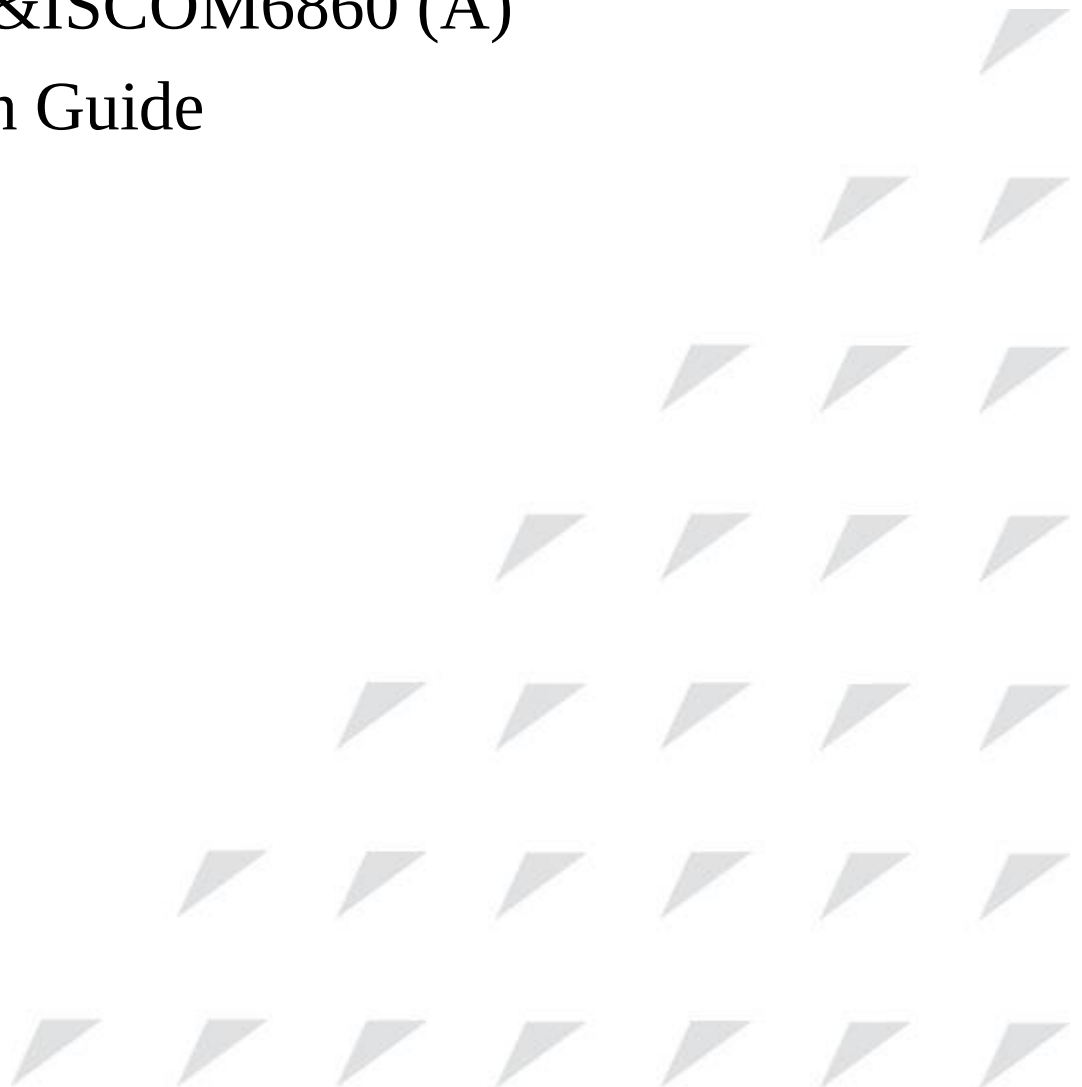


www.raisecom.com

ISCOM6800&ISCOM6860 (A) Configuration Guide (Rel_11)



Raisecom Technology Co., Ltd. provides customers with comprehensive technical support and services. For any assistance, please contact our local office or company headquarters.

Website: <http://www.raisecom.com>

Tel: 8610-82883305

Fax: 8610-82883056

Email: export@raisecom.com

Address: Raisecom Building, No. 11, East Area, No. 10 Block, East Xibeiwang Road, Haidian District, Beijing, P.R.China

Postal code: 100094

Notice

Copyright © 2023

Raisecom

All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in Writing from **Raisecom Technology Co., Ltd.**

RAISECOM is the trademark of Raisecom Technology Co., Ltd.

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

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 the warranty of any kind, express or implied.

Preface

Objectives

This document introduces features supported by and related configurations of the ISCOM6800 and ISCOM6860. The appendix lists terms, acronyms, and abbreviations involved in this document.

This document helps you master basic principles and configurations of the ISCOM6800 and ISCOM6860, as well as how to network with the ISCOM6800 and ISCOM6860.

Versions

The following table lists the product versions related to this document.

Product name	Hardware version	Software version
ISCOM6800	A.03 or later	V2.66 or later
ISCOM6860	A.03 or later	V2.66 or later

Conventions

Symbol conventions

The symbols that may be found in this document are defined as below.

Symbol	Description
 Warning	Indicate a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
 Caution	Indicate a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
 Note	Provide additional information to emphasize or supplement important points of the main text.

Symbol	Description
	Indicate a tip that may help you solve a problem or save time.

General conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Arial	Paragraphs in Warning, Caution, Notes, and Tip are in Arial.
Boldface	Buttons and navigation path are in Boldface .
Italic	Book titles are in <i>italics</i> .
Lucida Console	Terminal display is in <code>Lucida Console</code> .
Book Antiqua	Heading 1, Heading 2, Heading 3, and Block are in Book Antiqua.

Special conventions

Convention	Description
/.*	Indicate the serial number of the ONU interface. The value of * depends on the actual configurations.
.	Indicate the serial number of the PON interface. The value of * depends on the actual configurations.
//*.*	Indicate the serial number of the ONU UNI. The value of * depends on the actual configurations.

Command conventions

Convention	Description
Boldface	The keywords of a command line are in boldface .
Italic	Command arguments are in <i>italics</i> .
[]	Items (keywords or arguments) in square brackets [] are optional.
{ x y . }	Alternative items are grouped in braces and separated by vertical bars. Only one is selected.

Convention	Description
[x y .]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x y . } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x y .] *	Optional alternative items are grouped in square brackets and separated by vertical bars. A minimum of none or a maximum of all can be selected.

Change history

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Issue 11 (2022-12-31)

Eleventh commercial release

- Upgraded the software version to V2.66 SP1.

Issue 10 (2022-07-31)

Tenth commercial release

- Upgraded the software version to V2.66.

Issue 09 (2022-05-19)

Ninth commercial release

- Upgraded the software version to V2.65.

Issue 08 (2021-09-09)

Eighth commercial release

- Fixed known bugs.

Issue 07 (2021-04-19)

Seventh commercial release

- Added the function of bypassing password authentication when entering the privileged EXEC mode to user EXEC mode.
- Added the function of configuring the master/slave domain name of the IPhost interface on the management server.

Issue 06 (2021-01-11)

Sixth commercial release

- Added configurations of the XEP8 (B) card.
- Added P2P VLAN interconnection.
- Added anti-DoS attack.
- Improved QoS.
- Improved configuration examples.

Issue 05 (2020-08-10)

Fifth commercial release

Added the following functions:

- Wi-Fi (EPON)
- Voice SIP management
- LAN port VLAN
- DHCP server template management
- PON protection (EPON)

Issue 04 (2020-07-31)

Fourth commercial release

- Added the query function for the optical power of GPON ONU cards.
- Added GPON 5G Wi-Fi management.
- Added illegal ONU alarm limit and configurations of alarm reporting interval.
- Fixed known bugs.

Issue 03 (2020-05-07)

Third commercial release

- Added GPON automatic authentication rules.
- Fixed known bugs.

Issue 02 (2019-03-30)

Second commercial release

Added the following functions:

- SFTP server configurations
- MLD Proxy
- SIP server template
- IPv6 basic functions
- NDP
- Ring network protection

Issue 01 (2019-01-30)

Initial commercial release

Contents

1 Basic configurations	1
1.1 CLI	1
1.1.1 Overview	1
1.1.2 Levels and privileges	2
1.1.3 Modes.....	3
1.1.4 Shortcut keys.....	7
1.1.5 Display information	8
1.1.6 Showing history commands	10
1.1.7 Acquiring help.....	10
1.2 Accessing device	12
1.2.1 Accessing through Console interface	12
1.2.2 Accessing through Telnet	13
1.2.3 Accessing through SSHv2.....	15
1.2.4 Configuring Console terminal.....	17
1.2.5 Checking configurations	18
1.3 General operations	18
1.4 Managing users	20
1.4.1 Default configurations.....	20
1.4.2 Creating users.....	20
1.4.3 Managing user privileges	20
1.4.4 Refining user privileges	22
1.4.5 Checking configurations	23
1.5 Managing cards	23
1.5.1 Default configurations.....	23
1.5.2 Creating cards	24
1.5.3 Restarting cards.....	26
1.5.4 Energy conservation of card.....	26
1.5.7 Checking configurations	27
1.6 Managing interfaces	28
1.6.1 Default configurations of GE interface	28
1.6.2 Enabling/Disabling interfaces	29
1.6.3 Configuring basic properties of interfaces	29

1.6.4 Configuring interface statistics	30
1.6.5 Configuring flow control on interfaces	31
1.6.6 Configuring VLAN interface	31
1.6.7 Configuring out-of-band network management interface	32
1.6.8 Configuring serial interface	33
1.6.9 Switching interface services.....	35
1.6.10 Checking configurations	37
1.6.11 Maintenance	37
1.7 Managing time	38
1.7.1 Default configurations.....	38
1.7.2 Configuring time and time zone.....	38
1.7.3 Configuring DST	39
1.7.4 Configuring NTP	40
1.7.5 Configuring SNTP	42
1.7.6 Checking configurations	42
1.8 Upgrade and backup.....	43
1.8.1 Introduction.....	43
1.8.2 Configuring server	43
1.8.3 Upgrading OLT system files	44
1.8.4 Backing up OLT system files	46
1.8.5 Upgrading EPON ONU system file	46
1.8.6 Upgrading GPON ONU system file.....	47
1.8.7 Managing ONU configuration file	47
1.8.8 Configuring auto-save.....	48
1.8.9 Smart upgrade of ONU	48
1.8.10 Checking configurations	49
1.9 Task scheduling	50
1.9.1 Introduction.....	50
1.9.2 Default configurations.....	50
1.9.3 Configuring task scheduling	50
1.9.4 Checking configurations	51
1.10 Configuration examples	52
1.10.1 Example for configuring out-of-band network management	52
1.10.2 Example for configuring in-band network management.....	52
1.10.3 Configuring NTP	53
1.10.4 Example for upgrading OLT through TFTP.....	56
1.10.5 Smart upgrade of ONU	57
1.10.6 Example for refining user privileges.....	58
2 Configuring EPON services.....	60
2.1 Registration and deregistration.....	60
2.1.1 Default configuration	60

2.1.2 Registrating ONU	61
2.1.3 Configuring ONU registration authentication password	64
2.1.4 Deregistering ONU	64
2.1.5 Activating ONU	65
2.1.6 Checking configurations	65
2.2 Configuring EPON interface	66
2.2.1 Default configuration	66
2.2.2 Configuring interface	66
2.2.3 Configuring data encryption	66
2.2.4 Configuring the maximum round-trip time	67
2.2.5 Checking configuration	68
2.3 Configuring service template	68
2.3.1 Default configuration	68
2.3.2 Creating a template and configure it	68
2.3.3 Binding template	73
2.3.4 Checking configurations	73
2.4 Configuring voice template	74
2.4.1 Default configurations	74
2.4.2 Creating template	74
2.4.3 Configuring template	74
2.4.4 Checking configurations	75
2.5 Configuring rate-limit template	76
2.5.1 Default configuration	76
2.5.2 Configuring template	76
2.5.3 Binding template	76
2.5.4 Checking configurations	76
2.6 Configuring ONU IP address pool	77
2.6.1 Default configuration	77
2.6.2 Creating address pool	77
2.6.3 Binding PON interface	77
2.6.4 Checking configurations	78
2.7 Rebinding the ONU	78
2.8 Configuring data encryption	79
2.9 Configuring FEC	79
2.10 Configuration examples	80
2.10.1 Configuring automatic registration of ONU	80
2.10.2 Configuring ONU registration based on MAC authentication mode	81
2.10.3 Configuring Ethernet data services	82
2.10.4 Configuring PON+LAN typical networking	84
3 Configuring GPON services	88
3.1 Registration and deregistration	88

3.1.1 Default configurations.....	88
3.1.2 Registering ONU	89
3.1.3 Deregistering ONU	91
3.1.4 Activating ONUs.....	91
3.1.5 Clearing illegal ONU information	92
3.1.6 Checking configurations	92
3.2 Configuring ONU registration keywords	92
3.2.1 Default configurations.....	92
3.2.2 Configuring ONU registration keywords.....	92
3.3 Activating or suspending ONU	93
3.3.1 Default configurations.....	93
3.3.2 Activating or suspending ONU	93
3.4 Configuring GPON interface.....	94
3.4.1 Default configurations.....	94
3.4.2 Configuring interface	94
3.4.3 Checking configurations	95
3.5 Configuring adjustment value of Rx optical power.....	96
3.5.1 Default configurations.....	96
3.5.2 Configuring adjustment value of Rx optical power	96
3.5.3 Checking configurations	97
3.6 Configuring alarm profile.....	97
3.6.1 Default configurations.....	97
3.6.2 Configuring OLT alarm profile	99
3.6.3 Configuring ONU profile.....	102
3.6.4 Checking configurations	106
3.7 Configuring DBA profile	107
3.7.1 Default configurations.....	107
3.7.2 Creating DBA profile	107
3.7.3 Modifying DBA profile.....	108
3.7.4 Checking configurations	110
3.8 Configuring line profile.....	110
3.8.1 Default configurations.....	110
3.8.2 Configuring line profile	110
3.8.3 Binding line profile	113
3.8.4 Checking configurations	113
3.9 Configuring service profile	114
3.9.1 Default configurations.....	114
3.9.2 Configuring profile	114
3.9.3 Binding service profile.....	123
3.9.4 Checking configurations	123
3.10 Configuring rate limit profile	123
3.10.1 Default configuration	123

3.10.2 Configuring profile	124
3.10.3 Binding profile	124
3.10.4 Checking configurations	125
3.11 Configuring TR069 management template	125
3.11.1 Default configurations.....	125
3.11.2 Creating template	125
3.11.3 Configuring template	126
3.11.4 Checking configurations	127
3.12 Configuring VLAN	127
3.12.1 Default configurations.....	127
3.12.2 Configuring VLAN	127
3.12.3 Configuring VLAN mapping based on GEM	129
3.12.4 Checking configurations	130
3.13 Configuring auto-authentication rules	130
3.13.1 Default configuration	130
3.13.2 Configuring auto-authentication rules.....	130
3.13.3 Checking configurations	133
3.14 Configuring rate limiting on GEM interface	133
3.14.1 Checking configurations	133
3.15 Configuration examples	133
3.15.1 Configuring ONU auto-registration	133
3.15.2 Configuring ONU registration based on PASSWORD authentication mode	134
3.15.3 Configuring Ethernet data services	136
4 ONU remote management.....	140
4.1 Managing EPON ONU	140
4.1.1 Default configurations.....	140
4.1.2 ONU basic configurations.....	141
4.1.3 ONU management configurations.....	141
4.1.4 Configuring management IP address	142
4.1.5 Configuring SNMP parameters	145
4.1.6 Configuring UNI	146
4.1.7 Configuring UNI alarm	147
4.1.8 Configuring serial interface	155
4.1.9 Configuring DLF and BPDU forwarding.....	157
4.1.10 Configuring partner discovery	158
4.1.11 Configuring PPPoE Agent.....	159
4.1.12 Configuring PoE	161
4.1.13 Configuring IP interface.....	163
4.1.14 Configuring performance monitoring on PON interface.....	163
4.1.15 Configuring ONU HTTP access control mode	164
4.1.16 Configuring SNMP Trap	164

4.1.17 Configuring EPON ONU WAN interface	166
4.1.18 Configuring DHCP Server	171
4.1.19 Configuring LAN interface VLAN	172
4.1.20 Checking configurations	173
4.2 Configuring GPON ONU.....	175
4.2.1 Default configurations.....	175
4.2.2 Basic configurations.....	176
4.2.3 Configuring user interface	176
4.2.4 Configuring PPPoE proxy	177
4.2.5 Configuring rate-limit profile on ETH interface	178
4.2.6 Configuring ONU access control mode	179
4.2.7 Configuring ONU IPHost interface	179
4.2.8 Checking configurations	181
4.3 Wi-Fi (EPON)	182
4.3.1 Configuring Wi-Fi access point	182
4.3.2 Configuring virtual Wi-Fi access point	183
4.3.3 Checking configurations	184
4.4 Wi-Fi (GPON).....	184
4.4.1 Configuring Wi-Fi.....	184
4.4.2 Configuring 5G Wi-Fi.....	185
4.4.3 Configuring Wi-Fi access point	185
4.4.4 Configuring 5G Wi-Fi access point.....	187
4.4.5 Checking configurations	189
5 Configuring multicast services.....	190
5.1 Introduction	190
5.1.1 Multicast	190
5.1.2 IGMP Snooping	195
5.1.3 IGMP Proxy	195
5.1.4 MVR	196
5.1.5 Dynamic controllable multicast	197
5.2 Quick configurations of multicast services	197
5.2.1 Example for configuring IGMP Snooping	197
5.2.2 Example for configuring dynamic controllable multicast	200
5.3 Configuring static multicast	204
5.3.1 Preparing for configurations	204
5.3.2 Default configurations.....	204
5.3.3 Configuring static multicast	204
5.3.4 Checking configurations	206
5.4 Configuring IGMP Snooping	206
5.4.1 Preparing for configurations	206
5.4.2 Default configurations.....	206

5.4.3 Configuring IGMP Snooping	207
5.4.4 (Optional) configuring aging time of multicast routing entries.....	208
5.4.5 (Optional) configuring immediate leave	209
5.4.6 Checking configurations	210
5.5 Configuring IGMP Proxy.....	211
5.5.1 Preparing for configurations	211
5.5.2 Default configurations.....	211
5.5.3 Configuring IGMP Proxy	211
5.6 Configuring MVR	213
5.6.1 Preparing for configurations	213
5.6.2 Default configurations.....	213
5.6.3 Configuring basic MVR.....	214
5.6.4 Checking configurations	214
5.7 Configuring dynamic controllable multicast	214
5.7.1 Preparing for configurations	214
5.7.2 Default configurations.....	214
5.7.3 Configuring global parameters.....	215
5.7.4 Parameters.....	215
5.7.5 Configuring user management	215
5.7.6 Configuring multicast channel management.....	216
5.7.7 Configuring preview rules	216
5.7.8 Configuring CDR management.....	218
5.7.9 Checking configurations	218
5.8 Configuring MLD Snooping	219
5.8.1 Preparing for configurations	219
5.8.2 Default configurations.....	219
5.8.3 Configuring MLD Snooping	220
5.8.4 Checking configurations	220
5.9 Configuring MLD Proxy	220
5.9.1 Preparing for configurations	220
5.9.2 Default configurations.....	220
5.9.3 Configuring MLD Proxy.....	221
5.9.4 Checking configurations	222
5.10 Configuring multicast VLAN.....	222
5.10.1 Preparing for configurations	222
5.10.2 Default configurations.....	223
5.10.3 Configuring multicast VLAN.....	223
5.10.4 Checking configurations	225
5.11 Maintenance	225
6 Configuring VoIP services	228
6.1 Overview of VoIP services	228

6.1.1 VoIP.....	228
6.1.2 SIP.....	228
6.1.3 H.248.....	229
6.2 Quick configuration of VoIP services.....	231
6.2.1 Example for configuring SIP voice service (Proxy call)	231
6.2.2 Example for configuring SIP voice service (Direct call)	235
6.2.3 Example for configuring H.248 voice service.....	239
6.3 Configuring VoIP	243
6.3.1 Preparing for configurations	243
6.3.2 Default configurations.....	243
6.3.3 Configuring VoIP protocol type	244
6.3.4 Configuring VoIP network parameters	244
6.3.5 Configuring network parameters of media traffic	247
6.3.6 Configuring call process tone parameters	249
6.3.7 Checking configurations	250
6.4 Configuring POTS interface.....	251
6.4.1 Preparing for configurations	251
6.4.2 Default configurations.....	251
6.4.3 Configuring POTS interface	252
6.4.4 Checking configurations	254
6.5 Configuring SIP	254
6.5.1 Preparing for configurations	254
6.5.2 Default configurations.....	255
6.5.3 Configuring SIP transmission protocol	256
6.5.4 Configuring SIP Proxy/Register server	257
6.5.5 Registering and re-registering phone users	259
6.5.6 Configuring SIP heartbeat	259
6.5.7 Configuring SIP user authentication	260
6.5.8 Configuring SIP DigitMap	261
6.5.9 Configuring CID services	261
6.5.10 Configuring call waiting services.....	262
6.5.11 Configuring three-way calling services.....	262
6.5.12 Configuring Modem transparent transmission services	263
6.5.13 Configuring polarity reversal service	263
6.5.14 Configuring hotline service.....	264
6.5.15 Configuring mapping rule of SIP phone numbers.....	265
6.5.16 Configuring voice protocols of SIP server	266
6.5.17 Configuring SIP user parameters	267
6.5.18 Checking configurations	267
6.6 Configuring H.248	268
6.6.1 Preparing for configurations	268
6.6.2 Default configurations.....	269

6.6.3 Configuring H.248 authentication	270
6.6.4 Configuring MG.....	271
6.6.5 Configuring MGC	273
6.6.6 Configuring TID	274
6.6.7 Configuring MG heartbeat	275
6.6.8 Configuring H.248 digitmap	276
6.6.9 Configuring H.248 service management.....	278
6.6.10 Checking configurations	279
6.7 Configuring second dialing	280
6.7.1 Preparing for configurations	280
6.7.2 Default configurations.....	280
6.7.3 Configuring second dialing	280
6.7.4 Checking configurations	281
6.8 Configuring fax	281
6.8.1 Preparing for configurations	281
6.8.2 Default configurations.....	281
6.8.3 Configuring fax	282
6.8.4 Checking configurations	283
6.9 Configuring call emulation test	283
6.9.1 Preparing for configurations	283
6.9.2 Preparing for configurations	284
6.9.3 Configuring call emulation test.....	284
6.9.4 Checking configurations	286
6.10 Configuring SIP server profile	287
6.10.1 Preparing for configurations	287
6.10.2 Default configurations.....	287
6.10.3 Configuring SIP server profile	287
6.10.4 Referencing SIP server profile	291
6.10.5 Checking configurations	293
7 Configuring VoIP services (applicable to EPON POL scenario)	295
7.1 Introduction	295
7.1.1 VoIP.....	295
7.1.2 SIP.....	295
7.1.3 IMS-SIP	297
7.2 Configuring VoIP	297
7.2.1 Preparing for configurations	297
7.2.2 Default configurations.....	297
7.2.3 Configuring VoIP type	297
7.2.4 Checking configurations	298
7.3 Configuring SIP user parameters.....	298
7.3.1 Configuring SIP user parameters	298

7.3.2 Checking configurations	299
7.4 Configuring SIP server template	299
7.4.1 Preparing for configurations	299
7.4.2 Default configurations.....	299
7.4.3 Configuring SIP server template	299
7.4.4 Referencing SIP server template	301
7.4.5 Checking configurations	302
7.5 Examples for configuring MSG	302
7.5.1 Provisioning IMS-SIP voice services.....	302
7.5.2 Provisioning SIP voice service.....	306
8 Configuring CATV services.....	309
8.1 Overview of CATV services.....	309
8.2 Quick configuration of CATV services	310
8.2.1 Networking requirements.....	310
8.2.2 Configuration steps	311
8.2.3 Checking results.....	311
8.3 Configuring CATV services	311
8.3.1 Preparing for configurations	311
8.3.2 Configuring CATV services	312
8.3.3 Checking configurations	312
9 Configuring MAC address.....	314
9.1 Introduction.....	314
9.2 Configuring dynamic MAC address.....	316
9.2.1 Preparing for configurations	316
9.2.2 Default configurations.....	316
9.2.3 Configuring MAC address learning	317
9.2.4 (Optional) configuring aging time of MAC address	317
9.2.5 (Optional) configuring MAC address limit	318
9.2.6 Configuring MAC address flapping.....	320
9.2.7 Checking configurations	320
9.3 Configuring static MAC address.....	321
9.3.1 Preparing for configurations	321
9.3.2 Default configurations.....	322
9.3.3 Configuring static unicast MAC address	322
9.3.4 Configuring static multicast MAC address	323
9.3.5 Checking configurations	325
9.4 Maintenance and search	326
9.4.1 Preparing for configurations	326
9.4.2 Default configurations.....	326
9.4.3 Clearing MAC address.....	326
9.4.4 Searching MAC address.....	327

9.4.5 Tracing MAC address	328
9.5 Configuration examples	328
9.5.1 Example for configuring dynamic MAC address.....	328
9.5.2 Example for configuring static MAC address.....	330
10 Configuring VLAN	333
10.1 Introduction	333
10.1.1 VLAN	333
10.1.2 QinQ.....	338
10.1.3 VLAN mapping.....	338
10.2 Configuring VLAN	339
10.2.1 Preparing for configurations	339
10.2.2 Default configurations.....	339
10.2.3 Configuring OLT interface VLAN	340
10.2.4 Configuring VLAN on ONU UNI	344
10.2.5 Configuring VLAN on ONU SNI	348
10.2.6 Checking configurations	348
10.3 Configuring QinQ	349
10.3.1 Preparing for configurations	349
10.3.2 Default configurations.....	349
10.3.3 Configuring basic QinQ.....	350
10.3.4 Checking configurations	350
10.4 Configuring VLAN ACL.....	351
10.4.1 Preparing for configurations	351
10.4.2 Default configurations.....	351
10.4.3 Creating ACL	351
10.4.4 Configuring matching contents	351
10.4.5 Configuring actions for matched packets.....	353
10.4.6 Applying VLAN-ACL	353
10.4.7 Checking configurations	353
10.5 Configuring VLAN partitioning.....	354
10.5.1 Preparing for configurations	354
10.5.2 Default configurations.....	354
10.5.3 Configuring VLAN based on MAC address	355
10.5.4 Configuring VLAN based on IP subnet	355
10.5.5 Configuring VLAN based on protocol.....	355
10.5.6 Checking configurations	356
10.6 Configuring VLAN mapping	356
10.6.1 Preparing for configurations	356
10.6.2 Default configurations.....	356
10.6.3 Configuring VLAN mapping mode	357
10.6.4 Configuring 1:1 VLAN mapping	357

10.6.5 Configuring N:1 VLAN mapping	358
10.6.6 Configuring translation rules based on VLAN+CoS.....	359
10.6.7 Checking configurations	360
10.7 Configuring virtual interface.....	360
10.7.1 Default configurations.....	360
10.7.2 Configuring VLAN of virtual interface.....	361
10.7.3 Configuring VLAN translation on virtual interface	361
10.7.4 Checking configurations	362
10.8 Configuration examples	362
10.8.1 Example for configuring VLAN	362
10.8.2 Example for configuring basic QinQ	365
10.8.3 Example for configuring VLAN mapping	367
11 Configuring routing	370
11.1 Introduction	370
11.1.1 ARP	370
11.1.2 IPv6	371
11.1.3 Routing.....	371
11.1.4 NDP.....	373
11.2 Configuring ARP.....	374
11.2.1 Preparing for configurations.....	374
11.2.2 Default configurations.....	374
11.2.3 Configuring static ARP entries.....	374
11.2.4 Configuring dynamic ARP entries.....	375
11.2.5 Checking configurations	375
11.3 Configuring IPv6 basic functions	375
11.3.1 Preparing for configurations.....	375
11.3.2 Default configurations.....	375
11.3.3 Configuring IPv6 basic functions.....	376
11.3.4 Checking configurations	376
11.4 Configuring route management	377
11.4.1 Preparing for configurations.....	377
11.4.2 Configuring route management.....	377
11.4.3 Checking routing table	377
11.5 Configuring static routes	378
11.5.1 Preparing for configurations.....	378
11.5.2 Configuring default gateway	378
11.5.3 Configuring static routes	378
11.5.4 Configuring IPv6 static route	379
11.5.5 Checking configurations	380
11.6 Configuring NDP	380
11.6.1 Preparing for configurations.....	380

11.6.2 Configuring static neighbor entries	380
11.6.3 Configuring times of sending NS messages for detecting duplicated addresses	381
11.6.4 Configuring maximum number of NDPs allowed to be learnt.....	381
11.6.5 Configuring flag bit of stateful autoconfiguration.....	382
11.6.6 Configuring the reachable time of neighbors on an IPv6 interface	382
11.6.7 Configuring RA messages.....	383
11.6.8 Configuring router hops	384
11.6.9 Checking configurations	384
11.6.10 Maintenance	384
11.7 Configuration examples	384
11.7.1 Example for configuring ARP	384
11.7.2 Example for configuring static routes	385
12 Configuring DHCP	388
12.1 Introduction.....	388
12.1.1 DHCP packet.....	388
12.1.2 DHCP Snooping.....	390
12.1.3 DHCP Relay.....	391
12.1.4 DHCP Option 82	391
12.2 Configuring DHCP Snooping.....	392
12.2.1 Preparing for configurations	392
12.2.2 Default configurations.....	393
12.2.3 Configuring global DHCP Snooping/DHCPv6 Snooping.....	393
12.2.4 Configuring DHCP Snooping on interface	394
12.2.5 Configuring DHCP Snooping on interface (VLAN range mode)	394
12.2.6 Configuring DHCP Snooping trust on interface	394
12.2.7 (Optional) configuring DHCP Snooping supporting Option 82.....	395
12.2.8 Checking configurations	396
12.2.9 Maintenance	397
12.3 Configuring DHCP Relay	397
12.3.1 Preparing for configurations	397
12.3.2 Default configurations.....	398
12.3.3 Configuring global DHCP Relay	398
12.3.4 Configuring DHCP Relay on IP interface	398
12.3.5 Configuring destination IP address of interface	399
12.3.6 Configuring destination IPv6 address on interface	399
12.3.7 Configuring ONU DHCP Relay.....	400
12.3.8 Configuring DHCP Relay trusted interface.....	400
12.3.9 Configuring DHCPv6 Relay on IP interface	401
12.3.10 (Optional) configuring policies for processing DHCP Relay request packets	401
12.3.11 Checking configurations	401
12.4 Configuring DHCP Option 82.....	402

12.4.1 Preparing for configurations	402
12.4.2 Default configurations.....	402
12.4.3 Enabling DHCP Option 82.....	403
12.4.4 Configuring global DHCP Option attach-string.....	404
12.4.5 Configuring global DHCP Option remote-id	404
12.4.6 Configuring DHCP Option circuit-id on interface	405
12.4.7 Configuring processing policy of Option 82 packet	406
12.4.8 Checking configurations	407
12.5 Maintenance	408
12.6 Configuration examples	408
12.6.1 Example for configuring DHCP Snooping.....	408
12.6.2 Example for configuring DHCP Relay	410
13 Configuring QoS (Applicable to the XEP8 (B) card)	412
13.1 Introduction	412
13.1.1 Priority trust	412
13.1.2 Traffic classification.....	413
13.1.3 Traffic policy	414
13.1.4 Priority mapping	415
13.1.5 Congestion management	415
13.2 Configuring traffic classification.....	417
13.2.1 Preparing for configurations	417
13.2.2 Default configurations.....	417
13.2.3 Configuring priority trust	418
13.2.4 Configuring priority mapping	419
13.2.5 Checking configurations	420
13.3 Configuring traffic monitoring	420
13.3.1 Preparing for configurations	420
13.3.2 Default configurations.....	421
13.3.3 Configuring rate limiting	421
13.3.4 Checking configurations	421
13.4 Configuring traffic shaping	421
13.4.1 Preparing for configurations	421
13.4.2 Default configurations.....	422
13.4.3 Configuring traffic shaping.....	422
13.4.4 Checking configurations	422
13.5 Configuring congestion avoidance	423
13.5.1 Preparing for configurations	423
13.5.2 Default configurations.....	423
13.5.3 Configuring WRED scheduling	423
13.5.4 Checking configurations	423
13.6 Configuring congestion management.....	424

13.6.1 Preparing for configurations	424
13.6.2 Default configurations.....	424
13.6.3 Configuring SP scheduling.....	424
13.6.4 Configuring WRR scheduling.....	425
13.6.5 Checking configurations	425
13.7 Configuring traffic policy.....	426
13.7.1 Preparing for configurations	426
13.7.2 Default configurations.....	426
13.7.3 Configuring OLT traffic policy	426
13.8 Configuration examples	427
13.8.1 Example for configuring queue scheduling.....	427
14 Configuring system security	429
14.1 Introduction	429
14.1.1 ACL.....	429
14.1.2 RADIUS.....	429
14.1.3 TACACS+	430
14.1.4 Storm control	430
14.1.5 Interface isolation.....	430
14.2 Configuring ACL	431
14.2.1 Preparing for configurations	431
14.2.2 Default configurations.....	431
14.2.3 Configuring IP ACL	432
14.2.4 Configuring Layer 2 ACL	440
14.2.5 Configuring hybrid ACL	442
14.2.6 Configuring user ACL.....	453
14.2.7 Applying ACL to device.....	454
14.2.8 Checking configurations	457
14.3 Configuring RADIUS	457
14.3.1 Preparing for configurations	457
14.3.2 Default configurations.....	457
14.3.3 Configuring RADIUS authentication.....	458
14.3.4 Configuring RADIUS accounting.....	459
14.3.5 Checking configurations	460
14.4 Configuring TACACS+.....	460
14.4.1 Preparing for configurations	460
14.4.2 Default configurations.....	461
14.4.3 Configuring TACACS+	461
14.4.4 Configuring TACACS+ accounting	462
14.4.5 Checking configurations	462
14.5 Configuring storm control	463
14.5.1 Preparing for configurations	463

14.5.2 Default configurations.....	463
14.5.3 Configuring storm control.....	464
14.6 Configuring interface isolation.....	465
14.6.1 Preparing for configurations	465
14.6.2 Default configurations.....	466
14.6.3 Configuring OLT interface isolation	466
14.6.4 Configuring ONU interface isolation	467
14.6.5 Checking configurations	467
14.7 Configuring attack prevention.....	468
14.7.1 Preparing for configurations	468
14.7.2 Default configurations.....	468
14.7.3 Configuring attack prevention.....	468
14.7.4 Checking configurations	468
14.8 Configuring anti-DoS attacks.....	469
14.8.1 Preparing for configurations	469
14.8.2 Default configurations.....	469
14.8.3 Configuring anti-DoS attacks.....	469
14.8.4 Checking configurations	469
14.9 Maintenance	470
14.10 Configuration examples	470
14.10.1 Example for configuring ACL	470
14.10.2 Example for configuring RADIUS	472
14.10.3 Example for configuring TACACS+.....	473
14.10.4 Example for configuring storm control	474
14.10.5 Example for configuring anti-DoS attacks	475
15 Configuring link security	477
15.1 Introduction	477
15.1.1 Link aggregation	477
15.1.2 EPON port link protection	478
15.1.3 Interface backup.....	482
15.2 Configuring link aggregation	483
15.2.2 Default configurations.....	484
15.2.3 Configuring manual link aggregation	484
15.2.4 Configuring static LACP link aggregation.....	485
15.2.5 Configuring dynamic LACP	487
15.2.6 Checking configurations	488
15.3 Configuring EPON OLT backbone fiber protection (TypeB).....	488
15.3.1 Preparing for configurations	488
15.3.2 Default configurations.....	488
15.3.3 Configuring OLT backbone fiber protection (Type B).....	489
15.3.4 Configuring ONU backbone fiber protection (Type B)	489

15.3.5 Checking configurations	490
15.4 Configuring cross-OLT EPON port dual-homed protection (Type B)	490
15.4.1 Preparing for configurations	490
15.4.2 Default configurations.....	491
15.4.3 Configuring cross-OLT PON port dual-homed protection (Type B)	491
15.4.4 Configuring ONU PON protection	491
15.4.5 Checking configurations	492
15.5 Configuring port backup	492
15.5.1 Preparing for configurations	492
15.5.2 Default configurations.....	492
15.5.3 Creating interface backup group	493
15.5.4 Configuring interface backup group	493
15.5.5 Configuring force switch	494
15.5.6 Checking configurations	494
15.6 Maintenance	494
15.7 Configuration examples	495
15.7.1 Example for configuring manual link aggregation.....	495
15.7.2 Example for configuring static LACP link aggregation	496
15.7.3 Example for configuring OLT backbone fiber protection (TypeB)	498
15.7.4 Configuring cross-OLT PON port dual-homed protection (Type B).....	499
15.7.5 Example for configuring interface backup	502
16 Configuring system management.....	505
16.1 Introduction	505
16.1.1 SNMP.....	505
16.1.2 Optical module DDM.....	507
16.1.3 System log.....	507
16.1.4 Ping	511
16.1.5 Traceroute	511
16.1.6 Alarm and event management.....	512
16.1.7 PPPoE proxy	513
16.2 Configuring SNMP	513
16.2.1 Default configurations.....	513
16.2.2 Configuring basic functions of SNMPv1/v2c	514
16.2.3 Configuring basic functions of SNMPv3	515
16.2.4 Configuring other information about SNMP	518
16.2.5 Configuring Trap.....	519
16.2.6 Checking configurations	522
16.3 Configuring optical module DDM	522
16.3.1 Default configurations.....	522
16.3.2 Configuring optical module DDM	523
16.3.3 Configuring optical module DDM	523

16.3.4 Checking configurations	524
16.4 PPPoE Agent	525
16.4.1 Default configurations.....	525
16.4.2 Enabling PPPoE Agent.....	526
16.5 Watchdog.....	527
16.5.1 Default configurations.....	527
16.5.2 Configuring Watchdog.....	527
16.5.3 Checking configurations	527
16.6 Configuring system log	528
16.6.1 Default configurations.....	528
16.6.2 Configuring basic information about system log	528
16.6.3 Configuring output direction of system log	529
16.6.4 Checking configurations	531
16.7 Configuring port mirroring.....	532
16.7.1 Default configurations.....	532
16.7.2 Configuring port mirroring on OLT	532
16.7.3 Configuring ONU port mirroring.....	533
16.7.4 Checking configurations	533
16.8 Configuring link detection	534
16.8.1 Ping	534
16.8.2 Traceroute	535
16.9 Configuring PPPoE Agent.....	536
16.9.1 Default configurations.....	536
16.9.2 Configuring PPPoE Agent	537
16.9.3 Enabling PPPoE proxy.....	538
16.9.4 Checking configurations	538
16.10 Configuring system monitoring.....	538
16.10.1 Default configurations.....	538
16.10.2 Configuring temperature monitoring	539
16.10.3 Configuring CPU monitoring.....	540
16.10.4 Configuring memory monitoring	540
16.10.5 Checking configurations	541
16.11 Illegal ONU alarms	542
16.11.1 Default configurations.....	542
16.11.2 Configuring illegal ONU alarm reporting	542
16.11.3 Checking configurations	543
16.12 Configuring link monitoring	543
16.12.1 Default configurations.....	544
16.12.2 Configuring link monitoring	544
16.12.3 Checking configurations	546
16.13 Configuring alarm and event management.....	546
16.13.1 Default configurations.....	546

16.13.2 Configuring alarm management.....	546
16.13.3 Configuring event management	555
16.13.4 Checking configurations	557
16.14 Maintenance	558
16.15 Configuration examples	558
16.15.1 Example for configuring SNMP	558
16.15.2 Example for configuring KeepAlive Trap	560
16.15.3 Example for outputting system log to host.....	561
16.15.4 Example for configuring OLT port mirroring	562
17.2 Configuring G.8032	564
17.2.2 Default configurations of G.8032	565
17.2.3 Creating G.8032 ring.....	565
17.2.5 (Optional) creating G.8032 tributary ring	570
17.2.6 (Optional) configuring G.8032 switching control	574
17.2.7 Checking configurations	575
17.2.8 Maintenance	576
17.3 Configuration examples	576
17.3.1 Example for configuring single-ring G.8032 protection	576
17.3.2 Example for configuring intersecting ring G.8032 protection	579
18 Appendix	584
18.1 Terms.....	584
18.2 Acronyms and abbreviations	588

Figures

Figure 1-1 Accessing the device through a PC connected with Console interface.....	13
Figure 1-2 Communication parameters in Hyper Terminal.....	13
Figure 1-3 Networking with the OLT as the Telnet server	14
Figure 1-4 Networking with the OLT as the Telnet client	15
Figure 1-5 Configuring out-of-band network management.....	52
Figure 1-6 Configuring in-band network management	53
Figure 1-1 NTP networking	54
Figure 1-2 Upgrading OLT through TFTP	56
Figure 1-3 Networking of smart upgrade of ONU	58
Figure 2-1 ONU automatic registration.....	80
Figure 2-2 OUN registration based on MAC authentication mode	81
Figure 2-3 Data services.....	82
Figure 2-4 Configuring ONU independent network management (based on IP address pool)	85
Figure 3-1 ONU auto-registration	133
Figure 3-2 ONU registration based on PASSWORD authentication mode	134
Figure 3-3 Data service networking	136
Figure 5-1 Unicast transmission mode.....	191
Figure 5-2 Broadcast transmission mode	191
Figure 5-3 Multicast transmission mode	192
Figure 5-4 Mapping between an IPv4 multicast address and a multicast MAC address.....	193
Figure 5-5 Operating positions of the IGMP and Layer 2 multicast protocols.....	194
Figure 5-6 IGMP Snooping networking.....	198
Figure 5-7 Dynamic controllable multicast networking.....	201
Figure 6-1 Typical application of SIP in NGN.....	229
Figure 6-2 Position of H.248 in the network	230
Figure 6-3 H.248 H.248 connection model	230

Figure 6-4 Configuring SIP voice service (Proxy call)	232
Figure 6-5 Configuring SIP voice service (Direct call)	236
Figure 6-6 H.248 Configuring H.248 voice service	240
Figure 7-1 Typical application SIP in NGN	296
Figure 8-1 Typical triple-play networking.....	310
Figure 8-2 Configuring CATV services	311
Figure 9-1 Unicast forwarding mode of MAC address	315
Figure 9-2 Broadcast forwarding mode of MAC address	316
Figure 9-3 Configuring dynamic MAC address.....	328
Figure 9-4 Configuring static MAC address	330
Figure 10-1 Structures of Ethernet frame and 802.1Q frame	335
Figure 10-2 Basic QinQ networking	338
Figure 10-3 Configuring VLAN.....	362
Figure 10-4 Example for applying basic QinQ	365
Figure 10-5 Configuring VLAN mapping.....	368
Figure 11-1 Principles of NDP address resolution	373
Figure 11-2 ARP networking.....	385
Figure 11-3 Configuring static routes.....	386
Figure 12-1 DHCP packet structure	388
Figure 12-2 DHCP Snooping networking	390
Figure 12-3 Working principle of DHCP Relay	391
Figure 12-4 Working principle of DHCP Option 82	392
Figure 12-5 DHCP Snooping networking	409
Figure 12-6 DHCP Relay networking	410
Figure 13-1 Traffic classification process	413
Figure 13-2 IP packet header structure.....	413
Figure 13-3 Structures of ToS priority and DSCP priority packets	413
Figure 13-4 VLAN packet structure.....	414
Figure 13-5 CoS priority packet structure.....	414
Figure 13-6 SP scheduling	416
Figure 13-7 WRR scheduling.....	416
Figure 13-8 DRR scheduling.....	417
Figure 13-9 Configuring queue scheduling.....	427

Figure 14-1 ACL networking	470
Figure 14-2 RADIUS application networking	472
Figure 14-3 TACACS+ application networking.....	473
Figure 14-4 Storm control networking.....	474
Figure 14-5 Anti-DoS attack networking	475
Figure 15-1 Principle of OLT backbone fiber protection (Type B)	479
Figure 15-2 Principle of Type C full protection	480
Figure 15-3 Principle of PON full protection (Type D)	481
Figure 15-4 Principle of cross-OLT PON port dual-homed protection (Type B).....	481
Figure 15-5 Principle of interface backup	482
Figure 15-6 VLAN-based interface backup	483
Figure 15-7 Manual link aggregation networking	495
Figure 15-8 Static LACP link aggregation networking	496
Figure 15-9 OLT backbone fiber protection (Type B).....	498
Figure 15-10 Cross-OLT PON port dual-homed protection (Type B).....	500
Figure 15-11 Interface backup networking	502
Figure 16-1 Working mechanism of SNMP	506
Figure 16-2 Working principle of Ping.....	511
Figure 16-3 Working principle of Traceroute.....	512
Figure 16-4 Authentication mechanism of SNMPV3.....	516
Figure 16-5 SNMPv3 networking	558
Figure 16-6 KeepAlive networking.....	560
Figure 16-7 Outputting system log to host	561
Figure 16-8 OLT local port mirroring	563
Figure 17-1 Single ring G.8032 networking.....	576
Figure 17-2 Intersecting ring G.8032 networking	579

Tables

Table 1-1 Corresponding relationship between the CLI level and user level	2
Table 1-2 Shortcut keys about display features	9
Table 2-1 Parameter list of ONU IP address pool	84
Table 2-2 ONU SNMP template parameter list	85
Table 10-1 VLAN modes and packet processing modes	335
Table 10-2 Processing modes of Ethernet frames in VLAN Transparent mode	336
Table 10-3 Processing modes of Ethernet frames in VLAN Tagged mode	336
Table 10-4 Processing modes of Ethernet frames in VLAN Translation mode	337
Table 10-5 Processing modes of Ethernet frames in VLAN Trunk mode	337
Table 12-1 Meanings of fields in the DHCP packet	389
Table 16-1 Log levels	508
Table 16-2 Alarm fields	510
Table 16-3 Alarm levels	510

1 Basic configurations

This chapter describes basic configurations and configuration process of the ISCOM6800 and ISCOM6860, including the following sections:

- CLI
- Accessing device
- General operations
- Managing users
- Managing cards
- Managing interfaces
- Managing time
- Upgrade and backup
- Task scheduling
- Configuration examples

1.1 CLI

1.1.1 Overview

Command Line Interface (CLI) is the path for communication between users and the device. You can configure, monitor, and manage the device by executing related commands.

