with the VMAC address. In the upstream direction, the device replaces the source MAC address of user packets with the VMAC address, and then transmits the user packets in the network. In the downstream direction, the device replaces the VMAC address of user packets with the source MAC address, and then transmits the user packets in the network. The VMAC helps prevent user source MAC address spoofing, network-side BRAS MAC address spoofing, and user source MAC address conflict.
virtual channel connection (VCC)	A VC logical trail that carries data between two end points in an ATM network. A point-to-multipoint VCC is a set of ATM virtual connections between two or multiple end points.
virtual directory number (VDN)	A number of a virtual device on the call center platform. It represents applications of a certain type. In the call center, a VDN represents a virtual call center.
virtual file system (VFS)	A structure that is applicable to a file system to provide common file operation capabilities for upper-layer file systems and invoke the interfaces of the lower-layer file systems. With this structure, the differences between file systems can be shielded.
virtual path (VP)	A bundle of virtual channels, all of which are switched transparently across an ATM network based on a common VPI.
virtual path identifier (VPI)	The field in the Asynchronous Transfer Mode (ATM) cell header that identifies to which virtual path the cell belongs.
virtual private wire service (VPWS)	A technology that bears Layer 2 services. VPWS emulates services such as ATM, FR, Ethernet, low-speed TDM circuit, and SONET/SDH in a PSN.
virtual type terminal (VTY)	A logical terminal line that is used to access the device through Telnet.
virus	A small application, or string of code, that infects applications. The main function of a virus is to replicate, and it requires a host application to do this. It can damage data directly or degrade system performance.
voice mailbox (VM)	A new communications service that allows the voice data to be converted into digital data and stored on a server, and then the user can obtain the data stored on the server anytime at any place by using a phone or by other means.
voltage drop	The voltage developed across a component or conductor by the flow of current through the resistance or impedance of that component or conductor.

W

WAN	wide area network
WAPI	WLAN Authentication and Privacy Infrastructure
WAS	See web application server .
WCDMA	See Wideband Code Division Multiple Access .
WEEE	waste electrical and electronic equipment
WEP	wired equivalent privacy
WFQ	See weighted fair queuing .
WMM	See Wi-Fi Multimedia .
WRR	weighted round robin
WTR	See wait to restore .
Wi-Fi	See Wireless Fidelity .
Wi-Fi Multimedia (WMM)	A wireless QoS protocol used for guaranteeing preferential transmission for the packets with a higher priority. With the WMM protocol, applications (such as voice and video) enjoy a better quality over the wireless network.
Wideband Code Division Multiple Access (WCDMA)	A standard defined by the ITU-T for the third-generation wireless technology derived from the Code Division Multiple Access (CDMA) technology.
Wireless Fidelity (Wi-Fi)	A short-distant wireless transmission technology. It enables wireless access to the Internet within a range of hundreds of feet wide.
wait to restore (WTR)	The number of minutes to wait before services are switched back to the working line.
web application server (WAS)	The application server software based on Java and J2EE/EJB. It can be used to create a program interface in a web browser. It is a type of middleware that is widely accepted by integrators and customers.
weighted fair queuing (WFQ)	A fair queue scheduling algorithm based on bandwidth allocation weights. This scheduling algorithm allocates the total bandwidth of an interface to queues, according to their weights and schedules the queues cyclically. In this manner, packets of all priority queues can be scheduled.
well-known port	A set of protocol port numbers assigned by transport level protocols such as TCP and UDP to specific uses. Each server listens at a well-known port, and the clients can locate it.
white noise	The noise of which the spectrum density is even in the frequency domain or the space domain.

whitelist	A list or register of items that, for one reason or another, are being provided a particular privilege, service, mobility, access or recognition.
wiring terminal	A point to which a wire can be connected.
work order	A work order for handling a service request. The work order covers different nodes of a service process.
work state	State of an agent to which the call center platform does not distribute any calls. The Work state is similar to the busy state. The difference is that an agent in the Work state can answer internal calls but an agent in the busy state cannot answer internal calls.
working path	A path allocated to transport the normal traffic.
X	
X.25	A data link layer protocol. It defines the communication in the Public Data Network (PDN) between a host and a remote terminal.
XAUI	10 gigabit Ethernet Attachment Unit Interface
XDR	external data representation
XID	exchange identification
XML	See Extensible Markup Language .
xDSL	x digital subscriber line
xDSL access	A family of bandwidth-efficient modulation techniques, developed to achieve extremely high data transfer rates over twisted-pair cables. Where, letter "X" represents a variable and DSL stands for "Digital Subscriber Line". It consists of ADSL, HDSL, SDSL, and VDSL accesses. Users on the access network are usually scattered community users. The access network also carries data access service and voice service.
xTU-C	xDSL transceiver unit - central office end
xTU-R	xDSL transceiver unit - remote end
Y	
Y.1731	The OAM protocol introduced by the ITU-T. Besides the contents defined by IEEE802.1ag, ITU-T Recommendation Y.173 also defines the following combined OAM messages: Alarm Indication Signal (AIS), Remote Defect Indication (RDI), Locked Signal (LCK), Test Signal, Automatic Protection Switching (APS), Maintenance Communication Channel (MCC), Experimental (EXP), and Vendor Specific (VSP) for fault management and performance monitoring, such as frame loss measurement (LM), and delay measurement (DM).

- Y1731** This Recommendation provides mechanisms for user-plane OAM functionality in Ethernet networks.