You can log in to the Device through a PC that runs the terminal emulation program or the CPE device. You can enter CLI once the command prompt appears.

The features of CLI:

- Local configuration through the Console interface is available.
- Local or remote configuration through Telnet or Secure Shell v2 (SSHv2) is available.
- Provide protection for different command levels. Users in different levels can only execute commands in corresponding levels.
- Different command types belong to different command modes. You can only execute a type of configuration in its related command mode.
- Shortcut keys can be used to execute commands.

- Check a history command by checking command history. The last 5000 history commands can be saved on the Device.
- Online help is available by typing "?" at any time.
- Support smart analysis methods, such as incomplete matching and context association, to facilitate user input.

1.1.2 Levels and privileges

CLI levels

The ISCOM6800 and ISCOM6860 use hierarchical protection methods to divide command line into 4 levels from low to high:

- Visitor: you can execute the **ping**, **clear**, and **history** commands in this level.
- Monitor: you can execute the **show** command and so on.
- Operator: you can execute commands for different services like Virtual Local Area Network (VLAN), IP routing, and so on. Most service configuration commands can be executed in this level.
- Administrator: you can execute file system commands (saving, deleting, uploading, and downloading files), user management commands (user authorization and management), FTP commands, TFTP commands, and SFTP commands.

User levels

Corresponding to the CLI levels, users are divided into 16 levels from low to high. Users in different levels can execute commands in related CLI levels.

- 1–4: you can execute commands in visitor level.
- 5–9: you can execute commands in monitor level or lower.
- 10–14: you can execute commands in operator level or lower.
- 15: you can execute commands in administrator level or lower.

Privilege management

Table 1-1 lists the corresponding relationship between the CLI level and user level.

Table 1-1 Corresponding relationship between the CLI level and user level

Levels	Visitor	Monitor	Operator	Administrator
administrator	Permitted	Permitted	Permitted	Permitted
operator	Permitted	Permitted	Permitted	Forbidden
monitor	Permitted	Permitted	Forbidden	Forbidden
visitor	Permitted	Forbidden	Forbidden	Forbidden

1.1.3 Modes

Command mode is the CLI environment. All system commands are registered in one (or some) command line mode, and the command can only run in the corresponding mode.

Establish a connection with the device. If the device is in default configuration, it will enter user EXEC mode, and the screen will display:

```
Raisecom>
```

Input the **enable** command and correct password, and press **Enter** to enter privileged EXEC mode. The default password is raisecom.

```
Raisecom>enable
Password:
Raisecom#
```

In privileged EXEC mode, input the **config** command to enter global configuration mode.

```
Raisecom#config
Raisecom(config)#
```



Note

- Command line prompt "Raisecom" is the default host name. You can use the **hostname** *string* command to modify the host name in privileged EXEC mode.
- Some commands can be used both in global configuration mode and other modes, but the accomplished functions are closely related to command line modes.
- Generally, in a command line mode, you can return to the upper command line mode by using the **quit** or **exit** command, but in the privileged EXEC mode, you need to use the **disable** command to return to user EXEC mode.
- You can use the **end** command to return to privileged EXEC mode from any command line mode except the user EXEC mode or privileged EXEC mode.

The ISCOM6800 and ISCOM6860 support the following CLI modes:

Mode	Enter method	Description
User EXEC	Log in to the ISCOM6800 or ISCOM6860, input correct username and password	Raisecom>
Privileged EXEC	In user EXEC mode, enter the enable command and correct password.	Raisecom#

Mode	Enter method	Description
Global configuration	In privileged EXEC mode, enter the config command.	Raisecom(config)#
GE interface configuration	In global configuration mode, enter the interface gigabitethernet slot-id/port-id command.	Raisecom(config-if-gigabitethernet-slot-id:port-id)#
GE interface batch configuration	In global configuration mode, enter the interface range gigabitethernet slot-id/port-list command.	Raisecom(config-if-gigabitethernet-range)#
10GE interface configuration	In global configuration mode, enter the interface ten-gigabitethernet slot-id/port-id command.	Raisecom(config-if-ten-gigabitethernet-slot-id:port-id)#
10GE interface batch configuration	In global configuration mode, enter the interface range ten-gigabitethernet slot-id/port-list command.	Raisecom(config-if-ten-gigabitethernet-range)#
Aggregation group configuration	In global configuration mode, enter the interface port-channel group-id command.	Raisecom(config-port-channel-group-id)#
VLAN interface configuration	In global configuration mode, enter the interface vlanif vlan-id command.	Raisecom(config-vlanif-num)#
VLAN configuration	In global configuration mode, enter the vlan vlan-id command.	Raisecom(config-vlan-id)#
EPON interface configuration	In global configuration mode, enter the interface epon-olt slot-id/port-id command.	Raisecom(config-if-epon-olt-slot-id:port-id)#
EPON interface batch configuration	In global configuration mode, enter the interface range epon-olt slot-id/port-list command.	Raisecom(config-if-epon-olt-range)#
10G EPON interface configuration	In global configuration mode, enter the interface ten-giga-epon-olt slot-id/port-id command.	Raisecom(config-if-ten-epon-olt-slot-id:port-id)#
10G EPON interface batch configuration	In global configuration mode, enter the interface range ten-giga-epon-olt slot-id/port-list command.	Raisecom(config-if-ten-epon-olt-range)#
GPON interface configuration	In global configuration mode, enter the interface gpon-olt slot-id/port-id command.	Raisecom(config-if-gpon-olt-slot-id:port-id)#

Mode	Enter method	Description
GPON ONU interface	In global configuration mode, use the interface gpon-onu slot-id/olt-id/onu-id command.	Raisecom(config-if-gpon-onu-slot-id/olt-id:onu-id)#
GPON interface batch configuration	In global configuration mode, enter the interface range gpon-olt slot-id/port-list command.	Raisecom(config-if-gpon-olt-range)#
Serial interface configuration	In global configuration mode, enter the interface serial slot-id/port-id command	Raisecom(config-if-serial-slot-id:port-id)#
Serial interface batch configuration	In global configuration mode, enter the interface range serial slot-id/port-id command.	Raisecom(config-if-serial-range)#
EPON ONU management configuration	In global configuration mode, enter the epon-onu slot-id/olt-id/onu-id command.	Raisecom(config-epon-onu-slot-id/olt-id:onu-id)#
EPON ONU management batch configuration	In global configuration mode, enter the epon-onu range slot-id/olt-id/onu-list command.	Raisecom(config-epon-onu-range)#
EPON ONU voice service configuration	In global configuration mode, enter the epon-onu slot-id/olt-id/onu-id voice command.	Raisecom(config-epon-onu-voice-slot-id/olt-id:onu-id)#
EPON ONU UNI configuration	In global configuration mode, enter the epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id command.	Raisecom(config-epon-onu-ethernet-slot-id/olt-id/onu-id:uni-id)#
EPON ONU UNI batch configuration	In global configuration mode, enter the epon-onu uni ethernet range slot-id/olt-id/onu-id/uni-list command.	Raisecom(config-epon-onu-ethernet-range)#
EPON ONU serial interface configuration	In global configuration mode, enter the epon-onu uni serial-com slot-id/olt-id/onu-id/uni-id command.	Raisecom(config-epon-onu-serial-slot-id/olt-id/onu-id:ser-id)#
EPON ONU serial interface batch configuration	In global configuration mode, enter the epon-onu uni serial-com range slot-id/olt-id/onu-id/uni-list command.	Raisecom(config-epon-onu-serial-range)#
EPON ONU SNI configuration	In global configuration mode, enter the epon-onu slot-id/olt-id/onu-id sni command.	Raisecom(config-epon-onu-sni-slot-id/olt-id:onu-id)#
EPON ONU TDM interface configuration	In global configuration mode, enter the epon-onu uni e1t1 slot-id/olt-id/onu-id/uni-id command.	Raisecom(config-epon-onu-e1t1-slot-id/olt-id/onu-id:uni-id)#

Mode	Enter method	Description
EPON ONU TDM interface batch configuration	epon-onu uni e1t1 range slot-id/olt-id/onu-id/uni-list	Raisecom(config-epon-onu-e1t1-range)#
EPON ONU TDM BUNDLE configuration	In global configuration mode, enter the epon-onu bundle slot-id/olt-id/onu-id/bundle-id command.	Raisecom(config-epon-onu-bundle-slot-id/olt-id/onu-id:bundle-id)#
EPON ONU TDM BUNDLE batch configuration	In global configuration mode, enter the epon-onu bundle range slot-id/olt-id/onu-id/bundle-list command.	Raisecom(config-epon-onu-bundle-range)#
EPON ONU TDM service configuration	In global configuration mode, enter the epon-onu slot-id/olt-id/onu-id tdm command.	Raisecom(config-epon-onu-tdm-slot-id/olt-id:onu-id)#
EPON ONU service profile configuration	In global configuration mode, enter the epon-onu-service-profile profile-id command.	Raisecom(config-epon-onu-service-profile:profile-id)#
L2 ACL configuration	In global configuration mode, enter the l2-access-list acl-id command.	Raisecom(config-l2-acl-acl-id)#
GPON ONU management configuration	In global configuration mode, enter the gpon-onu slot-id/olt-id/onu-id command.	Raisecom(config-gpon-onu-slot-id/olt-id:onu-id)#
GPON ONU management batch configuration	In global configuration mode, enter the gpon-onu range slot-id/olt-id/onu-list command.	Raisecom(config-gpon-onu-range)#
GPON automatic authentication rule configuration	In global configuration mode, enter the gpon-auto-authentication-rule profile-id command.	Raisecom(config-gpon-auto-auth-rule:*)#
L2 ACL configuration	In global configuration mode, enter the l2-access-list acl-id command.	Raisecom(config-l2-acl-acl-id-rule-rule-id)#
L2 ACL sub-rule configuration	In L2 ACL configuration mode, enter the rule rule-id command.	Raisecom(config-ip-acl-acl-id)#
IPv4 ACL configuration	In global configuration mode, enter the ip-access-list acl-id command.	Raisecom(config-ip-acl-acl-id-rule-rule-id)#
IPv4 ACL sub-rule configuration	In IPv4 ACL configuration mode, enter the rule rule-id command.	Raisecom(config-ipv6-acl-acl-id)#

Mode	Enter method	Description
IPv6 ACL configuration	In global configuration mode, enter the ipv6-access-list <i>acl-id</i> command.	Raisecom(config-ipv6-acl-acl-id-rule-rule-id)#
IPv6 ACL sub-rule configuration	In IPv6 ACL configuration mode, enter the rule <i>rule-id</i> command.	Raisecom(config-hybrid-acl-acl-id)#
Hybrid ACL configuration	In global configuration mode, enter the hybrid-access-list <i>acl-id</i> command.	Raisecom(config-hybrid-acl-acl-id-rule-rule-id)#
Hybrid ACL sub-rule configuration	In Hybrid ACL configuration mode, enter the rule <i>rule-id</i> command.	Raisecom(config-user-acl-acl-id)#
User ACL configuration	In global configuration mode, enter the user-access-list <i>acl-id</i> command.	Raisecom(config-user-acl-acl-id-rule-rule-id)#
User ACL sub-rule configuration	In User ACL configuration mode, enter the rule <i>rule-id</i> command.	Raisecom(config-12-acl-acl-id-rule-rule-id)#

1.1.4 Shortcut keys

The ISCOM6800 and ISCOM6860 support following shortcut keys.

Shortcut key	Description
Up Arrow (↑)	Show the previous command if there is any command entered earlier; the displayed command does not change if the current command is the earliest one in history records.
Down Arrow (↓)	Show the next command if there is any newer command. The displayed command does not change if the current command is the newest one in history records.
Left Arrow (←)	Move the cursor leftward by one character. The displayed command does not change if the cursor is already at the beginning of the command.
Right Arrow (→)	Move the cursor rightward by one character. The displayed command does not change if the cursor is already at the end of the command.
Backspace	Delete the character before the cursor. The displayed command does not change if the cursor is already at the beginning of the command.

Shortcut key	Description
Tab	Press Tab after entering a complete keyword, and the cursor will automatically appear a space to the end. Press Tab again, and the system will show the follow-up available keywords. Press Tab after entering an incomplete keyword, and the system automatically executes partial helps: ● When only one keyword matches the entered incomplete keyword, the system takes the complete keyword to replace the entered incomplete keyword and leaves one space between the cursor and end of the keyword. ● When no keyword or multiple keywords match the entered incomplete keyword, the system displays the prefix, and you can press Tab to check words circularly. In this case, there is no space from the cursor to the end of the keyword. Press Space bar to enter the next word. ● If you enter an incorrect keyword, pressing Tab will move the cursor to the next line and the system will prompt an error. In this case, the entered keyword does not change.
Ctrl+A	Move the cursor to the beginning of the command.
Ctrl+B	Identical to the Left Arrow key.
Ctrl+C	Interrupt the ongoing command, such as ping and tracert .
Ctrl+D	Return to the previous mode.
Ctrl+E	Move the cursor to the end of the command.
Ctrl+F	Identical to the Right Arrow key
Ctrl+G	Delete the entire line.
Ctrl+K	Delete all characters from the cursor to the end of the command.
Ctrl+L	Clear screen information.
Ctrl+S	Identical to the Down Arrow key
Ctrl+X	Delete all characters before the cursor (except the cursor location).
Ctrl+Y	Show history commands.
Ctrl+Z	Return to privileged EXEC mode from the current mode (except user EXEC mode).
Space bar or Y	Scroll down one screen.
Enter	Scroll down one line.

1.1.5 Display information

Display features

The CLI provides the following display features:

- The help information and prompt messages displayed at the CLI are in English.
- When messages are displayed at more than one screen, you can suspend displaying them with one of the following operations, as listed in Table 1-2.

Table 1-2 Shortcut keys about display features

Function key	Description
Press Space bar or Y	Scroll down one screen.
Press Enter	Scroll down one line.
Press any letter key (except Y)	Stop displaying and executing commands.

Filtering display information

The ISCOM6800 and ISCOM6860 support a series of commands starting with **show**, to check device configurations, operation and diagnostic information. Generally, these commands can output more information, and then user needs to add filtering rules to filter out unnecessary information.



Note

The **show** command of the ISCOM6800 and ISCOM6860 support three kinds of filtering modes:

- | **begin string**: show all lines starting from the assigned string.
- | **exclude string**: show all lines mismatching the assigned string.
- | **include string**: show all lines only matching the assigned string.

Page-break

Page-break is used to suspend displaying messages when they are displayed at more than one screen. After page-break is enabled, you can use shortcut keys listed in Table 1-2. If page-break is disabled, all messages are displayed when they are displayed at more than one screen.

Step	Command	Description
1	Raisecom# terminal page-break enable	Enable page-break. You can use the terminal page-break disable command to restore default status.  Note Page break is enabled.

1.1.6 Showing history commands

The ISCOM6800 and ISCOM6860 support checking or executing some history command by using the **history** command in any command line mode. By default, the device can save at least 5000 history commands.

You can use the **terminal history** command to configure the number of history commands that can be saved in common EXEC mode.

```
Raisecom>terminal history count
```

1.1.7 Acquiring help

Complete help

You can acquire complete help under following three conditions:

- You can enter a question mark (?) at the system prompt to display a list of commands and brief descriptions in any command line mode.

```
Raisecom>?
```

The command output is as below:

```
clear    Clear screen
enable   Turn on privileged mode command
exit     Exit current mode and down to previous mode
help     Message about help
history  Most recent history command
language Language of help message
list     List command
quit     Exit current mode and down to previous mode
terminal Configure terminal
```

- After you enter a keyword, press the **Space bar** and enter a question mark (?), all related commands and their brief descriptions are displayed if the question mark (?) matches another keyword.

```
Raisecom#clock ?
```

The command output is as below:

```
set      Set system time and date
```



```
summer-time Enable summer time
timezone Set system timezone offset
```

- After you enter a parameter, press the **Space bar** and enter a question mark (?), all related parameters and descriptions are displayed if the question mark (?) matches a parameter.

```
Raisecom(config)#interface vlanif ?
```

The command output is as below:

```
<1-4094> VLAN ID
```

Partial help

You can acquire partial help under following three conditions:

- After you enter a particular character string and a question mark (?), a list of key words that begin with the particular character string is displayed.

```
Raisecom(config)#c?
```

The command output is as below:

```
clear Clear screen
cpu CPU monitor
create Create operation
```

- After you enter a command, press **Space bar**, and enter a particular character string and a question mark (?), a list of commands that begin with a particular character string is displayed.

```
Raisecom#show c?
```

The command output is as below:

```
card Card
card-power card power information
card-temperature card temperature information
clock system date and time
command_set command set config information
```

cpu-utilization CPU utilization

- After you enter a partial command name and press **Tab**, the full form of the keyword is displayed if there is a unique match command. Otherwise, press **Tab** continuously to display different keywords and then you can select the required one.

Error message

The ISCOM6800 and ISCOM6860 print out the following error messages according to the error type when you input incorrect commands.

Error message	Description
% " * " Incomplete command.	The input command is incomplete.
% Invalid input at '^' marked.	The keyword marked with '^' is invalid or does not exist.
% Ambiguous input at '^' marked, follow keywords match it.	The keyword marked with '^' is unclear.
% " * " Unconfirmed command.	The input command is not unique.
% " * " Unknown command.	The input command does not exist.
% You Need higher priority!	You need more authority to execute the command.

1.2 Accessing device

1.2.1 Accessing through Console interface

The Console interface is the control interface for local management.



Note

- You must use the dedicated configuration cable for Raisecom devices when logging into the device through the Console interface.
- For technical specifications of the Console interface and model of the configuration cable, see *ISCOM6800 and ISCOM6860 Hardware Description*.

If you want to access the device through the Console interface, connect the Console interface and RS-232 serial interface of the PC, as shown in Figure 1-1; then run the terminal emulation program such as Windows XP Hyper Terminal program in the PC to configure communication parameters as shown in Figure 1-2, and then log in to the device.

Figure 1-1 Accessing the device through a PC connected with Console interface

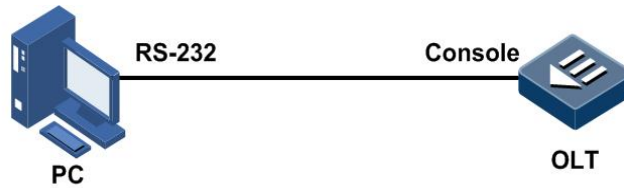
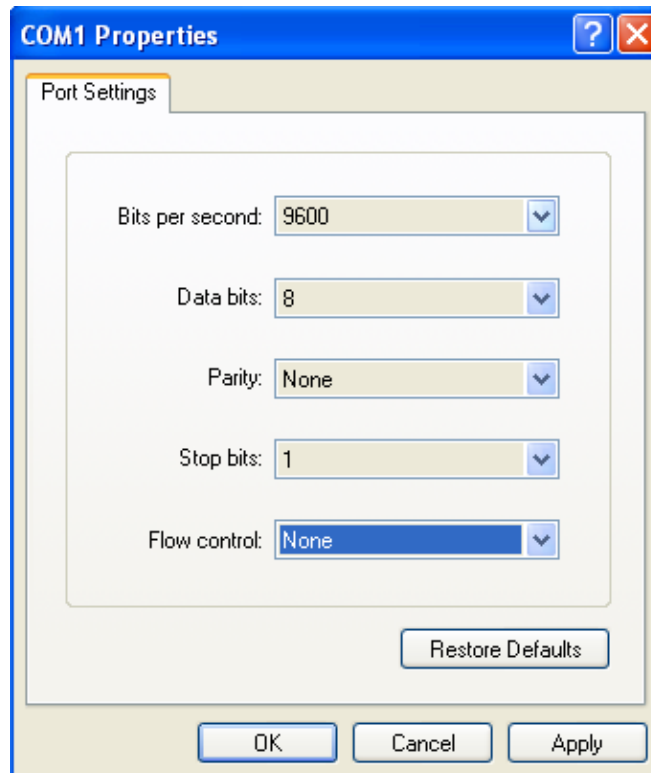


Figure 1-2 Communication parameters in Hyper Terminal



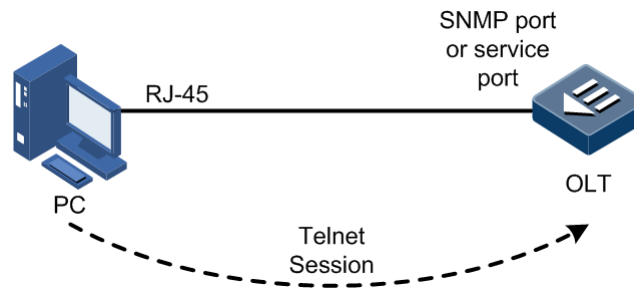
1.2.2 Accessing through Telnet

To use a PC to log in to the device remotely through Telnet, log in to a device from the PC at first, and then Telnet other ISCOM6800 and ISCOM6860 devices on the network. Thus, you do not need to connect a PC to each device. Moreover, you need to ensure that the device can ping through the PC.

The OLT provides the following Telnet services:

- **Telnet Server:** run the Telnet client program on a PC to log in to the device, and then configure and manage it. As shown in Figure 1-3, the OLT works as the Telnet server.

Figure 1-3 Networking with the OLT as the Telnet server



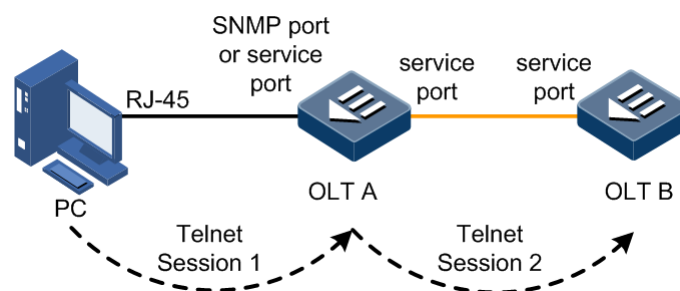
Before accessing the device through Telnet, you need to log in to the device through the Console interface and enable Telnet services. Configure the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlanif <i>vlan-id</i> example: Raisecom(config)#interface vlanif 1	Enter VLAN interface configuration mode. • <i>vlan-id</i> : VLAN interface ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlanif-num)#ip address <i>ip-address</i> [<i>ip-mask</i>] [<i>vlan-id</i>] example: Raisecom(config-vlanif-1)#ip address 10.0.0.1 255.0.0.0	Configure the IP address and mask and bind the IP address to the VLAN. The VLAN is the one in which the interface which needs to enable Telnet services is. • <i>ip-address</i> : IP address, in dotted decimal notation, such as 10.10.10.1 • <i>ip-mask</i> : IP subnet mask, in dotted decimal notation, such as 255.0.0.0 • <i>vlan-id</i> : VLAN interface ID, an integer, ranging from 1 to 4094
4	Raisecom(config-vlanif-num)#exit	Exit VLAN interface configuration mode.
5	Raisecom(config)#telnet-server accept { add remove } interface { epon-olt gigabitethernet gpon-olt ten-giga-epon-olt ten-gigabitethernet } slot-id/port-list example: Raisecom(config)#telnet-server accept add interface gigabitethernet 3/1	(Optional) add/delete the interface enabled with Telnet. By default, Telnet is enabled on all interfaces. • <i>add</i> : add an interface which can be Telneted to by the device. • <i>remove</i> : delete the interface which can be Telneted to by the device. • <i>epon-olt</i> : EPON interface ID • <i>gigabitethernet</i> : GE interface ID • <i>ten-gigabitethernet</i> : 10GE interface ID • <i>slot-id/ port-id</i> : specify the interface which allows Telnet. • <i>slot-id</i> : slot ID, an integer • <i>port-id</i> : interface ID, an integer
6	Raisecom(config)#telnet-server max-session <i>number</i> example: Raisecom(config)#telnet-server max-session 4	(Optional) configure the maximum number of Telnet sessions. • <i>max-session-num</i> : the maximum Telnet connections allowed by the device, an integer, ranging from 0 to 10

Step	Command	Description
7	<pre>Raisecom(config)#telnet-server close terminal-telnet session-number example: Raisecom(config)#telnet-server close terminal-telnet 4</pre>	(Optional) disconnect a specified Telnet session. session-num: terminal ID of Telnet connection, an integer, ranging from 0 to 4

- Telnet Client: after you log in to OLT A through the PC terminal emulation program or Telnet client program on a PC, then log in to OLT B using the **telnet** command to configure and manage it. As shown in Figure 1-4, OLT A works as the Telnet server as well as the Telnet client.

Figure 1-4 Networking with the OLT as the Telnet client



Configure the device working as the Telnet client as below.

Step	Command	Description
1	<pre>Raisecom#telnet { ipv4-address ipv6-address [scopeid string] } [port port-id] example: Raisecom#telnet 10.0.0.1 port 555</pre>	Log into other devices through Telnet. - ip-address: IP address of the remote destination device, in dotted decimal notation, such as 10.10.10.1 - port port-id: ID of the Telnet server interface provided by the remote destination device - port-id: an integer, ranging from 1 to 65535 - ipv6-address: IP address of the remote destination device, in colon hexadecimal notation, such as 3001::1 - scopeid string: Scope ID of the remote destination device

1.2.3 Accessing through SSHv2

Telnet transmits data in plaintext. The user name, password, and configurations are easy to be intercepted by other users, which brings potential security hazards. Therefore, Telnet is mainly used to manage devices inside a network.

SSHv2 is a secure data transmission protocol, which can effectively prevent disclosure of information in remote management through data encryption, and provide greater security for remote login and other network services.

Before accessing the device through SSHv2, you must log in to the device through the Console interface and enable the SSHv2 service.

Default configurations of the SSHv2 service on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
SSHv2 server status	Disable
RSA public key	N/A
SSHv2 key pair length	512 bit
Authentication mode	local user-password
SSHv2 authentication timeout	600s
Allowable times of SSHv2 authentication failure	20
SSHv2 interception interface ID	22
SSHv2 session status	Enable

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# generate ssh-key [<i>key-length</i>] example: Raisecom(config)#generate ssh-key 512	Generate local SSHv2 secret key. length: secret key length, an integer, ranging from 512 to 2048, in units of bit
3	Raisecom(config)# ssh2 server	Start the SSHv2 server. You can use the no ssh2 server command to disable SSHv2 Server.
4	Raisecom(config)# ssh2 server authentication { password rsa-key public-key } example: Raisecom(config)#ssh2 server authentication rsa-key	Configure SSHv2 authentication mode and meanwhile register Public-Key. You can use the no ssh2 server authentication command to restore default configurations. - password: authenticate the SSHv2 client by local password. - rsa-key: authenticate the SSHv2 client by RSA key. - public-key: in rsa-key authentication mode, enter the public key of SSHv2 client into the device.
5	Raisecom(config)# ssh2 server authentication-timeout <i>timeout</i> example: Raisecom(config)#ssh2 server authentication-timeout 300	(Optional) configure SSHv2 authentication timeout. When the client authentication time exceeds this limit, the device will refuse to continue authentication and disconnect. You can use the no ssh2 server authentication-timeout command to restore default configurations. second: SSHv2 authentication timeout, an integer, ranging from 100 to 65535, in units of second

Step	Command	Description
6	<pre>Raisecom(config)#ssh2 server authentication-retries count</pre> example: <pre>Raisecom(config)#ssh2 server authentication-retries 3</pre>	(Optional) configure the number of failed SSHv2 authentication attempts. When the number of client authentication failures exceeds this limit, the device will refuse to continue authentication and disconnect. counts: allowed failure attempts of SSHv2 authentication, an integer, ranging from 1 to 100
7	<pre>Raisecom(config)#ssh2 server port port-id</pre> example: <pre>Raisecom(config)#ssh2 server port 2000</pre>	Configure SSHv2 listening port number. You can use the no ssh2 server port command to restore default configurations.  Note When you configure the SSHv2 listening port number of a device, the parameters entered do not take effect immediately. Instead, they only take effect until the SSHv2 server is restarted. port-id: SSHv2 listening port number of the device, an integer, ranging from 1 to 65535
8	<pre>Raisecom(config)#ssh2 server session session-list { enable disable }</pre> example: <pre>Raisecom(config)#ssh2 server session 1,4 disable</pre>	Enable/Disable the specified SSHv2 sessions. - session-list: SSHv2 session list, an integer, ranging from 0 to 4. It supports specific values, such as "0,1,2"; it also supports a range, such as "0-2". - enable: enable SSHv2 sessions. - disable: disable SSHv2 sessions.

1.2.4 Configuring Console terminal

If the user enters the login password incorrectly more than three times, the terminal will prohibit the user from continuing the operation. In this case, the user needs to wait for a certain period of time before login again.

The device supports timeout disconnection for all user interfaces. If the user does not perform any operation within the specified time, the user will be automatically disconnected. After the timeout expires, the user needs to log in to the device through the console terminal again.

The Console terminal configuration is the basic configuration for the user to log in to the device and perform device operations. You can configure the Console terminal based on the actual condition.

Configure the device as below.

Step	Command	Description
1	Raisecom> terminal time-out { <i>period</i> disable } example: #Raisecom>terminal time-out 1000	Configure timeout exit time of the Console terminal. - period: timeout exit time, an integer, ranging from 1 to 65535, in units of second. - disable: it never times out.
2	Raisecom> enable	Enter privileged EXEC mode.
3	Raisecom# logout	Log out the device.
4	Raisecom# show terminal	Show configurations of the terminal user.

1.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show telnet-server	Show Telnet configurations.
2	Raisecom# show ssh2 server	Show the SSHv2 server.
3	Raisecom# show ssh2 session	Show SSHv2 session.
4	Raisecom# show ssh2 public-key authentication	Show the SSHv2 authentication key.
5	Raisecom# show ssh2 public-key rsa	Show the SSHv2 RSA key.
6	Raisecom# show interface vlanif [id] detail	Show configurations of the VLAN interface.

1.3 General operations

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# hostname <i>name</i> example: Raisecom(config-epon-onu-3/1:1)#hostname onu1	(Optional) configure the device name. By default, the device name is Raisecom.  Note The system supports changing the device name to facilitate users distinguishing different devices on the network. The device name takes effect immediately after it is changed, and you can see the modified name at the terminal prompt. string: ONU name, a character string. The length of the character string varies with the model of the ONU.

Step	Command	Description
2	Raisecom#language { chinese english } example: Raisecom#language chinese	(Optional) configure the system prompt language. By default, the system prompt is in English. - chinese: display CLI descriptions in Chinese. - english: display CLI descriptions in English.
3	Raisecom#write	(Optional) save configurations. After the configuration of the device is complete, you need to save the configurations to the device. The newly saved configurations will overwrite the original configurations. After the configuration is complete, if you don't save it, the new configuration will be lost after the device restarts, and the original configuration will continue.  Caution You can use the erase file-name command to delete the configuration file. The deleted file cannot be restored after the erase file-name command is executed. Use it with caution.
4	Raisecom#reboot [now]	(Optional) restart the device. When the device is faulty, you can try to solve the fault by restarting the device according to the actual situation.  Caution - Restarting the device will interrupt the service. Please be cautious. - Save the configuration as needed before restarting the device to avoid configuration loss.
5	Raisecom#reboot epon-onu all device-type <i>onu-type</i> example: Raisecom#reboot epon-onu all device-type 5104	(Optional) restart the ONU device of a specified model. device-type onu-type: ONU type. The onu-type refers to the ONU model, such as 5104.
6	Raisecom#reboot gpon-onu slot-id/olt-id/onu-id [now] example: Raisecom#reboot gpon-onu 3/1/1	(Optional) restart the specified ONU. - slot-id/olt-id/onu-id: ONU ID - slot-id: slot ID, an integer - olt-id: interface ID, an integer - onu-id: ONU ID, an integer - now: restart now.

1.4 Managing users

1.4.1 Default configurations

Default user configurations of the device are as below.

Function	Default value
Default user	• User name: raisecom • Password: raisecom • User privilege: 15 (Administrator)
New user privilege	15 (Administrator)



Note

We recommend modifying the default user name and password to prevent illegal visits from breaking down the device.

1.4.2 Creating users

Configure the device as below.

Step	Command	Description
1	Raisecom# user name <i>username</i> password <i>password</i> example: Raisecom#user name raisecom1 password raisecom1	Create a user, or modify the user name and password. • user-name: user name, a string of 1 to 16 characters • password: user login password, a string of 1 to 16 characters
2	Raisecom# password please input password: please input again:	Modify the current password.
3	Raisecom# no username <i>username</i> example: Raisecom#no username raisecom1	Delete a login user.  Caution Online users cannot be deleted. • user-name: user name, a string of 1 to 16 characters



Note

- When modifying the password, you should input the same password for two times. Otherwise, the modification fails.
- The newly created user is the administrator by default, with the user privilege of 15.

1.4.3 Managing user privileges

Configure the device as below.

Step	Command	Description
1	Raisecom#user name <i>username</i> privilege level example: Raisecom#user name raisecom1 privilege 1	Configure the user privilege. • user-name: user name, a string of 1 to 16 characters • privilege: user privilege, an integer, ranging from 1 to 15
2	Raisecom# enable password	Modify the password in privilege EXEC mode.
3	Raisecom#user login { local-radius local-user radius-local radius-user tacacs-user tacacs-local local-tacacs } example: Raisecom#user login local-radius	Configure the authentication mode for user login. • local-radius: when local authentication and RADIUS authentication coexist, use local authentication. • local-tacacs: when local authentication and TACACS+ authentication coexist, use local authentication. • local-user: use local authentication • radius-local: when local authentication and RADIUS authentication coexist, use RADIUS authentication. • radius-user: use RADIUS authentication • tacacs-local: when local authentication and TACACS+ authentication coexist, use TACACS+ authentication. • Tacacs-user: use TACACS+ authentication.
4	Raisecom#enable login { local-radius local-user radius-local radius-user tacacs-user tacacs-local local-tacacs } example: Raisecom#enable login radius-user	Configure the authentication mode for login in privilege EXEC mode. • local-radius: when local authentication and RADIUS authentication coexist, use local authentication. • local-tacacs: when local authentication and TACACS+ authentication coexist, use local authentication. • local-user: use local authentication • radius-local: when local authentication and RADIUS authentication coexist, use RADIUS authentication. • radius-user: use RADIUS authentication • tacacs-local: when local authentication and TACACS+ authentication coexist, use TACACS+ authentication. • Tacacs-user: use TACACS+ authentication.
5	Raisecom# enable auth bypass	(Optional) bypass password authentication when entering the privileged EXEC mode to user EXEC mode. Use the no enable auth bypass command to restore the default password authentication mode.

1.4.4 Refining user privileges

User privilege refining provides the concept of command set and enhances users' executive capability of commands. You can flexibly define a command set as needed by arranging commands of different levels into a set, and specifying to allow or forbid users from executing the command set. Thus, it facilitates you to manage user privileges flexibly according to actual conditions.

The system supports 10 command sets. One command set contains 50 commands. The administrator can control the command set configuration for some common users. In this case, the common users are allowed or forbidden to execute commands in the command set.



Note

User privilege refining cannot be operated on the administrator.

Configure the device as below.

Step	Command	Description
1	Raisecom#command-set <i>comsetname</i> example: Raisecom#command-set set1	Create a command set can enter command set configuration mode. You can use the no command-set <i>comsetname</i> command to delete the command set.  Note When you delete a command set, the system prompts deleting successfully if the command set does not exist; the system prompts deleting unsuccessfully if the command set is in use. • <i>cmdsetname</i>: name of the command set, a string of 1 to 16 characters
2	Raisecom(command-set:*)#command "comkeywords" example: Raisecom(command-set:abc)#command "create"	You can use the keyword to add commands to the command set. You can use the no command-set { all comnum } command to delete commands in the command set. • <i>cmdkeywords</i>:: key words of the command, separated by spaces, up to 10
3	Raisecom(command-set:*)#exit Raisecom#user <i>username</i> { allow-exeset disallow-exeset } <i>comsetname</i> example: Raisecom#user raisecom1 allow-exeset com1	Configure the command set privilege, that is, to allow or forbid some user to execute commands in the command set. You can use the no user <i>username</i> { allow-exeset disallow-exeset } <i>comsetname</i> command to delete configurations of the command set privilege. • <i>user-name</i>: user name, a string of 1 to 16 characters • <i>allow-exeset</i>: command sets which are allowed to be executed by users • <i>disallow-exeset</i>: command sets that users are forbidden to execute • <i>commandset</i>: name of the command set



Note

When using the **command** "comkeywords" command to add commands to the command set, pay attention to the following points:

- *comkeywords* refers to the keyword, which does include the parameter in the command line.
- *comkeywords* should be put between the double quotation marks ("").
- If you need to add a command only, input all keywords of the command. If you want to add commands in batch, input the shared part of the commands.

For example, when you need to add the **create vlan** *vlan-id* command to the command set, operate as below:

```
Raisecom#command-set cmd1  
Raisecom(command-set:cmd1)#command "creat vlan"
```

When you need to add commands containing the "vlan" keyword, operate as below:

```
Raisecom#command-set cmd1  
Raisecom(command-set:cmd1)#command "vlan"
```

1.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show user [detail]	Show information about login users.
2	Raisecom# show command-set	Show information about all command sets, including the name, number of commands, and user status.
3	Raisecom# show command-set detail [<i>comsetname</i>]	Show details of the command set, including the name, number of commands, detailed commands, and user status.

1.5 Managing cards

1.5.1 Default configurations

Default configurations of cards on the device are as below.

Function	Default value
Created type	• Slots 1–16 and slots 19–22 are null. • Slots 23–24 are for ISCOM6800 and ISCOM6860-power, which cannot be configured. • Slot 25 is for ISCOM6800 and ISCOM6860-fan, which cannot be configured.
Actual type	N/A
Serial number	N/A
Card status	Not-used
Card power status	off
Fan management mode	auto
Fan gear	8, namely, working at the maximum rotational speed
Maximum rotational speed	3300 r/min
Minimum rotational speed	900 r/min

1.5.2 Creating cards

The ISCOM6800 and ISCOM6860 do not support creating cards. The system defines the card status through the following two types:

- Created type: the card type specified by users using the command.
- Actual type: the card type detected by the system automatically when the card is inserted into the slot.

Only when the created type and actual type are consistent can the card work properly.



Note

Values of the card status indicate as below:

- not-used: the card is not created nor inserted into the slot.
- offline: the card is created but is not inserted into the slot.
- non-provisioned: the card is not created but is inserted into the slot.
- type-mismatched: the card is created and inserted into the slot, but the created type and actual type are inconsistent.
- version-mismatched: the card is created and inserted into the slot, and the created type and actual type are consistent, but the versions do not match.
- disable: the card is created and inserted into the slot, and the created type and actual type are consistent, but communication fails.
- loading-config: the card is created and inserted into the slot, the created type and actual type are consistent, communication runs properly, and configuration files are being loaded.
- loading-config-failed: configuration files fail to be loaded.
- inservice: configuration files are loaded successfully and the card works properly.
- Standby: the card is in standby status (this status is for MCC only).

After the card is inserted into the slot, you need to create the card in the system to configure and manage the card. When creating the card, you need to specify the slot ID and card type.

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)# create card slot slot-id type { auto cica ep12 ep16 ep1x ge16 gp16 xg16 gp8a xep8 xep8b xp2a xp4a xp4b xp4l xp4t xp8t xp12t } example: Raisecom(config)#create card slot 1 type ep16	Create a card on the device. You can use the no create card slot slot-id [now] command to delete the card. • slot-id: slot ID, an integer • cica: the type of card that can be installed is ISCOM6800-CICA • ep12: the type of card that can be installed is ISCOM6800-EP12 • ep16: the type of card that can be installed is ISCOM6800-EP16 • ep1x: the type of card that can be installed is ISCOM6800-18-FANS382 • ge16: the type of card that can be installed is ISCOM6800-GE16 • xep8: the type of card that can be installed is ISCOM6800-XEP8 • xep8b: the type of card that can be installed is ISCOM6800-XEP8 (B). • xp2a: the type of card that can be installed is ISCOM6800-XP2A • xp4a: the type of card that can be installed is ISCOM6800-XP4A • xp4l: the type of card that can be installed is ISCOM6800-XP4L • xp4t: the type of card that can be installed is ISCOM6800-XP4T • gp16: the type of card that can be installed is ISCOM6800-GP16 • gp8a: the type of card that can be installed is ISCOM6800-GP8A
3	Raisecom(config)#device description description example: Raisecom(config)#device description olt1	(Optional) configure descriptions for the device to identify different devices. You can use the no device description command to delete the descriptions. • string: description of the OLT, a character string
4	Raisecom(config)#slot slot-id description description example: Raisecom(config)#slot 3 description EP4B	(Optional) configure slot description for distinguishing different slots. You can use the no slot slot-id description command to delete the description. • slot-id: slot ID, an integer • string: description, a string of 1 to 64 characters
5	Raisecom(config)#exit Raisecom#reboot slot { slot-id all } [now] example: Raisecom#reboot slot 1	(Optional) restart the card. • slot-id: restart the card of a specified slot. It is an integer. • all: restart cards in all slots. • now: restart now.

1.5.3 Restarting cards

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# reboot { slot { <i>slot-id</i> all } { epon-onu gpon-onu } { <i>slot-id/olt-id/onu-list</i> all } } [now]	Reboot the card in a specified slot or all cards. • slot-id: restart the card in a specified slot. It is an integer. • all: restart cards in all slots. • now: restart immediately.
2	Raisecom# config	Enter global configuration mode.
3	Raisecom(config)# power { on off } slot <i>id</i> example: Raisecom(config)#power on slot 4	Turning on/off the card power. • on: turn on the power card. • off: turn off the power card. • id: slot ID, an integer, ranging from 1 to 4

1.5.4 Energy conservation of card

The cards on the ISCOM6800 and ISCOM6860 devices support power-saving features. An idle card can be powered off to reduce power consumption.



Note

You need to create a card first to perform power-saving operations based on the type of the card.

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# power { on off } slot <i>slot-id</i> example: Raisecom(config)#power on slot 4	Turn on/off the power slot and enter power-saving mode. • On: power on the power card. • off: power off the power card. • id: slot ID, an integer, ranging from 1 to 4



Note

The system enters the power-saving mode based on the service status of the card. If there is normal service running on the card, the card fails to enter the power-saving mode.

1.5.5 Card switching

The Main Control Card (MCC) of the ISCOM6800 and ISCOM6860 supports active and standby backup. When upgrading or replacing the MCC, you need to perform the active/standby switchover to switch the system and services to the standby MCC, to prevent device failure or service interruption due to MCC.

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# ha forced-switch	Forced switch of active and standby card

1.5.6 Fan management

The ISCOM6800 and ISCOM6860 support smart fans of which the gear position and rotational speed can be automatically or manually adjusted.

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# fan speed mode { auto manual } example: Raisecom(config)#fan speed mode manual	Configure the fan management mode. You can use the no fan speed mode command to restore default configurations. • auto: configure the fan control mode to automatic control. • manual: configure the fan control mode to manual control.
3	Raisecom(config)# fan speed manual <i>level</i> example: Raisecom(config)#fan speed manual 2	Configure the fan gear. You can use the no fan manual command to restore default configurations. • level: gear of the rotational speed, an integer, ranging from 1 to 8
4	Raisecom(config)# fan speed low-alarm threshold <i>threshold</i> example: Raisecom(config)#fan speed low-alarm threshold 70	Configure the fan exception threshold. • threshold: fan exception alarm threshold, an integer, ranging from 1 to 99

1.5.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show card	Show information about all cards.
2	Raisecom# show cpu-utilization slot <i>slot-list</i> [<i>dynamic</i>]	Show the CPU utilization rate of the card.
3	Raisecom# show device	Show information about the device, including the type, MAC address, serial number, and slots on the main control card.

No.	Command	Description
4	Raisecom#show version slot { <i>min_slot_start-max_solt_start</i> }	Show version information about the card in a specified slot, including card type, card hardware version, system software version, bootrom version, firmware version, and CPLD version.
5	Raisecom#show slot slot-id	Show information about the specified slot, including the type of the card supported by the slot, description of the slot, the available status of the slot, the slot ID, the actual card type of the slot, and the type of card that should be installed. It will display null if the type of card is not specified and the actual card is not in place.
6	Raisecom#show ha	Check configurations of card protection, including protection group members, status of each member, and switching information.
7	Raisecom#show ha register-module	Show resource synchronization of primary/secondary card.
8	Raisecom#show fan	Show fan status.

1.6 Managing interfaces

1.6.1 Default configurations of GE interface

Default configurations of GE interfaces on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Status	Enable
Rate and duplex mode	Auto-negotiation
Flow control	Disable
Auto-MDI/MDIX	Normal
MTU	1522 Bytes
Refresh frequency of interface dynamic statistics	2s

Default configurations of the serial interface

Default configurations of the serial interface on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Port status	Enable

Function	Default value
Port baud rate	9600 bit/s
Serial communication protocol	RS-485
Serial data digits	8bit
Serial stop bits	1bit
Check mode of serial port data	none
Operation mode of serial interface	tcp_realport
Network service interface of the serial interface	10990 + serial interface ID
Peer service interface of the serial interface	1025
Peer IP address of the serial interface	0.0.0.0
Condition of session connection initiation	always
Maximum sessions of serial interface	16

1.6.2 Enabling/Disabling interfaces

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { gigabitethernet ten- gigabitethernet epon-olt ten- giga-epon-olt gpon-olt serial } <i>slot-id/port-id</i>	Enter physical interface configuration mode. • slot-id: slot ID, an integer • olt-id: port ID, an integer
3	Raisecom(config-if-*/*)#shutdown	Disable the interface. You can use the no shutdown command to enable the interface.

1.6.3 Configuring basic properties of interfaces

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)# system mtu size example: Raisecom(config)#system mtu 6000	Configure the global MTU. You can use the no system mtu command to restore default configurations. size: maximum forwarding frame length, an integer, ranging from 1500 to 9000, in units of byte
3	Raisecom(config)# interface ten-gigabitethernet slot-id/port-id example: Raisecom(config)#interface ten-gigabitethernet 3/1	Enter 10GE interface configuration mode. - slot-id: slot ID, an integer - olt-id: interface ID, an integer
4	Raisecom(config-if-ten-gigabitethernet-*)# speed { 10000 1000 } example: Raisecom(config-if-ten-gigabitethernet-3/1)#speed 1000	Configure the interface rate. 1000: forced 1000 Mbit/s 10000: forced 1000 Mbit/s (supported by the 10GE interface only)
	Raisecom(config-if-ten-gigabitethernet-*)# description word example: Raisecom(config-if-ten-gigabitethernet-3/1)#description optical	Configure interface description. You can use the no description command to restore default configurations. name: interface description, a string of 1 to 64 characters or starting with number
5	Raisecom(config-if-ten-gigabitethernet-*)# exit	Return to global configuration mode.
6	Raisecom(config)# interface gigabitethernet slot-id/port-id example: Raisecom(config)#interface gigabitethernet 4/1	Enter GE interface configuration mode. - slot-id: slot ID, an integer - olt-id: interface ID, an integer
7	Raisecom(config-if-gigabitethernet-*)# speed { 1000 100 10 auto } example: Raisecom(config-if-gigabitethernet-4/1)#speed 100	Configure the interface rate. - auto: auto-negotiation 100: forced 100 Mbit/s 1000: forced 1000 Mbit/s
	Raisecom(config-if-gigabitethernet-*)# description word example: Raisecom(config-if-gigabitethernet-4/1)#description optical	Configure interface description. You can use the no description command to restore default configurations. name: interface description, a string of 1 to 64 characters or starting with number

1.6.4 Configuring interface statistics

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)# dynamic statistics time period example: Raisecom(config)#dynamic statistics time 10	Configure the interval of dynamic statistics on the interface. You can use the no dynamic statistics time command to restore default configurations. period: period, an integer, ranging from 1 to 300, in units of second
3	Raisecom(config)# clear interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet serial } slot-id/port-id statistics example: Raisecom(config)#clear interface epon-olt 3/1 statistics	Clear interface statistics. - epon-olt slot-id/port-list: clear statistics on the specified EPON interface. - gpon-olt slot-id/port-list: clear statistics on the specified GPON interface. - ten-giga-epon-olt slot-id/port-list: clear statistics on the 10G EPON interface. - gigabitethernet slot-id/port-list: clear statistics on the specified GE interface. - serial slot-id/port-list: clear statistics on the specified serial interface. - ten-gigabitethernet slot-id/port-list: clear statistics on the specified 10GE interface.

1.6.5 Configuring flow control on interfaces

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface { gigabitethernet ten-gigabitethernet } slot-id/port-id example: Raisecom(config)#interface gigabitethernet 3/1	Enter physical interface configuration mode. - slot-id: slot ID, an integer - olt-id: interface ID, an integer
3	Raisecom(config-if- *:*)#flowcontrol { receive send } example: Raisecom(config-if-gigabitethernet-3/1)#flowcontrol send	Configure flow control on the interface. You can use the no flowcontrol { receive send } command to restore default configurations. - receive: flow control over traffic in the receiving direction - send: flow control over traffic in the sending direction

1.6.6 Configuring VLAN interface

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)# interface vlanif <i>vlan-id</i> example: Raisecom(config)#interface vlanif 1	Enter VLAN interface configuration mode. • vlan-id : VLAN ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlanif-num)# ip address <i>ip-address</i> [<i>ip-mask</i>] [<i>vlan-id</i>] example: Raisecom(config-vlanif-2)#ip address 10.10.10.1	(Optional) configure the IP address of the VLAN interface. You can use the no ip address ip-address command to delete the configuration. • ip-address : primary IP address of the VLAN interface, in dotted decimal notation, such as 10.0.0.1 • mask : subnet mask, in dotted decimal notation, such as 255.0.0.0 • vlan-id : VLAN ID, an integer, ranging from 1 to 4094
	Raisecom(config-vlanif-num)# ipv6 address <i>ipv6-address/prefix-length</i> [<i>eui-64</i>] [<i>link-local</i>] example: Raisecom(config-vlanif-2)#ipv6 address 1030:0::48AA:1A2B/60	(Optional) configure the IPv6 address of the VLAN interface. You can use the no ipv6 address ipv6-address command to delete the configuration. • ipv6-address/prefix-length : IPv6 address with the mask length, such as A:B::C:D/M • eui-64 : use the eui-64 as the interface ID
4	Raisecom(config-vlanif-*)# description <i>word</i> example: Raisecom(config-vlanif-2)#description optical	Configure interface description. You can use the no description command to restore to default values. • name : interface description, a string of 1 to 64 characters, starting with a letter or number



Note

The VLAN IP address cannot be in the same network segment as the IP address of the out-of-band management interface (SNMP).

1.6.7 Configuring out-of-band network management interface

The SNMP interface on the MCC is used for out-of-band network management.

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# management-port ip address <i>ip-address</i> [<i>mask</i>] example: Raisecom(config)#management-port ip address 10.0.0.1	Configure the IPv4 address for the out-of-band management interface. • ip-address : IP address, in dotted decimal notation, such as 10.10.10.1 • ip-mask : IP mask, in dotted decimal notation, such as 255.255.255.0

Step	Command	Description
	<pre>Raisecom(config)#management-port ipv6 address ip-address [link-local]</pre> example: <pre>Raisecom(config)#management-port ipv6 address 3001::1</pre>	Configure the IPv6 address for the out-of-band management interface. • ipv6-address: IP address of the remote destination device, in colon hexadecimal notation, such as 3001::1



Note

- The IP address of the out-of-band management interface is 192.168.1.100.
- The IP address of the out-of-band management interface cannot be in the same network segment as that of the VLAN interface.

1.6.8 Configuring serial interface

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#serial-com max- session-num number</pre> example: <pre>Raisecom(config)#serial-com max- session-num 20</pre>	Configure the maximum sessions of the serial interface. • number: maximum sessions allowed by the serial interface, an integer, ranging from 4 to 64
3	<pre>Raisecom(config)#interface serial slot-id/port-id</pre> example: <pre>Raisecom(config)#interface serial 9/1</pre>	Enter serial interface configuration mode. • slot-id: slot ID, an integer • port -id: interface ID, an integer
4	<pre>Raisecom(config-serial- */*)#serial-protocol { rs232 rs485 }</pre> example: <pre>Raisecom(config-serial- 9:1)#serial-protocol rs232</pre>	Configure the serial communication protocol of the serial interface. • rs232: configure the serial interface communication protocol to RS232. • rs485: configure the serial interface communication protocol to RS485.

Step	Command	Description
5	Raisecom(config-serial-*/*)#baud-rate { 300 1200 2400 4800 9600 14400 19200 28800 38400 57600 115200 } example: Raisecom(config-serial-9:1)#baud-rate 1200	Configure the baud rate of the serial interface. • 300: the baud rate of the serial interface is 300 bit/s. • 1200: the baud rate of the serial interface is 1200 bit/s. • 2400: the baud rate of the serial interface is 2400 bit/s. • 4800: the baud rate of the serial interface is 4800 bit/s. • 9600: the baud rate of the serial interface is 9600 bit/s. • 14400: the baud rate of the serial interface is 14400 bit/s. • 19200: the baud rate of the serial interface is 19200 bit/s. • 28800: the baud rate of the serial interface is 28800 bit/s. • 38400: the baud rate of the serial interface is 38400 bit/s. • 57600: the baud rate of the serial interface is 57600 bit/s. • 115200: the baud rate of the serial interface is 115200 bit/s.
6	Raisecom(config-serial-*/*)#data-bits <i>bits</i> example: Raisecom(config-serial-9:1)#data-bits 6	Configure the data bit of the serial interface. • bits: data bits of the serial interface, an integer, ranging from 5 to 8
7	Raisecom(config-serial-*/*)#stop-bits { bit1 bit1dot5 bit2 } example: Raisecom(config-serial-9:1)#stop-bits 2	Configure the stop bit of the serial interface data. • bits: stop bit of the serial interface, with the value of: • 1 • 1.5 • 2
8	Raisecom(config-serial-*/*)#parity { none odd even mark space } example: Raisecom(config-serial-9:1)#parity odd	Configure the check mode of the serial interface data. • none: no checking • odd: odd check • even: even check • mark: mark mode • space: space mode
9	Raisecom(config-serial-*/*)#loopback <i>slot-id/port-id</i> example: Raisecom(config-serial-9:1)#loopback 1/2	Configure loopback on the serial interface. • slot-id/com-id: ID of the serial interface which loops back to the current serial interface, an integer. The slot-id is the slot ID. The com-id is the serial interface ID. The value of the com-id is 1.
10	Raisecom(config-serial-*/*)#work-mode { tcp-realport tcp-client tcp-server udp } example: Raisecom(config-serial-9:1)#work-mode tcp-client	Configure the operation mode of the serial interface. • tcp-realport: TCP realport mode • tcp-client: TCP client mode • tcp-server: TCP server mode • udp: UDP mode
11	Raisecom(config-serial-*/*)#service-port <i>port-id</i> example: Raisecom(config-serial-9:1)#service-port 5000	Configure the service interface of the serial interface network. • port-id: service interface, an integer, ranging from 1025 to 65535

Step	Command	Description
12	Raisecom(config-serial-*/*)# peer service-port <i>port-id</i> example: Raisecom(config-serial-1:1)#peer service-port 4000	Configure the peer network service interface. • com-id: serial interface, an integer, ranging from 1025 to 65535
13	Raisecom(config-serial-*/*)# peer ip-address <i>ip-address</i> example: Raisecom(config-serial-1:1)#peer ip-address 10.10.10.25	Configure the IP address of the serial interface. • ip-address: peer device IP address of serial interface communication, in dotted decimal notation, such as 10.10.10.1
14	Raisecom(config-serial-*/*)# connect-condition { always char } example: Raisecom(config-serial-1:1)#connect-condition char	Configure the condition for the serial interface to initiate session. • always: the serial interface server, after being powered on, initiates a connection immediately and will re-initiate a connection immediately after being disconnected. • char: the serial interface server, after receiving data, will initiate a connection immediately.
15	Raisecom(config-serial-*/*)# session-write-right { first all } example: Raisecom(config-serial-1:1)#session-write-right all	Configure the write right of the serial interface session. • first: the session established first has the write right. • all: all sessions have write rights.

1.6.9 Switching interface services

When the source interface fails, you can transfer all configurations on the specified source interface to the destination interface. When services in the links under the source interface are switched to the destination interface, all services continue to run normally.

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# running-config from interface gigabitethernet slot-id/port-id to interface gigabitethernet slot-id/port-id [clear source] example: Raisecom(config)#running-config from interface gigabitethernet 1/1 to interface gigabitethernet 1/2	Switch services on the GE interface. • gigabitethernet: 1000 Mbit/s Ethernet interface • slot-id/olt-id/onu-id: ONU ID • slot-id: slot ID, an integer • olt-id: PON interface ID, an integer

Step	Command	Description
	Raisecom(config)#running-config from interface ten-gigabitethernet slot-id/port-id to interface ten-gigabitethernet slot-id/port-id [clear source] example: Raisecom(config)#running-config from interface ten-gigabitethernet 2/1 to interface ten-gigabitethernet 2/2	Switch services on the 10GE interface. • ten-gigabitethernet: 10 Gbit/s Ethernet interface • ten-giga-epon-olt: 10G EPON interface • port-channel: link aggregation group interface • slot-id: slot ID, an integer • olt-id: PON interface ID, an integer
	Raisecom(config)#running-config from interface epon-olt slot-id/port-id to interface epon-olt slot-id/port-id [clear source] example: Raisecom(config)#running-config from interface epon-olt 3/1 to interface epon-olt 3/2	Switch services on the EPON interface. • epon-olt: EPON interface • slot-id: slot ID, an integer • olt-id: PON interface ID, an integer
	Raisecom(config)#running-config from interface ten-giga-epon-olt slot-id/port-id to interface ten-giga-epon-olt slot-id/port-id [clear source] example: Raisecom(config)#running-config from interface ten-giga-epon-olt 4/1 to interface ten-giga-epon-olt 4/2	Switch services on the 10GEPON interface. • ten-giga-epon-olt: 10G EPON interface • slot-id: slot ID, an integer • olt-id: PON interface ID, an integer
	Raisecom(config)#running-config from interface gpon-olt slot-id/port-id to interface gpon-olt slot-id/port-id [clear source] example: Raisecom(config)#running-config from interface gpon-olt 5/1 to interface gpon-olt 5/2	Switch services on the GPON interface. • gpon-olt: EPON interface • slot-id: slot ID, an integer • olt-id: PON interface ID, an integer
	Raisecom(config)#running-config from port-channel group-id to port-channel group-id [clear source] example: Raisecom(config)#running-config from port-channel 1 to port-channel 2	Switch services on the link aggregation group interface. • port-channel: link aggregation group interface • group-id: aggregation group ID, an integer, ranging from 1 to 32



Note

- When enabling interface service switching, pay attention to the following matters:
- Types of the source and destination interfaces should be consistent and cannot be the same one.
 - The source and destination interfaces cannot belong to any interface backup group, uplink interface protection group, or PON protection group.
 - When you switch services on the EPON interface, no online ONU should exist under the destination PON interface.

1.6.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id	Show interface configurations, including interface status, rate, duplex mode, and forwarding mode.
2	Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id description	Show interface description.
3	Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id statistics	Show interface statistics.
4	Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id flowcontrol	Show flow control information about the interface.
5	Raisecom#show system mtu	Show the maximum length of forwarding frame.
6	Raisecom#show management-port { ip-address ipv6-address }	Show IP configurations of the out-of-band network management interface.
7	Raisecom#show { ip ipv6 } interface brief	Show IP configurations of the IP interface.
8	Raisecom#show interface vlanif statistics	Show basic information about the VLAN interface.
9	Raisecom#show interface serial slot-id/port-list	Show basic parameters of the serial interface.
10	Raisecom#show interface serial slot-id/port-list service	Show parameter information about the serial interface.
11	Raisecom#show interface serial slot-id/port-list statistics	Show statistics on the serial interface.
12	Raisecom#show interface serial slot-id/port-list session information [current history]	Show sessions of the serial interface.
13	Raisecom#show interface serial slot-id/port-list session statistics [current history]	Show session statistics on the serial interface.
14	Raisecom#show serial slot-id/port-list heartbeat statistics	Show heartbeat statistics on the serial interface.
15	Raisecom#show serial-com	Show global configurations of the serial interface.

1.6.11 Maintenance

You can use the following commands to maintain the running and configuration of the port management feature.

No.	Command	Description
1	<pre>Raisecom#clear interface { epon-olt slot-id/port-list gpon-olt slot-id/port-list ten-giga-epon-olt slot-id/port-list gigabitethernet slot-id/port-list ip statistics serial slot-id/port-list ten-gigabitethernet slot-id/port-list port-channel group-id vlanif vlan-id } statistics</pre> example: Raisecom(config)#clear interface epon-olt 3/1 statistics	Clear interface statistics. • epon-olt slot-id/ port-id: EPON interface ID • gpon-olt slot-id/ port-id: GPON interface ID • gigabitethernet slot-id/ port-id: 1000 Mbit/s Ethernet interface ID • ten-gigabitethernet slot-id/ port-id: 10 Gbit/s Ethernet interface ID • ten-giga-epon-olt slot-id/port-id: 10GE PON interface ID • port-channel group-id: aggregation group interface ID. • group-id: aggregation group interface ID • vlan-id: VLAN ID, an integer, ranging from 1 to 4094

1.7 Managing time

1.7.1 Default configurations

Default configurations of time management on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Default time	2000-01-01 08:00:00.000
Default clock mode	System clock
Default time zone offset	+08:00
Default DST	Disable
IP address of NTP server	0.0.0.0
IP address of NTP symmetric peer	0.0.0.0
NTP mode	Slave
SNTP Client	Disable
IP address of SNTP server	224.0.1.1

1.7.2 Configuring time and time zone

Configuring time

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom#clock set hour minute second year month day example: Raisecom#clock set 8 0 0 2011 1 1	Configure the system time, including hour, minute, second, year, month, and day. • hour: hour, an integer, ranging from 0 to 23 • minute: minute, an integer, ranging from 0 to 59 • second: second, an integer, ranging from 0 to 59 • year: year an integer, ranging from 2000 to 2099 • month: month, an integer, ranging from 1 to 12 • day: day, an integer, ranging from 1 to 31

Configuring time zone

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom#clock timezone { + - } <i>hour minute</i> example: Raisecom#clock timezone -5 40	Configure the time zone. You can use the clock timezone command to restore default configurations. • +: east hemisphere time zone • -: west hemisphere time zone • hour: time zone offset hour, an integer, ranging from 0 to 11 • minute: time zone offset minute, an integer, ranging from 0 to 59

1.7.3 Configuring DST

DST (DST) is a local time regulation for saving energy. At present, there are nearly 110 countries using DST every summer around the world, but different countries have different stipulations for DST. Thus, you should consider the local conditions when configuring DST.

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom#clock summer-time	Enable DST. You can use the no clock summer-time command to disable DST.

Step	Command	Description
2	<pre>Raisecom#clock summer-time recurring { week last } { fri mon sat sun thu tue wed } { month month } hour minute { week last } { fri mon sat sun thu tue wed } { month month } hour minute offset-minutes example: Raisecom#clock summer-time recurring 2 sun 4 2 0 2 sun 9 2 0 60</pre>	Configure the calculating period of DST. You can use the no clock summer-time recurring command to restore default configurations. • week: the nth week in which the DST starts, an integer, ranging from 1 to 4 • last: DST starts in the last week of the month • sun: DST starts on Sunday of the week • mon: DST starts on Monday of the week • tue: DST starts on Tuesday of the week • wed: DST starts on Wednesday of the week • thu: DST starts on Thursday of the week • fri: DST starts on Friday of the week • sat: DST starts on Saturday of the week • month-number: DST starting month, an integer, ranging from 1 to 12 • month-word: DST starting month, English full spelling format • hour: DST starting hour, an integer, ranging from 0 to 24 • minute: DST starting minute, an integer, ranging from 0 to 59 • shift: DST offset, an integer, ranging from 1 to 1440, in units of minute



Note

- When you configure the system time manually, if the system uses DST, such as DST from 2 A.M. on the second Sunday, April to 2 a.m. on the second Sunday, September every year, you have to adjust the clock one hour forward during this period, that is, set the time offset as 60min. So the period from 2 a.m. to 3 a.m. on the second Sunday, April each year is inexistent. Configuring time manually in this period will fail.
- The DST in southern hemisphere is opposite to the northern hemisphere, which is from September to April next year. If the start time is later than end time, the system will suppose that it is in the southern hemisphere. That is to say, the DST is the period from the start time this year to the end time next year.

1.7.4 Configuring NTP

Network Time Protocol (NTP) is a time synchronization protocol defined by RFC1305, used to synchronize time between distributed time servers and clients. NTP transportation is based on UDP, using port 123.

The purpose of NTP is to synchronize all clocks in a network quickly and then the device can provide different applications over a unified time. Meanwhile, NTP can ensure very high accuracy, with accuracy of 10ms around.

The device in support of NTP cannot only accept synchronization from other clock source, but also synchronize other devices as a clock source.

The device adopts multiple NTP working modes for time synchronization:

- Server mode

In this mode, the device works as the NTP server. The client sends the clock synchronization request packet to the NTP server. The server sends a response after receiving the request. Then the client performs clock synchronization after receiving the response packet.

- Client mode

In this mode, the device works as the NTP client. You should specify the IP address of the NTP server for the client to realize clock synchronization.

- Symmetric peer mode

In this mode, the symmetric active peer sends the clock synchronization packet to the symmetric passive peer. The symmetric passive peer works in passive mode automatically after receiving the packet, and sends the response packet. The symmetric active peer and symmetric passive peer in this mode can synchronize with each other.

By default, the IP address of the NTP server is not configured. If the version is not configured when you configure the NTP server, the version No. is 3.

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ntp server { ip-address ipv6-address } [version version-number] example: Raisecom(config)#ntp server 10.0.0.1	(Optional) configure the IP address of the NTP server. You can use the no ntp server { ip-address ipv6-address } command to restore default configurations. • ip-address: IP address of the remote server, in dotted decimal notation, such as 10.10.10.1 • ipv6-address: IPv6 address of the remote peer, in colon hexadecimal notation, such as 3001::1 • version version-number: NTP version • version-number: v1/v2/v3. The NTP version is V3 by default.
3	Raisecom(config)#ntp peer { ip-address ipv6-address } [version version-number] example: Raisecom(config)#ntp peer 10.0.0.1	(Optional) configure the IP address of the NTP symmetric peer. You can use the no ntp peer { ip-address ipv6-address } command to restore default configurations. • ip-address: IP address of the remote server, in dotted decimal notation, such as 10.10.10.1 • ipv6-address: IPv6 address of the remote peer, in colon hexadecimal notation, such as 3001::1 • version version-number: NTP version • version-number: v1/v2/v3. The NTP version is V3 by default.
4	Raisecom(config)#ntp refclock-master [stratum] example: Raisecom(config)#ntp refclock-master	(Optional) configure the local clock as the NTP reference clock source. You can use the no ntp refclock-master command to delete the configuration. stratum: stratum in which the device is located in the tree NTP topology, an integer, ranging from 2 to 15, the smaller the stratum is, the mode precise the clock is. If you do not choose this parameter, it is 8 by default.



Note

If the device is configured as the NTP reference clock source, it cannot be configured as the NTP server or NTP symmetric peer; and vice versa.

1.7.5 Configuring SNTP

Simple Network Time Protocol (SNTP) is used to synchronize the system time with the time of the SNTP server. You can specify the IP address of the SNTP server on the device to synchronize its system time with the SNTP server, thus implementing time synchronization on the whole network. The ISCOM6800 and ISCOM6860 can act as SNTP clients only.

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#sntp-client	Enable SNTP Client. You can use the no sntp client command to disable this function.
3	Raisecom(config)#sntp-client server { ip-address ipv6-address } example: Raisecom(config)#sntp-client server 224.0.1.10	Configure the IP address of the SNTP client. You can use the no sntp-client server command to restore default configurations. - ip-address: IPv4 address of the SNTP server, in dotted decimal notation, such as 10.10.10.1 - ipv6-address: IPv6 address of the SNTP server, in colon hexadecimal notation, such as 3001::1



Note

SNTP and NTP are mutually exclusive. Therefore, they cannot be used at the same time.

1.7.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show ntp status	Show the NTP status.
2	Raisecom#show ntp associations	Show information about the NTP connection.
3	Raisecom#show clock	Show configurations of the system time and time zone.
4	Raisecom#show sntp-client	Show configurations of the SNTP client.

1.8 Upgrade and backup

1.8.1 Introduction

The device supports two system extended boot files and two system startup files, and provides 1:1 backup and protection for system files. Thus, it decreases faults and service interruption caused by corrupted system files and system upgrade.

- When loading of the system file fails, the system will automatically switch to load the backup file. You can troubleshoot the primary file after starting the system using the backup file.
- When upgrading the system file, you can upgrade the backup file first, and switch the system to the backup file, and then upgrade the primary file. In this way, you can decrease the service interruption caused by system upgrade.
- When upgrading the system file, you can upgrade the primary file and back up the original system file. When the network fails due to the upgrade, you can switch to the original file immediately to ensure the normal service.

1.8.2 Configuring server

The device supports upgrade and backup through the FTP/TFTP/SFTP server.

Before upgrading system software through FTP/TFTP/SFTP, you should build a FTP/TFTP/SFTP environment. Basic requirements are as below:

- The device is connected to the FTP/TFTP/SFTP server correctly.
- Configure the FTP/TFTP/SFTP server and ensure the server can be accessed.
- Configure related parameters of the FTP/TFTP/SFTP server on the device to enable it to access the FTP/TFTP/SFTP server.

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# ftp ip-address username password example: Raisecom#ftp 10.10.10.1 name pwd	Configure the IPv4 parameters of the FTP. • ip-address: IP address of the destination host, in dotted decimal notation, such as 10.10.10.1 • username: FTP-connected user name, a string of 1 to 40 characters • password: FTP-connected password, a string of 1 to 40 characters
2	Raisecom# ftp ipv6-address [scopeid scopeid-id] username password example: Raisecom#ftp 3001::1 name pwd	Configure the IPv6 parameters of the FTP. • username: FTP-connected user name, a string of 1 to 40 characters • password: FTP-connected password, a string of 1 to 40 characters • ipv6-address: IP address of the destination host, in colon hexadecimal notation, such as 3001::1/64 • scopeid scope-id: specified scope ID
3	Raisecom# tftp ip-address example: Raisecom#tftp 10.10.10.1	Configure the IPv4 parameters of the TFTP. • ip-address: IP address of the destination host, in dotted decimal notation, such as 10.10.10.1

Step	Command	Description
4	Raisecom# tftp ipv6-address [scopeid scopeid-id] example: Raisecom#tftp 3001::1/64	Configure the IPv6 parameters of the TFTP. • ipv6-address: IP address of the destination host, in colon hexadecimal notation, such as 3001::1/64 • scopeid scope-id: specified scope ID
5	Raisecom# sftp ip-address username password example: Raisecom#sftp 10.10.10.1 name pwd	Configure SFTP IPv4 parameters. • ip-address: destination host IP address, in dotted decimal notation, such as 10.10.10.1 • username: SFTP-connected user name, a string of 1 to 40 characters
6	Raisecom# sftp ipv6-address [scopeid scopeid-id] username password example: Raisecom#sftp 3001::1 name pwd	Configure SFTP IPv6 parameters. • username: SFTP-connected user name, a string of 1 to 40 characters • password: SFTP-connected password, a string of 1 to 40 characters • ipv6-address: destination host IP address, in colon hexadecimal notation, such as 3001::1/64 • scopeid scope-id: specified Scope ID

1.8.3 Upgrading OLT system files

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# download { mainrom1 mainrom2 cp1d system1 system2 oemfile } { ftp {ip-address ipv6-address [scopeid string] } sftp {ip-address ipv6-address [scopeid string] } username password filename slot slot-id Raisecom# download { system1 system2 } { ftp {ip-address ipv6-address [scopeid string] } sftp {ip-address ipv6-address [scopeid string] } username password filename slot slot-list card-type { ep12 ep16 ep1x ge16 gp16 gp8a xep8 xep8b xg16 } Raisecom# download startup-config { ftp {ip-address ipv6-address [scopeid string] } sftp {ip-address ipv6-address [scopeid string] } username password filename slot slot-id	(Optional) upgrade the system bootfile, system startup file, system CPLD file, or OEM file through FTP or SFTP.

Step	Command	Description
2	<pre>Raisecom#download { mainrom1 mainrom2 cpld system1 system2 oemfile } tftp { ip-address ipv6-address [scopeid string] } filename slot slot- id Raisecom#download { system1 system2 } tftp { ip-address ipv6-address [scopeid string] } filename slot slot- list card-type { ep12 ep16 ep1x ge16 gp16 gp8a xep8 xep8b xg16 } Raisecom#download startup-config tftp { ip-address ipv6-address [scopeid string] } filename slot slot-id</pre>	(Optional) upgrade the system boot file, startup file, system CPLD file, or OEM file through TFTP.
3	<pre>Raisecom#download license { ftp { ip- address ipv6-address [scopeid string] username password filename [schedule-list list-number] tftp { ip-address ipv6-address [scopeid string] filename sftp { ip-address ipv6-address [scopeid string] username password filename }</pre>	(Optional) upgrade the license file through TFTP, FTP, or SFTP.
4	<pre>Raisecom#download patch { ftp { ip- address ipv6-address [scopeid string] sftp { ip-address ipv6- address [scopeid string] } username password filename [schedule-list list- number] tftp { ip-address ipv6- address [scopeid string] } filename [schedule-list list-number] }</pre>	(Optional) upgrade the patch file through TFTP, FTP, or SFTP.
5	<pre>Raisecom#commit { mainrom1 mainrom2 system1 system1 system2 } slot slot-id example: Raisecom#commit mainrom1</pre>	Specify the version of the software to be loaded.  Note After specifying the version, you need to reboot the device to switch to the specified version. • mainrom1: system extension boot file 1 • mainrom2: system extension boot file 2 • system1: system boot file 1 • system2: system boot file 2
6	Raisecom#write startup-config	Save current configurations.
7	Raisecom#erase startup-config	(Optional) clear current system configurations.  Caution This command will clear the configuration file in the system and cause service interruption. Please use it with caution.

1.8.4 Backing up OLT system files

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# upload { startup-config oemfile } { ftp { <i>ip-address</i> <i>ipv6-address</i> [<i>scopeid string</i>] } <i>username password filename</i> sftp { <i>ip-address</i> <i>ipv6-address</i> [<i>scopeid string</i>] } <i>username password filename</i> tftp { <i>ip-address</i> <i>ipv6-address</i> [<i>scopeid string</i>] } <i>filename</i> } slot slot	(Optional) back up the system file through FTP/SFTP/TFTP.
2	Raisecom# upload history-cmd { ftp { <i>ip-address</i> <i>ipv6-address</i> [<i>scopeid string</i>] sftp { <i>ip-address</i> <i>ipv6-address</i> [<i>scopeid string</i>] } <i>username password filename</i>	(Optional) back up the history operation file through FTP/SFTP.
3	Raisecom# upload { patch license } { ftp { <i>ip-address</i> <i>ipv6-address</i> [<i>scopeid string</i>] <i>username password filename</i>	(Optional) back up the license file through FTP/TFTP/SFTP.

1.8.5 Upgrading EPON ONU system file

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# download startup-config { ftp <i>ip-address username password filename</i> tftp <i>ip-address filename</i> } epon-onu slot-id/olt-id/onu-id Raisecom# download startup-config [ftp <i>ipv6-address</i> [<i>scopeid scopeid</i>] <i>username password</i> tftp <i>ipv6-address</i> [<i>scopeid scopeid</i>]] <i>filename</i> epon-onu slot-id/olt-id/onu-id Raisecom# download system1 { ftp <i>ip-address username password filename</i> tftp <i>ip-address filename</i> } epon-onu { slot slot-id / all } device-type type-name [version hardversion] [commit] Raisecom# download system1 { ftp <i>ip-address username password filename</i> tftp <i>ip-address filename</i> } epon-onu slot-id/olt-id/onu-id [device-type type-name [version hardversion] [commit]] Raisecom# download system1 { ftp <i>ipv6-address</i> [<i>scopeid scopeid</i>] <i>username password filename</i> tftp <i>ipv6-address</i> [<i>scopeid scopeid</i>] <i>filename</i> } epon-onu { slot slot-id / all } device-type type-name [version hardversion] [commit] Raisecom# download system1 { ftp <i>ipv6-address</i> [<i>scopeid scopeid</i>] <i>username password filename</i> tftp <i>ipv6-address</i> [<i>scopeid scopeid</i>] <i>filename</i> } epon-onu slot-id/olt-id/onu-id [device-type type-name [version hardversion] [commit]]	(Optional) upgrade EPON ONU system files through FTP/TFTP.

1.8.6 Upgrading GPON ONU system file

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	<pre>Raisecom#download { system1 system2 } { ftp { ip-address ipv6-address [scopeid scopeid] } username password filename tftp { ip-address ipv6-address [scopeid scopeid] } filename sftp { ip-address ipv6-address [scopeid scopeid] } username password filename } gpon-onu { slot slot-list / all / port slot-id/olt-id } device-type type-name [[hardware hardware] [auto-commit] [schedule-list list-number]] Raisecom#download { system1 system2 } { ftp { ip-address ipv6-address [scopeid scopeid] } username password filename tftp { ip-address ipv6-address [scopeid scopeid] } filename sftp { ip-address ipv6-address [scopeid scopeid] } username password filename } gpon-onu slot-id/olt-id/onu-list [device-type type-name [hardware hardware]] [auto-commit] [schedule-list list-number]</pre>	(Optional) upgrade the GPON ONU system file through FTP/TFTP/SFTP.

1.8.7 Managing ONU configuration file

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	<pre>Raisecom(config-epon-onu- *//*/*:*)#download startup- config { ftp ip-address username password filename tftp ip-address filename } epon-onu slot-id/olt-id/onu-id example: Raisecom(config-epon-onu- 2/1/1:1)#download startup- config tftp 10.0.0.1 iscom6800-roap_2.1.5_20121212 epon-onu 2/1/1</pre>	(Optional) download ONU configuration data storage files through FTP/TFTP. • tftp ip-address: IP address of the TFTP server, in dotted decimal notation, such as 10.10.10.1 • ftp ip-address: IP address of the FTP server, in dotted decimal notation, such as 10.10.10.1 • sftp ip-address: IP address of the SFTP server, in dotted decimal notation, such as 10.10.10.1 • ipv6-address: IPv6 address, in colon hexadecimal notation, such as 3001::1/64 • user-name: user name of the FTP server • password: password of the FTP server • file-name: downloaded file name • gpon-onu slot-id/olt-id/onu-id: download the file to the ONU, that is, to upgrade the ONU. slot-id/olt-id/onu-id: ONU ID; slot-id: slot ID; olt-id: PON interface ID; onu-id: ONU ID of the PON interface
2	<pre>Raisecom(config-epon-onu- *//*/*:*)#restore startup-config</pre>	(Optional) restore the ONU to the factory configuration.
3	<pre>Raisecom(config-epon-onu- *//*/*:*)#reload startup-config</pre>	(Optional) reload the configuration files of the ONU.

Step	Command	Description
4	Raisecom(config-epon-onu- */*/*:*)# write	Save the configuration files of the ONU.

1.8.8 Configuring auto-save

The ISCOM6800 and ISCOM6860 support the auto-save feature. This feature can avoid loss of system configurations due to human carelessness, such as forgetting to save the configuration.

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# auto-write { enable disable }	Enable/Disable the auto-save feature.
3	Raisecom(config)# auto-write time time example: Raisecom(config)#auto-write time 5	(Optional) configure the time for auto-save. time: time for automatically saving configurations, an integer, ranging from 0 to 23, in units of hour

1.8.9 Smart upgrade of ONU

Smart upgrade of the ONU allows users to configure a specified type of ONU to automatically download files that need to be upgraded from a specified FTP/TFTP server at a specified time and complete the batch upgrade. It is convenient for users to manage and maintain the ONU in batches.

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# auto-upgrade { enable disable }	Enable/Disable smart upgrade of the ONU.
3	Raisecom(config)# auto-upgrade time start-time example: Raisecom(config)#auto-upgrade time 5	Configure the start time for executing smart upgrade. You can use the no auto-upgrade time command to restore the default value. time: start time, an integer, ranging from 2 to 5 (24-hour system, namely, from 2 am to 5 am), in units of hour

Step	Command	Description
4	Raisecom(config)#auto-upgrade add device-type onu-type { ftp ip-address username password filename tftp ip-address filename } example: Raisecom(config)#auto-upgrade add device-type 5104 tftp 10.0.0.1 version1	Add a smart upgrade plan (based on FTP/TFTP). • type-name: ONU type, such as 5104 • tftp ip-address: IP address of the TFTP server, in dotted decimal notation, such as 10.10.10.1 • ftp ip-address: IP address of the FTP server, in dotted decimal notation, such as 10.10.10.1 • username: login name of the FTP server • password: password of the FTP server • filename: name of the file to be upgraded
	Raisecom(config)#auto-upgrade delete device-type onu-type example: Raisecom(config)#auto-upgrade delete device-type 5104	(Optional) delete a smart upgrade plan. • onu-type: ONU type, a character string, such as 5104
5	Raisecom(config)#auto-upgrade device-type { type-name now all } example: Raisecom(config)#auto-upgrade device-type 5104 now	Perform smart upgrade for a specified ONU or all ONUs. • type-name: ONU type, such as 5104 • now: start smart upgrade now. • all: smart upgrade all ONUs now.

1.8.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show { ftp tftp sftp }	Show configuration parameters of the FTP, TFTP, and SFTP.
2	Raisecom#show startup-config	Show configurations loaded when the device starts.
3	Raisecom#show running-config	Show current configurations of the device.
4	Raisecom#show version [detail-information all]	Show the system version.
4	Raisecom#show version epon-onu slot slot- list Raisecom#show version epon-onu slot- id/olt-id/onu-list Raisecom#show version epon-onu epon-olt slot-id/olt-list Raisecom#show version epon-onu ten-giga- epon-olt slot-id/olt-list	Show the version in the specified slot or of a single device.

No.	Command	Description
5	Raisecom# show version gpon-onu [<i>slot-id/olt-id/onu-list</i>] Raisecom# show version gpon-onu slot <i>slot-list</i> Raisecom# show version gpon-onu gpon-olt <i>slot-id/olt-list</i> Raisecom# show version gpon-onu xgspon-olt <i>slot-id/olt-list</i>	Show the version in the specified slot or of a single device.
6	Raisecom# show auto-write	Show auto-save time.
7	Raisecom# show auto-upgrade information	Show configurations and running status of smart upgrade.

1.9 Task scheduling

1.9.1 Introduction

When you need to use some commands periodically or at a specified time, configure task scheduling.

The ISCOM6800 and ISCOM6860 support implementing task scheduling by combining a schedule list with command lines. You just need to specify the start time, interval, and end time of the task in the schedule list, and then bind the schedule list to command lines to realize the periodic execution of command lines.

1.9.2 Default configurations

N/A

1.9.3 Configuring task scheduling

Configure the ISCOM6800 and ISCOM6860 as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#schedule-list <i>number</i> start { up-time <i>days time</i> [every <i>days time</i> [stop <i>days time</i>]] date-time <i>date time</i> [every { day week <i>days time</i> } [stop <i>date time</i>]] }</pre> example: <pre>Raisecom(config)#schedule-list 1 start <i>date-time</i> 01-01-2011 01:00:00 every <i>day</i> stop 01-01-2012 01:00:00</pre>	Add or modify the task scheduling plan, including the start time, end time, and scheduling period. You can use the no schedule-list list-number command to delete the plan. • list-number: schedule ID, an integer, ranging from 0 to 99 • start: scheduling start time. Start executing certain command • stop: scheduling end time. Stop scheduling certain command • date-time: absolute time. Start or end scheduling when the system time is the same as the configured time. • up-time: relative time. Start counting after the system starts up. After the configured time period, the system starts scheduling or ends scheduling. • mm-dd-yyyy: date of absolute time point, month-day-year. For example, the input mode of January 2, 2011 is 01-02-2011. • hh:mm:ss: date of absolute time point, hour-minute-second. For example, the input mode of 23:00 o'clock 1 minute and 10 seconds is 23:01:10. • days-after-startup: relative time period, an integer, ranging from 0 to 365, in units of day. It indicates the period after which the system starts or ends scheduling. • every: executing period, namely, the scheduling interval • day: perform scheduling every day. • week: perform scheduling every week. • days-interval: interval days, an integer, ranging from 0 to 365 • time-interval: interval, in form of hh:mm:ss • command: delete the specified schedule in the scheduling list. That is, perform scheduling when there is no command. If the parameter is not selected, the entire scheduling list will be deleted. • command-number: command ID, an integer, ranging from 0 to 99 • all: delete information about all schedules in the schedule list.
3	<pre>Raisecom(config)#<i>command-string</i> schedule-list <i>number</i></pre> example: <pre>Raisecom(config)#ip dhcp relay schedule-list 1</pre>	Add commands to the schedule list. You can use the no schedule-list number command cmd-number command to delete commands in the schedule list. • command-string: configuration command • number: schedule ID, an integer, ranging from 0 to 99

1.9.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show schedule-list	Show configurations of the schedule list.

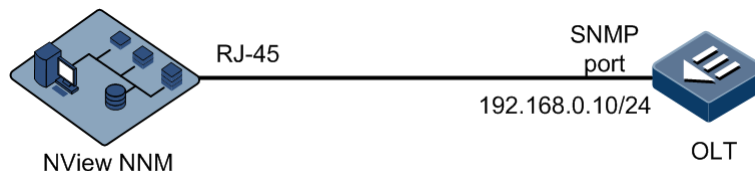
1.10 Configuration examples

1.10.1 Example for configuring out-of-band network management

Networking requirements

As shown in Figure 1-5, the NView NNM system manages the OLT through out-of-band network management. The IP address of the out-of-band management interface is 192.168.0.10.

Figure 1-5 Configuring out-of-band network management



Configuration steps

Configure the IP address of the out-of-band management interface.

```
Raisecom#config
Raisecom(config)#management-port ip address 192.168.0.10 255.255.255.0
```

Checking results

Show the IP address of the out-of-band management interface.

```
Raisecom#show management-port ip-address
Prifix IF    Address      NetMask      Source      Catagory
-----
OB      0      192.168.0.10  255.255.255.0  assigned   primary
```

1.10.2 Example for configuring in-band network management

Networking requirements

As shown in Figure 1-6, the NView NNM system manages the OLT through in-band network management. The IP address of the VLAN interface is 192.168.0.1. The mask is 255.255.255.0. The VLAN ID is 2.

Figure 1-6 Configuring in-band network management



Configuration steps

Step 1 Create a VLAN and configure properties of the interface.

```

Raisecom#config
Raisecom(config)#create vlan 2 active
Raisecom(config)#interface ten-gigabitethernet 10/1
Raisecom(config-if-ten-gigabitethernet-10:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-10:1)#switchport trunk allowed
vlan 2
Raisecom(config-if-ten-gigabitethernet-10:1)#exit
  
```

Step 2 Configure the IP address of the VLAN interface and associate it with the VLAN ID.

```

Raisecom(config)#interface vlanif 2
Raisecom(config- vlanif-2)#ip address 192.168.0.1 255.255.255.0 2
  
```

Checking results

Show the IP address of the VLAN interface.

```

Raisecom#show interface vlanif
VRF          IF          Address      NetMask
-----
Default-IP-Routing-Table vlan2      192.168.0.1 255.255.255.0
  
```

1.10.3 Configuring NTP

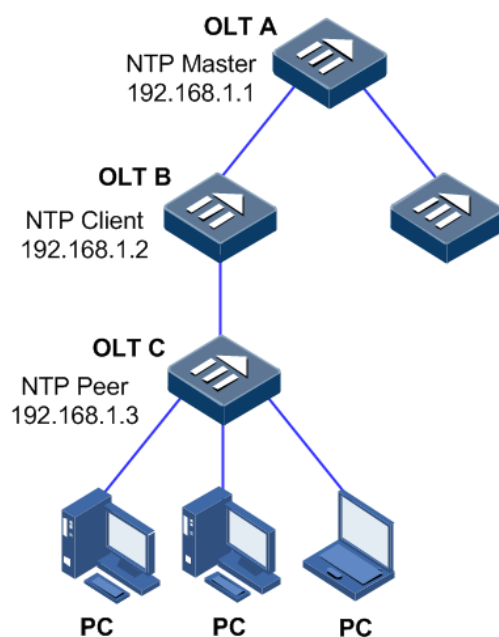
Networking requirements

A company needs to build a stable clock synchronization system to keep the company's internal device consistent and accurate. The basic plan is:

- OLT A serves as the master clock source of the clock synchronization system.
- OLT B serves as the client of the clock synchronization system, and you need to configure the upper OLT A as the NTP server.

- Configure OLT C as the NTP peer of OLT B to receive the downstream synchronous data stream sent by OLT B.

Figure 1-1 NTP networking



Configuration steps

Step 1 Configure OLT A.

```
Raisecom#config
Raisecom(config)#ntp refclock-master
```

Step 2 Configure OLT B.

```
Raisecom#config
Raisecom(config)#ntp server 192.168.1.1
Raisecom(config)#ntp peer 192.168.1.3
```

Checking results

- Check OLT A.

Use the **show ntp state** command to check whether configurations of OLT A are correct.

```
Raisecom#show ntp status
Clock status :      synchronized
```

```

NTP peer :      0.0.0.0
NTP version :   3
NTP mode :      ntpMaster
Leap :          0
Poll :          6
Stratum :       8
Precision :     2**-16
Reference clock : 127.127.1.0
Reference time : 00000000.00000000(Thu 1970-01-01,08:00:00)
Current clock :  5333d6de.33428f00(Thu 2014-03-27,15:45:44.070)
Root delay :    0.000000
Root dispersion : 0.000000

```

- Check OLT B.

Use the **show ntp status** command to check whether configurations of OLT B are correct.

```

Raisecom#show ntp status
Clock status :      synchronized
NTP peer :          192.168.1.3
NTP version :       3
NTP mode :          ntpSlave
Leap :              0
Poll :              6
Stratum :           9
Precision :         2**-16
Reference clock :   192.168.1.1
Reference time :    5333d671.383980f6(Thu 2014-03-27,15:44:58.466)
Current clock :     5333d697.0a917f54(Thu 2014-03-27,15:45:58.765)
Root delay :        0.000000
Root dispersion :   0.010004

```

Use the **show ntp associations** command to check NTP sessions of OLT B.

```

Raisecom#show ntp associations
Server(ip)      refid      stratum poll when      delay
offset          dispersion  mode reach
-----
(s)192.168.1.1  127.127.1.0    8      6    55      0.000000    -
1.965874      14.875517     4      255
Peer(ip)        refid      stratum poll when      delay
offset          dispersion  mode reach
-----
(u)192.168.1.3  0.0.0.0        16     6    125     0.000000
0.000000      16.000000     0      0

```

- Check OLT C.

Use the **show ntp status** command to check whether OLT C configurations are correct.

```
Raisecom#show ntp status
Clock status :    synchronized
NTP peer :       192.168.1.2
NTP version :    3
NTP mode :       ntpSlave
Leap :           0
Poll :           6
Stratum :        10
Precision :      2**-22
Reference clock : 192.168.1.2
Reference time :  4d62a905.00000000(Mon 2011-02-22,02:03:49)
Current clock :   5333dd97.00000000(Thu 2014-03-27,16:13:11)
Root delay :      4.154726
Root dispersion : 14.034068
```

Use the **show ntp associations** command to check NTP sessions of OLT C.

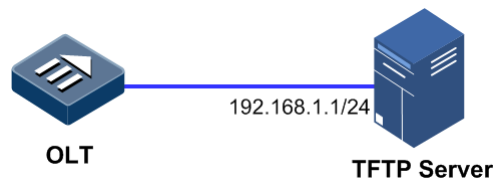
```
Raisecom#show ntp associations
Active(IP)      refid      stratum poll  when      delay      offset
dispersion      mode reach
-----
(s)192.168.1.2  192.168.1.1      9        6      97596571   4.154726
13447.112484   0.000930         1        6
```

1.10.4 Example for upgrading OLT through TFTP

Networking requirements

As shown in Figure 1-2, the TFTP server is connected to the OLT. Configure the system startup file to upgrade the OLT as system1. The IP address of the TFTP server is 192.168.1.1. The system file to be upgraded is ISCOM6800-SMCA_ROAP_2.61.1(a)_20160817.

Figure 1-2 Upgrading OLT through TFTP



Configuration steps

Step 1 Download the system startup file through TFTP.

- Step 2 Use the **download system1 tftp 192.168.1.1 ISCOM6800-SMCA_ROAP_2.61.1(a)_20160817** command to restart the device and the device will automatically load the downloaded system startup file.

Raisecom#**reboot**

Checking results

Show OLT versions.

```
Raisecom#show version
Product Name      : ISCOM6800
Product Version   : P300R003C00
ROAP Version      : 1.3
System MAC Address: 000e.5e00.1101

Slot ID: 2
Card Type         : ISCOM6800-SMCA
System1 Version   : ISCOM6800-SMCA_ROAP_2.61.1(a)_20160817
System2 Version   : ISCOM6800-SMCA_ROAP_2.61.1(a)_20160817(active)(committed)
Mainrom1 Version  : ISCOM6800-SMCA_FLASH_MAINROM_2.0.5_20140801(active)(committed)
Mainrom2 Version  : --
Bootrom Version   : ISCOM6800-SMCA_FLASH_BOOTROM_2.0.3_20120928
Hardware Version  : A.02
CPLD Version      : V1.1
Serial number     : 000000001038B14A27B0027P
System Uptime     : 0 days, 17 hours, 2 minutes
```

1.10.5 Smart upgrade of ONU

Networking requirements

As shown in Figure 1-3, smart upgrade of the ONU enables remote upgrade of ONU according to the configuration. The requirements are shown below:

- IP address of TFTP server: 192.168.1.1/24
- Type of ONU needed to be upgraded intelligently: ISCOM5304
- Time of smart upgrade: 2 o'clock a.m.
- Name of the file to be upgraded intelligently: startup_config

Figure 1-3 Networking of smart upgrade of ONU



Configuration steps

Step 1 Configure the IP address of TFTP server and add one smart upgrade configuration plan.

```
Raisecom#config
Raisecom(config)#auto-upgrade add device-type 5304 tftp 192.168.1.1
startup_config
```

Step 2 Configure the execution starting time of smart upgrade to 2 a.m.

```
Raisecom(config)#auto-upgrade time 2
```

Step 3 Enable smart upgrade.

```
Raisecom(config)#auto-upgrade enable
```

Checking results

Show configurations and running status of smart upgrade.

```
Raisecom#show auto-upgrade information
Auto-upgrade : enable
Execution time everyday: 2:00AM
```

1.10.6 Example for refining user privileges

Networking requirements

To refining user privileges, create a common set cmd1, which contains the level 15 command, **create vlan** *vlan-id*. Create a level 10 user, user 1; and allow the user to execute commands in cmd1.

Configuration steps

Step 1 Create a command set cmd1 and add related commands to the command set.

```
Raisecom#command-set cmd1  
Raisecom(command-set:cmd1)#command "create vlan"  
Raisecom(command-set:cmd1)#exit
```

Step 2 Create user1 and specify the user privilege to 10.

```
Raisecom#user name user1 password 123  
Raisecom#user name user1 privilege 10
```

Step 3 Configure the privilege of user1 in cmd1.

```
Raisecom#user user1 allow-exeset cmd1
```

Checking results

Show details of user1.

```
Raisecom#show user detail  
Username: raisecom  
Priority: 15  
Server: Local  
Userstatus: online  
  
Username: user1  
Priority: 10  
Server: Local  
Userstatus: offline  
User command control config:  
Type   Command set name  
-----  
allow  cmd1
```

2 Configuring EPON services



Note

This chapter describes the GEPON and 10GEPON services and configuration procedures (hereafter referred to as configuring EPON services) of the ISCOM6800 and ISCOM6860 devices.

This chapter contains the following information:

- Registration and deregistration
- Configuring EPON interface
- Configuring service template
- Configuring voice template
- Configuring rate-limit template
- Configuring ONU IP address pool
- Rebinding the ONU
- Configuring data encryption
- Configuring FEC
- Configuration examples

2.1 Registration and deregistration

2.1.1 Default configuration

Default configuration of EPON services:

Function	Default value
ONU registration mode	MAC (authentication mode based on MAC address)

2.1.2 Registratering ONU

Step	Configuration	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { epon-olt ten-giga-epon-olt } slot-id/olt-id example: Raisecom(config)#interface epon-olt 2/1	Enter EPON interface configuration mode. • epon-olt: EPON interface • ten-giga-epon-olt: 10G EPON interface • slot-id/port-id: distributed interface ID

Step	Configuration	Description
3	<pre>Raisecom(config-if-*-olt- *:*)#authorization mode { hybrid mac none password loid loid-password } example: Raisecom(config-if-epon-olt- 2:1)#authorization mode mac</pre>	Configure the registration mode of the ONU.  Note None mode refers to the automatic registration mode of the ONU. In none mode, you can register the ONU by merely connecting it to the PON interface on the OLT through a physical line. • hybrid: hybrid authentication mode, the ONUs that join the PON can be flexibly configured as one of the MAC, SN, PASSWORD, and PASSWORD+SN authentication modes as needed. The system automatically compares the ONU authentication mode with the local authorization record. If they match, registration can be successful, otherwise registration fails. • none: automatic authentication mode, which means that the ONU can be automatically registered • mac: MAC authentication mode. For the ONU added to the OLT, the MAC address must be in the MAC address table authorized by the OLT so that the ONU registration can be successfully, otherwise the registration will fail. • password: password authentication mode. For the ONU added to the OLT, the local Password must be in the password list authorized by the OLT so that the ONU registration can be successfully, otherwise the registration will fail. • loid: LOID authentication mode. For the ONU added to the OLT, the local LOID must be in the LOID list authorized by the OLT so that the ONU registration can be successfully, otherwise the registration will fail. • loid-password: LOID+Password authentication mode. For the ONU added to the OLT, the local LOID and password must fully match the LOID and password authorized by the OLT so that the ONU registration can be successfully, otherwise the registration will fail.

Step	Configuration	Description
4	Raisecom(config-if-*olt-*:*)#create epon-onu [<i>onu-id</i>] mac <i>mac-address</i> [device-type <i>type-name</i>] [suspend] [description <i>name</i>] [auto] example: Raisecom(config-if-epon-olt-2:1)#create epon-onu 1 password raisecom device-type 5204	(Optional) create an ONU which is to be registered based on MAC address.  Note The mac <i>mac-address</i> field in the command refers to the PON MAC of the ONU. • <i>onu-id</i>: ONU ID, an integer • mac <i>mac-address</i>: creating an ONU based on MAC authentication, in dotted hexadecimal notation, such as 000E.5E12.3456 • device-type <i>type-name</i>: ONU type, a character string, such as 5104 • suspend: suspending the ONU • description: configure the description of the ONU, in form of a character string, usually describing the ONU installation location
	Raisecom(config-if-*olt-*:*)#create epon-onu [<i>onu-id</i>] loid <i>snstring</i> [device-type <i>type-name</i>] [suspend] [description <i>name</i>] example: Raisecom(config-if-epon-olt-2:1)#create epon-onu 1 loid abc device-type 5104	(Optional) create an ONU which is to be registered based on SN. • <i>onu-id</i>: ONU ID, an integer • loid <i>snstring</i>: create an ONU based on LOID authentication which is a character string. • device-type <i>type-name</i>: ONU type, a character string, such as 5104 • suspend: suspending the ONU • description: configure the description of the ONU, in form of a character string, usually describing the ONU installation location
	Raisecom(config-if-*olt-*:*)#create epon-onu [<i>onu-id</i>] password <i>password</i> [device-type <i>type-name</i>] [suspend] [description <i>name</i>] example: Raisecom(config-if-epon-olt-2:1)#create epon-onu 1 password 1234 device-type type-name 5104	(Optional) create an ONU which is to be registered based on password.  Note For configuration mode of the ONU registration password, see section 2.1.3 Configuring ONU registration authentication password. • <i>onu-id</i>: ONU ID, an integer • password <i>password</i>: creating an ONU based on password authentication which is a character string • device-type <i>type-name</i>: ONU type, a character string, such as 5104 • suspend: suspending the ONU • description: configure the description of the ONU, in form of a character string, usually describing the ONU installation location

Step	Configuration	Description
	<pre>Raisecom(config-if-*olt-*:*)#create epon-onu [onu-id] loid string password password [device-type type-name] [suspend] [description name]</pre> example: <pre>Raisecom(config-if-epon-olt-2:1)#create epon-onu 1 loid abc password 123 device-type 5104</pre>	(Optional) create an ONU which is to be registered based on SN. • onu-id: ONU ID, an integer • loid string: create an ONU based on LOID authentication which is a character string. • password password: creating an ONU based on password authentication which is a character string • device-type type-name: ONU type, a character string, such as 5104 • suspend: suspending the ONU • description description: configure the description of the ONU, in form of a character string, usually describing the ONU installation location
5	<pre>Raisecom(config-if-epon-onu-*/*:*)#creation-type automatic-to-manual</pre>	Change the creation type of the ONU from automatic system creation to manual creation by the user.

2.1.3 Configuring ONU registration authentication password

Step	Configuration	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#interface epon-onu slot-id/olt-id/onu-id</pre> example: <pre>Raisecom(config)#interface epon-onu 3/1/1</pre>	Enter EPON ONU virtual interface configuration mode. • epon-olt: EPON interface • slot-id/port-id: distributed interface ID
3	<pre>Raisecom(config-if-epon-onu-*/*:*)#password password</pre> example: <pre>Raisecom(config-if-epon-onu-3/1:1)#password 123</pre>	Configure the registration authentication password of the ONU. • password: password, a string of 1 to 12 characters

2.1.4 Deregistering ONU

You can re-register the ONU after deregistering it, which is typically used for engineering maintenance. When you expect that the logical link of an ONU is working abnormally, you can try to recover the ONU by deregistering it.

Configure the ISCOM6800 and ISCOM6860 as below:

Step	Configuration	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.

Step	Configuration	Description
2	<code>Raisecom(config)#interface epon-onu slot-id/olt-id/onu-id</code>	Enter EPON ONU virtual interface configuration mode.
3	<code>Raisecom(config-if-*onu-*/*:*)#deregister</code>	Deregister the ONU.

2.1.5 Activating ONU

Step	Configuration	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#activate epon-onu all</code>	(Optional) activate all ONUs.
3	<code>Raisecom(config)#interface epon-onu slot-id/olt-id/onu-id</code> example: <code>Raisecom(config)#interface epon-onu 3/1/1</code>	Enter EPON ONU virtual interface configuration mode. • epon-olt: EPON interface • slot-id/port-id: distributed interface ID
4	<code>Raisecom(config-if-epon-onu-*/*:*)#state { active suspend }</code> example: <code>Raisecom(config-if-gpon-onu-3/1:1)#state active</code>	Configure the ONU status (active/suspend). • active: activate the ONU. • suspend: suspend the ONU.

2.1.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show interface epon-onu creation-information</code>	Show information about the created ONU, including creation type, ONU type, and ONU status.
2	<code>Raisecom#show epon-onu information</code>	Show information about all ONUs in the system.
3	<code>Raisecom#show interface epon-onu duplicate creation-information</code>	Show information about the created OUNs with duplicated MAC addresses on different PON interfaces.
4	<code>Raisecom#show interface epon-onu mac msc-address creation-information</code>	Retrieve ONU creation information by MAC address.
5	<code>Raisecom#show interface epon-onu slot-id/olt-id/onu-id online-information</code>	Show ONU online information.
6	<code>Raisecom#show interface epon-onu offline [logout-date before mm-dd-yyyy hh:mm:ss]</code>	Show information about offline ONUs.
7	<code>Raisecom#show interface { epon-olt ten-giga-epon-olt } slot-id/olt-id illegal-onu</code>	Show information about ONUs which are registered illegally on the EPON interface.

No.	Command	Description
8	Raisecom#show epon-onu [slot-id/olt-id] device statistics	Count the number of ONUs by information, such as status/type.

2.2 Configuring EPON interface

2.2.1 Default configuration

Function	Default value
Data encryption mode	Tri-churning
Data encryption function	Disable
Data encryption direction	Downstream
Maximum round trip time	14000TQ (1 TQ = 16 ns)

2.2.2 Configuring interface

Step	Configuration	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface epon-olt slot-id/olt-id example: Raisecom(config)#interface epon-olt 3/	Enter EPON interface configuration mode. • epon-olt: EPON interface • ten-giga-epon-olt: 10G EPON interface • slot-id/port-id: distributed interface ID
3	Raisecom(config-if-*olt-*:*)#reset	(Optional) reset the EPON interface.  Note When the device fails, you can use this command to reset the interface to resume services.

2.2.3 Configuring data encryption

Step	Configuration	Description
1	Raisecom#config	Enter global configuration mode.

Step	Configuration	Description
2	<pre>Raisecom(config)#encryption slot <i>slot-id</i> triple-churning { key-response-timeout <i>time</i> key-update-period <i>period</i> } example: Raisecom(config)#encryption slot 3 triple- churning key-response-timeout 100</pre>	(Optional) configure parameters of the triple churning key, including key request response timeout and key renewal period. - slot-id: slot ID, an integer - time: secret key request timeout time, an integer, ranging from 10 to 2550, in units of second - period: secret key renewal period, an integer, ranging from 1 to 255, in units of second
3	<pre>Raisecom(config)#interface { epon-olt ten- giga-epon-olt } <i>slot-id/olt-id</i> example: Raisecom(config)#interface epon-olt 3/1</pre>	Enter EPON interface configuration mode. - epon-olt: EPON interface - ten-giga-epon-olt: 10G EPON interface - slot-id/port-id: distributed interface ID
4	<pre>Raisecom(config-if-<i>*-olt-*.*)#encryption mode</i></pre> <pre>{ aes-128 triple-churning } example: Raisecom(config-if-epon-olt-3:1)#encryption mode triple-churning</pre>	Configure data encryption mode. - aes-128: AES-128 encryption mode - triple-churning: triple churning encryption mode



Note

- Currently, it only supports triple churning mode. The AES-128 mode can be configured but will not take effect.
- Currently, data encryption can be only performed in the downlink direction.

2.2.4 Configuring the maximum round-trip time

Step	Configuration	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#interface { epon-olt ten- giga-epon-olt } <i>slot-id/olt-id</i> example: Raisecom(config)#interface epon-olt 3/1</pre>	Enter EPON interface configuration mode. - epon-olt: EPON interface - ten-giga-epon-olt: 10G EPON interface - slot-id/port-id: distributed interface ID
3	<pre>Raisecom(config-if-<i>*-olt-*.*)#rtt max <i>rtt</i> example: Raisecom(config-if-epon-olt-3:1)#rtt max 20000</i></pre>	Configure the maximum round-trip time. You can use the no rtt max command to restore default configurations. time: maximum round-trip time, an integer, ranging from 100 to 32767, in units of TQ, 1TQ=16ns



Note

The default maximum round trip time corresponds to a fiber distance of approximately 21km. We don't recommend modifying the maximum round trip time.

2.2.5 Checking configuration

Step	Configuration	Description
1	<code>Raisecom#show interface { epon-olt ten-giga-epon-olt } [slot-id/olt-list] information</code>	Show configurations of the EPON interface.
2	<code>Raisecom#show interface { epon-olt ten-giga-epon-olt } slot-id/olt-id firmware</code>	Show information about the firmware on the EPON interface.
3	<code>Raisecom#show slot slot-id encryption triple-churning timer</code>	Show the update response timeout of triple churning encryption key and key update interval.

2.3 Configuring service template

2.3.1 Default configuration

N/A

2.3.2 Creating a template and configure it

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#epon-onu-service-profile profile-id</code> example: <code>Raisecom(config)#epon-onu-service-profile 1</code>	Enter service profile configuration mode. If the template exists, the system will directly enter template configuration mode, otherwise it creates a template before entering template configuration mode. • profile-id: EPON service template, an integer, ranging from 1 to 128
3	<code>Raisecom(config-epon-onu-service-profile:*)#name name</code> example: <code>Raisecom(config-epon-onu-service-profile:1)#name template</code>	(Optional) configure the service template name. • name: template name, a string of 1 to 16 characters
4	<code>Raisecom(config-epon-onu-service-profile:*)#ip igmp immediate-leave</code>	(Optional) configure ONU IGMP immediate leave.

Step	Command	Description
5	Raisecom(config-epon-onu-service-profile:*) #ip igmp mode { ctrl-multicast proxy snooping transparent } example: Raisecom(config-epon-onu-3/1:1)#ip igmp mode ctrl-multicast	(Optional) configure ONU IGMP mode. - ctrl-multicast: controllable multicast mode - proxy: IGMP Proxy mode - snooping: IGMP Snooping mode - transparent: transparent transmission mode
6	Raisecom(config-epon-onu-service-profile:*) #ip igmp vlan-aware { enable disable }	(Optional) configure ONU IGMP to be VLAN-aware when forwarding multicast services.
7	Raisecom(config-epon-onu-service-profile:*) #mac-address-table aging-time aging-time example: Raisecom(config-gpon-onu-service-profile:10)#mac-address-table aging-time 100	(Optional) configure the aging time of the ONU MAC address table. aging-time: aging time of the ONU MAC address table, ranging from 10 to 1000000, in units of second
8	Raisecom(config-epon-onu-service-profile:*) #mng-mode { snmp oam } example: Raisecom(config-if-epon-onu-3/1:1)#mng-mode oam	(Optional) configure the ONU management mode. - oam: use OAM mode. - snmp: use SNMP mode.
9	Raisecom(config-epon-onu-service-profile:*) #storm-control multicast { enable disable }	(Optional) configure ONU multicast storm control.
10	Raisecom(config-epon-onu-service-profile:*) #uni-eth-num sensitive { enable disable }	(Optional) enable the unity attribute of the service template.  Note - When the unity attribute of the ONU service template is enabled, the number of interfaces on the template must be the same as the number of the ONU interfaces bound. At this time, the configuration of each interface on the ONU corresponds to that of each interface of the template. - When the unity attribute of the ONU service template is disabled, the number of interfaces on the template can be different from the number of the ONU interfaces bound. At this time, the configuration of each interface on the ONU adopts the configuration of the first interface of the template.
11	Raisecom(config-epon-onu-service-profile:*) #uplink rate-limit rate example: Raisecom(config-epon-onu-service-profile:1)#uplink rate-limit 100	(Optional) configure the rate-limit rate of the ONU uplink interface. rate: rate-limiting rate on the ONU uplink interface, ranging from 0 to 1023, in units of Mbit/s

Step	Command	Description
12	<pre>Raisecom(config-epon-onu-service-profile: *)#uni ethernet uni-list loopback- detection down-time { infinite time } example: Raisecom(config-epon-onu-service- profile:1)#uni ethernet 1 loopback- detection down-time 100</pre>	(Optional) configure the shutdown time of the ONU UNI loop interface. • uni-list: ONU UNI list, an integer, with the value decided by the ONU type • infinite: infinitely shut down the loop interface. • time: shutdown time of the loop interface, an integer, ranging from 0 to 65534, in units of second; the value 0 indicates that the interface is not shut down.
13	<pre>Raisecom(config-epon-onu-service-profile: *)#uni ethernet uni-list mac-address-table threshold { unlimited number } example: Raisecom(config-epon-onu-service- profile:1)#uni ethernet 1 mac-address-table threshold 100</pre>	(Optional) configure the maximum number of MAC address tables on the ONU UNI. • uni-list: ONU UNI list, an integer, with the value decided by the ONU type • unlimited: the MAC address table of the ONU UNI is unlimited. • number: maximum size of the MAC address table of the ONU UNI, ranging from 0 to 128
14	<pre>Raisecom(config-epon-onu-service-profile: *)#uni ethernet uni-list multicast vlan vlan-id example: Raisecom(config-epon-onu-service- profile:1)#uni ethernet 1 multicast vlan 2- 5</pre>	(Optional) configure the multicast VLAN ID of the ONU UNI. You can use the no uni ethernet uni-list multicast vlan command to delete the multicast VLAN. • uni-list: ONU UNI list, an integer with the value decided by the ONU type • vlan-list: VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
15	<pre>Raisecom(config-epon-onu-service-profile: *)#uni ethernet uni-list multicast vlan tag-strip { enable disable } example: Raisecom(config-epon-onu-service- profile:1)#uni ethernet 8 multicast vlan tag-strip enable</pre>	(Optional) enable the Ethernet interface to remove the VLAN Tag of multicast service packets. You can use the uni ethernet multicast vlan tag-strip disable command to disable this function. • uni-list: ONU UNI list, an integer with the value decided by the ONU type • enable: enable the interface to remove the multicast VLAN tag. • disable: disable the interface from removing the multicast VLAN tag.
16	<pre>Raisecom(config-epon-onu-service-profile: *)#uni ethernet uni-list native vlan vlan- id example: Raisecom(config-gpon-onu-service- profile:10)#uni ethernet 1-4 native vlan 5</pre>	(Optional) configure the default VLAN ID of the ONU UNI. • uni-list: ONU UNI list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • vlan vlan-id: VLAN ID, an integer, ranging from 1 to 4094

Step	Command	Description
17	<pre>Raisecom(config-epon-onu-service-profile: *)#uni ethernet uni-list policing { egress ingress } { enable disable } example: Raisecom(config-epon-onu-service- profile:1)#uni ethernet 1 policing ingress enable</pre>	(Optional) enable downlink rate limiting over the ONU UNI. • uni-list: ONU UNI list, an integer, with the value decided by the ONU type • egress: rate limiting over data in the downlink direction • ingress: rate limiting over data in the uplink direction • enable: enable rate limiting. • disable: disable rate limiting.
18	<pre>Raisecom(config-epon-onu-service-profile: *)#uni ethernet uni-list speed auto example: Raisecom(config-epon-onu-service- profile:1)#uni ethernet 1 speed 100 duplex full</pre>	(Optional) configure auto-negotiation of the interface rate and duplex mode of the ONU UNI. • uni-list: ONU UNI list, an integer, with the value decided by the ONU type
19	<pre>Raisecom(config-epon-onu-service-profile: *)#uni ethernet uni-list speed { 10 100 1000 } duplex { half full } example: Raisecom(config-epon-onu-service- profile:1)#uni ethernet 1 speed 100 duplex full</pre>	(Optional) configure the interface rate and duplex mode of the ONU UNI. • uni-list: ONU UNI list, an integer, with the value decided by the ONU type • auto: the rate and duplex mode are auto-negotiable. • 10: the rate is forcible 10 Mbit/s. • 100: the rate is forcible 100 Mbit/s. • 1000: the rate is forcible 1000 Mbit/s. • full: full duplex mode • half: half duplex mode
20	<pre>Raisecom(config-epon-onu-service-profile: *)#uni ethernet uni-list switchport isolation { disable enable } example: Raisecom(config-epon-onu-service- profile:1)#uni ethernet 1 switchport isolation enable</pre>	(Optional) enable/disable ONU UNI isolation. • uni-list: ONU UNI list, an integer, with the value decided by the ONU type • enable: enable ONU UNI isolation. • disable: disable ONU UNI isolation.
21	<pre>Raisecom(config-epon-onu-service-profile: *)#uni ethernet uni-list vlan mode { tagged transparent trunk } example: Raisecom(config-gpon-onu-service- profile:10)#uni ethernet 1-4 vlan mode tagged</pre>	(Optional) configure the VLAN mode of the ONU UNI. • uni-list: ONU UNI list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • tagged: VLAN tagging mode • transparent: transparent transmission mode • trunk: Trunk mode

Step	Command	Description
22	<pre>Raisecom(config-epon-onu-service-profile:*)#uni ethernet uni-list vlan trunk allowed vlan-list example: Raisecom(config-gpon-onu-service-profile:10)#uni ethernet 1-4 vlan trunk allowed 100-150</pre>	(Optional) configure the VLAN list allowed by the ONU UNI Trunk interface. You can use the no uni ethernet uni-list vlan trunk allowed command to restore default configurations. • uni-list: ONU UNI index, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • vlan-list: VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". It supports up to 8 VLANs.
23	<pre>Raisecom(config-epon-onu-service-profile:*)#uni ethernet uni-list epon- policing-profile profile-id example: Raisecom(config-epon-onu-service-profile:1)#uni ethernet 1 epon-policing- profile 1</pre>	(Optional) associate the EPON rate-limit template with the service template. • uni-list: ONU UNI list, an integer, with the value decided by the ONU type • profile-id: EPON rate-limiting template ID, an integer, ranging from 1 to 24
24	<pre>Raisecom(config-epon-onu-service-profile:*)#voip-profile profile-id example: Raisecom(config-epon-onu-service-profile:1)#voip-profile 1</pre>	(Optional) associate the voice template with the service template. profile-id: voice template ID, an integer, ranging from 1 to 256
25	<pre>Raisecom(config-epon-onu-service-profile:*)#create lan-vlan vlan-id [ip- address ip-address ip-mask] example: Raisecom(config-epon-onu-service-profile:1)#create lan-vlan 1</pre>	Create a VLAN for the LAN port. You can use the no create lan-vlan vlan-id command to delete the LAN port VLAN. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • ip-address: IP address, in dotted decimal notation • ip-mask: subnet mask, in dotted decimal notation
26	<pre>Raisecom(config-epon-onu-service-profile:*)#lan-vlan vlan-id ip-address ip- address ip-mask example: Raisecom(config-epon-onu-service-profile:1)#lan-vlan 1 ip-address 10.0.0.1 255.255.255.0</pre>	Configure the IP address and mask of the VLAN interface. You can use the no lan-vlan vlan-id ip-address command to delete the configuration. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • ip-address: IP address, in dotted decimal notation • ip-mask: subnet mask, in dotted decimal notation

2.3.3 Binding template

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#interface epon-onu 3/1/1	Enter EPON ONU virtual interface configuration mode. - slot-id: slot ID, an integer - olt-id: PON port ID, an integer - onu-id: ONU ID on the PON port, an integer
3	Raisecom(config-if-epon-onu-*//*:*)#rebind epon-onu-service-profile profile-id epon-onu-line-profile profile-id Raisecom(config-if-epon-onu-*//*:*)#exit example: Raisecom(config-if-epon-onu-3/1:1)# rebind epon-onu-service-profile 1 epon-onu-line-profile 1	Rebind the EPON service template and line profile to the ONU. - epon-onu-service-profile profile-id: EPON service template, an integer, ranging from 1 to 128 - epon-onu-line-profile profile-id: EPON line profile, an integer, ranging from 1 to 1024
4	Raisecom(config)#epon-onu-service-profile profile-id example: Raisecom(config)#epon-onu-service-profile 1	Enter service template configuration mode. If the template exists, enter template configuration mode directly; if the template does not exist, create a template and enter template configuration mode. profile-id: EPON line profile, an integer, ranging from 1 to 1024
5	Raisecom(config-epon-onu-service-profile:*)#lan-vlan vlan-id dhcp-server-profile profile-id Raisecom(config-epon-onu-service-profile:*)#exit example: Raisecom(config-epon-onu-service-profile:1)# lan-vlan 1 dhcp-server-profile 2	Bind the VLAN interface with the DHCP server template. You can use the no lan-vlan vlan-id dhcp-server-profile command to delete the configuration. - vlan-id: VLAN ID, an integer, ranging from 1 to 4094 - profile-id: DHCP server template ID, an integer, ranging from 1 to 128

2.3.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show epon-onu-service-profile { all profile-list }	Show SNMP template configurations.

2.4 Configuring voice template



Note

The voice template can realize the batch configuration of ONU voice-related parameters, which greatly reduces the configuration workload and relieves the burden of configuration personnel.

2.4.1 Default configurations

N/A

2.4.2 Creating template

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#create sip-agent-profile-id <i>profile-id</i>	(Optional) create a SIP server template based on the template ID. You can use the no form of this command to delete the template.
3	Raisecom(config)#create sip-agent-profile-name <i>profile-name</i>	(Optional) create a SIP server template based on the template name. You can use the no form of this command to delete the template.
4	Raisecom(config)#create voip-profile <i>profile-id</i> name <i>profile-name</i> pots <i>pot-id</i>	Create a voice template and configure the template parameters. You can use the no create voip-profile { all profile-list } command to delete the template.
5	Raisecom(config)#epon-onu-service-profile <i>profile-id</i>	Enter service profile configuration mode. If the template exists, the system will directly enter template configuration mode, otherwise it creates a template before entering template configuration mode.
6	Raisecom(config-epon-onu-service-profile:*)#voip-profile <i>profile-id</i>	(Optional) associate the voice template with the service template.

2.4.3 Configuring template

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#voip-profile <i>profile-id</i>	Enter voice template configuration mode. If the template exists, the system enters template configuration mode.
3	Raisecom(config-epon-onu-voip-profile:*)#name <i>name</i>	(Optional) configure the voice template name.
4	Raisecom(config-epon-onu-voip-profile:*)#digitmap <i>match-mode</i> { max min }	(Optional) configure the voice template digitmap matching mode to max/min.

Step	Command	Description
5	Raisecom(config-epon-onu-voip-profile:*)# h248 pots tid name <i>name pot-id</i>	(Optional) configure the voice template H.248 port ID. You can use the no h248 pots tid name pot-id command to delete the configuration.
6	Raisecom(config-epon-onu-voip-profile:*)# voip-protocol { sip h248 ims-sip }	(Optional) configure the ONU voice protocol type.
7	Raisecom(config-epon-onu-voip-profile:*)# h248-profile <i>profile-id</i>	(Optional) bind the EPON ONU voice profile to the H.248 profile.
8	Raisecom(config-epon-onu-voip-profile:*)# sip-profile <i>profile-id</i>	(Optional) bind the EPON ONU voice template to the SIP template.
9	Raisecom(config-epon-onu-voip-profile:*)# ims-sip-profile <i>profile-id</i>	(Optional) bind the EPON ONU voice template to the IMS-SIP template.
10	Raisecom(config-epon-onu-voip-profile:*)# secondary sip-agent-profile-name <i>profile-name</i>	(Optional) configure the backup SIP server template. You can use the no sip-agent-profile secondary command to delete the configuration.
11	Raisecom(config-epon-onu-voip-profile:*)# secondary sip-agent-profile-id <i>profile-id</i>	(Optional) configure the backup SIP server template. You can use the no sip-agent-profile secondary command to delete the configuration.
12	Raisecom(config-epon-onu-voip-profile:*)# sip-agent-profile-name <i>profile-name</i> [secondary sip-agent-profile-name <i>profile-name</i>]	(Optional) bind the EPON ONU voice template to the SIP server template. You can use the no sip-agent-profile [secondary] command to delete the configuration.
13	Raisecom(config-epon-onu-voip-profile:*)# sip-agent-profile-id <i>profile-id</i> [secondary sip-agent-profile-id <i>profile-id</i>]	(Optional) bind the EPON ONU voice template with the SIP server template. You can use the no sip-agent-profile [secondary] command to delete the configuration.



Note

The template must exit. The template in use cannot be modified.

2.4.4 Checking configurations

Step	Configuration	Description
1	Raisecom# show voip-profile { all <i>profile-list</i> }	Show configurations of the voice template.

2.5 Configuring rate-limit template

2.5.1 Default configuration

N/A

2.5.2 Configuring template

Step	Configuration	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#create epon-policing-profile <i>profile-id</i> name <i>profile-name</i> example: Raisecom(config)#create epon-policing-profile 10 name raisecom	Create a rate-limit template. You can use the no create epon-policing-profile <i>profile-id</i> command to delete the template. • profile-id: rate-limiting template ID, an integer, ranging from 1 to 24 • profile-name: rate-limiting template name, a string of 1 to 16 characters

2.5.3 Binding template

Step	Configuration	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu uni ethernet <i>slot-id/olt-id/onu-id/uni-id</i> example: Raisecom(config)#epon-onu uni ethernet 3/2/1/1-4	Enter EPON ONU UNI configuration mode. • slot-id/olt-id/onu-id/uni-id: UNI ID
3	Raisecom(config-if-epon-onu-ethernet-*/*/*:*)#policing-profile <i>profile-id</i> example: Raisecom(config-epon-onu-ethernet-range)#policing-profile 10	Bind a rate-limit template on the ONU UNI. You can use the no policing-profile command to release the binding relation. • profile-id: rate-limiting template ID, an integer, ranging from 1 to 24

2.5.4 Checking configurations

Step	Configuration	Description
1	Raisecom#show epon-policing-profile <i>profile-list</i>	Show configurations of the rate-limit template.

2.6 Configuring ONU IP address pool

2.6.1 Default configuration

N/A

2.6.2 Creating address pool

Step	Configuration	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip-pool pool-id pool-name begin ip-address end ip-address mask default-gw ip-address vlan svlan-id cvlan-id priority example: Raisecom(config)#ip-pool 1 POOL1 begin 192.168.1.2 end 192.168.1.100 255.255.255.0 default-gw 192.168.1.1 vlan 0 10 5	Configure the ONU IP address pool. You can use the no ip-pool pool-id command to delete the address pool. • pool-id: address pool ID, an integer, ranging from 1 to 224 • pool-name: address pool name, a string of 1 to 16 characters • begin ip-address: start IP address of the address pool, in dotted decimal notation, such as 10.0.0.1 • end ip-address: end IP address of the address pool, in dotted decimal notation, such as 10.0.0.1 • mask: IP address mask, in dotted decimal notation, such as 255.0.0.0 • default-gw ip-address: default gateway, in dotted decimal notation, such as 10.0.0.1 • svlan-id: CVLAN ID, an integer, ranging from 0 to 4094 where 0 indicates untagged • cvlan-id: SVLAN ID, an integer, ranging from 0 to 4094 where 0 indicates untagged • priority: CoS priority, an integer, ranging from 0 to 7

2.6.3 Binding PON interface

Step	Configuration	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { epon-olt ten-giga-epon-olt } slot-id/olt-id example: Raisecom(config)#interface epon-olt 3/1	Enter EPON interface configuration mode. • epon-olt: EPON interface • ten-giga-epon-olt: 10G EPON interface • slot-id/port-id: distributed interface ID
3	Raisecom(config-if-*olt-*:*)#ip-pool pool-id example: Raisecom(config-if-epon-olt-3:1)#ip-pool 1	Bind the EPON interface with an IP address pool. You can use the no ip-pool command to delete the binding relation.  Note • Multiple EPON interfaces are allowed to be bound to the same OUN IP address pool. • Each EPON interface can be bound to one OUN IP address pool only. • pool-id: IP address pool ID, an integer, ranging from 1 to 224



Note

To enable the ONU to obtain a management address from the PON port address pool, you need to use the **ip-config auto overlay-local-ip** command to configure the distribution mode of ONU management IP address automatic obtainment.

2.6.4 Checking configurations

Step	Configuration	Description
1	<code>Raisecom#show ip-pool [pool-id] information</code>	Show configurations of the IP address pool.
2	<code>Raisecom#show interface { epon-olt ten-giga-epon-olt } [slot-id/olt-list] ip-pool information</code>	Show IP address pool binding information about the EPON interface.

2.7 Rebinding the ONU

When creating an ONU, you need to specify its MAC address, which is used as the basis for justifying the legality during registration. When the ONU is replaced, the new ONU is considered to be an illegal ONU due to the change of the MAC address and need to be re-registered, which results in configuration loss.

Rebind the MAC address of the ONU and replace the MAC address in the ONU authentication and authorization, so that the new ONU has legality and retains the original configuration.

Step	Configuration	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface epon-onu slot-id/olt-id/onu-id</code> example: <code>Raisecom(config)#interface epon-onu 3/1/1</code>	Enter EPON ONU management configuration mode. • slot-id/olt-id/onu-id: ONU ID
3	<code>Raisecom(config-if-epon-onu*/*:*)#rebind mac mac-address [device-type onu-type]</code> example: <code>Raisecom(config-if-epon-onu-3/1:1)#rebind mac 0000.1234.abcd</code>	Rebind the MAC address of the ONU. The device type can be changed into other types of the same interface. • mac-address: MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456 • device-type onu-type: ONU type, including all types of OUNs produced by Raisecom. At the same time, it supports the universal ONU type, which is convenient for the binding ONUs of other vendors. For example: ONU-16 represents a universal 16-port ONU.

Step	Configuration	Description
4	<pre>Raisecom(config-if-epon-onu-/*:*)#rebind epon-onu- service-profile <i>profile-id</i> epon-onu-line-profile <i>profile-id</i> example: Raisecom(config-if-epon-onu- 3/1:1)#rebind epon-onu- service-profile 1 epon-onu- line-profile 1</pre>	Rebind the EPON service template and line profile to the ONU. • epon-onu-service-profile profile-id: EPON service template, an integer, ranging from 1 to 128 • epon-onu-line-profile profile-id: EPON line profile, an integer, ranging from 1 to 1024

2.8 Configuring data encryption

Step	Configuration	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#interface epon-onu slot- id/olt-id/onu-id example: Raisecom(config)#interface epon-onu 3/1/1</pre>	Enter EPON ONU virtual interface configuration mode. • slot-id/olt-id/onu-id: ONU ID
3	<pre>Raisecom(config-if-epon-onu-/*:*)#encryption { enable disable }</pre>	Enable/Disable data encryption.
4	<pre>Raisecom(config-if-epon-onu-/*:*)#encryption direction { down up- down } example: Raisecom(config-if-epon-onu- 3/1:1)#encryption direction down</pre>	Configure the data encryption direction. • down: downlink encryption • down-up: concurrent uplink and downlink encryption

2.9 Configuring FEC

Step	Configuration	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#interface epon-onu slot- id/olt-id/onu-id</pre>	Enter EPON ONU virtual interface configuration mode.
3	<pre>Raisecom(config-if-epon-onu-/*:*)#fec { enable disable }</pre>	Enable/Disable FEC.



Note

- It supports bidirectional FEC. In the receiving direction at both ends of the ONU, FEC is fixed at adaptive receiving mode (mixed mode). In other words, the receiving party can correctly receive packets regardless of whether the sending end is enabled with FEC.
- It supports enabling/disabling FEC in the sending direction of the OLT/ONU.
- It only supports enabling/disabling FEC in both directions concurrently.

2.10 Configuration examples

2.10.1 Configuring automatic registration of ONU

Networking requirements

As shown in Figure 2-1, the ONU authentication mode is configured to none on the OLT interface 3/1. The ONU joins the OLT through automatic registration.

Figure 2-1 ONU automatic registration



Configuration steps

Configure the ONU authentication mode to none.

```

Raisecom#config
Raisecom(config)#interface epon-olt 3/1
Raisecom(config-if-epon-olt-3:1)#authorization mode none
  
```

Checking results

Show ONU authentication mode.

```
Raisecom#show interface epon-olt 3/1 information
```

OLT ID	MaxRTT (TQ)	Encryption Mode	Automatic Authorization	Created ONUs	Registered ONUs	SFP
3/1	14000	tri-churning	none	1	1	ok

Show information about the ONUs registered on the OLT.

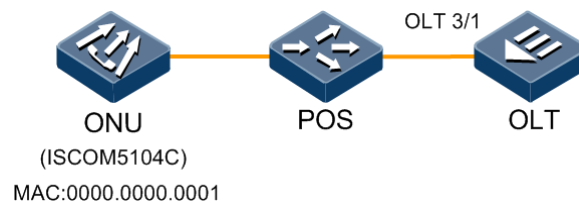
```
Raisecom#show interface epon-onu creation-information
ONU ID      MAC Address Mode Creation Date  Device Type  State  Mng-mode
-----
3/1/1      000e.5e0a.7a0e auto  2000-01-01,08:00 ISCOM5304D active  oam
```

2.10.2 Configuring ONU registration based on MAC authentication mode

Networking requirements

As shown in Figure 2-2, MAC authentication mode is enabled on OLT interface 3/1 for ONU registration. The model of the ONU to be registered is 5104c and the MAC address is 0000.0000.0001.

Figure 2-2 OUN registration based on MAC authentication mode



Configuration steps

Step 1 Configure the ONU authentication mode to MAC authentication.

```
Raisecom#config
Raisecom(config)#interface epon-olt 3/1
Raisecom(config-if-epon-olt-3:1)#authorization mode mac
```

Step 2 Create an ONU authentication entry based on MAC address.

```
Raisecom(config-if-epon-olt-3:1)#create epon-onu 1 mac 0000.0000.0001
device-type 5104c
```

Checking results

Show ONU authentication mode.

```
Raisecom#show interface epon-olt 3/1 information
MaxRTT Encryption Automatic Created Registered
OLT ID (TQ) Mode Authorization ONUS ONUS SFP
```

```
-----
-----
3/1    14000    tri-churning    none        1        1        ok
```

Show information about the ONUs registered on the OLT.

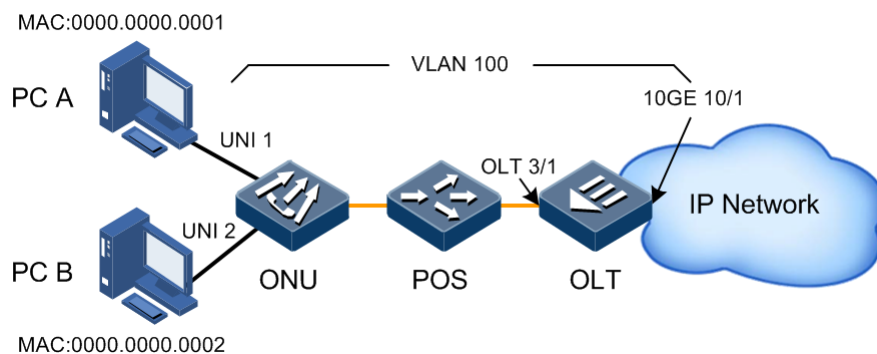
```
Raisecom#show interface epon-onu creation-information
ONU ID  MAC Address    Mode  Creation Date  Device Type  State  Mng-mode
-----
3/1/1  0000.0000.0001  mac   2000-01-01,08:00  ISCOM5104(C)  active  oam
```

2.10.3 Configuring Ethernet data services

Networking requirements

As shown in Figure 2-3, PC A is connected to UNI 1 of the ONU, and the user VLAN is 100. PON interface 3/1 of ISCOM6800 or ISCOM6860 is connected downstream to the ONU. The 10GE interface 10/1 is connected upstream to the IP network. In this network topology, data services are provisioned.

Figure 2-3 Data services



Configuration steps

- Configure OLT.

Step 1 Create a VLAN and configure interface VLAN mode.

```
Raisecom#config
Raisecom(config)#create vlan 100 active
Raisecom(config)#interface ten-gigabitethernet 10/1
Raisecom(config-if-ten-gigabitethernet-10:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-10:1)#switchport trunk allowed
vlan 100
Raisecom(config-if-ten-gigabitethernet-10:1)#exit
Raisecom(config)#interface epon-olt 3/1
Raisecom(config-if-epon-olt-3:1)#switchport mode trunk
```



```
Raisecom(config-if-epon-olt-3:1)#switchport trunk allowed vlan 100
```

Step 2 Configure the ONU authentication mode to automatic registration.

```
Raisecom(config-if-epon-olt-3:1)#authorization mode none  
Raisecom(config-if-epon-olt-3:1)#exit
```

- Configure the ONU.

Step 3 Configure user data VLAN.

```
Raisecom(config)#epon-onu uni ethernet 3/1/1/1  
Raisecom(config-epon-onu-ethernet-3/1/1:1)#vlan mode tagged  
Raisecom(config-epon-onu-ethernet-3/1/1:1)#native vlan 100  
Raisecom(config-epon-onu-ethernet-3/1/1:1)#end
```

Checking results

Show VLAN configurations of OLT 10GE interface 10/1.

```
Raisecom#show interface ten-gigabitethernet 10/1 vlan  
Port: 10/1  
Administrative Mode: trunk  
Operational Mode: trunk  
Access Mode VLAN: 1  
Trunk Native Mode VLAN: 1  
Administrative Trunk Allowed VLANs: 100  
Operational Trunk Allowed VLANs: 1,100  
Administrative Trunk Untagged VLANs: n/a  
Operational Trunk Untagged VLANs: 1  
Drop Untagged: No
```

Show VLAN configurations of OLT PON interface 3/1.

```
Raisecom#show interface epon-olt 3/1 vlan  
Port: 3/1  
Administrative Mode: trunk  
Operational Mode: trunk  
Access Mode VLAN: 1  
Trunk Native Mode VLAN: 1  
Administrative Trunk Allowed VLANs: 100  
Operational Trunk Allowed VLANs: 1,100  
Administrative Trunk Untagged VLANs: n/a  
Operational Trunk Untagged VLANs: 1
```

Show information about the registered ONUs.

```
Raisecom#show interface epon-onu creation-information
ONU ID      MAC Address      Mode      Creation Date      Device Type
State      Mng-mode      Description
-----
3/1/1      000e.5e07.7ac0  auto      2005-07-29,09:00:03  ISCOM5304D
active     oam           --
```

Show UNI VLAN configurations of the ONU.

```
Raisecom#show epon-onu 3/1/1 uni ethernet 1 vlan
Port ID: 3/1/1/1
VLAN mode      : Tagged
Native VLAN    : 100(CoS 0)
Trans-rule list : n/a
Trunk allowed VLAN: n/a
Agg-rule list  : n/a
```

2.10.4 Configuring PON+LAN typical networking

Networking requirements

As shown in Figure 2-4, IP address pool function is adopted to implement management parameter configurations of the ONU in batches. The requirements are as below.

- Configure the ONU IP address pool and SNMP parameter template on the OLT. The ONU obtains the management parameters in batches through IP address pool and SNMP template.
- Table 2-1 lists the requirements for the IP address pool.

Table 2-1 Parameter list of ONU IP address pool

Parameter	Value
IP address pool ID	Automatic assignment by the system
IP address pool name	raisecom-ippool
Start IP address of the IP address pool	192.168.1.11
End IP address of the IP address pool	192.168.1.254
Subnet mask of IP address pool	255.255.255.0
Default gateway address of the IP address pool	192.168.1.1
IP address pool management data CVLAN	10
IP address pool management data SVLAN	0 (the packet does not carry a VLAN tag)

Parameter	Value
IP address pool management data priority	6 (the management packet requires a higher priority)

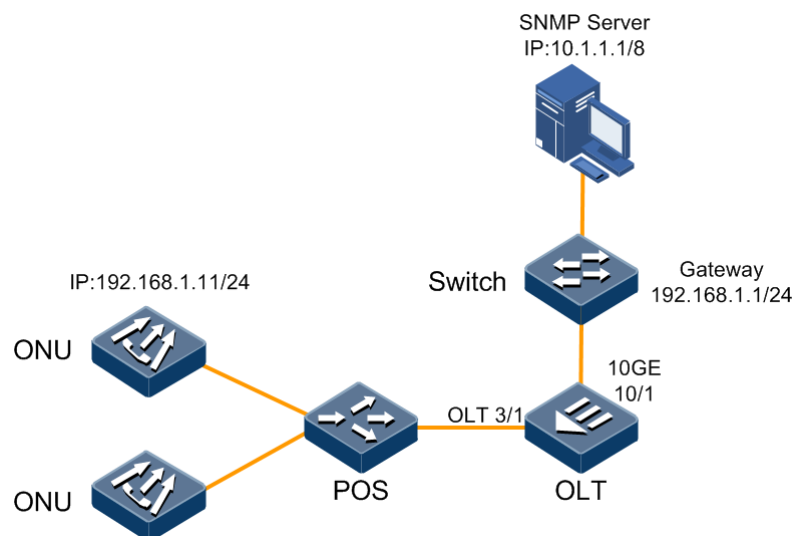
- Table 2-2 lists configuration requirements of NView NNM.

Table 2-2 ONU SNMP template parameter list

Parameter	Value
SNMP template ID	Automatic assignment by the system
SNMP template name	raisecom1
SNMP version	SNMP v2
IP address of the SNMP Trap host	10.1.1.1
Trap interface	161
UDP interface ID	162
SNMP host name	public
SNMP read community name	public
SNMP write community name	private

- The VLAN of ONU data service channel is 20.

Figure 2-4 Configuring ONU independent network management (based on IP address pool)



Configuration steps

- Step 1 Create the ONU IP address pool.

```
Raisecom#config  
Raisecom(config)#ip-pool 1 raisecom-ippool begin 192.168.1.11 end  
192.168.1.254 255.255.255.0 default-gw 192.168.1.1 vlan 0 10 6
```

Step 2 Bind the PON interface with the IP address pool.

```
Raisecom(config)#interface epon-olt 3/1  
Raisecom(config-if-epon-olt-3:1)#ip-pool 1  
Raisecom(config-if-epon-olt-3:1)#exit
```

Step 3 Create an ONU SNMP parameter template.

```
Raisecom(config)#snmp-template 1 raisecom1 snmp-server 10.1.1.1 version  
v2 trap-port 161 udp-port 162 security public community ro public rw  
private
```

Step 4 Configure the ONU management IP configuration mode in batch and bind the SNMP template.

```
Raisecom(config)#epon-onu range 3/1/1-64  
Raisecom(config-epon-onu-range)#ip-config auto overlay-local-ip  
Raisecom(config-epon-onu-range)#snmp-template 1  
Raisecom(config-epon-onu-range)#exit
```

Step 5 Configure the ONU management mode.

```
Raisecom(config)#interface range epon-onu 3/1/1-64  
Raisecom(config-if-epon-onu-range)#mng-mode snmp  
Raisecom(config-if-epon-onu-range)#exit
```

Step 6 Configure the PON interface to Trunk mode, allowing VLAN 10 to pass.

```
Raisecom(config)#interface epon-olt 3/1  
Raisecom(config-if-epon-olt-3:1)#switch mode trunk  
Raisecom(config-if-epon-olt-3:1)#switchport trunk allowed vlan 10 confirm  
Raisecom(config-if-epon-olt-3:1)#exit
```

Step 7 Configure the VLAN attributes of the data service interface on the OLT.

```
Raisecom(config)#interface epon-olt 3/1
Raisecom(config-if-epon-olt-3:1)#switch mode trunk
Raisecom(config-if-epon-olt-3:1)#switchport trunk native vlan 20
Raisecom(config-if-epon-olt-3:1)#exit
Raisecom(config)#interface ten-gigabitethernet 10/1
Raisecom(config-if-ten-gigabitethernet-10:1)#switch mode trunk
Raisecom(config-if-ten-gigabitethernet-10:1)#switchport trunk allowed
vlan 20 confirm
```

Checking results

Show information about the ONU IP address pool bound to the OLT PON interface.

```
Raisecom#show interface epon-olt 3/1 ip-pool information
  OLT ID  Pool ID  Pool Name
-----
  3/1      1       raisecom1
```

Show ONU management information, including ONU management mode, IP address configuration, and the bound SNMP parameter template.

```
Raisecom#show epon-onu 3/1/1 mng-information
ONU ID  Mng-mode  IP Config Mode  SNMP Template ID  SNMP Template Name
-----
3/1/1    SNMP      auto            1                 raisecom1
```

3

Configuring GPON services

This chapter describes GPON services and the configuration process of the device, and provides related configurations examples, including the following sections:

- Registration and deregistration
- Configuring ONU registration keywords
- Activating or suspending ONU
- Configuring GPON interface
- Configuring adjustment value of Rx optical power
- Configuring alarm profile
- Configuring DBA profile
- Configuring line profile
- Configuring service profile
- Configuring rate limit profile
- Configuring TR069 management template
- Configuring VLAN
- Configuring auto-authentication rules
- Configuring rate limiting on GEM interface
- Configuration examples

3.1 Registration and deregistration

3.1.1 Default configurations

Default configurations of registration and deregistration on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
ONU auto-discovery period	5s
ONU registration mode	SN

3.1.2 Registering ONU

Configuring ONU registration distance

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface gpon-olt slot-id/olt-id example: Raisecom(config)#interface gpon-olt 3/1	Enter GPON interface configuration mode. • slot-id: slot ID • olt-id: PON interface ID
3	Raisecom(config-if-gpon-olt-*:*)#distance min min-distance max max-distance example: Raisecom(config-if-gpon-olt-3:1)#distance min 100 max 10000	Configure the range of ONU registration distance. • min min-distance: minimum registration distance, an integer, ranging from 0 to 60000, in units of meter • max max-distance: maximum registration distance, an integer, ranging from 0 to 60000, in units of meter

Configuring ONU auto-registration

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface gpon-olt slot-id/olt-id	Enter GPON interface configuration mode.
3	Raisecom(config-if-gpon-olt-*:*)#authorization mode none	Configure the ONU to work in the auto-registration mode.

Creating ONU manually

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface gpon-olt slot-id/olt-id example: Raisecom(config)#interface gpon-olt 3/1	Enter GPON interface mode. • slot-id: slot ID • olt-id: PON interface ID

Step	Command	Description
3	<pre>Raisecom(config-if-gpon-olt-*:*)#authorization mode { hybrid loid loid-checkcode none sn sn-password password } example: Raisecom(config-if-gpon-olt-3:1)#authorization mode loid</pre>	Configure the ONU registration mode. You can use the no authorization mode command to restore default configuration. • none: automatic authentication mode, the ONU can automatically registered. • hybrid: registration mode based on hybrid authentication • Loid: LOID-based registration • loid-checkcode: registration based on LOID+Checkcode • sn: SN-based registration • sn-password: registration based on SN+Password • password: password-based registration
4	<pre>Raisecom(config-if-gpon-olt-*:*)#create gpon-onu [onu-id] sn snstring [password password] { line-profile-id line-profile-id line-profile-name line-profile-name } { service-profile-id service-profile-id service-profile-name service-profile-name } [onu_type { auto gpon xgpon xgspon }] Raisecom(config-if-gpon-olt-*:*)#create gpon-onu [onu-id] sn snstring example: Raisecom(config-if-gpon-olt-3:1)#create gpon-onu sn abc line-profile-id 10 service-profile-id 200</pre>	(Optional) create the ONU registered based on the SN or SN+PASSWORD, and bind the corresponding line profile and service profile. You can use the no create gpon-onu onu-id command to delete the ONU. • onu-id: ONU ID, an integer. If this parameter is omitted while inputting this command, the system will automatically assign effective ONU IDs to the ONU. • sn snstring: ONU ID, a string of 16 characters • line-profile-id: line profile ID, an integer, ranging from 1 to 1025 • line-profile-name: line profile name, a string of 1 to 16 characters • service-profile-id: service template ID, an integer, ranging from 1 to 1024 • service-profile-name: service template name, a string of 1 to 16 characters
	<pre>Raisecom(config-if-gpon-olt-*:*)#create gpon-onu [onu-id] password password { line-profile-id line-profile-id line-profile-name line-profile-name } { service-profile-id service-profile-id service-profile-name service-profile-name } [onu_type { auto gpon xgpon xgspon }] example: Raisecom(config-if-gpon-olt-3:1)#create gpon-onu password 1234 line-profile-id 10 service-profile-id 200</pre>	(Optional) create the ONU registered based on the password, and bind the corresponding line profile and service profile. You can use the no create gpon-onu onu-id command to delete the ONU. • onu-id: ONU ID, an integer. If this parameter is omitted while inputting this command, the system will automatically assign effective ONU IDs to the ONU. • password: ONU registration password, an integer, ranging from 1 to 10 • line-profile-id line-profile-id: line profile ID, an integer, ranging from 1 to 1024 • line-profile-name: line profile name, a string of 1 to 16 characters • service-profile-id: service template ID, an integer, ranging from 1 to 1024 • service-profile-name: service template name, a string of 1 to 16 characters

Step	Command	Description
	<pre>Raisecom(config-if-gpon-olt-*:*)#create gpon-onu [onu-id] loid loid [checkcode checkcode] { line-profile-id line-profile-id line-profile-name line-profile-name } { service-profile-id service-profile-id service-profile-name service-profile-name } [onu_type { auto gpon xgpon xgspon }] example: Raisecom(config-if-gpon-olt-3:1)#create gpon-onu loid 123 line-profile-id 10 service-profile-id 200</pre>	(Optional) create the ONU registered based LOID or LOID+checkcode, and bind the corresponding line profile and service profile. You can use the no create gpon-onu onu-id command to delete the ONU. • onu-id: ONU ID, an integer. If this parameter is omitted while inputting this command, the system will automatically assign effective ONU IDs to the ONU. • loid loid: ONU logical ID, an integer, ranging from 1 to 24 • line-profile-id: line profile ID, an integer, ranging from 1 to 1024 • line-profile-name: line profile name, a string of 1 to 16 characters • service-profile-id: service template ID, an integer, ranging from 1 to 1024 • service-profile-name: service template name, a string of 1 to 16 characters

3.1.3 Deregistering ONU

You can enable the ONU to resend the registration request by deregistering it, which is usually used in engineering maintenance. If you suspect the logical link of an ONU working improperly, you can resume it through deregistration.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface gpon-onu slot-id/olt-id/onu-id	Enter GPON ONU virtual interface configuration mode.
3	Raisecom(config-if-gpon-onu-*/*:*)#deregister	Configure ONU deregistration.

3.1.4 Activating ONUs

Configure the device which needs activating ONUs.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface gpon-olt slot-id/olt-id	Enter GPON interface configuration mode.
3	Raisecom(config-if-gpon-olt-*:*)#active all-suspend-onu	Activate all ONUs which are in suspended status.  Note After the ONU is activated, it will restart the registration process.

3.1.5 Clearing illegal ONU information

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface gpon-olt slot-id/olt-id	Enter GPON interface configuration mode.
3	Raisecom(config-if-gpon-olt-*:*)#clear illegal-onu	Clear information about illegal ONUs.

3.1.6 Checking configurations

No.	Command	Description
1	Raisecom#show interface gpon-olt slot-id/olt-id auth information	Show information about ONU registration under a GPON interface.
2	Raisecom#show interface gpon-onu slot-id/olt-id/onu-id sn	Show information about SN-based ONU registration.
3	Raisecom#show interface gpon-onu slot-id/olt-id/onu-id loid	Show information about LOID-based ONU registration.
4	Raisecom#show interface gpon-onu slot-id/olt-id/onu-id creation-information	Show ONU registration information.
5	Raisecom#show interface gpon-onu slot-id/olt-id/onu-id online-information	Show ONU online information.
6	Raisecom#show interface gpon-olt slot-id/olt-id illegal-onu	Show information about illegally registered ONUs under the OLT GPON interface.
7	Raisecom#show interface gpon-onu [slot-id/olt-id/onu-list] description-information	Show the ONU description.
8	Raisecom#show interface gpon-onu [slot-id/olt-id/onu-list] download-information	Show the loaded configurations of the ONU.

3.2 Configuring ONU registration keywords

3.2.1 Default configurations

N/A

3.2.2 Configuring ONU registration keywords

No.	Command	Description
1	Raisecom#config	Enter global configuration mode.

No.	Command	Description
2	Raisecom(config)#interface gpon-onu slot-id/olt-id/onu-id example: Raisecom(config)#interface gpon-onu 3/1/1	Enter GPON ONU virtual interface configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-if-gpon-onu-*/*:*)#rebind sn sn example: Raisecom(config-if-gpon-onu-3/1:1)#rebind sn raisecom	(Optional) configure the ONU to register the keywords based on SN. • sn: device serial number, an integer, fixed at 16  Note Only the offline ONU can be configured. The online ONU cannot be configured.
4	Raisecom(config-if-gpon-onu-*/*:*)#password password example: Raisecom(config-if-gpon-onu-3/1:1)#password raisecom	(Optional) configure the ONU to register the keywords based on password. • password: password, a string of 1 to 12 characters  Note Only the offline ONU can be configured. The online ONU cannot be configured.
5	Raisecom(config-if-gpon-onu-*/*:*)#loid checkcode checkcode example: Raisecom(config-if-gpon-onu-3/1:1)#loid checkcode raisecom	(Optional) configure the ONU to register keywords based on LOID. • checkcode: LOID authentication keywords, a string of 1 to 12 characters  Note Only the offline ONU can be configured. The online ONU cannot be configured.

3.3 Activating or suspending ONU

3.3.1 Default configurations

N/A

3.3.2 Activating or suspending ONU

No.	Command	Description
1	Raisecom# config	Enter global configuration mode.

No.	Command	Description
2	<pre>Raisecom(config)#interface gpon-onu slot-id/olt-id/onu-id</pre> example: <pre>Raisecom(config)#interface gpon-onu 3/1/1</pre>	Enter GPON ONU virtual interface configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-if-gpon-onu-*/*:*)#state { active suspend }</pre> example: <pre>Raisecom(config-if-gpon-onu-3/1:1)#state active</pre>	Activate or suspend the ONU. - active: activate the ONU. - suspend: suspend the ONU.

3.4 Configuring GPON interface

3.4.1 Default configurations

Default configurations of GPON interface on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
FEC in downstream direction	Disable
GPON interface bound alarm profile	1
GEM port used by broadcast, unknown multicast, and unknown unicast packets	- GPON: 4095 - XGSPON: 5119
GEM port used by multicast packets	- GPON: 4094 - XGSPON: 5118
GPON interface end-to-end access	Disable

3.4.2 Configuring interface

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#interface gpon-olt slot-id/olt-id</pre>	Enter GPON interface configuration mode.
3	<pre>Raisecom(config-if-gpon-olt-*/*:*)#fec { enable disable }</pre>	(Optional) enable/disable FEC on the GPON interface in downlink direction.

Step	Command	Description
4	<code>Raisecom(config-if-gpon-olt-*:*)#multicast gempport port-id</code>	(Optional) configure the GEM interface used by multicast packets. You can use the no multicast gempport command to restore default configuration.  Note This command can be used on the XGSPON interface only, instead of the GPON interface.
4	<code>Raisecom(config-if-gpon-olt-*:*)#broadcast gempport port-id</code>	(Optional) configure the GEM interface used by broadcast packets on the GPON interface. You can use the no broadcast gempport command to restore default configuration.  Note This command can be used on the XGSPON interface only, instead of the GPON interface.
6	<code>Raisecom(config-if-gpon-olt-*:*)#p2p-access enable</code>	(Optional) enable the point-to-point protocol. You can use the p2p-access disable command to disable this function.
7	<code>Raisecom(config-if-gpon-olt-*:*)#dba-mode { normal extended }</code>	(Optional) configure the DBA mode of the GPON interface. You can use the no dba-mode command to restore default configuration.  Note This command can be used on the XGSPON interface only, instead of the GPON interface.
8	<code>Raisecom(config-if-gpon-olt-*:*)#reset</code>	(Optional) reset the GPON interface.  Note When the device fails, you can use this command to reset the interface to resume services. The GP16 card and XG16 card do not support this command. The GP8A card supports this command.

3.4.3 Checking configurations

No.	Command	Description
1	<code>Raisecom#show interface gpon-olt slot-id/olt-id basic information</code>	Show GPON interface configurations.
2	<code>Raisecom#show interface gpon-olt slot-id/olt-id { upstream downstream } ni statistics</code>	Show traffic statistics in the ingress and egress interfaces of the PON chip.

No.	Command	Description
3	Raisecom#show interface gpon-onu slot-id/olt-id/onu-list upstream gmac statistics	Show the statistics on the uplink traffic of all gemports on the specified ONU.  Note • The ONU on the ISCOM6800-GP16 card cannot be viewed.
4	Raisecom#show interface gpon-onu slot-id/olt-id/onu-list port port-id { upstream downstream } gmac statistics	Show statistics on the uplink/downlink traffic of the specified gemport on the specified ONU.  Note • The ONU on the ISCOM6800-GP16 card cannot be viewed.
5	Raisecom#show gempport-tcont current-use-count	Show the number of gempports used by the entire machine and the number of tconts.
6	Raisecom#show interface gpon-onu slot-id/olt-id/onu-list assign-info	Show the gemport and tcont used by the specified ONU.
7	Raisecom#show interface gpon-onu slot-id/olt-id/onu-list statistics	Show performance statistics on the specified ONU.

3.5 Configuring adjustment value of Rx optical power

3.5.1 Default configurations

N/A

3.5.2 Configuring adjustment value of Rx optical power

No.	Command	Description
1	Raisecom#gpon-onu slot-id/olt-id/onu-id onu-rx-olt-power { decrease increase } value [decimal decimal-value] example: Raisecom#gpon-onu 14/1/1 onu-rx-olt-power increase 2 decimal 3	Configure the adjustment value of OLT optical power received by the ONU. • onu-rx-olt-power: OLT optical power received by the ONU • decrease value: decreasing power adjustment value, an integer, ranging from 0 to 10 • increase value: increasing power adjustment value, an integer, ranging from 0 to 10 • decimal-value: decimal value, an integer, ranging from 0 to 9

No.	Command	Description
2	<pre>Raisecom#gpon-onu slot- id/olt-id/onu-id olt-rx- onu-power { decrease increase } value decimal decimal-value example: Raisecom#gpon-onu 14/1/1 olt-rx-onu-power increase 2 decimal 3</pre>	Configure the adjustment value of ONU optical power received by the OLT. • olt-rx-onu-power: ONU optical power received by the OLT • decrease value: decreasing power adjustment value, an integer, ranging from 0 to 10 • increase value: increasing power adjustment value, an integer, ranging from 0 to 10 • decimal-value: decimal value, an integer, ranging from 0 to 9

3.5.3 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show gpon-onu { olt-rx-onu-power onu-rx-olt-power }</pre>	Show adjustment value of Rx optical power.

3.6 Configuring alarm profile

3.6.1 Default configurations

Default configurations of OLT alarm profile

Default configurations of the OLT alarm profile with a default ID of 1 on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Alarm profile ID	1
Alarm profile name	profile-1
All alarm	Enable
PON interface LOF alarm	Disable
ONU LOF alarm	Disable
ONU LOS alarm	Disable
ONU window drift alarm	Disable
ONU remote indication alarm	Disable
ONU Ploam loss alarm	Disable
ONU GEM delineation loss alarm	Disable
ONU acknowledgement loss alarm	Disable

Function	Default value
ONU signal degradation alarm	Disable
ONU signal degradation alarm threshold	5
ONU signal failure alarm	Disable
ONU signal failure alarm threshold	4
ONU physical equipment error alarm	Disable
ONU key update error alarm	Disable
ONU transmission layer warning	Disable
ONU transmission layer alarm	Disable
ONU registration failure alarm	Enable
ONU laser-always-on alarm	Disable
ONU laser-always-on alarm threshold	12

Default configurations of ONU alarm profile

Default configurations of the ONU alarm profile with a default ID of 1 on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Alarm profile ID	1
Alarm profile name	profile-1
GEM port packet loss count alarm threshold	0
GEM port packet mistransmission count alarm threshold	0
GEM port impaired data block count alarm threshold	0
FCS error frame count alarm threshold	0
Excessive collision frame alarm threshold	0
Tx delay collision alarm threshold	0
Oversized frame alarm threshold	0
Rx buffer overflow alarm threshold	0
Tx buffer overflow alarm threshold	0
Single-collision Tx frame alarm threshold	0
Multi-collision Tx frame alarm threshold	0
Synchronous queue element test error alarm threshold	0
Delay frame alarm threshold	0

Function	Default value
Alarm threshold of Tx failure frame due to MAC sub-layer transmission error	0
Carrier sense loss error alarm threshold	0
Unaligned frame alarm threshold	0
Alarm threshold of Rx failure frame due to MAC sub-layer receiving error	0
Alarm threshold of discarded frame due to PPPoE frame filtering	0
Alarm threshold of discarded frame event due to resource shortage	0
Undersized frame alarm threshold	0
Fragment alarm threshold	0
Jabber frame alarm threshold	0
Alarm threshold of discarded frame due to timeout	0
Alarm threshold of discarded frame due to oversized MTU	0
Rx error frame alarm threshold	0
FEC corrected byte alarm threshold	0
FEC corrected code word alarm threshold	0
FEC uncorrected code word alarm threshold	0
FEC duration alarm threshold	0

3.6.2 Configuring OLT alarm profile

Configuring OLT alarm profile

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#snmp-trap-gpon-olt-profile <i>profile-id</i> example: Raisecom(config)#snmp-trap-gpon-olt-profile 10</pre>	Create the OLT alarm profile and enter OLT alarm profile configuration mode. You can use the no snmp-trap-gpon-olt-profile <i>profile-id</i> command to delete the profile.  Note • If the profile exists, enter profile configuration mode directly. • If the profile does not exist, you need to create the profile first, and then enter profile configuration mode. • profile-id: template index, an integer, ranging from 1 to 150
3	<pre>Raisecom(config-gpon-olt-snmpt-trap-profile:*)#name <i>profile-name</i> example: Raisecom(config-snmpt-trap-gpon-olt-profile:10)#name raisecom</pre>	(Optional) configure the name of the OLT alarm profile. • profile-name: template name, a string of 1 to 16 characters
4	<pre>Raisecom(config-gpon-olt-snmpt-trap-profile:*)#all-trap { enable disable }</pre>	(Optional) enable/disable all alarms.
5	<pre>Raisecom(config-gpon-olt-snmpt-trap-profile:*)#pon-upstream-frame-loss { enable disable }</pre>	(Optional) enable/disable LOF alarm on the PON interface.
6	<pre>Raisecom(config-gpon-olt-snmpt-trap-profile:*)#onu-upstream-frame-loss { enable disable }</pre>	(Optional) enable/disable ONU LOF alarm.
7	<pre>Raisecom(config-gpon-olt-snmpt-trap-profile:*)#onu-signal-loss { enable disable }</pre>	(Optional) enable/disable ONU LOS alarm.
8	<pre>Raisecom(config-gpon-olt-snmpt-trap-profile:*)#onu-window-drift { enable disable }</pre>	(Optional) enable/disable ONU window drift alarm.
9	<pre>Raisecom(config-gpon-olt-snmpt-trap-profile:*)#onu-remote-defect-indication { enable disable }</pre>	(Optional) enable/disable ONU remote indication alarm.
10	<pre>Raisecom(config-gpon-olt-snmpt-trap-profile:*)#onu-ploam-loss { enable disable }</pre>	(Optional) enable/disable ONU Ploam loss alarm.
11	<pre>Raisecom(config-gpon-olt-snmpt-trap-profile:*)#onu-gem-channel-delineatin-loss { enable disable }</pre>	(Optional) enable/disable ONU GEM delineation loss alarm.
12	<pre>Raisecom(config-gpon-olt-snmpt-trap-profile:*)#onu-acknowledge-loss { enable disable }</pre>	(Optional) enable/disable ONU acknowledgement loss alarm.
13	<pre>Raisecom(config-gpon-olt-snmpt-trap-profile:*)#onu-signal-degraded { enable disable }</pre>	(Optional) enable/disable ONU signal degradation alarm.

Step	Command	Description
14	Raisecom(config-gpon-olt-snmp-trap-profile:*)#onu-signal-degraded threshold <i>value</i>	(Optional) configure ONU signal degradation alarm threshold.
15	Raisecom(config-gpon-olt-snmp-trap-profile:*)#onu-signal-failure { enable disable }	(Optional) enable/disable ONU signal failure alarm.
16	Raisecom(config-gpon-olt-snmp-trap-profile:*)#onu-signal-failure threshold <i>value</i>	(Optional) configure ONU signal failure alarm threshold.
17	Raisecom(config-gpon-olt-snmp-trap-profile:*)#onu-physical-quipment-error { enable disable }	(Optional) enable/disable ONU physical equipment error alarm.
18	Raisecom(config-gpon-olt-snmp-trap-profile:*)#onu-key-loss { enable disable }	(Optional) enable/disable ONU key update error alarm.
19	Raisecom(config-gpon-olt-snmp-trap-profile:*)#onu-transmission-interference-warning { enable disable }	(Optional) enable/disable ONU transmission layer warning.
20	Raisecom(config-gpon-olt-snmp-trap-profile:*)#onu-transmission-interference-alarm { enable disable }	(Optional) enable/disable ONU transmission layer alarm.
21	Raisecom(config-gpon-olt-snmp-trap-profile:*)#onu-auth-failed { enable disable }	(Optional) enable/disable ONU registration failure alarm.
22	Raisecom(config-gpon-olt-snmp-trap-profile:*)#onu-laster-always-on { enable disable }	(Optional) enable/disable ONU laser-always-on alarm.
23	Raisecom(config-gpon-olt-snmp-trap-profile:*)#onu-laster-always-on threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-olt-profile:10)#onu-laster-always-on threshold 15	(Optional) configure ONU laser-always-on alarm threshold. • value: alarm threshold, an integer, ranging from 1 to 55

Binding profile

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface gpon-olt slot-id/olt-id example: Raisecom(config)#interface gpon-olt 3/1	Enter GPON interface configuration mode. • slot-id: slot ID • olt-id: PON interface ID
3	Raisecom(config-if-gpon-olt-*:*)# snmp-trap-gpon-olt-profile profile-id example: Raisecom(config-if-gpon-olt-3:1)#snmp-trap-gpon-olt-profile 10	Configure the GPON interface bound alarm profile. • profile-id: template index, an integer, ranging from 1 to 150

3.6.3 Configuring ONU profile

Configuring ONU profile

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#snmp-trap-gpon-onu-profile <i>profile-id</i> example: Raisecom(config)#snmp-trap-gpon-onu-profile 10	Create the ONU alarm profile and enter ONU alarm profile configuration mode. You can use the no snmp-trap-gpon-olt-profile <i>profile-id</i> command to delete the profile. profile-id: template index, an integer, ranging from 1 to 50
3	Raisecom(config-gpon-onu-snmp-trap-profile:*)#name <i>profile-name</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#name raisecom	(Optional) configure the name of the ONU alarm profile. profile-name: template name, a string of 1 to 16 characters
4	Raisecom(config-gpon-onu-snmp-trap-profile:*)#gemport-lost-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#gemport-lost-packets threshold 8	(Optional) configure GEM port packet loss alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
5	Raisecom(config-gpon-onu-snmp-trap-profile:*)#gemport-misinserted-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#gemport-misinserted-packets threshold 8	(Optional) configure GEM port packet mis-transmission alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
6	Raisecom(config-gpon-onu-snmp-trap-profile:*)#gemport-impaired-blocks threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#gemport-impaired-blocks threshold 8	(Optional) configure GEM port impaired data block alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
7	Raisecom(config-gpon-onu-snmp-trap-profile:*)#ethernet-fcs-error-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-fcs-error-packets threshold 8	(Optional) configure FCS error frame alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
8	Raisecom(config-gpon-onu-snmp-trap-profile:*)#ethernet-excessive-collision-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-excessive-collision-packets threshold 8	(Optional) configure excessive collision frame alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100

Step	Command	Description
9	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-late-collision-counter threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-late-collision-counter threshold 8	(Optional) configure Tx delay collision alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
10	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-too-long-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-too-long-packets threshold 8	(Optional) configure oversized frame alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
11	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-rx-buffer-overflow-counter threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-rx-buffer-overflow-counter threshold 8	(Optional) configure Rx buffer overflow alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
12	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-tx-buffer-overflow-counter threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-tx-buffer-overflow-counter threshold 8	(Optional) configure Tx buffer overflow alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
13	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-single-collision-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-single-collision-packets threshold 8	(Optional) configure single-collision Tx frame alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
14	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-multiple-collision-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-multiple-collision-packets threshold 8	(Optional) configure multi-collision Tx frame alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
15	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-sqe-counter threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-sqe-counter threshold 8	(Optional) configure synchronous queue element test error alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100

Step	Command	Description
16	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-deferred-transmission-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-deferred-transmission-packets threshold 8	(Optional) configure delay frame alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
17	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-internal-mac-tx-error-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-internal-mac-tx-error-packets threshold 8	(Optional) configure alarm threshold of Tx failure frame due to MAC sub-layer transmission error. value: alarm threshold, an integer, ranging from 0 to 100
18	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-carrier-sense-error-counter threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-carrier-sense-error-counter threshold 8	(Optional) configure carrier sense loss error alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
19	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-alignment-error-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-alignment-error-packets threshold 8	(Optional) configure unaligned frame alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
20	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-internal-mac-rx-error-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-internal-mac-rx-error-packets threshold 8	(Optional) configure alarm threshold of Rx failure frame due to MAC sub-layer receiving error. value: alarm threshold, an integer, ranging from 0 to 100
21	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-pppoe-filter-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-pppoe-filter-packets threshold 8	(Optional) configure alarm threshold of discarded frame due to PPPoE frame filtering. value: alarm threshold, an integer, ranging from 0 to 100
22	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-drop-event-counter threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-drop-event-counter threshold 8	(Optional) configure alarm threshold of discarded frame event due to resource shortage. value: alarm threshold, an integer, ranging from 0 to 100

Step	Command	Description
23	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-undersize-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-undersize-packets threshold 8	(Optional) configure undersized frame alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
24	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-fragments-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-fragments-packets threshold 8	(Optional) configure fragment alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
25	Raisecom(config-gpon-onu-snmp-trap-profile:*) #ethernet-jabbers-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#ethernet-jabbers-packets threshold 8	(Optional) configure Jabber frame alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
26	Raisecom(config-gpon-onu-snmp-trap-profile:*) #mac-bridge-port-delay-exceeded-discard-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#mac-bridge-port-delay-exceeded-discard-packets threshold 8	(Optional) configure alarm threshold of discarded frame due to timeout. value: alarm threshold, an integer, ranging from 0 to 100
27	Raisecom(config-gpon-onu-snmp-trap-profile:*) #mac-bridge-port-mtu-exceeded-discard-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#mac-bridge-port-mtu-exceeded-discard-packets threshold 8	(Optional) configure alarm threshold of discarded frame due to oversized MTU. value: alarm threshold, an integer, ranging from 0 to 100
28	Raisecom(config-gpon-onu-snmp-trap-profile:*) #mac-bridge-port-rx-error-discard-packets threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#mac-bridge-port-rx-error-discard-packets threshold 8	(Optional) configure Rx error frame alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100
29	Raisecom(config-gpon-onu-snmp-trap-profile:*) #fec-corrected-bytes threshold <i>value</i> example: Raisecom(config-snmp-trap-gpon-onu-profile:10)#fec-corrected-bytes threshold 8	(Optional) configure FEC corrected byte alarm threshold. value: alarm threshold, an integer, ranging from 0 to 100

Step	Command	Description
30	Raisecom(config-gpon-onu-snmpt-trap-profile:*)# fec-corrected-code-words threshold <i>value</i> example: Raisecom(config-snmpt-trap-gpon-onu-profile:10)#fec-corrected-code-words threshold 8	(Optional) configure FEC corrected code word alarm threshold. • value: alarm threshold, an integer, ranging from 0 to 100
31	Raisecom(config-gpon-onu-snmpt-trap-profile:*)# fec-uncorrected-code-words threshold <i>value</i> example: Raisecom(config-snmpt-trap-gpon-onu-profile:10)#fec-uncorrected-code-words threshold 8	(Optional) configure FEC corrected code word alarm threshold. • value: alarm threshold, an integer, ranging from 0 to 100
32	Raisecom(config-gpon-onu-snmpt-trap-profile:*)# fec-seconds threshold <i>value</i> example: Raisecom(config-snmpt-trap-gpon-onu-profile:10)#fec-seconds threshold 10	(Optional) configure FEC duration alarm threshold. • value: alarm threshold, an integer, ranging from 0 to 100

Binding ONU profile

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# gpon-onu slot-id/olt-id/onu-id example: Raisecom(config)#gpon-onu 3/2/1	Enter GPON ONU remote management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID on the PON interface
3	Raisecom(config-gpon-onu-*/*:*)# snmpt-trap-gpon-onu-profile profile-id example: Raisecom(config-gpon-onu-3/2:1)#snmpt-trap-gpon-onu-profile 10	Configure the ONU bound alarm profile. You can use the no snmpt-trap-gpon-onu-profile command to cancel the binding. • profile-id: profile index, an integer, ranging from 1 to 50

3.6.4 Checking configurations

No.	Command	Description
1	Raisecom# show snmpt-trap-gpon-olt-profile profile-id	Show OLT alarm profile configurations.
2	Raisecom# show interface gpon-olt slot-id/olt-list basic information	Show binding relationship between the OLT GPON interface and alarm profile.
3	Raisecom# show snmpt-trap-gpon-onu-profile { all profile-list }	Show ONU alarm profile configurations.

No.	Command	Description
4	<code>Raisecom#show gpon-onu slot-id/olt-id/onu-id snmp-trap-profile</code>	Show binding relationship between the ONU and alarm profile.

3.7 Configuring DBA profile

3.7.1 Default configurations

Default configurations of the DBA profile with a default ID of 1 on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
DBA profile ID	• GPON and XGPON: 1 • XGPON ONU: 517 • EPON: 516
DBA profile name	Profile-1
DBA profile type	Type 3
Fixed bandwidth	0 kbit/s
Assured bandwidth	1024 kbit/s
Maximum bandwidth	1024000 kbit/s
Priority (DBA priority)	0
Weight (DBA weight)	0

3.7.2 Creating DBA profile

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#create dba-profile profile-id name profile-name type1 fix fix-bandwidth</code>	Create the DBA profile of the fixed bandwidth type. You can use the no create dba-profile profile-id command to delete the profile.
	<code>Raisecom(config)#create dba-profile profile-id name profile-name type2 assure assure-bandwidth</code>	Create the DBA profile of the assured bandwidth type. You can use the no create dba-profile profile-id command to delete the profile.
	<code>Raisecom(config)#create dba-profile profile-id name profile-name type3 assure assure-bandwidth max max-bandwidth</code>	Create the DBA profile of the assured bandwidth+maximum bandwidth type. You can use the no create dba-profile profile-id command to delete the profile.

Step	Command	Description
	Raisecom(config)# create dba-profile <i>profile-id</i> name <i>profile-name</i> type4 max <i>max-bandwidth</i>	Create the DBA profile of the maximum bandwidth type. You can use the no create dba-profile <i>profile-id</i> command to delete the profile.
	Raisecom(config)# create dba-profile <i>profile-id</i> name <i>profile-name</i> type5 fix <i>fix-bandwidth</i> assure <i>assure-bandwidth</i> max <i>max-bandwidth</i>	Create the DBA profile of the fixed bandwidth+assured bandwidth+maximum bandwidth type. You can use the no create dba-profile <i>profile-id</i> command to delete the profile.



Note

The profile in use cannot be deleted.

3.7.3 Modifying DBA profile

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# dba-profile <i>profile-id</i> name <i>profile-name</i> example: Raisecom(config)#dba-profile 1 name raisecom	Modify the name of the DBA profile. - dba-profile profile-id: template ID, an integer, ranging from 1 to 517. By default, profile 1 is created for GPON, profile 517 is created for XGSPON, and profile 516 is created for EPON, which can be modified. - name profile-name: template name, a string of 1 to 16 characters
	Raisecom(config)# dba-profile [<i>profile-id</i> name <i>profile-name</i>] type1 fix <i>fix-bandwidth</i> example: Raisecom(config)#dba-profile 10 type1 fix 1024	Modify the DBA profile of the fixed bandwidth type. fix fix-bandwidth: fixed bandwidth, which is fixedly allocated to users. Even though the fixed bandwidth is not used, it cannot be occupied by other users. It is an integer ranging from 1 to 12288000.
	Raisecom(config)# dba-profile [<i>profile-id</i> name <i>profile-name</i>] type2 assure <i>assure-bandwidth</i> [method { sr tm }] example: Raisecom(config)#dba-profile 10 type2 assure 1024	Modify the DBA profile of the assured bandwidth type. assure assure-bandwidth: guaranteed bandwidth. When the guaranteed bandwidth is allocated to users, if users do not use the bandwidth, other users can occupy the bandwidth. It is an integer ranging from 1 to 1228800.

Step	Command	Description
	<pre>Raisecom(config)#dba-profile [profile-id name profile- name]type3 assure assure- bandwidth max max-bandwidth [method { sr tm }] example: Raisecom(config)#dba-profile 10 type3 assure 1024 max 2000</pre>	Modify the DBA profile of the assured bandwidth+maximum bandwidth type. - fix fix-bandwidth: fixed bandwidth, which is fixedly allocated to users. Even though the fixed bandwidth is not used, it cannot be occupied by other users. It is an integer ranging from 1 to 12288000. - max max-bandwidth: max max-bandwidth: maximum bandwidth, which means the maximum bandwidth available to users. It is an integer ranging from 1 to 12288000. In a type3 DBA template, the maximum bandwidth must be greater than or equal to the guaranteed bandwidth. In a type5 DBA template, the maximum bandwidth must be greater than or equal to the sum of the fixed bandwidth and the guaranteed bandwidth.
	<pre>Raisecom(config)#dba-profile [profile-id name profile- name]type4 max max-bandwidth [priority priority] [weight weight] [method { sr tm }] example: Raisecom(config)#create dba- profile 10 type4 max 2000</pre>	Modify the DBA profile of the maximum bandwidth type.
	<pre>Raisecom(config)#dba-profile [profile-id name profile- name]type5 fix fix-bandwidth assure assure-bandwidth max max-bandwidth [additional- bandwidth non-assure] [method { sr tm }] Raisecom(config)#dba-profile [profile-id name profile- name] type5 fix fix-bandwidth assure assure-bandwidth max max-bandwidth additional- bandwidth best-effort [priority priority] [weight weight] [method { sr tm }] example: Raisecom(config)#dba-profile 10 type5 fix 1000 assure 1024 max 2000</pre>	Modify the DBA profile of the fixed bandwidth+assured bandwidth+maximum bandwidth type.



Note

- The profile to be modified must exist.
- The profile in use cannot be modified.

3.7.4 Checking configurations

No.	Command	Description
1	Raisecom# show dba-profile { all <i>profile-list</i> }	Show DBA profile configurations.

3.8 Configuring line profile

3.8.1 Default configurations

There is a default GPON ONU line profile with the ID of 1024 and a default XGSPON ONU line profile with the ID of 1025 on the ISCOM6800 and ISCOM6860. Their configurations are as below.

Function	Default value
XGPON ONU line profile ID	1025
GPON/XGPON line profile ID	1024

3.8.2 Configuring line profile

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# gpon-onu-line-profile <i>profile-id</i> example: Raisecom(config)#gpon-onu-line-profile 10	Create the line profile and enter line profile configuration mode. You can use the no gpon-onu-line-profile <i>profile-id</i> command to delete the profile.  Note • If the profile exists, enter profile configuration mode directly. • If the profile does not exist, you need to create the profile first, and then enter profile configuration mode.
3	Raisecom(config-gpon-onu-line-profile:*)# name <i>profile-name</i> example: Raisecom(config-gpon-onu-line-profile:10)#name raisecom	(Optional) configure the profile name. • profile-id: line profile ID, an integer, ranging from 1 to 128
4	Raisecom(config-gpon-onu-line-profile:*)# omcc encryption { enable disable }	(Optional) enable/disable OMCC encryption.

Step	Command	Description
5	<code>Raisecom(config-gpon-onu-line-profile:*)#fec upstream { enable disable }</code>	(Optional) enable FEC on the uplink channel.
6	<code>Raisecom(config-gpon-onu-line-profile:*)#create gem gem-index tcont tcont-id</code>	(Optional) create the GEM port and configure its binding relationship with T-CONT. You can use the no create gem gem-index command to delete the configuration.
7	<code>Raisecom(config-gpon-onu-line-profile:*)#mapping mode { vlan vlan-pri pri port port-vlan port-pri port-vlan-pri }</code> example: <code>Raisecom(config-gpon-onu-line-profile:10)#mapping mode vlan</code>	(Optional) configure mapping between the GEM port and services. • vlan: based on VLAN mapping • vlan-pri: based on VLAN+802.1p priority mapping • pri: based on priority mapping • port: based on ETH interface mapping • port-vlan: based on ETH interface + VLAN mapping • port-pri: based on ETH interface + 802.1p priority mapping • port-vlan-pri: based on ETH interface + VLAN+802.1p priority mapping
8	<code>Raisecom(config-gpon-onu-line-profile:*)#gem gem-index mapping mapping-index { vlan vlan-id [priority pri] } priority pri ethernet port-id ethernet port-id vlan vlan-id [priority pri] ethernet port-id priority pri }</code> <code>Raisecom(config-gpon-onu-line-profile:*)#gem gem-index mapping mapping-index priority pri</code> <code>Raisecom(config-gpon-onu-line-profile:*)#gem gem-index mapping mapping-index { ethernet port-id ip-host ip-host-id veip veip-id } [priority pri]</code> <code>Raisecom(config-gpon-onu-line-profile:*)# gem gem-index mapping mapping-index { ethernet port-id ip-host ip-host-id veip veip-id } vlan vlan-id [priority pri]</code> example: <code>Raisecom(config-gpon-onu-line-profile:10)#gem 1 mapping 5 vlan 20</code>	(Optional) configure mapping between the GEM port and ONU-side services. You can use the no gem gem-index mapping mapping-index command to delete the mapping. • gem gem-index: GEM Port index, an integer, ranging from 1 to 128 • mapping mapping-index: Mapping index, an integer, ranging from 1 to 8 • vlan vlan-id: VLAN mapping mode. Configure this parameter when you need to map the service flow of the specified VLAN to the GEM Index. The vlan-id argument is an integer, ranging from 1 to 4094. If you specify a VLAN and continue to specifying the priority, adopt the VLAN+priority mapping mode. • priority pri: priority mapping mode, an integer, ranging from 0 to 7 • ethernet port-id: ETH interface mapping mode. Configure this parameter when you need to map the service flow of the ETH port to the specified GEM Index. • port-id: an integer, ranging from 1 to 24. If you specify an interface and continue to specifying a VLAN, use the interface + VLAN mapping mode. If you specify an interface and continue to specifying the priority, use the interface + priority mapping mode. If you specify an interface and a VLAN and continue to specifying the priority, use the interface + VLAN + priority mapping mode.

Step	Command	Description
9	<pre>Raisecom(config-gpon-onu-line-profile:*)#gem gem-index encryption { enable disable } encryption-us { enable disable } example: Raisecom(config-gpon-onu-line-profile:10)#gem 20 encryption enable</pre>	(Optional) enable/disable GEM port encryption. - gem gem-index: GEM Port index, an integer, ranging from 1 to 128 - enable: enable GEM Prot encryption. - disable: disable GEM Prot encryption. - encryption-us: encrypt the uplink packets.
10	<pre>Raisecom(config-gpon-onu-line-profile:*)#gem gem-index { upstream downstream } policing-profile profile-id Raisecom(config-gpon-onu-line-profile:*)#gem gem-index { upstream downstream } policing-profile-name profile-name example: Raisecom(config-gpon-onu-line-profile:10)#gem 1 upstream policing-profile 5</pre>	(Optional) bind the GEM port with the rate limiting profile to limit the rate of GEM port. You can use the no gem gem-index { upstream downstream } policing-profile command to cancel the binding.  Note - For uplink rate limiting, support the maximum bandwidth and maximum burst size. - For downlink rate limiting, support the assured bandwidth and assured burst size, and maximum bandwidth and maximum burst size.
11	<pre>Raisecom(config-gpon-onu-line-profile:*)#gem gem-index priority-queue priority-queue-id</pre>	(Optional) modify the priority queue of the GEM port.
12	<pre>Raisecom(config-gpon-onu-line-profile:*)#gem gem-index mac- address-learning limit count example: Raisecom(config-gpon-onu-line-profile:10)#gem 1 mac-address- learning limit 100</pre>	(Optional) configure MAC address learning limit on the GEM port. You can use the no gem gem-index mac-address-learning limit command to restore default configuration. - gem gem-index: GEM Port index, an integer, ranging from 1 to 128 - limit count: MAC address limit, an integer, ranging from 0 to 126 where 0 indicates that there is no limit to MAC addresses
13	<pre>Raisecom(config-gpon-onu-line-profile:*)#create tcont tcont-id dba-profile profile-id Raisecom(config-gpon-onu-line-profile:*)#create tcont tcont-id dba-profile-name profile-name example: Raisecom(config-gpon-onu-line-profile:10)#create tcont 2 dba- profile 5</pre>	(Optional) create the T-CONT and configure its binding relationship with the DBA profile. You can use the no create tcont tcont-id command to delete the configuration. - tcont tcont-id: T-CONT ID, an integer, ranging from 1 to 31 - dba-profile profile-id: DBA template ID, an integer, ranging from 1 to 516
14	<pre>Raisecom(config-gpon-onu-line-profile:*)#tcont tcont-id dba- profile profile-id example: Raisecom(config-gpon-onu-line-profile:10)#tcont 2 dba-profile 9</pre>	(Optional) modify the DBA profile bound to TCONT. - tcont tcont-id: T-CONT ID, an integer, ranging from 0 to 31 - dba-profile profile-id: DBA template ID, an integer, ranging from 1 to 516

Configure the device that needs to enter the line profile with the template name as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# gpon-onu-line-profile name profile-name Raisecom(config-gpon-onu-line-profile:*)# example: Raisecom(config)# gpon-onu-line-profile name raisecom Raisecom(config-gpon-onu-line-profile:*)#	Enter line profile configuration mode through profile name. - tcont tcont-id: T-CONT ID, an integer, ranging from 0 to 31 - dba-profile-name name: profile name, a string of 1 to 16 characters

3.8.3 Binding line profile

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface gpon-onu slot-id/olt-id/onu-id example: Raisecom(config)# interface gpon-onu 3/2/1	Enter GPON ONU virtual interface mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID on the PON interface
3	Raisecom(config-if-gpon-onu-*/*:*)# line-profile-id profile-id example: Raisecom(config-if-gpon-onu-3/1:1)# line-profile-id 10	(Optional) change the line profile configured on the ONU through modifying the line profile ID. profile-id: line profile ID, an integer, ranging from 1 to 1025
	Raisecom(config-if-gpon-onu-*/*:*)# line-profile-name profile-name example: Raisecom(config-if-gpon-onu-3/1:1)# line-profile-name raisecom	(Optional) change the line profile configured on the ONU through modifying the line profile name. profile-name: line profile name, a string of 1 to 16 characters



Note

- When you change the line profile configured on the ONU through modifying the line profile ID, the system will automatically update the profile name to make it consistent with the new profile.
- When you change the line profile configured on the ONU through modifying the line profile name, the system will automatically update the profile ID to make it consistent with the new profile.

3.8.4 Checking configurations

No.	Command	Description
1	Raisecom# show gpon-onu-line-profile { all profile-list }	Show line profile configurations.

No.	Command	Description
2	Raisecom# show gpon-onu-line-profile name <i>profile-name</i>	Show information about the line profile by name.

3.9 Configuring service profile

3.9.1 Default configurations

N/A

3.9.2 Configuring profile

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# gpon-onu-service-profile <i>profile-id</i> example: Raisecom(config)#gpon-onu-service-profile 10	Create a service template and enter service template configuration mode. You can use the no gpon-onu-service-profile <i>profile-id</i> command to delete the template.  Note • If the template exists, the system will directly enter template configuration mode. • If the template does not exist, the system will create a template before entering template configuration mode. • profile-id: service template ID, an integer, ranging from 1 to 1024
3	Raisecom(config-gpon-onu-service-profile:*)# name <i>profile-name</i> example: Raisecom(config-gpon-onu-service-profile:10)#name raisecom	(Optional) configure the name of the service profile. • profile-name: template name, a string of 1 to 16 characters
4	Raisecom(config-gpon-onu-service-profile:*)# port-num { ethernet <i>eth-id</i> [pots <i>pots-id</i>] pots <i>pots-id</i> veip <i>veip-id</i> catv <i>pots-id</i> } example: Raisecom(config-gpon-onu-service-profile:10)#port-num ethernet 4 pots 2	(Optional) configure the number of ONU interfaces. • ethernet eth-id: number of Ethernet interfaces, an integer, ranging from 0 to 24 • pots pots-id: number of voice interfaces, an integer, ranging from 0 to 24 • veip veip-id: number of virtual Ethernet interfaces, an integer, ranging from 0 to 4 • catv pots-num: the number of CATV interfaces, an integer, ranging from 0 to 1

Step	Command	Description
5	Raisecom(config-gpon-onu-service-profile:*)# mac-address-table learning { enable disable }	(Optional) enable/disable dynamic MAC address learning on the ONU.
6	Raisecom(config-gpon-onu-service-profile:*)# switchport isolation { enable disable }	(Optional) enable/disable ONU UNI isolation.
7	Raisecom(config-gpon-onu-service-profile:*)# mac-address-table dlfc discard { enable disable }	(Optional) enable/disable ONU DLF packet discarding.
8	Raisecom(config-gpon-onu-service-profile:*)# mac-address-table aging-time aging-time example: Raisecom(config-gpon-onu-service-profile:10)#mac-address-table aging-time 100	(Optional) configure the aging time of the service template MAC address table. • 0: aging time. The value 0 indicates that dynamic MAC address entries are not aged out. • period: aging time, in units of second, an integer. The OLT MAC address table ranges from 10 to 1000000; the ONU MAC address table ranges from 5 to 57 600.
9	Raisecom(config-gpon-onu-service-profile:*)#{ uni ethernet uni-list veip id } igmp-forward { translation vlan-id [priority] transparent tag vlan-id [priority] } example: Raisecom(config-gpon-onu-service-profile:10)#veip 1 igmp-forward transparent	(Optional) configure the policy for the ONU Ethernet interface or VEIP interface to process packets of uplink multicast VLAN. • uni ethernet uni-list: ONU UNI list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • veip id: ID of the uplink virtual interface at the ONU LAN side, an integer, ranging from 1 to 4 • translation: translate the VLAN of the uplink multicast packets. • transparent: transparently transmit the VLAN of the uplink multicast packets. • tag: add the VLAN ID to the uplink multicast packets. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • priority: VLAN priority, an integer, ranging from 0 to 7
10	Raisecom(config-gpon-onu-service-profile:*)#{ uni ethernet uni-list veip id } multicast vlan { strip transparent translation vlan-id } example: Raisecom(config-gpon-onu-service-profile:10)#veip 1 multicast vlan strip	(Optional) configure the policy for the ONU Ethernet interface or VEIP interface to process downlink multicast VLAN. You can use the no { uni ethernet uni-list veip id } multicast vlan command to restore default configuration. • uni ethernet uni-list: ONU UNI list, an integer, ranging from 1 to 24 . It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • veip id: ID of the uplink virtual interface at the ONU LAN side, an integer, ranging from 1 to 4 • strip: VLAN strip mode • transparent: VLAN transparent transmission mode • translation: VLAN translation mode • vlan-id: translating VID, an integer, ranging from 1 to 4094

Step	Command	Description
11	<pre>Raisecom(config-gpon-onu- service-profile:*)#{ uni ethernet uni-list veip id } igmp-version { v2 v3 } example: Raisecom(config-gpon-onu- service-profile:10)#veip 1 igmp- version v2</pre>	(Optional) configure the IGMP version of the ONU Ethernet interface or VEIP interface. • uni ethernet uni-list: ONU UNI list, an integer, ranging from 1 to 24 . It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • veip id: ID of the uplink virtual interface at the ONU LAN side, an integer, ranging from 1 to 4 • v2: IGMP version 2 • v3: IGMP version 3
12	<pre>Raisecom(config-gpon-onu- service-profile:*)#{ uni ethernet uni-list veip id } immediate-leave enable example: Raisecom(config-gpon-onu- service-profile:10)#veip 1 immediate-leave enable</pre>	(Optional) enable immediate leave on the ONU Ethernet interface or VEIP interface. You can use the disable form to disable this function. • uni ethernet uni-list: ONU UNI list, an integer, ranging from 1 to 24 . It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • veip id: ID of the uplink virtual interface at the ONU LAN side, an integer, ranging from 1 to 4 • enable: enable immediate leave. • disable: disable immediate leave.
13	<pre>Raisecom(config-gpon-onu- service-profile:*)#{ uni ethernet uni-list veip id } mcast-vlan vlan-list example: Raisecom(config-gpon-onu- service-profile:10)#veip 1 mcast-vlan 1-4</pre>	(Optional) configure the multicast VLAN list of the ONU Ethernet interface or VEIP interface. • ONU UNI list, an integer, ranging from 1 to 24 . It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • veip id: ID of the uplink virtual interface at the ONU LAN side, an integer, ranging from 1 to 4 • vlan-list: multicast VLAN list, an integer, ranging from 1 to 4094
14	<pre>Raisecom(config-gpon-onu- service-profile:*)#{ uni ethernet uni-list veip id } unauth-join enable example: Raisecom(config-gpon-onu- service-profile:10)#veip 1 unauth-join enable</pre>	(Optional) configure unauthenticated join of the ONU Ethernet interface or VEIP interface. You can use the disable form to disable this function. • uni ethernet uni-list: ONU UNI list, an integer, ranging from 1 to 24 . It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • veip id: ID of the uplink virtual interface at the ONU LAN side, an integer, ranging from 1 to 4 • enable: enable unauthorized Join. • disable: disable unauthorized Join.
15	<pre>Raisecom(config-gpon-onu- service-profile:*)#{ uni ethernet uni-list veip id } work-mode { multicast-ctrl normal } example: Raisecom(config-gpon-onu- service-profile:10)#veip 1 work- mode multicast-ctrl</pre>	(Optional) enable the working mode of the ONU Ethernet interface or VEIP interface. • uni ethernet uni-list: ONU UNI list, an integer, ranging from 1 to 24 . It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • veip id: ID of the uplink virtual interface at the ONU LAN side, an integer, ranging from 1 to 4 • multicast-ctrl: controllable multicast mode • normal: normal mode

Step	Command	Description
16	<pre>Raisecom(config-gpon-onu- service-profile:*)#multicast vlan translation vlan-id example: Raisecom(config-epon-onu- ethernet-3/1/1:1)#multicast vlan translation 1</pre>	(Optional) configure the destination VLAN ID for the ONU to translate downlink multicast VLAN. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
17	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet uni-id vlan mode { transparent tagged translation aggregation trunk } example: Raisecom(config-gpon-onu- service-profile:10)#uni ethernet 1-4 vlan mode tagged</pre>	(Optional) configure the VLAN mode of the ONU UNI. You can use the no uni ethernet uni-id vlan mode command to restore default configuration. • uni-id: ONU UNI list, an integer, ranging from 1 to 24 . It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • tagged: VLAN tagged mode • translation: translation mode • transparent: transparent transmission mode • aggregation: aggregation mode • trunk: Trunk mode
18	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet uni-id native vlan vlan-id [priority] example: Raisecom(config-gpon-onu- service-profile:10)#uni ethernet 1-4 native vlan 5</pre>	(Optional) configure the default VLAN ID of the ONU UNI. You can use the no uni ethernet uni-id native vlan command to restore default configuration. • uni-list: ONU UNI list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • vlan vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • priority: VLAN priority, an integer, ranging from 0 to 7
19	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet uni-id vlan translation-rule rule-id example: Raisecom(config-gpon-onu- service-profile:10)#uni ethernet 1-4 vlan translation-rule 2</pre>	(Optional) configure the VLAN mapping rule of the ONU UNI. You can use the no uni ethernet uni-id vlan translation-rule command to restore default configuration. • uni-list: ONU UNI ID, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • rule-list: VLAN translation rule ID, an integer, ranging from 1 to 2048. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". The number of rule IDs entered should not exceed 7.

Step	Command	Description
20	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet uni-id vlan aggregation-rule rule-id example: Raisecom(config-gpon-onu- service-profile:10)#uni ethernet 1-4 vlan aggregation-rule 2</pre>	(Optional) configure the VLAN aggregation rule of the ONU UNI. You can use the no uni ethernet uni-id vlan aggregation-rule command to restore default configuration. • uni-list: ONU UNI index, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • rule-list: VLAN aggregation rule index, an integer, ranging from 1 to 2048. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". The number of rule IDs entered should not exceed 8.
21	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet uni-id vlan trunk allowed vlan- list example: Raisecom(config-gpon-onu- service-profile:10)#uni ethernet 1-4 vlan trunk allowed 100-150</pre>	(Optional) configure the VLAN lists allowed to pass through the ONU UNI in Trunk mode. You can use the no uni ethernet uni-id vlan trunk allowed command to restore default configuration. • uni-list: ONU UNI index, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • vlan-list: VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". It supports configuring up to 8 VLANs.
22	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet uni-id mac-address-table threshold { value unlimited } example: Raisecom(config-gpon-onu- service-profile:10)#uni ethernet 1-4 mac-address-table threshold 20</pre>	(Optional) configure the threshold of MAC addresses on the ONU UNI. You can use the no uni ethernet uni-id mac-address-table threshold command to restore default configuration. • uni-list: ONU UNI index, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • value: threshold, an integer, ranging from 1 to 128 • unlimited: unlimited
23	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet uni-id max-frame-size size example: Raisecom(config-gpon-onu- service-profile:10)#uni ethernet 1-4 max-frame-size 1600</pre>	(Optional) configure the maximum frame size allowed to pass through the ONU UNI. You can use the no uni ethernet uni-id max-frame-size command to restore default configuration. • uni-list: ONU UNI index, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • size: maximum frame length, an integer, ranging from 1 to 65535

Step	Command	Description
24	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet uni-id { ingress egress } policing-profile profile-id Raisecom(config-gpon-onu- service-profile:*)#uni ethernet uni-list { ingress egress } policing-profile-name profile- name example: Raisecom(config-gpon-onu- service-profile:10)#uni ethernet 1-4 ingress policing-profile 5</pre>	(Optional) bind a rate-limit profile to the ONU UNI. You can use the no uni ethernet uni-list { ingress egress } command to restore default configuration. • uni-list: ONU UNI index, an integer, ranging from 1 to 24 . It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • ingress: rate limiting over data in the uplink direction • egress: rate limiting over data in the downlink direction • profile-id: rate-limiting profile ID, an integer, ranging from 1 to 1024
25	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet id vlan drop-untagged enable example: Raisecom(config-gpon-onu- service-profile:10)#uni ethernet 1 vlan drop-untagged enable</pre>	(Optional) enable the ONU Ethernet interface to discard untagged packets. You can use the disable form to disable this function. • uni ethernet id: ONU user-side Ethernet interface index, an integer, ranging from 1 to 24
26	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet id vlan dot1q-tunnel enable example: Raisecom(config-gpon-onu- service-profile:1)#uni ethernet 1 vlan dot1q-tunnel enable</pre>	(Optional) enable Tunnel on the ONU Ethernet interface. You can use the disable form to disable this function. • uni ethernet id: ONU user-side Ethernet interface index, an integer, ranging from 1 to 24
27	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet vlan dot1q-tunnel enable</pre>	(Optional) enable the service template to enable Tunnel on the Ethernet interface. You can use the disable form of this command to disable this function.
28	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet uni-list pre-alloc-vlan-num vlan-num example: Raisecom(config-gpon-onu- service-profile:10)#uni ethernet 1-4 pre-alloc-vlan-num 10</pre>	(Optional) configure the number of pre-assigned VLANs on the ONU UNI. • uni-list: ONU UNI index, an integer, ranging from 1 to 24 . It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • vlan-num: the number of VLANs, an integer, ranging from 0 to 4094
29	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet id poe pse { enable disable }</pre>	Enable PoE power supply on the ONU Ethernet interface. Use the disable form of this command to disable this function.
30	<pre>Raisecom(config-gpon-onu- service-profile:*)#uni ethernet uni-list mctrl package package- list example: Raisecom(config-gpon-onu- service-profile:10)#uni ethernet 1-4 mctrl package 1-10</pre>	(Optional) configure binding the controllable multicast package on the ONU UNI. • uni-list: ONU UNI index, an integer, ranging from 1 to 24 . It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • package-list: package list, an integer, ranging from 1 to 128

Step	Command	Description
31	Raisecom(config-gpon-onu-service-profile:*)# veip <i>veip-id</i> tr-069-profile <i>profile-id</i> example: Raisecom(config-gpon-onu-service-profile:1)#veip 1 tr-069-profile 10	(Optional) bind the service template with the TR069 template. • veip-id: ID of the uplink virtual interface at the LAN side, an integer, ranging from 1 to 4 • profile-id: TR069 management template ID, an integer, ranging from 1 to 64
32	Raisecom(config-gpon-onu-service-profile:*)# veip <i>veip-id</i> iphost <i>iphost-id</i> example: Raisecom(config-gpon-onu-service-profile:10)#veip 1 iphost 8	(Optional) bind the service template with the specified IPhost interface. • veip-id: ID of the uplink virtual interface at the ONU LAN side, an integer, ranging from 1 to 4 • iphost-id: ONU IPhost interface ID, an integer, ranging from 0 to 8
33	Raisecom(config-gpon-onu-service-profile:*)# iphost-num <i>iphost-num</i> example: Raisecom(config-gpon-onu-service-profile:10)#iphost-num 8	(Optional) configure the maximum number of IPhost interfaces. • iphost-num: maximum number of IPhost interfaces, an integer, ranging from 0 to 8
34	Raisecom(config-gpon-onu-service-profile:*)# iphost index mode { dhcp pppoe static } example: Raisecom(config-gpon-onu-service-profile:10)#iphost 2 mode dhcp	(Optional) configure the internet access mode of the IPhost interface. • index: IPhost interface index, an integer, ranging from 1 to 8 • dhcp: the IPhost interface adopts dynamic host configuration mode, which means that the device can automatically obtain an IP address for accessing the Internet. • pppoe: the IPhost interface adopts Ethernet P2P mode, which means that the device accesses the Internet through PPPoE dialing. • static: the IPhost interface adopts static operation mode to access the Internet.
35	Raisecom(config-gpon-onu-service-profile:*)# iphost index native vlan <i>id</i> [<i>priority</i>] example: Raisecom(config-gpon-onu-service-profile:10)#iphost 2 native vlan 100	(Optional) configure the local VLAN of the IPhost interface. • index: IPhost interface index, an integer, ranging from 0 to 8 • id: local VLAN ID, an integer, ranging from 1 to 4094 • priority: priority, an integer, ranging from 0 to 7
36	Raisecom(config-gpon-onu-service-profile:*)# iphost index pre-alloc-vlan-num <i>num</i> example: Raisecom(config-gpon-onu-service-profile:10)#iphost 2 pre-alloc-vlan-num 10	(Optional) configure the number of pre-assigned VLANs on the IPhost interface. • index: IPhost interface index, an integer, ranging from 1 to 8 • num: the number of pre-allocated VLANs, an integer, ranging from 0 to 4094

Step	Command	Description
37	<pre>Raisecom(config-gpon-onu- service-profile:*)#iphost index service { internet iptv voip-sinalling voip-media management }* example: Raisecom(config-gpon-onu- service-profile:10)#iphost 2 service internet</pre>	(Optional) configure the service type of the IPhost interface. • index: IPhost interface index, an integer, ranging from 1 to 8 • internet: Internet access channel, the WAN interface automatically generates static routes only. • iptv: IPTV channel, applied to the IPTV-supportive device only • voip-sinalling: voice signalling channel, applied to voice-supportive device only • voip-media: voice media channel, applied to voice-supportive device only • management: management channel, the WAN interface automatically generates policy routes only. • pppoe-srv-name name: PPPOE server name
38	<pre>Raisecom(config-gpon-onu- service-profile:*)#iphost index type { ipv4 ipv6 both } example: Raisecom(config-gpon-onu- service-profile:1)#iphost 1 type ipv4</pre>	(Optional) configure the IP address type of the IPhost. • index: iphost ID, an integer, ranging from 1 to 8 • ipv4: configure the IP address type of the iphost to ipv4. • ipv6: configure the IP address type of the iphost to ipv6. • both: configure the IP address type of the iphost to ipv4 + ipv6.
39	<pre>Raisecom(config-gpon-onu- service-profile:*)#iphost index access-control { http https ping telnet } { enable disable }</pre>	(Optional) configure the access control mode of the IPhost interface based on WAN connection.
40	<pre>Raisecom(config-gpon-onu- service-profile:*)#voip-protocol { sip h248 } example: Raisecom(config-gpon-onu- service-profile:10)#voip- protocol h248</pre>	(Optional) configure the voice protocol type of the service template. • h248: H.248 • sip: SIP
41	<pre>Raisecom(config-gpon-onu- service-profile:*)#country-code { num china undefine } example: Raisecom(config-gpon-onu- service-profile:10)#country-code china</pre>	(Optional) configure the country code of the service template. • num: country code, an integer, ranging from 0 to 1023 • china: China country code serial number (12) • undefined: undefined country
42	<pre>Raisecom(config-gpon-onu- service-profile:*)#time-zone { num beijing undefine } example: Raisecom(config-gpon-onu- service-profile:10)#time-zone beijing</pre>	(Optional) configure the timezone code of the service template. • num: time zone code, an integer, ranging from 0 to 395 • Beijing: Beijing time zone • undefined: undefined country code

Step	Command	Description
43	Raisecom(config-gpon-onu-service-profile:*)# commit	Submit template configurations to validate the profile.  Caution For any parameter modifications in ONU service profile configuration mode, you must execute the commit command to validate them.
44	Raisecom(config-gpon-onu-service-profile:*)# manage-server iphost index primary-domain priname [no backup-domain backup-domain bakname] Raisecom(config-gpon-onu-service-profile:*)# manage-server iphost index no primary-domain [no backup-domain backup-domain bakname]	(Optional) configure the master/slave domain name of the IPhost interface on the management server. Use the no manage-server command to delete the configuration.

Entering profile with profile name

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# gpon-onu-service-profile profile-id example: Raisecom(config)#gpon-onu-service-profile 10	Create a service template and enter service template configuration mode. You can use the no gpon-onu-service-profile profile-id command to delete this template.  Note • If the template already exists, the system directly enters template configuration mode. • If the template does not exist, the system first creates a template and then enter template configuration mode. • profile-id: service template ID, an integer, ranging from 1 to 128
3	Raisecom(config-gpon-onu-service-profile:*)# name profile-name example: Raisecom(config-gpon-onu-service-profile:10)#name raisecom	Configure the profile name. • profile-name: profile name, a string of 1 to 16 characters
4	Raisecom(config-gpon-onu-service-profile:*)# exit Raisecom(config)# gpon-onu-service-profile name profile-name example: Raisecom(config)#gpon-onu-service-profile name raisecom	Enter service profile configuration mode through profile name. • profile-name: profile name, a string of 1 to 16 characters

3.9.3 Binding service profile

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface gpon-onu slot-id/olt-id/onu-id example: Raisecom(config)#interface gpon-onu 3/2/1	Enter GPON ONU virtual interface mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID on the PON interface
3	Raisecom(config-if-gpon-onu-*/*:*)#service-profile-id profile-id example: Raisecom(config-if-gpon-onu-3/1:1)#service-profile-id 10	(Optional) change the service profile configured on the ONU through modifying the service profile ID. profile-id: service template ID, an integer, ranging from 1 to 1024
	Raisecom(config-if-gpon-onu-*/*:*)#service-profile-name profile-name example: Raisecom(config-if-gpon-onu-3/1:1)#service-profile-name raisecom	(Optional) change the service profile configured on the ONU through modifying the service profile name. profile-name: service template name, a string of 1 to 16 characters



Note

- When you change the service profile configured on the ONU through modifying the service profile ID, the system will automatically update the profile name to make it consistent with the new profile.
- When you change the service profile configured on the ONU through modifying the service profile name, the system will automatically update the profile ID to make it consistent with the new profile.

3.9.4 Checking configurations

No.	Command	Description
1	Raisecom#show gpon-onu-service-profile { all name profile-name profile-list }	Show service profile configurations.

3.10 Configuring rate limit profile

3.10.1 Default configuration

N/A

3.10.2 Configuring profile

No.	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#create policing-profile <i>profile-id</i> name <i>profile-name</i> example: Raisecom(config)#create policing-profile 10 name raisecom	Create a rate limit profile. You can use the no create policing-profile <i>profile-id</i> command to delete the profile. • profile-id: rate-limiting template ID, an integer, ranging from 1 to 1024 • profile-name: rate-limiting template name, a string of 1 to 16 characters
3	Raisecom(config)#policing- profile <i>profile-id</i> name <i>profile-name</i> example: Raisecom(config)#policing- profile 10 name raisecom	(Optional) modify the name of the rate limit profile. • profile-id: rate-limiting template ID, an integer, ranging from 1 to 1024 • profile-name: rate-limiting template name, a string of 1 to 16 characters
4	Raisecom(config)#policing- profile [<i>profile-id</i> name <i>profile-name</i>] cir cir pir pir cbs cbs pbs pbs example: Raisecom(config)#policing- profile 1 cir 1024 pir 5000 cbs 1000 pbs 500	Configure the parameters of the rate limit profile. • profile-id: rate-limiting template ID, an integer, ranging from 1 to 1024 • profile-name: rate-limiting profile name, a string of 1 to 16 characters • cir cir: committed information rate, an integer, ranging from 0 to 10000000, in units of kbit/s • pir pir: peak information rate, an integer, ranging from 0 to 10000000, in units of kbit/s • cbs cbs: committed burst size, an integer, ranging from 1 to 65535, in units of byte • pbs pbs: peak burst size, an integer, ranging from 1 to 65535, in units of byte

3.10.3 Binding profile

No.	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#gpon-onu uni ethernet <i>slot-id/olt-id/onu-id/uni-id</i> example: Raisecom(config)#gpon-onu uni ethernet 3/2/1/1-4	Enter GPON ONU UNI configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID on the PON interface • uni-id: ONU UNI ID

No.	Command	Description
3	<pre>Raisecom(config-if-gpon- onu-ethernet- */*/*:*)#policing-profile { ingress egress } profile-id example: Raisecom(config-gpon-onu- ethernet-range)#policing- profile ingress 10</pre>	Bind a rate limit profile to the ONU UNI. You can use the no policing-profile { ingress egress } command to delete the binding relationship. • profile-id: rate-limiting template ID, an integer, ranging from 1 to 1024 • ingress: bind the template to the uplink direction of the UNI. • egress: bind the template to the downlink direction of the UNI

3.10.4 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show policing-profile { all profile-list }</pre>	Show configurations of the rate limit profile.

3.11 Configuring TR069 management template



Note

The device can manage the GPON HGU remotely through the Automatic Configuration Server by using TR-069.

The TR069 management template is a sub-template of service template. By configuring the template ID, you can associate the sub-template with the service template. For the association method, see section 3.9 Configuring service profile.

When the service template is bound to the ONU, so will be the sub-template.

3.11.1 Default configurations

N/A

3.11.2 Creating template

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#create tr069- mng-profile profile-id example: Raisecom(config)#create tr069- mng-profile 1</pre>	Create a TR069 management template. You can use the no create tr069-mng-profile <i>profile-id</i> command to delete the template. • profile-id: TR069 management template ID, an integer, ranging from 1 to 64

3.11.3 Configuring template

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#tr069-mng-profile <i>profile-id</i> enable example: Raisecom(config)#tr069-mng-profile 1 enable	Enable TR069 management template. You can use the tr069-mng-profile <i>profile-id</i> disable command to disable this template. • profile-id: TR069 management template ID, an integer, ranging from 1 to 64
3	Raisecom(config)#tr069-mng-profile <i>profile-id</i> acs-addr <i>address</i> example: Raisecom(config)#tr069-mng-profile 1 acs-addr 10.0.0.2	Configure the ACS address of the TR069 management template. • profile-id: TR069 management template ID, an integer, ranging from 1 to 64 • address: automatically configured server address, in dotted decimal notation, such as 10.10.10.10
4	Raisecom(config)#tr069-mng-profile <i>profile-id</i> acs-cpe-username <i>name</i> acs-cpe-password <i>password</i> example: Raisecom(config)#tr069-mng-profile 1 acs-cpe-username raisecom acs-cpe-password 123456	Configure the ACS CPE user name and password of the TR069 management template. • profile-id: TR069 management template ID, an integer, ranging from 1 to 64 • name: ACS CPE user name, a string of 1 to 50 characters • password: ACS CPE password, a string of 1 to 25 characters
5	Raisecom(config)#tr069-mng-profile <i>profile-id</i> acs-inform { enable disable } example: Raisecom(config)#tr069-mng-profile 1 acs-inform enable	Enable ACS notification of the TR069 management profile. • profile-id: TR069 management profile ID, an integer, ranging from 1 to 64
	Raisecom(config)#tr069-mng-profile <i>profile-id</i> acs-inform interval <i>time</i> example: Raisecom(config)#tr069-mng-profile 1 acs-inform 20	Configure the ACS notification period of the TR069 management profile. • profile-id: TR069 management profile ID, an integer, ranging from 1 to 64 • time: ACS notification period, an integer, ranging from 1 to 86400, in units of second
6	Raisecom(config)#tr069-mng-profile <i>profile-id</i> acs-username <i>name</i> acs-password <i>password</i> example: Raisecom(config)#tr069-mng-profile 1 acs-username raisecom acs-password 123456	Configure the ACS user name and ACS password of the TR069 management template. • profile-id: TR069 management template ID, an integer, ranging from 1 to 64 • name: ACS user name, a string of 1 to 50 characters • password: ACS password, a string of 1 to 25 characters

Step	Command	Description
7	Raisecom(config)# tr069-mng-profile <i>profile-id</i> vlan <i>vlan-id</i> priority <i>priority</i> example: Raisecom(config)#tr069-mng-profile 1 vlan 10 priority 2	(Optional) configure the VLAN and priority of the TR069 management template. • profile-id: TR069 management template ID, an integer, ranging from 1 to 64 • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • priority: priority of VLAN partition mode, an integer, ranging from 0 to 7



Note

Do not delete the template in use.

3.11.4 Checking configurations

No.	Command	Description
1	Raisecom# show tr069-mng-profile { all <i>profile-list</i> }	Show the TR069 management template.

3.12 Configuring VLAN

This function can be only configured on the GP16 card.

3.12.1 Default configurations

N/A

3.12.2 Configuring VLAN

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface gpon-onu <i>slot-id/olt-id/onu-id</i> example: Raisecom(config)#gpon-onu 3/2/1	Enter GPON ONU virtual interface mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID on the PON interface
3	Raisecom(config-if-gpon-onu-*/*:*)# vlan-access-list <i>list</i> gempport <i>port</i> example: Raisecom(config-if-gpon-onu-3/1:1)#vlan-access-list 1-100 gempport 2	(Optional) configure the VLAN ACL on the GEM interface. • list: VLAN list, an integer, ranging from 1 to 1000. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • port: GEM interface range, an integer, ranging from 1 to 8

Step	Command	Description
4	<pre>Raisecom(config-if-gpon-onu- */*:*)#vlan-mapping egress outer vlan-id translate outer vlan-id gemport port-id example: Raisecom(config-if-gpon-onu- 3/1:1)#vlan-mapping egress outer 1 translate outer 100 gemport 2</pre>	(Optional) configure VLAN mapping in the egress direction of the interface. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • port-id: GEM interface range, an integer, ranging from 1 to 8
5	<pre>Raisecom(config-if-gpon-onu- */*:*)#vlan-mapping ingress outer vlan-id translate outer vlan-id inner { add vlan-id unchange } gemport port-id example: Raisecom(config-if-gpon-onu- 3/1:1)#vlan-mapping egress outer 1 translate outer 100 inner add 2 gemport 2</pre>	(Optional) configure VLAN mapping in the ingress direction of the interface. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • port-id: GEM interface range, an integer, ranging from 1 to 8
6	<pre>Raisecom(config-if-gpon-onu- */*:*)#vlan-mapping outer vlan- list aggregate outer vlan-id inner { add vlan-list unchange } gemport port-id example: Raisecom(config-if-gpon-onu- 3/1:1)#vlan-mapping outer 1 aggregate outer 100 inner add 2 gemport 2</pre>	(Optional) configure inner and outer VLAN mapping of the VLAN aggregation group. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • port-id: GEM interface range, an integer, ranging from 1 to 8
7	<pre>Raisecom(config-if-gpon-onu- */*:*)#native vlan vlan-id gemport port-list example: Raisecom(config-if-gpon-onu- 3/1:1)#native vlan 10 gemport 1</pre>	(Optional) configure local VLAN of the GEM interface. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • port-list: GEM interface range, an integer, ranging from 1 to 8
8	<pre>Raisecom(config-if-gpon-onu- */*:*)#vlan upstream gem gem-id vlan vlan-id mode { replace replace-vlan vlan-id replace- stacking replace-vlan vlan-id stacking-vlan vlan-id stacking stacking-vlan vlan-id } example: Raisecom(config-if-gpon-onu- 3/1:1)#vlan upstream gem 1 vlan 2 mode replace replace-vlan 10</pre>	(Optional) configure the replacement and adding of VLAN for the uplink traffic of the GEM interface. • transparent: transparent transmission mode • trunk: Trunk mode • port-list: GEM interface range, an integer, ranging from 1 to 8 • replace-vlan vlan-id: replacing VLAN ID, an integer, ranging from 1 to 4094 • stacking-vlan vlan-id: adding VLAN ID, an integer, ranging from 1 to 4094 • gem-id: GEM interface ID, an integer, ranging from 1 to 128 • vlan-id: VLAN ID, an integer, ranging from 1 to 4094

Step	Command	Description
9	<pre>Raisecom(config-if-gpon-onu- */*:*)#vlan mode { transparent trunk } gempport port-list example: Raisecom(config-if-gpon-onu- 3/1:1)#vlan mode trunk gempport 1- 8</pre>	(Optional) configure the VLAN mode of the GEM interface. - transparent: transparent transmission mode - trunk: Trunk mode - port-list: GEM interface range, an integer, ranging from 1 to 8
10	<pre>Raisecom(config-if-gpon-onu- */*:*)#vlan dot1q-tunnel gempport port-list example: Raisecom(config-if-gpon-onu- 3/1:1)#vlan dot1q-tunnel gempport 1-8</pre>	(Optional) enable interface Tunnel and configure the GEM interface range. port-list: GEM interface range, an integer, ranging from 1 to 8

3.12.3 Configuring VLAN mapping based on GEM

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface gpon-onu slot-id/olt-id/onu-id	Enter GPON ONU virtual interface mode.
3	<pre>Raisecom(config-if-gpon-onu-*/*:*)#vlan- mapping both outer outer-vlan-id translate outer outer-vlan-id inner { inner-vlan-id add inner-vlan-id copy-from-outer remove unchange } gempport port Raisecom(config-if-gpon-onu-*/*:*)#vlan- mapping both outer outer-vlan-id inner inner-vlan-id translate outer outer-vlan-id inner { inner-vlan-id remove copy-from- outer } gempport port</pre>	(Optional) configure the 1:1 VLAN mapping rule based on GEM interface. Use the no vlan-mapping both outer outer-vlan-id to delete the configuration.
4	<pre>Raisecom(config-if-gpon-onu-*/*:*)#vlan- mapping both outer outer-vlan-list aggregate outer outer-vlan-id inner { add inner-vlan- id unchange } gempport port</pre>	(Optional) configure the VLAN aggregation mapping rule based on GEM interface. Use the no form of this command to delete the configuration.
5	<pre>Raisecom(config-if-gpon-onu-*/*:*)#vlan- mapping both cos-aware outer before-outer before-cos translate outer after-outer [after-cos] inner { inner-vlan-id add inner-vlan-id copy-from-outer remove unchange } gempport port</pre>	(Optional) configure the VLAN+CoS VLAN mapping rule based on GEM interface. Use the no form of this command to delete the configuration.

3.12.4 Checking configurations

Showing ONU configurations

No.	Command	Description
1	<code>Raisecom#show interface gpon-onu slot-id/olt-id/onu-id gempport port { vlan vlan-access-list }</code>	Show VLAN configurations of the ONU GEM interface.
2	<code>Raisecom#show interface gpon-onu slot-id/olt-id/onu-id gempport port vlan-mapping { aggregate egress translate ingress translate }</code>	Show ONU GEM interface aggregation and ingress/egress VLAN mapping.
3	<code>Raisecom#show interface gpon-onu slot-id/olt-id/onu-list vlan upstream</code>	Show configurations of the GEM VLAN of the specified ONU.
4	<code>Raisecom#show interface gpon-onu slot-id/olt-id/onu-list gempport port vlan-mapping both translate</code>	Show the 1:1 VLAN mapping rule in both directions of the GEM interface.
5	<code>Raisecom#show interface gpon-onu slot-id/olt-id/onu-list gempport port vlan-mapping both aggregate</code>	Show the VLAN aggregation mapping rule in both directions of the GEM interface.
6	<code>Raisecom#show interface gpon-onu slot-id/olt-id/onu-list gempport port vlan-mapping both cos-aware translate</code>	Show the VLAN+CoS VLAN mapping rule based on GEM interface.

3.13 Configuring auto-authentication rules

3.13.1 Default configuration

N/A

3.13.2 Configuring auto-authentication rules

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#gpon-auto-authentication-rule rule-id</code> example: <code>Raisecom#config</code> <code>Raisecom(config)#gpon-auto-authentication-rule 2</code> <code>Raisecom(config-gpon-auto-auth-rule:2)#</code>	Enter GPON ONU auto-authentication rule configuration mode. If there is a rule, directly enter the auto-authentication rule configuration mode; otherwise create a rule before entering the auto-authentication rule configuration mode. rule-id: ID of GPON ONU auto-authentication rule, an integer, ranging from 1 to 1024

Step	Command	Description
3	Raisecom(config-gpon-auto-auth-rule:id)#service-profile-id { <i>profileid-id</i> auto } example: Raisecom(config-gpon-auto-auth-rule:2)#service-profile-id 1 Raisecom(config-gpon-auto-auth-rule:2)#service-profile-id auto	Configure the service template used when the ONU is online in the auto-authentication rule. You can use the no form of this command to delete the template. • profileid-list: ID of the service template used when the ONU is online in the auto-authentication rule, an integer, ranging from 1 to 1024 • auto: automatically search for the line profile.
	Raisecom(config-gpon-auto-auth-rule:id)#service-profile-name <i>name</i> example: Raisecom(config-gpon-auto-auth-rule:2)#service-profile-name raisecom	Configure the name of the service template used when the ONU is online in the auto-authentication rule. • name: name of the service template used when the ONU is online in the auto-authentication rule
4	Raisecom(config-gpon-auto-auth-rule:id)#line-profile-id { <i>profileid-id</i> auto } example: Raisecom(config-gpon-auto-auth-rule:2)#line-profile-id 1 Raisecom(config-gpon-auto-auth-rule:2)#line-profile-id auto	Configure the line profile used when the ONU is online in the auto-authentication rule. You can use the no form of this command to delete the template. • profileid-id: ID of the line profile used when the ONU is online in the auto-authentication rule, an integer, ranging from 1 to 1024 • auto: automatically search for the service template.
	Raisecom(config-gpon-auto-auth-rule:id)#line-profile-name { <i>profileid-name</i> auto } example: Raisecom(config-gpon-auto-auth-rule:2)#line-profile-name raisecom	Configure the name of the line profile used when the ONU is online in the auto-authentication rule. • profileid-name: name of the line profile used when the ONU is online in the auto-authentication rule • auto: automatically search for the line profile.
5	Raisecom(config-gpon-auto-auth-rule:id)#match port [add remove] <i>slot-id/olt-list</i> example: Raisecom(config-gpon-auto-auth-rule:2)#match port 3/1	Configure the matching interface in the auto-authentication rule. You can use the no form of this command to delete the matching interface. • slot-id/olt-list: PON interface ID, an integer. The slot-id refers to the slot ID; the olt-id refers to the PON interface ID. • add: add the matching interfaces in the auto-authentication rule. • remove: remove the matching interfaces in the auto-authentication rule.

Step	Command	Description
6	Raisecom(config-gpon-auto-auth-rule:id)#match onu-device-type <i>device-type</i> example: Raisecom(config-gpon-auto-auth-rule:2)#match onu-device-type HT803	Configure the matching condition for ONU device type in the auto-authentication rule. You can use the no form of this command to delete the matching condition. • ONU device type, a string of 1 to 2 characters, in units of Byte
7	Raisecom(config-gpon-auto-auth-rule:id)#match ethernet port-num <i>port-num</i> example: Raisecom(config-gpon-auto-auth-rule:2)#match ethernet port-num 20	Configure the matching condition for the number of ONU Ethernet interfaces in the auto-authentication rule. You can use the no form of this command to delete the matching condition. • port-num: number of ONU Ethernet interface, an integer, ranging from 0 to 24
8	Raisecom(config-gpon-auto-auth-rule:id)#match wlan port-num <i>port-num</i> example: Raisecom(config-gpon-auto-auth-rule:2)#match wlan port-num 3	Configure the matching condition for the number of ONU WLAN interfaces in the auto-authentication rule. You can use the no form of this command to delete the matching condition. • port-num: number of ONU WLAN interfaces in the auto-authentication rule, an integer, ranging from 0 to 8
9	Raisecom(config-gpon-auto-auth-rule:id)#match catv port-num <i>port-num</i> example: Raisecom(config-gpon-auto-auth-rule:2)#match catv port-num 2	Configure the matching condition for the number of ONU CATV interfaces in the auto-authentication rule. You can use the no form of this command to delete the matching condition. • port-num: number of ONU CATV interfaces in the auto-authentication rule, an integer, ranging from 0 to 2
10	Raisecom(config-gpon-auto-auth-rule:id)#match veip port-num <i>port-num</i> example: Raisecom(config-gpon-auto-auth-rule:2)#match veip port-num 2	Configure the matching condition for the number of ONU VEIP interfaces in the auto-authentication rule. You can use the no form of this command to delete the matching condition. • port-num: number of ONU CATV interfaces in the auto-authentication rule, an integer, ranging from 0 to 8
11	Raisecom(config-gpon-auto-auth-rule:id)#match pots port-num <i>port-num</i> example: Raisecom(config-gpon-auto-auth-rule:2)#match pots port-num 2	Configure the matching condition for the number of ONU voice interfaces in the auto-authentication rule. You can use the no form of this command to delete the matching condition. • port-num: number of ONU voice interfaces in the auto-authentication rule, an integer, ranging from 0 to 24

3.13.3 Checking configurations

No.	Command	Description
1	Raisecom#show gpon-auto-authentication-rule { all rule-id }	Show configurations of auto-authentication rules.
2	Raisecom#show interface gpon-olt [slot-id/olt-list] auto-authentication-rule	Show configurations of auto-authentication rules associated with an interface.

3.14 Configuring rate limiting on GEM interface

3.14.1 Checking configurations

No.	Command	Description
1	Raisecom#show interface gpon-olt slot-id/olt-id service-port port-id	Show information about the service interface.
2	Raisecom#show interface gpon-olt slot-id/olt-id service-port port-id shaping	Show shaping information about the service interface.

3.15 Configuration examples

3.15.1 Configuring ONU auto-registration

Networking requirements

As shown in Figure 3-1, when you enable none authentication mode on OLT interface 3/1, the ONU will be added to the OLT through auto-registration.

Figure 3-1 ONU auto-registration



Configuration steps

Configure the ONU authentication mode to none.

```

Raisecom#config
Raisecom(config)#interface gpon-olt 3/1

```

```
Raisecom(config-if-gpon-olt-13:1)#authorization mode none
```

Checking results

Show the ONU authentication mode.

```
Raisecom#show interface gpon-olt 3/1 auth information
Distance(m)  onu-auto  onu-auto-find  Authorization Created
Registered
OLT ID min  max  find  Period(s)  Mode  Onus  Onus
-----
3/1  1  60000  enable  5  none  2  2
```

Show information about the ONU registered on the OLT.

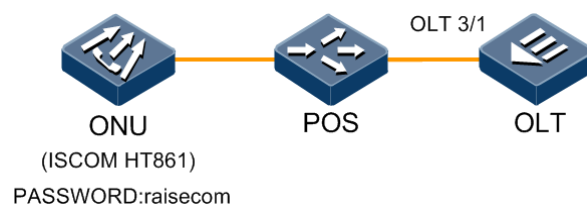
ONU ID	SN	Device Type	Creation Date	State
Line	Profile	Service Profile	Description	
ID	name	ID	name	
3/1/1	52434d47d0922999	Unknown	2020-12-29,16:14:08	
active	9	profile-9	8	profile-8 3/1/1

3.15.2 Configuring ONU registration based on PASSWORD authentication mode

Networking requirements

As shown in Figure 3-2, enable PASSWORD authentication mode on OLT interface 3/1 to register ONU. The model of the ONU to be registered is HT861 and the PASSWORD is raisecom.

Figure 3-2 ONU registration based on PASSWORD authentication mode



Configuration steps

Step 1 Configure the ONU authentication mode to PASSWORD.

```
Raisecom#config
Raisecom(config)#interface gpon-olt 3/1
Raisecom(config-if-gpon-olt-3:1)#authorization mode password
```

Step 2 Create the ONU authorization entry based on PASSWORD.

```
Raisecom(config-if-gpon-olt-3:1)#create gpon-onu password raisecom line-
profile-id 9 servic service-profile-id 8
```

Checking results

Show ONU authentication mode.

```
Raisecom#show interface gpon-olt 3/1 auth information
```

```
Distance(m)  onu-auto  onu-auto-find  Authorization Created
Registered
```

```
OLT ID  min   max   find   Period(s)   Mode      Onus   Onus
```

```
-----
-----
```

```
3/1  1    60000  enable  5      password  2     2
```

Show information about the ONU registered on the OLT.

```
Raisecom#show interface gpon-onu creation-information
```

```
ONU ID    SN                Device Type      Creation Date      State
Line Profile      Service Profile    Description
```

```
ID      name                ID      name
```

```
-----
-----
```

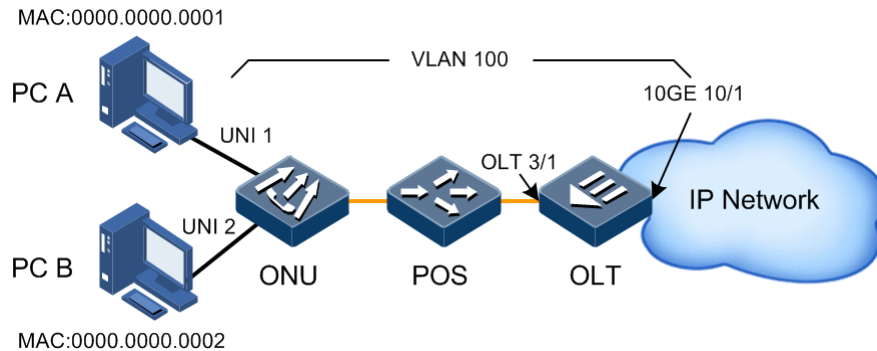
```
3/1/1  52434d47d0922999    Unknown          2020-12-29,16:14:08
active      9  profile-9  8  profile-8  3/1/1
```

3.15.3 Configuring Ethernet data services

Networking requirements

As shown in Figure 3-3, PC A connects UNI 1 on the ONU. The user VLAN is 100. PON interface 3/1 on the device is connected downstream to the ONU while the 10GE interface 10/1 is connected upstream to the IP network. In such case, you can activate the data services.

Figure 3-3 Data service networking



Configuration steps



Note

The method of configuring Ethernet data services is different between GPON and EPON:

- In EPON, you can configure data services directly on the ONU interface.
- In GPON, you need to create a line profile and a service template in global configuration mode first and then enter the ONU interface mode where you can quote the created line profile and service template.
- Configure the OLT.

Step 1 Configure a line profile.

```
Raisecom#config
Raisecom(config)#gpon-onu-line-profile 100
Raisecom(config-gpon-onu-line-profile:100)#mapping-mode port
Raisecom(config-gpon-onu-line-profile:100)#create tcont 1 dba-profile 1
Raisecom(config-gpon-onu-line-profile:100)#create gem 1 tcont 1
Raisecom(config-gpon-onu-line-profile:100)#commit
Raisecom(config-gpon-onu-line-profile:100)#gem 1 mapping 1 ethernet 1
Raisecom(config-gpon-onu-line-profile:100)#commit
Raisecom(config-gpon-onu-line-profile:100)#exit
```

Step 2 Configure a service template.

```
Raisecom(config)#gpon-onu-service-profile 200
Raisecom(config-gpon-onu-service-profile:200)#port-num ethernet 4
```

```
Raisecom(config-gpon-onu-service-profile:200)#uni ethernet 1 vlan trunk
allowed 100
Raisecom(config-gpon-onu-service-profile:200)#commit
Raisecom(config-gpon-onu-service-profile:200)#exit
```

Step 3 Configure the GPON downlink interface.

```
Raisecom(config)#interface gpon-olt 3/1
Raisecom(config-if-gpon-olt-3:1)#authorization mode none
Raisecom(config-if-gpon-olt-3:1)#auto-authentication service-profile-id
200
Raisecom(config-if-gpon-olt-3:1)#auto-authentication line-profile-id 1024
Raisecom(config-if-gpon-olt-3:1)#switchport trunk allowed vlan 100
Trunk allow vlan will be reconfigured,please input 'yes' to confirm set
allowed vlan:[yes]yes
Raisecom(config-if-gpon-olt-3:1)#switchport trunk untagged vlan remove 1
Raisecom(config-if-gpon-olt-3:1)#switchport mode trunk
Raisecom(config-if-gpon-olt-3:1)#quit
```

Step 4 Configure the uplink interface.

```
Raisecom#config
Raisecom(config)#create vlan 100 active
Raisecom(config)#interface ten-gigabitethernet 10/1
Raisecom(config-if-ten-gigabitethernet-10:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-10:1)#switchport trunk allowed
vlan 100
Raisecom(config-if-ten-gigabitethernet-10:1)#exit
```

- Configure the ONU.

```
Raisecom(config)#interface gpon-onu 3/1/1
Raisecom(config-if-gpon-onu-3/1:1)#service-profile-id 200
Raisecom(config-if-gpon-onu-3/1:1)#line-profile-id 100
Raisecom(config-if-gpon-onu-3/1:1)#end
```

Checking results

Show information about the ONU created on the OLT.

```
Raisecom#show interface gpon-onu creation-information
```

ONU ID	SN	Device Type	Creation Date	State
Line Profile		Service Profile	Description	

ID	name	ID	name
3/1/1	52434d47d0922999	Unknown	2020-12-29,16:14:08
active	100	profile-100 200	profile-200 3/1/1

Show ONU online information.

Raisecom#show interface gpon-onu online-information

ONU ID	State	Distance(m)	Login Date	Logout Date	Logout Reason
3/1/1	online	46	2000-08-10,22:09:55	2000-08-10,22:09:49	Branch fiber cut

Show VLAN configurations on the ONU Ethernet interface.

Raisecom#show gpon-onu 3/1/1 uni ethernet vlan

```

UNI Ethernet ID: 1
work Mode       : normal
VLAN mode       : transparent
Native VLAN(pri) : 1 (0)
Trunk Allowed VLAN : 100
Translation-rule : n/a
Aggregation-rule : n/a
MAC Address Threshold : 0
Max Frame Size   : 1522
Ingress Policing-profile: 0
Egress Policing-profile: 0
Drop Untagged    : disable
Dot1q-tunnel     : disable
  
```

Show the status of the Ethernet interface on the ONU.

Raisecom#show gpon-onu 3/1/1 uni ethernet information US-

Port ID	Speed(actual)	Admin Link Profile	Profile	Loopback
filter PoE	alarm-ctrl	FlowControl		

3/1/1/1	auto/auto(unknown)	enable	down	0	0	disable	disable
disable	disable	disable					

4 ONU remote management

This chapter describes the ONU management and Wi-Fi functions of the ISCOM6800 and ISCOM6860, including the following sections:

- Managing EPON ONU
- Configuring GPON ONU
- Wi-Fi (EPON)
- Wi-Fi (GPON)

4.1 Managing EPON ONU

The device can be managed by EMS through SNMP. Meanwhile, it can be a SNMP proxy, that is, it functions as a proxy for the NMS and EPON ONU, controlling the ONU remotely through EPON OAM.

4.1.1 Default configurations

Function	Default value
ONU status	Activated
Maximum round trip time of EPON interface	14000TQ
Default VLAN of the UNI in the ONU service profile	VLAN1
List of VLANs allowed by the trunk Ethernet port in the ONU service profile	Empty
Working mode of the Ethernet port in the ONU service template	Auto-negotiation
Rate limiting over the Ethernet port in the ONU service profile	Disable
Removing the VLAN Tag of multicast packets on the Ethernet interface of the ONU service profile	Disable
Rate limit of the ONU uplink interface	0Mbps
Rate-limit profile bound to the UNI	Unbound

Default configurations of DHCP Server are as below:

Function	Default value
DHCP Server status	Enable
DHCP server subnet IP address and subnet mask, start and end IP address, gateway IP address, primary/backup DNS server address	0.0.0.0
Lease time	0 (indefinite)
DHCP server reserved IP address	No IP address reserved

4.1.2 ONU basic configurations

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu eoc { enable disable }	(Optional) enable EOC ONU resource synchronization. Use the disable form of this comand to disable this function.
3	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
4	Raisecom(config-epon-onu-*//*:*)#write	(Optional) save configuration data.
5	Raisecom(config-epon-onu-*//*:*)#reload startup-config	(Optional) reload the startup configuration file.
6	Raisecom(config-epon-onu-*//*:*)#restore startup-config	(Optional) restore default configuration.
7	Raisecom(config-epon-onu-*//*:*)#reboot [now]	(Optional) restart the ONU.



Caution

When remotely managing and configuring the ONU through the ISCOM6800/ISCOM6860, you should save configurations in ONU configuration mode; otherwise, configurations will be lost when the ISCOM6800/ISCOM6860 is restarted.

4.1.3 ONU management configurations

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)# epon-onu <i>slot-id/olt-id/onu-id</i> example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU management configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*/:*)# hostname <i>string</i> example: Raisecom(config-epon-onu-3/1:1)#hostname onu1	(Optional) configure the ONU name. You can use the no hostname command to restore default configurations. string: ONU name, a string. The character length varies with the ONU model.
4	Raisecom(config-epon-onu-*/:*)# telnet { enable disable }	(Optional) enable/disable Telnet.
5	Raisecom(config-epon-onu-*/:*)# mng-characteristic { rc ctc2dot1 ctc3dot0 } example: Raisecom(config-epon-onu-3/1:1)#mng-characteristic ctc2dot1	(Optional) configure the management channel of the ONU. - rc: Raisecom private management mode - ctc2dot1: CTC2.1 management mode - ctc3dot0: CTC3.0 management mode
6	Raisecom(config-epon-onu-*/:*)# transceiver tx-power-supply { primary standby both } reenabe example: Raisecom(config-epon-onu-3/1:1)#transceiver tx-power-supply primary reenabe	(Optional) configure the working mode of the optical transceiver on the ONU PON interface. - primary: primary optical module - standby: standby optical module - both: primary and standby optical modules
7	Raisecom(config-epon-onu-*/:*)# transceiver tx-power-supply { primary standby both } shutdown { time permanently } example: Raisecom(config-epon-onu-3/1:1)#transceiver tx-power-supply primary shutdown permanently	(Optional) configure the power shutdown time of the optical transceiver on the ONU PON interface. - primary: primary optical module - standby: standby optical module - both: primary and standby optical modules - time: power shutdown time, an integer, ranging from 1 to 65534, in units of second - permanently: permanent shutdown

4.1.4 Configuring management IP address

Configuring management IP mode

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# epon-onu <i>slot-id/olt-id/onu-id</i> example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU management configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-list: ONU ID under the PON interface

Step	Command	Description
3	<pre>Raisecom(config-epon- onu-*/*:*)#ip-config { static auto [overlay-local-ip] } example: Raisecom(config-epon- onu-3/1:1)#ip-config auto overlay-local-ip</pre>	Configure the allocation mode of ONU management IP address.  Note • static: you should configure the management IP address of the ONU manually. • auto: the ONU can obtain the IP address from the ONU IP address pool bound with the related PON interface automatically. The overlay-local-ip parameter refers to that the automatically obtained IP address will overlay the configured IP address of the ONU. • static: you need to manually configure the management IP address of the ONU. • auto: the ONU can automatically obtain an IP address from the ONU IP address pool bound to the OLT PON interface. • overlay-local-ip: when this parameter is configured, the IP address obtained from the OLT PON interface by the ONU will override the locally configured management IP address.

Configuring management IP address

ONU management IP address is divided into two types:

- Management IP address of PON interface: after configuring the IP address of the PON interface, you can remotely telnet to the ONU for management on the OLT.
- Management IP address of UNI: after configuring the IP address of the LAN interface, you can manage the ONU locally through the LAN interface.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#epon- onu slot-id/olt-id/onu- id example: Raisecom(config)#epon- onu 3/2/1</pre>	Enter EPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-list: ONU ID under the PON interface

Step	Command	Description
3	<pre>Raisecom(config-epon- onu-*/*:*)#mng-ip address ip- address[mask] default- gw default-gw vlan svlan-id cvlan-id priority example: Raisecom(config-epon- onu-3/1:1)#mng-ip address 10.0.0.2 default-gw 10.0.0.1 vlan 0 10 5</pre>	(Optional) configure the management IP address of the ONU PON interface. Use this configuration when you adopt the SNMP method to manage the ONU. You can use the no mng-ip address command to restore default configuration. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • mask: IP subnet mask, in dotted decimal notation, such as 255.0.0.0 • default-gw: default gateway, in dotted decimal notation, such as 10.10.10.1 • svlan-id: SVLAN ID, an integer, ranging from 0 to 4094, where 0 indicates untagged. • cvlan-id: CVLAN ID, an integer, ranging from 0 to 4094, where 0 indicates untagged. • priority: CoS priority, an integer, ranging from 0 to 7
	<pre>Raisecom(config-epon- onu-*/*:*)#mng-ipv6 address ipv6- address/prefix-length default-gw default-gw vlan svlan-id cvlan-id priority example: Raisecom(config-epon- onu-3/1:1)#mng-ipv6 address 3001::1/64 default-gw 3002::1 vlan 0 10 5</pre>	(Optional) configure the IPv6 management IP address of the ONU PON interface. Use this configuration when you adopt the SNMP method to manage the ONU. You can use the no mng-ipv6 address command to restore default configuration. • ipv6-address/prefix: IPv6 address and prefix, in colon hexadecimal notation, such as 3001:1/64 • default-gw: default gateway, in colon hexadecimal notation, such as 3002::1 • svlan-id: SVLAN ID, an integer, ranging from 0 to 4094 where 0 indicates untagged. • cvlan-id: CVLAN ID, an integer, ranging from 0 to 4094 where 0 indicates untagged. • priority: CoS priority, an integer, ranging from 0 to 7
4	<pre>Raisecom(config-epon- onu-*/*:*)#lan-ip address ip-address [mask] example: Raisecom(config-epon- onu-3/1:1)#lan-ip address 10.0.0.1 255.0.0.0</pre>	(Optional) configure the IP address of the ONU UNI. You can use the no lan-ip address command to restore default configuration. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • mask: IP address mask, in dotted decimal notation, such as 255.0.0.0



Note

The IP address of the ONU PON interface cannot be in the same network segment with that of the ONU UNI. For management IP addresses of PON interfaces on different ONUs, you should make sure that they do not conflict with each other.

4.1.5 Configuring SNMP parameters

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU management configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-list: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*/*:*)#snmp-server host ip-address example: Raisecom(config-epon-onu-3/1:1)#snmp-server host 10.0.0.1	Configure the IP address of the ONU SNMP server. You can use the no snmp-server host command to restore default configuration. ip-address: IPv4 address of the target host, in dotted decimal notation, such as 10.10.10.1
4	Raisecom(config-epon-onu-*/*:*)#snmp-server version { 1 2c v3 } example: Raisecom(config-epon-onu-3/1:1)#snmp-server version 1	Configure ONU SNMP version. You can use the no snmp-server version command to restore default configuration. 1: use SNMPv1. 2c: use SNMPv2. - v3: use SNMPv3.
5	Raisecom(config-epon-onu-*/*:*)#snmp-server trap-port port example: Raisecom(config-epon-onu-3/1:1)#snmp-server trap-port 100	Configure the SNMP Trap interface ID of the ONU. You can use the no snmp-server trap-port command to restore default configuration. port: interface ID, an integer, ranging from 1 to 65535
6	Raisecom(config-epon-onu-*/*:*)#snmp-server udp-port port example: Raisecom(config-epon-onu-3/1:1)#snmp-server udp-port 100	Configure the SNMP UDP port number of the ONU. You can use the no snmp-server udp-port command to restore default configuration. port: interface ID, an integer, ranging from 1 to 65535
7	Raisecom(config-epon-onu-*/*:*)#snmp-server security name example: Raisecom(config-epon-onu-3/1:1)#snmp-server security raisecom	Configure the name of SNMP security principal of the ONU. You can use the no snmp-server security command to restore default configuration. name: name, a character string

Step	Command	Description
8	<pre>Raisecom(config-epon-onu- */*:*)#snmp-server community name { ro rw } example: Raisecom(config)#snmp- server community guest view mib1 ro</pre>	Configure the SNMP community name and properties of the ONU. You can use the no snmp-server community { ro rw } command to restore default configuration. • name: the MIB view that the community can access. If you do not select this parameter, the view that can be accessed is internet by default. The view name is a string of 1 to 32 characters. • ro: the community permission is read-only and can only read the agent's data. • rw: the community's permission is read-write. You can read the data of the agent or write the data to it.

4.1.6 Configuring UNI

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id example: Raisecom(config)#epon-onu uni ethernet 3/2/1/1</pre>	Enter EPON ONU UNI configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • uni-id: ONU UNI ID
3	<pre>Raisecom(config-epon-onu-ethernet- */*:*)#uni name string example: Raisecom(config-epon-onu-ethernet- 3/1/1:1)#uni name raisecom</pre>	(Optional) configure the UNI name. You can use the no uni name command to restore default configuration. • string: UNI ID, a character string
4	Raisecom(config-epon-onu-ethernet-*/*:*)#speed auto	(Optional) configure the rate and duplex mode of the UNI to auto .
5	<pre>Raisecom(config-epon-onu-ethernet- */*:*)#speed { 10 100 1000 } duplex { full half } example: Raisecom(config-gpon-onu-ethernet- 3/1/1:1)#speed 100 duplex full</pre>	(Optional) configure the rate and duplex mode of the UNI. • 10: the rate is forced 10 Mbit/s. • 100: the rate is forced 100 Mbit/s. • 1000: the rate is forced 1000 Mbit/s. • full: full duplex mode • half: half duplex mode
6	Raisecom(config-epon-onu-ethernet-*/*:*)#flowcontrol { enable disable }	(Optional) enable/disable flow control on the UNI.
7	Raisecom(config-epon-onu-ethernet-*/*:*)#auto-negotiation restart	(Optional) force the UNI to perform auto-negotiation again.

Step	Command	Description
8	Raisecom(config-epon-onu-ethernet- */*/*:*)# shutdown	(Optional) shut down the UNI. You can use the no shutdown to enable the UNI.  Note When you use this command to shut down the ONU UNI in CLI mode, no Trap is reported by default. If required, you need to enable the Trap function. For details, see section 4.1.7 Configuring UNI alarm.

4.1.7 Configuring UNI alarm

Configuring alarm

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id	Enter EPON ONU UNI configuration mode.
3	Raisecom(config-epon-onu-ethernet- */*/*:*)# snmp trap auto-neg-failure { enable disable }	(Optional) enable/disable UNI auto-negotiation failure alarm.
4	Raisecom(config-epon-onu-ethernet- */*/*:*)# snmp trap congestion { enable disable }	(Optional) enable/disable UNI congestion alarm.
5	Raisecom(config-epon-onu-ethernet- */*/*:*)# snmp trap down-crc-error-alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI downstream CRC error packets exceeds the threshold.
6	Raisecom(config-epon-onu-ethernet- */*/*:*)# snmp trap down-crc-error-warning { enable disable }	(Optional) enable/disable warning when the number of UNI downstream CRC error packets exceeds the threshold.
7	Raisecom(config-epon-onu-ethernet- */*/*:*)# snmp trap down-discard-alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI downstream discarded packets exceeds the threshold.
8	Raisecom(config-epon-onu-ethernet- */*/*:*)# snmp trap down-discard-warning { enable disable }	(Optional) enable/disable warning when the number of UNI downstream discarded packets exceeds the threshold.
9	Raisecom(config-epon-onu-ethernet- */*/*:*)# snmp trap down-drop-event-warning { enable disable }	(Optional) enable/disable warning when the number of UNI downstream packet loss events exceeds the threshold.

Step	Command	Description
10	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-drop-event- alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI downstream packet loss events exceeds the threshold.
11	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-error-alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI downstream error packets exceeds the threshold.
12	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-error- warning { enable disable }	(Optional) enable/disable warning when the number of UNI downstream error packets exceeds the threshold.
13	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-fragment- alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI downstream Fragments exceeds the threshold.
14	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-fragment- warning { enable disable }	(Optional) enable/disable warning when the number of UNI downstream Fragments exceeds the threshold.
15	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-jabber-alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI downstream Jabbers exceeds the threshold.
16	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-jabber- warning { enable disable }	(Optional) enable/disable warning when the number of UNI downstream Jabbers exceeds the threshold.
17	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-oversize- alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI downstream oversized packets exceeds the threshold.
18	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-oversize- warning { enable disable }	(Optional) enable/disable warning when the number of UNI downstream oversized packets exceeds the threshold.
19	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-undersize- alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI downstream undersized packets exceeds the threshold.
20	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-undersize- warning { enable disable }	(Optional) enable/disable warning when the number of UNI downstream undersized packets exceeds the threshold.
21	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap failure { enable disable }	(Optional) enable/disable UNI failure alarm.
22	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap loopback { enable disable }	(Optional) enable/disable UNI loopback alarm.
23	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap loss { enable disable }	(Optional) enable/disable UNI LOS alarm.
24	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap status-change- times-alarm { enable disable }	(Optional) enable/disable alarm when the times of UNI status change exceed the threshold.
25	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap status-change- times-warning { enable disable }	(Optional) enable/disable warning when the times of UNI status change exceed the threshold.

Step	Command	Description
26	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-crc-error- alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI upstream CRC error packets exceeds the threshold.
27	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-crc-error- warning { enable disable }	(Optional) enable/disable warning when the number of UNI upstream CRC error packets exceeds the threshold.
28	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-discard-alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI upstream discarded packets exceeds the threshold.
29	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-discard- warning { enable disable }	(Optional) enable/disable warning when the number of UNI upstream discarded packets exceeds the threshold.
30	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-drop-event- warning { enable disable }	(Optional) enable/disable warning when the number of UNI upstream packet loss events exceeds the threshold.
31	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-drop-event- alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI upstream packet loss events exceeds the threshold.
32	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-error-alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI upstream error packets exceeds the threshold.
33	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-error-warning { enable disable }	(Optional) enable/disable warning when the number of UNI upstream error packets exceeds the threshold.
34	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-fragment-alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI upstream Fragments exceeds the threshold.
35	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-fragment- warning { enable disable }	(Optional) enable/disable warning when the number of UNI upstream Fragments exceeds the threshold.
36	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-jabber-alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI upstream Jabbers exceeds the threshold.
37	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-jabber-warning { enable disable }	(Optional) enable/disable warning when the number of UNI upstream Jabbers exceeds the threshold.
38	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-oversize-alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI upstream oversized packets exceeds the threshold.
39	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-oversize- warning { enable disable }	(Optional) enable/disable warning when the number of UNI upstream oversized packets exceeds the threshold.
40	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-undersize- alarm { enable disable }	(Optional) enable/disable alarm when the number of UNI upstream undersized packets exceeds the threshold.

Step	Command	Description
41	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-undersize- warning { enable disable }	(Optional) enable/disable warning when the number of UNI upstream undersized packets exceeds the threshold.

Configuring alarm threshold

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id example: Raisecom(config)#epon-onu uni ethernet 3/2/1/1	Enter EPON ONU UNI configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface - uni-id: ONU UNI ID
3	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-crc-error-alarm threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-crc-error-alarm threshold 100	(Optional) configure the alarm threshold of UNI downstream CRC error packets. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
4	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-crc-error-warning threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-crc-error-warning threshold 100	(Optional) configure the warning threshold of UNI downstream CRC error packets. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
5	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-discard-alarm threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-discard-alarm threshold 100	(Optional) configure the alarm threshold of UNI downstream discarded packets. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
6	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-discard-warning threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-discard-warning threshold 100	(Optional) configure the warning threshold of UNI downstream discarded packets. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
7	Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-drop-event-warning threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-drop-event-warning threshold 100	(Optional) configure the warning threshold of UNI downstream packet loss events. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647

Step	Command	Description
8	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-drop-event-alarm threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-drop-event-alarm threshold 100</pre>	(Optional) configure the alarm threshold of UNI downstream packet loss events. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
9	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-error-alarm threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-error-alarm threshold 100</pre>	(Optional) configure the alarm threshold of UNI downstream error packets. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
10	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-error-warning threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-error-warning threshold 100</pre>	(Optional) configure the warning threshold of UNI downstream error packets. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
11	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-fragment-alarm threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-fragment-alarm threshold 100</pre>	(Optional) configure the alarm threshold of UNI downstream Fragments. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
12	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-fragment-warning threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-fragment-warning threshold 100</pre>	(Optional) configure the warning threshold of UNI downstream Fragments. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
13	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-jabber-alarm threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-jabber-alarm threshold 100</pre>	(Optional) configure the alarm threshold of UNI downstream Jabbers. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
14	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap down-jabber-warning threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-jabber-warning threshold 100</pre>	(Optional) configure the warning threshold of UNI downstream Jabbers. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647

Step	Command	Description
15	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap down-oversize-alarm threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-oversize-alarm threshold 100	(Optional) configure the alarm threshold of UNI downstream oversized packets. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
16	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap down-oversize-warning threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-oversize-alarm threshold 100	(Optional) configure the warning threshold of UNI downstream oversized packets. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
17	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap down-undersize-alarm threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet-3/2/1:1)# snmp trap down-undersize-alarm threshold value 100	(Optional) configure the alarm threshold of UNI downstream undersized packets. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
18	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap down-undersize-warning threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap down-undersize-warning threshold 100	(Optional) configure the warning threshold of UNI downstream undersized packets. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
19	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap status-change-times- alarm threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap status-change-times- alarm threshold 100	(Optional) configure the alarm threshold of UNI status change times. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
20	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap status-change-times- warning threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap status-change-times- warning threshold 100	(Optional) configure the warning threshold of UNI status change times. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
21	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap up-crc-error-alarm threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-crc-error-alarm threshold 100	(Optional) configure the alarm threshold of UNI upstream CRC error packets. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647

Step	Command	Description
22	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap up-crc-error-warning threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-crc-error-warning threshold 100	(Optional) configure the warning threshold of UNI upstream CRC error packets. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
23	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap up-discard-alarm threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-discard-alarm threshold 100	(Optional) configure the alarm threshold of UNI upstream discarded packets. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
24	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap up-discard-warning threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-discard-warning threshold 100	(Optional) configure the warning threshold of UNI upstream discarded packets. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
25	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap up-drop-event-warning threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-drop-event-warning threshold 100	(Optional) configure the warning threshold of UNI upstream packet loss events. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
26	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap up-drop-event-alarm threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-drop-event-alarm threshold 100	(Optional) configure the alarm threshold of UNI upstream packet loss events. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
27	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap up-error-alarm threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-error-alarm threshold 100	(Optional) configure the alarm threshold of UNI upstream error packets. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
28	Raisecom(config-epon-onu-ethernet- */*/*:*)#snmp trap up-error-warning threshold <i>value</i> example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-error-warning threshold 100	(Optional) configure the warning threshold of UNI upstream error packets. • threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647

Step	Command	Description
29	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-fragment-alarm threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-fragment-alarm threshold 100</pre>	(Optional) configure the alarm threshold of UNI upstream Fragments. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
30	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-fragment-warning threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-fragment-warning threshold 100</pre>	(Optional) configure the warning threshold of UNI upstream Fragments. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
31	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-jabber-alarm threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-jabber-alarm threshold 100</pre>	(Optional) configure the alarm threshold of UNI upstream Jabbers. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
32	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-jabber-warning threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-jabber-warning threshold 100</pre>	(Optional) configure the warning threshold of UNI upstream Jabbers. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
33	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-oversize-alarm threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-oversize-alarm threshold 100</pre>	(Optional) configure the alarm threshold of UNI upstream oversized packets. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
34	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-oversize-warning threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-oversize-warning threshold 100</pre>	(Optional) configure the warning threshold of UNI upstream oversized packets. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647
35	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#snmp trap up-undersize-alarm threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-undersize-alarm threshold 100</pre>	(Optional) configure the alarm threshold of UNI upstream undersized packets. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647

Step	Command	Description
36	<pre>Raisecom(config-epon-onu-ethernet- *//*/*:*)#snmp trap up-undersize-warning threshold value example: Raisecom(config-epon-onu-ethernet- 3/2/1:1)#snmp trap up-undersize-warning threshold 100</pre>	(Optional) configure the warning threshold of UNI upstream undersized packets. threshold value: alarm reporting threshold, an integer, ranging from 1 to 2147483647

4.1.8 Configuring serail interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu uni serial-com slot-id/olt-id/onu- id/uni-id example: Raisecom(config)#epon-onu uni serial-com 9/1/1/1</pre>	Enter ONU serial interface configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface - uni-id: ONU UNI ID
3	<pre>Raisecom(config-epon-onu- serial-*//*/*:*)#serial- protocol { rs232 rs485 } example: Raisecom(config-serial- 1:1)#serial-protocol rs232</pre>	Configure the communication protocol of the serial interface. - rs232: configure the communication protocol of the serial interface to RS232. - rs485: configure the communication protocol of the serial interface to RS485.
4	<pre>Raisecom(config-epon-onu- serial-*//*/*:*)#baud-rate { 300 1200 2400 4800 9600 14400 19200 28800 38400 57600 115200 } example: Raisecom(config-epon-onu- serial-3/1/1:1)#baud-rate 1200</pre>	Configure the baud rate of the serial interface. You can use the no baud-rate command to restore default configuration. 300: the baud rate is 300 bit/s. 1200: the baud rate is 1200 bit/s. 2400: the baud rate is 2400 bit/s. 4800: the baud rate is 4800 bit/s. 9600: the baud rate is 9600 bit/s. 14400: the baud rate is 14400 bit/s. 19200: the baud rate is 19200 bit/s. 28800: the baud rate is 28800 bit/s. 57600: the baud rate is 57600 bit/s. 115200: the baud rate is 115200 bit/s.
5	<pre>Raisecom(config-epon-onu- serial-*//*/*:*)#data-bits bits example: Raisecom(config-epon-onu- serial-3/1/1:1)#data-bits 6</pre>	Configure data bits of the serial interface. You can use the no data-bits command to restore default configuration. bits: serial interface data bit, an integer, ranging from 5 to 8

Step	Command	Description
6	<pre>Raisecom(config-epon-onu-serial-*//*/*:*)#stop-bits { 1 1.5 2 }</pre> example: <pre>Raisecom(config-epon-onu-serial-3/1/1:1)#stop-bits 2</pre>	Configure the stop bit of the serial interface. You can use the no stop-bits command to restore default configuration. - bits: stop bit of the serial interface, with the following values: • 1 • 1.5 • 2
7	<pre>Raisecom(config-epon-onu-serial-*//*/*:*)#parity { none odd even mark space }</pre> example: <pre>Raisecom(config-serial-1:1)#parity odd</pre>	Configure the check mode of the serial interface. You can use the no parity command to restore default configuration. - none: no parity check - odd: odd parity check - even: even parity check - mark: marking mode - space: spacing mode
8	<pre>Raisecom(config-epon-onu-serial-*//*/*:*)#loopback slot-id/com-id</pre> example: <pre>Raisecom(config-serial-1:1)#loopback 1/2</pre>	Configure the loopback serial interface. You can use the no loopback command to restore default configuration. slot-id/com-id: ID of the serial interface which loops back with the current serial interface, which is an integer. The slot-id refers to slot ID; the com-id refers to serial interface number; the com-id is 1.
9	<pre>Raisecom(config-epon-onu-serial-*//*/*:*)#shutdown</pre>	Shut down the serial interface. You can use the no shutdown command to enable the serial interface.
10	<pre>Raisecom(config-epon-onu-serial-*//*/*:*)#work-mode { tcp-realport tcp-client tcp-server udp }</pre> example: <pre>Raisecom(config-serial-21:1)#work-mode tcp-client</pre>	Configure the working mode of the serial interface. You can use the no work-mode command to restore default configuration. - tcp-realport: TCP realport mode - tcp-client: TCP client mode - tcp-server: TCP server mode - udp: UDP mode
11	<pre>Raisecom(config-epon-onu-serial-*//*/*:*)#service-port port-id</pre> example: <pre>Raisecom(config-serial-1:1)#service-port 5000</pre>	Configure the network service interface of the serial interface. You can use the no service-port command to restore default configuration. port-id: service interface, an integer, ranging from 1025 to 65535
12	<pre>Raisecom(config-epon-onu-serial-*//*/*:*)#peer service-port port-id</pre> example: <pre>Raisecom(config-epon-onu-serial-3/1/1:1)#peer service-port 4000</pre>	Configure the peer network service interface of the serial interface. You can use the no peer service-port command to restore default configuration. port-id: interface ID, an integer, ranging from 1025 to 65535

Step	Command	Description
13	Raisecom(config-epon-onu-serial-*/*/*:*)# peer ip-address <i>ip-address</i> example: Raisecom(config-epon-onu-serial-3/1/1:1)#peer ip-address 10.10.10.25	Configure the IP address of the serial interface. You can use the no peerip-address command to restore default configuration. ip-address: peer IP address, in dotted decimal notation, such as 10.10.10.1
14	Raisecom(config-epon-onu-serial-*/*/*:*)# connect-condition { always char dcd-on dsr-on } example: Raisecom(config-epon-onu-serial-3/1/1:1)#connect-condition char	Configure the condition to initiate a session on the serial interface. You can use the no connect-condition command to restore default configuration. - always: the device immediately starts a connection after being powered on, and will immediately reconnect even though being disconnected. - char: the device immediately starts a connection after receiving data. - dcd-on: carrier detection signals are On. - dsr-on: data ready signals are On.
15	Raisecom(config-epon-onu-serial-*/*/*:*)# session-write-right { first all } example: Raisecom(config-epon-onu-serial-3/1/1:1)#session-write-right all	Configure the write right in a session on the serial interface. - first: the first established session - all: all sessions
16	Raisecom(config-epon-onu-serial-*/*/*:*)# break-condition { none dcd-off dsr-off } example: Raisecom(config-epon-onu-serial-3/1/1:1)#break-condition dcd-off	Configure the condition to break down a session on the serial interface. You can use the no break-condition command to restore default configuration. - none: no condition - dcd-off: carrier detection signals are Off. - dsr-off: data ready signals are Off.

4.1.9 Configuring DLF and BPDU forwarding

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# epon-onu <i>slot-id/olt-id/onu-id</i>	Enter EPON ONU management configuration mode.
3	Raisecom(config-epon-onu-*/*/*:*)# d1f-pkt forwarding { enable disable }	Enable/Disable DLF packet forwarding.
4	Raisecom(config-epon-onu-*/*/*:*)# relay bpdu { enable disable }	Transparently transmit/Terminate BPDU packets.

4.1.10 Configuring partner discovery

The ONU uses Raisecom private partner discovery protocol to discover downlink Raisecom partner device, such as EoC device. You can configure the management IP address, VLAN, and so on for the partner device through the OLT to manage the partner device.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id	Enter EPON ONU management configuration mode.
3	Raisecom(config-epon-onu-*/*:*)#partner discovery { enable disable }	Enable/Disable ONU partner discovery.
4	Raisecom(config-epon-onu-*/*:*)#partner partner-id mng-ip address ip-address mask mask default-gw default-gw vlan svlan-id cvlan-id priority example: Raisecom(config-epon-onu-3/1:1)#partner 1 mng-ip 10.0.0.2 default-gw 10.0.0.1 vlan 0 10 5	(Optional) configure the management IP address of the ONU partner device. You can use the no partner partner-id mng-ip command to restore default configuration. • partner-id: partner device ID, an integer, ranging from 1 to 24 • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • mask: IP address mask, in dotted decimal notation, such as 255.0.0.0 • default-gw: default gateway, in dotted decimal notation, such as 10.10.10.1 • cvlan-id: CVLAN ID, an integer, ranging from 0 to 4094 where 0 indicates untagged • svlan-id: SVLAN ID, an integer, ranging from 0 to 4094 where 0 indicates untagged • priority: CoS priority, an integer, ranging from 0 to 7
5	Raisecom(config-epon-onu-*/*:*)#partner partner-id mng-ip address-type { dynamic manual } example: Raisecom(config-epon-onu-3/1:1)#partner 1 mng-ip address-type dynamic	(Optional) configure the management IP address type of the ONU partner device. You can use the no partner partner-id mng-ip address-type command to restore default configuration. • partner-id: partner device ID, an integer, ranging from 1 to 24 • dynamic: the IP address type is auto-configuration. • manual: the IP address type is manual configuration.
6	Raisecom(config-epon-onu-*/*:*)#partner partner-id outband default-gw default-gw example:	(Optional) configure the default gateway for out-of-band management of the ONU partner device. You can use the no partner partner-id outband default-gw command to restore default configuration.

Step	Command	Description
7	<pre>Raisecom(config-epon-onu-*/*:*)#partner partner-id outband ip- address ip-address mask example: Raisecom(config-epon-onu-3/1:1)#partner 1 outband ip-address 10.0.0.1 255.0.0.0</pre>	(Optional) configure the IP address and mask for out-of-band management of the ONU partner device. You can use the no partner partner-id outband ip-address command to restore default configuration. • partner-id: ONU partner device ID, an integer, ranging from 1 to 24 • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • mask: IP address mask, in dotted decimal notation, such as 255.0.0.0
8	<pre>Raisecom(config-epon-onu-*/*:*)#partner partner-id snmp-server host ip-address example: Raisecom(config-epon-onu-3/1:1)#partner 1 snmp-server-host 10.0.0.1 255.0.0.0</pre>	(Optional) configure the IP address of the SNMP server for the ONU partner device. You can use the no partner partner-id snmp-server host command to restore default configuration. • partner-id: ONU partner device ID, an integer, ranging from 1 to 24 • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1
9	<pre>Raisecom(config-epon-onu-*/*:*)#partner partner-id snmp-server security name example: Raisecom(config-epon-onu-3/1:1)#partner 1 snmp-server security raisecom</pre>	(Optional) configure the security principal name the SNMP server for the ONU partner device. You can use the no partner partner-id snmp-server security command to restore default configuration. • partner-id: ONU partner device ID, an integer, ranging from 1 to 24 • name: message body name, a character string
10	<pre>Raisecom(config-epon-onu-*/*:*)#partner partner-id snmp-server community name { ro rw } example: Raisecom(config-epon-onu-3/1:1)#partner 1 snmp-server community read ro</pre>	(Optional) configure the community name and properties for the ONU partner device. You can use the no partner partner-id snmp-server community command to restore default configuration. • partner-id: ONU partner device ID, an integer, ranging from 1 to 24 • name: message body name, a character string • ro: configure read-only SNMP community name. • rw: configure read-write SNMP community name.

4.1.11 Configuring PPPoE Agent

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)# epon-onu <i>slot-id/olt-id/onu-id</i> example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU remote management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*//*:*)# pppoe-agent { enable disable }	Enable/Disable PPPoE Agent.
4	Raisecom(config-epon-onu-*//*:*)#pppoe-agent user-define suboption { enable disable }	(Optional) enable/disable customizing PPPoE Agent options.
5	Raisecom(config-epon-onu-*//*:*)# pppoe-agent circuit-id attach-string <i>string</i> example: Raisecom(config-gpon-onu-3/2:1)#pppoe-agent circuit-id pppoe-0-8-1-1	(Optional) configure the attach-string field in the Circuit_ID option of PPPoE Agent. You can use the no pppoe-agent circuit-id attach-string command to restore default configuration. • string: interface customized character string, a string of 1 to 64 characters
6	Raisecom(config-epon-onu-*//*:*)#pppoe-agent remote-id mode { onumac-binary clientmac-binary onumac-ascii clientmac-ascii user-define } example: Raisecom(config-gpon-onu-3/2:1)#pppoe-agent remote-id mode onu-eth-id	(Optional) configure the filling mode of the Remote_ID option for PPPoE Agent. You can use the no pppoe-agent remote-id mode command to restore default configuration. • onu-eth-id: ONU Ethernet interface ID • onu-mac: ONU MAC address • client-mac: client MAC address • user-define: user-defined
7	Raisecom(config-epon-onu-*//*:*)# pppoe-agent remote-id string <i>string</i> Raisecom(config-epon-onu-*//*:*)# exit example: Raisecom(config-gpon-onu-3/2:1)#pppoe-agent remote-id string pppoe-0-8-1-1	(Optional) configure the user-defined value of the Remote_ID for PPPoE Agent. • string: user-defined Remote ID option, a string of 1 to 64 characters
8	Raisecom(config)# epon-onu uni ethernet <i>slot-id/olt-id/onu-id/uni-id</i> example: Raisecom(config)#epon-onu uni ethernet 3/2/1/1	Enter EPON ONU UNI configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • uni-id: ONU UNI ID
9	Raisecom(config-epon-onu-ethernet-*//*:*)# pppoe-agent circuit-id string <i>string</i> example: Raisecom(config-epon-onu-ethernet-3/2/1:1)#pppoe-agent circuit-id string pppoe-0-8-1-1	(Optional) configure the user-defined value of the Circuit_ID option for PPPoE Agent. You can use the no pppoe-agent circuit-id command to restore default configuration. • string: interface customized character string, a string of 1 to 64 characters

4.1.12 Configuring PoE

Power Over Ethernet (PoE) refers to providing power through the 10BASE-T, 100BASE-TX, or 1000BASE-T Ethernet. The reliable power distance cannot exceed 100 m. PoE can be used to provide power to cameras, data collectors, and so on

The PoE system includes the following two device types:

- Powered Device (PD): receive power through the Ethernet interface.
- Power-sourcing Equipment (PSE): provide power to other devices, and consist of the power module and PSE module.



Note

Only some ONU models can work as the PD or PSE.

Enabling PoE

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id	Enter EPON ONU UNI configuration mode.
3	Raisecom(config-epon-onu-ethernet-*/*/*:*)#poe pse { enable disable }	Enable/Disable PoE on UNI.

Configuring PoE parameters

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id example: Raisecom(config)#epon-onu uni ethernet 3/2/1/1	Enter EPON ONU UNI configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • uni-id: ONU UNI ID
3	Raisecom(config-epon-onu-ethernet-*/*/*:*)#poe pse max-power value example: Raisecom(config-epon-onu-ethernet-3/1/1:1)#poe pse max-power 5000	(Optional) configure the maximum output power of the UNI. You can use the no poe pse max-power command to restore default configuration. • value: maximum output power, an integer, ranging from: • IEEE802.3af: 4000 to 15400 • IEEE802.3at: 4000 to 30000, in units of mW

Step	Command	Description
4	Raisecom(config-epon-onu-ethernet-*/*/*:*)# poe pse power-priority { critical high low } example: Raisecom(config-epon-onu-ethernet-3/1/1:1)#poe pse power-priority high	(Optional) configure the power supply priority of UNI. You can use the no poe pse power-priority command to restore default configuration. - critical: critical priority - high: high priority - low: low priority
5	Raisecom(config-epon-onu-ethernet-*/*/*:*)# poe pse-off service { enable disable }	(Optional) configure whether to allow services to pass when the UNI is not connected with the PD.
6	Raisecom(config-epon-onu-ethernet-*/*/*:*)# poe pse compatibility { enable disable }	(Optional) configure the interface to provide power to the non-standard PD.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU management configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*/*/*:*)# poe pse power-management { auto manual } example: Raisecom(config-epon-onu-3/1:1)#poe pse power-management manual	(Optional) configure the power supply management mode. You can use the no poe pse power-management command to restore default configuration. - auto: automatic mode - manual: manual mode
4	Raisecom(config-epon-onu-*/*/*:*)# poe pse power-threshold value example: Raisecom(config-epon-onu-3/2:1)#poe pse power-threshold 80	(Optional) configure the power threshold. You can use the no poe pse power-threshold command to restore default configuration. value: power threshold percentage, namely, PSE current power/PSE rated power, an integer, ranging from 1 to 99 indicating 1% to 99%
5	Raisecom(config-epon-onu-*/*/*:*)# poe pse temperature-protection { enable disable }	(Optional) enable/disable overtemperature protection on the PoE module.
6	Raisecom(config-epon-onu-*/*/*:*)# poe pse trap { enable disable }	(Optional) enable/disable Trap report on the PoE module.

4.1.13 Configuring IP interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/1/1	Enter EPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*//*:*)#ip-if ip-if address ip-address [mask] [vlan vlan-id] default-gw ip-address example: Raisecom(config-epon-onu-3/1:1)#ip-if 1 address 10.0.0.2 vlan 10 default-gw 10.0.0.1	(Optional) configure the IP interface address, VLAN ID, and default gateway. • ip-if: IP interface, an integer, ranging from 0 to 14 • address ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • mask: IP address mask, in dotted decimal notation, such as 255.0.0.0 • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • default-gw ip-address: default gateway, in dotted decimal notation, such as 10.10.10.1
4	Raisecom(config-epon-onu-*//*:*)#iptv-mode { sdtv hdtv } example: Raisecom(config-epon-onu-3/1:1)#iptv-mode sdtv	(Optional) configure the IPTV mode. • sdtv: standard definition TV • hdtv: high definition TV

4.1.14 Configuring performance monitoring on PON interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*//*:*)#pon performance monitoring enable	(Optional) enable performance monitoring on the PON interface. You can use the pon performance monitoring disable command to disable this function.
4	Raisecom(config-epon-onu-*//*:*)#pon performance monitoring period value example: Raisecom(config-epon-onu-3/2:1)#pon performance monitoring period 10	(Optional) configure the PON performance monitoring period. • value: PON performance detection time, an integer, ranging from 1 to 2147483647, in units of second

4.1.15 Configuring ONU HTTP access control mode

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*/*:*)#http-access-control mode { allowall allowlan allowwan blockall } example: Raisecom(config-epon-onu-3/1:1)#http-access-control mode allowall	Configure the ONU HTTP access control mode. • allowall: allow all accesses. • allowlan: allow LAN access. • allowwan: allow WAN access. • blockall: deny all accesses.

4.1.16 Configuring SNMP Trap

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*/*:*)#snmp trap power { enable disable }	(Optional) enable ONU SNMP Trap power anomaly alarm. You can use the snmp trap power disable command to disable this function.
4	Raisecom(config-epon-onu-*/*:*)#snmp trap { temperature-high temperature-low } { disable enable threshold value [value] } example: Raisecom(config-epon-onu-3/1:1)#snmp trap temperature-high enable	(Optional) configure SNMP Trap. • temperature-high: temperature over high • temperature-low: temperature over low • threshold value: alarm threshold, an integer, ranging from 0 to 127 • value: alarm clearing threshold, an integer, ranging from 0 to 127
5	Raisecom(config-epon-onu-*/*:*)#snmp trap transceiver { bias rx-power temp tx-power voltage } { high-alarm high-warning low-alarm low-warning } { disable enable threshold value clear-value } example: Raisecom(config-epon-onu-3/1:1)#snmp trap transceiver bias high-alarm enable	(Optional) configure the SNMP Trap optical module. • bias: bias current • rx-power: Rx optical power • temp: temperature • tx-power: Tx optical power • voltage: voltage • high-alarm: high alarm • high-warning: high warning • low-alarm: low alarm • low-warning: low warning

		• disable: disable SNMP Trap optical module. • enable: enable SNMP Trap optical module. • threshold value: alarm generation threshold, an integer, ranging from 0 to 131070 • clear-value: alarm clearance threshold
6	Raisecom(config-epon-onu-*/:*)#snmp trap pon { down-crc-error-alarm down-crc-error-warning down-discard-alarm down-discard-warning down-drop-event-alarm down-drop-event-warning down-error-alarm down-error-warning down-fragment-alarm down-fragment-warning down-jabber-alarm down-jabber-warning down-oversize-alarm down-oversize-warning down-undersize-alarm down-undersize-warning up-crc-error-alarm up-crc-error-warning up-discard-alarm up-discard-warning up-drop-event-alarm up-drop-event-warning up-error-alarm up-error-warning up-fragment-alarm up-fragment-warning up-jabber-alarm up-jabber-warning up-oversize-alarm up-oversize-warning up-undersize-alarm up-undersize-warning } { enable disable threshold <i>value</i> <i>clear-value</i> } example: Raisecom(config-epon-onu-3/1:1)#snmp trap pon down-crc-error-alarm enable	(Optional) configure SNMP Trap PON interface. • down-crc-error-alarm: alarm threshold of downstream CRC error packets • down-crc-error-warning: warning threshold of downstream CRC error packets • down-discard-alarm: alarm threshold of downstream dropped packets • down-discard-warning: warning threshold of downstream dropped packets • down-drop-event-alarm: alarm threshold of downstream packet loss events • down-drop-event-warning: warning threshold of downstream packet loss events • down-error-alarm: alarm threshold of downstream error packets • down-error-warning: warning threshold of downstream error packets • down-fragment-alarm: alarm threshold of downstream Fragments • down-fragment-warning: warning threshold of downstream Fragments • down-jabber-alarm: alarm threshold of downstream Jabbers • down-jabber-warning: warning threshold of downstream Jabbers • down-oversize-alarm: alarm threshold of downstream oversize packets • down-oversize-warning: warning threshold of downstream oversize packets • down-undersize-alarm: alarm threshold of downstream downsize packets • down-undersize-warning: warning threshold of downstream undersize packets • up-crc-error-alarm: alarm threshold of upstream CRC error packets • up-crc-error-warning: warning threshold of upstream CRC error packets • up-discard-alarm: alarm threshold of upstream dropped packets • up-discard-warning: warning threshold of upstream dropped packets • up-drop-event-alarm: alarm threshold of upstream packet loss events • up-drop-event-warning: warning threshold of upstream packet loss events • up-error-alarm: alarm threshold of upstream error packets • up-error-warning: warning threshold of upstream error packets

		• up-fragment-alarm: alarm threshold of upstream Fragments • up-fragment-warning: warning threshold of upstream Fragments • up-jabber-alarm: alarm threshold of upstream Jabbers • up-jabber-warning: warning threshold of upstream Jabbers • up-oversize-alarm: alarm threshold of upstream oversize packets • up-oversize-warning: warning threshold of upstream oversize packets • up-undersize-alarm: alarm threshold of upstream undersize packets • up-undersize-warning: warning threshold of upstream undersize packets • enable: enable SNMP Trap on the PON interface. • disable: disable SNMP Trap on the PON interface. • threshold value: alarm generation threshold value, an integer, ranging from 1 to 2147483647 • clear-value: alarm clearance threshold, an integer, ranging from 1 to 2147483647

4.1.17 Configuring EPON ONU WAN interface

Configuring IP mode of EPON ONU WAN interface

Configure the device on which the EPON ONU WAN interface needs to be configured to IP static operation mode.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*/*:*)#wan id mode static example: Raisecom(config-epon-onu-3/2:1)#wan id mode static	Configure the IP mode of the EPON ONU WAN interface to IP static mode. • id: WAN index, an integer, ranging from 1 to 8

Step	Command	Description
4	Raisecom(config-epon-onu-*/*:*)#wan id static ip-address <i>ip-address</i> [<i>mask-address</i>] default-gw <i>ip-address</i> [primary-dns <i>ip-address</i>] [secondary-dns <i>ip-address</i>] example: <pre>Raisecom(config-epon-onu-3/1:1)#wan 1 static ip-address 10.0.0.2 255.255.255.0 default-gw 10.0.0.1 primary-dns 10.0.0.3</pre>	Configure the static IP address of the EPON ONU WAN interface. • id: WAN index, an integer, ranging from 1 to 8 • ip-address: static IP address, in dotted decimal notation, such as 10.10.10.1 • mask-address: IP address mask, in dotted decimal notation, such as 255.0.0.0 • default-gw ip-address: gateway IP address, in dotted decimal notation, such as 10.10.10.1 • primary-dns ip-address: primary DNS server IP address, in dotted decimal notation, such as 10.10.10.1 • secondary-dns ip-address: secondary DNS server IP address, in dotted decimal notation, such as 10.10.10.1
	Raisecom(config-epon-onu-*/*:*)#wan id static ipv6-address <i>ipv6-address</i> default-gw <i>ipv6-address</i> [primary-dns <i>ipv6-address</i>] [secondary-dns <i>ipv6-address</i>] example: <pre>Raisecom(config-epon-onu-3/1:1)#wan 1 static ip-address 3001: : 1 default-gw 3002: : 1 primary-dns 3003: : 1</pre>	Configure the static IPv6 address of the EPON ONU WAN interface. • id: WAN index, an integer, ranging from 1 to 8 • ipv6-address: static IPv6 address, IPv6 address, in colon hexadecimal notation, 3001::1 • default-gw ipv6-address: gateway IPv6 address, IPv6 address, in colon hexadecimal notation, 3001::1 • primary-dns ipv6-address: primary DNS server IPv6 address, in colon hexadecimal notation, 3001::1 • secondary-dns ipv6-address: secondary DNS server IPv6 address, in colon hexadecimal notation, 3001::1

Configure the device on which the EPON ONU WAN interface needs to be configured to IP DHCP operation mode.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: <pre>Raisecom(config)#epon-onu 3/2/1</pre>	Enter EPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*/*:*)#wan id mode dhcp example: <pre>Raisecom(config-epon-onu-3/2:1)#wan 1 mode dhcp</pre>	Configure the EPON ONU WAN interface to IP DHCP operation mode. • id: WAN index, an integer, ranging from 1 to 8

Configure the device on which the EPON ONU WAN interface needs to be configured to IP PPPoE operation mode.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*/*:*)#wan id mode pppoe example: Raisecom(config-epon-onu-3/2:1)#wan 1 mode pppoe	Configure the EPON ONU WAN interface to IP PPPoE operation mode. • id: WAN index, an integer, ranging from 1 to 8
4	Raisecom(config-epon-onu-*/*:*)#wan id pppoe { username username password password } example: Raisecom(config-epon-onu-3/1:1)#wan 1 vlan mode tag	Configure the PPPoE user name and password of the EPON ONU WAN interface. • id: WAN index, an integer, ranging from 1 to 8 • username: user name, a string of 1 to 64 characters • password: password, an integer, ranging from 1 to 32
5	Raisecom(config-epon-onu-*/*:*)#wan id service pppoe-srv-name name example: Raisecom(config-epon-onu-3/1:1)#wan 1 service pppoe-srv-name raisecom	Configure the EPON ONU PPPoE service name. • id: WAN index, an integer, ranging from 1 to 8 • name: ONU PPPOE service name, a string of 1 to 31 characters

Configuring services on EPON ONU WAN interface

Configure the device on which the EPON ONU WAN interface should be configured with a service mode.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/1/1	Enter EPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface

Step	Command	Description
3	<pre>Raisecom(config-epon-onu- /*:*)#wan id service mode { route [nat { enable disable }] bridge hybrid [nat { enable disable }]} cos cos [portlist portlist] [ssidlist ssidlist] example: Raisecom(config-epon-onu- 3/1:1)#wan 1 service mode route cos 1</pre>	Configure the service mode of the EPON ONU WAN interface. • id: WAN index, an integer, ranging from 1 to 8 • route: routing mode • hybrid: hybrid mode • bridge: bridge mode • enable: enable NAT. • disable: disable NAT. • cos: priority, an integer, ranging from 0 to 7 • portlist: configure the interface list, which is an integer ranging from 1 to 8. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • ssidlist: configure the SSID list, which is an integer ranging from 1 to 8. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
4	<pre>Raisecom(config-epon-onu- /*:*)#wan id service { internet iptv voip- signalling voip-media management } example: Raisecom(config-epon-onu- 3/1:1)#wan 1 service internet</pre>	Configure the service type of the EPON ONU WAN interface. • id: WAN index, an integer, ranging from 1 to 8 • internet: Internet • iptv: IPTV • voip-signalling: voice signalling • voip-media: voice media • management: management
5	<pre>Raisecom(config-epon-onu- /*:*)#wan id vlan vlan-id example: Raisecom(config-epon-onu- 3/1:1)#wan 1 vlan 1</pre>	Configure the VLAN bound to the ONU WAN interface. • id: WAN index, an integer, ranging from 1 to 8 • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
6	<pre>Raisecom(config-epon-onu- /*:*)#wan id vlan mode { tag untag } example: Raisecom(config-epon-onu- 3/1:1)#wan id vlan mode tag</pre>	Configure the VLAN mode of the EPON ONU WAN interface. • id: WAN index, an integer, ranging from 1 to 8 • tag: tagged mode • untag: untagged mode

Configuring rate limiting on EPON ONU WAN interface

Configure the device on which the EPON ONU WAN interface should be configured with rate limiting.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/1/1</pre>	Enter EPON ONU management configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-epon-onu- */*:*)#wan id policing { ingress egress both } { enable disable } example: Raisecom(config-epon-onu- 3/1:1)#wan 1 policing ingress enable</pre>	Enable rate limiting on the EPON ONU WAN interface. You can use the disable form of this command to disable this function. - id: WAN index, an integer, ranging from 1 to 8 - ingress: uplink rate limiting - egress: downlink rate limiting - both: rate limiting in both uplink and downlink - enable: enable - disable: disable
4	<pre>Raisecom(config-epon-onu- */*:*)#wan id { ingress egress } pir pir example: Raisecom(config-epon-onu- 3/1:1)#wan 1 ingress pir 100</pre>	Configure the peak rate of EPON ONU WAN interface rate limiting. You can use the no form of this command to delete the configuration. - id: WAN index, an integer, ranging from 1 to 8 - ingress: uplink rate limiting - egress: downlink rate limiting - pir: peak rate, an integer, ranging from 1 to 1048568, in units of Kbps

Configuring the IP type of EPON ONU WAN interface

Configure the device on which the EPON ONU WAN interface should be configured with the IP type.

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/1/1</pre>	Enter EPON ONU management configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-epon-onu- */*:*)#wan id ip-type { ipv4 ipv6 ipv4-ipv6 } example: Raisecom(config-epon-onu- 3/1:1)#wan 1 ip-type ipv4</pre>	Configure the IP type of the EPON ONU WAN interface. You can use the no form of this command to delete this configuration. - id: WAN index, an integer, ranging from 1 to 8 - ipv4: the IP type is IPv4. - ipv6: the IP type is IPv6. - ipv4-ipv6: the IP type is IPv4-IPv6.

Step	Command	Description
4	<pre>Raisecom(config-epon-onu- */:*)#wan id global-addr-mode { auto-no-status dhcp manual }</pre> example: <pre>Raisecom(config-epon-onu- 3/1:1)#wan 1 global-addr-mode auto-no-status</pre>	Configure the IPv6 global address obtainment mode. You can use the no form of this command to delete this configuration. • id: WAN index, an integer, ranging from 1 to 8 • auto-no-status: stateless automatic obtainment mode • dhcp: DHCP mode • manual: manual mode
5	<pre>Raisecom(config-epon-onu- */:*)#wan id ipv6-ds-lite { enable disable }</pre> example: <pre>Raisecom(config-epon-onu- 3/1:1)#wan 1 ipv6-ds-lite enable</pre>	Enable WAN IPv6 DSLite. You can use the disable form of this command to disable this function. • id: WAN index, an integer, ranging from 1 to 8 • enable: stateless automatic obtainment mode • disable: DHCP mode
6	<pre>Raisecom(config-epon-onu- */:*)#wan id aftr-mode { dhcpv6 manual }</pre> example: <pre>Raisecom(config-epon-onu- 3/1:1)#wan 1 aftr-mode dhcpv6</pre>	Configure the IPv6 DSLite AFTR obtainment mode. • id: WAN index, an integer, ranging from 1 to 8 • dhcpv6: DHCPv6 mode • manual: manual mode
7	<pre>Raisecom(config-epon-onu- */:*)#wan id aftr-address address</pre> example: <pre>Raisecom(config-epon-onu- 3/1:1)#wan 1 aftr-address 123</pre>	Configure the IPv6 AFTR address. You can use the no form of this command to delete this configuration. • id: WAN index, an integer, ranging from 1 to 8 • address: IPv6 AFTR address, a string of 1 to 64 characters

4.1.18 Configuring DHCP Server

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#create dhcp-server-profile <i>profile-id</i> [name <i>profile-name</i>]	Create a DHCP server template. You can use the no create dhcp-server-profile profile-list command to delete the DHCP server template.
3	Raisecom(config)#dhcp-server-profile <i>profile-id</i>	Enter the configuration mode of the specified DHCP server template.
4	Raisecom(config-dhcp-server-profile:*)#name <i>vlan-name</i>	Configure the name of the DHCP server template. You can use the no form of this command to restore to the default condition.

Step	Command	Description
5	Raisecom(config-dhcp-server-profile:*)# dhcp-server { enable disable }	Enable DHCP Server. You can use the disable form of this command to disable this function.
6	Raisecom(config-dhcp-server-profile:*)# dhcp-server subnet-ip-address mask-address start-ip-address end-ip-address [gateway ip-address] [primary-dns ip-address] [secondary-dns ip-address]	Configure the DHCP server subnet IP address and subnet mask, start and end IP address, gateway IP address, primary/backup DNS server address. You can use the no dhcp-server ip-address command to restore to the default condition.
7	Raisecom(config-dhcp-server-profile:*)# dhcp-server reserved-ip-address ip-address [ip-address] [ip-address] [ip-address] [ip-address] [ip-address] [ip-address] [ip-address]	Configure the DHCP server to reserve the IP address. You can use the no dhcp-server reserved-ip-address command to restore to the default condition.
8	Raisecom(config-dhcp-server-profile:*)# dhcp-server lease-time days hours minutes	Configure the lease time of the DHCP server. You can use the no dhcp-server lease-time command to restore to the default condition..
9	Raisecom(config-dhcp-server-profile:*)# dhcp-server max-lease-time 100	(Optional) configure the maximum lease time of the DHCP server. You can use the no dhcp-server lease-time command to restore to the default condition.

4.1.19 Configuring LAN interface VLAN

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# epon-onu-service-profile 1 profile-id	Enter EPON ONU service template configuration mode.
3	Raisecom(config-epon-onu-service-profile:*)# create lan-vlan vlan-id [ip-address ip-address ip-mask]	Create the LAN interface VLAN. You can use the no create lan-vlan vlan-id command to delete it.
4	Raisecom(config-epon-onu-service-profile:*)# lan-vlan vlan-id ip-address ip-address ip-mask	Configure the IP address and mask of the VLAN interface. You can use the no lan-vlan vlan-id ip-address command to delete the configuration.
5	Raisecom(config-epon-onu-service-profile:*)# lan-vlan vlan-id dhcp-server-profile profile-id Raisecom(config-epon-onu-service-profile:*)# exit	Bind the VLAN interface with the DHCP server template. You can use the no lan-vlan vlan-id dhcp-server-profile command to delete the configuration.
6	Raisecom(config)# epon-onu slot-id/olt-id/onu-id	Enter EPON ONU management configuration mode.

Step	Command	Description
7	Raisecom(config-epon-onu- */*:*)# lan-vlan <i>vlan-id</i> ip- address <i>ip-address ip-mask</i>	Configure the IP address and mask of the VLAN interface. You can use the no lan-vlan <i>vlan-id</i> ip-address command to delete the configuration.
8	Raisecom(config-epon-onu- */*:*)# lan-vlan <i>vlan-id</i> dhcp-server-profile <i>profile- id</i> Raisecom(config-epon-onu- */*:*)# exit	Bind the VLAN interface with the DHCP server template. You can use the no lan-vlan <i>vlan-id</i> dhcp-server-profile command to delete the configuration.

4.1.20 Checking configurations

No.	Command	Description
1	Raisecom# show epon-onu <i>slot-id/olt- id/onu-id</i> information	Show basic information about the ONU, including the name of the ONU.
2	Raisecom# show epon-onu <i>slot-id/olt- id/onu-id</i> detail-information	Show detailed information about the ONU, including ONU model and MAC address.
3	Raisecom# show epon-onu <i>slot-id/olt- id/onu-id</i> pon-chip information	Show information about the ONU PON chip.
4	Raisecom# show epon-onu <i>slot-id/olt- id/onu-id</i> capability	Show ONU capability.
5	Raisecom# show interface epon-onu <i>slot- id/olt-id/onu-id</i> creation-information	Show creation information about the ONU, including the management mode of the ONU.
6	Raisecom# show epon-onu <i>slot-id/olt- id/onu-id</i> mng-ip	Show the management IP address of the ONU PON interface.
7	Raisecom# show epon-onu <i>slot-id/olt- id/onu-id</i> lan-ip	Show the IP address of the ONU UNI.
8	Raisecom# show epon-onu <i>slot-id/olt- id/onu-id</i> telnet	Show the status of ONU Telnet.
9	Raisecom# show epon-onu <i>slot-id/olt- id/onu-id</i> uni ethernet uni-id name	Show the name of the UNI.
10	Raisecom# show epon-onu <i>slot-id/olt- id/onu-id</i> uni ethernet uni-id information	Show information about the UNI, such as rate, duplex mode, flow control, and connection status.
11	Raisecom# show epon-onu <i>slot-id/olt- id/onu-id</i> uni ethernet uni-id isolation	Show the status of UNI isolation.
12	Raisecom# show epon-onu <i>slot-id/olt- id/onu-id</i> uni ethernet uni-id alarm	Show the status of UNI Loss alarm.
13	Raisecom# show epon-onu <i>slot-id/olt- id/onu-id</i> mirror	Show port mirroring configurations of the ONU.
14	Raisecom# show epon-onu <i>slot-id/olt- id/onu-id</i> system	Show system configurations of the ONU, including BPDU transparent transmission and DLF packet forwarding.

No.	Command	Description
15	Raisecom#show epon-onu slot-id/olt-id/onu-id partner [discovery]	Show the status and configurations of ONU partner discovery.
16	Raisecom#show epon-onu slot-id/olt-id/onu-id partner [partner-id]	Show information about the ONU partner device.
17	Raisecom#show epon-onu slot-id/olt-id/onu-id partner [partner-id] snmp-server	Show SNMP parameters of the ONU partner device.
18	Raisecom#show epon-onu slot-id/olt-id/onu-id poe pse information	Show ONU power information.
19	Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet [uni-id] poe pse information	Show configurations of the PSE interface for the ONU UNI.
20	Raisecom#show epon-onu slot-id/olt-id/onu-id poe information	Show ONU UNI power information.
21	Raisecom#show epon-onu slot-id/olt-id/onu-list pppoe-agent	Show PPPoE configurations of the ONU.
22	Raisecom#show epon-onu slot-id/olt-id/onu-list uni ethernet [uni-id] pppoe-agent	Show PPPoE interface configurations of the ONU.
23	Raisecom#show epon-onu slot-id/olt-id/onu-list uni ethernet [uni-id] pppoe-agent statistics	Show PPPoE statistics of the ONU.
24	Raisecom#show epon-onu slot-id/olt-id/onu-list mng-information	Show management information about the ONU.
25	Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id information	Show parameters of the ONU serial interface.
26	Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id auto-negotiation ability	Show configurations for ONU serial interface management.
27	Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id name	Show configurations of the ONU serial interface service.
28	Raisecom#show epon-onu slot-id/olt-id/onu-id system	Show information about ONU serial interface session.
29	Raisecom#show epon-onu slot-id/olt-id/onu-list config-counter	Show the value of the configuration counter at the OLT/ONU side.
30	Raisecom#show interface epon-onu slot-id/olt-id/onu-list oam loopback	Show configurations of OAM remote loopback.
31	Raisecom#show interface epon-onu slot-id/olt-id/onu-list oam	Show local configurations and status of the OAM channel, including mode configuration, management status, working status, MTU, configuration version, and supported functions.
32	Raisecom#show interface epon-onu slot-id/olt-id/onu-list oam peer	Show information about the peer device on the OAM channel.
33	Raisecom#show interface epon-onu slot-id/olt-id/onu-list oam peer event	Show events reported by the peer ONU, including fault and link monitoring event.

No.	Command	Description
34	<code>Raisecom#show interface epon-onu slot-id/olt-id/onu-list oam statistics</code>	Show OAM statistics.
35	<code>Raisecom#show interface epon-onu slot-id/olt-id/onu-list encryption</code>	Show configurations of ONU data encryption.
36	<code>Raisecom#show interface epon-onu slot-id/olt-id/onu-id sla</code>	Show configurations of ONU uplink SLA configurations made through the OLT.
37	<code>Raisecom#show interface epon-onu slot-id/olt-id/onu-id fec</code>	Show the status of ONU FEC.
38	<code>Raisecom#show epon-onu slot-id/olt-id/onu-list environment</code>	Show the ambient temperature and power voltage of the ONU.
39	<code>Raisecom#show epon-onu device-type onu-type snmp trap</code>	Show SNMP Trap information of specified ONU model.
40	<code>Raisecom#show interface epon-onu slot-id/olt-id/onu-list mpcp</code>	Show MPCP information about the ONU.
41	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id wan id policing</code>	Show rate limiting over the EPON ONU WAN interface.
42	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id wan [id] information</code>	Show information about the EPON ONU WAN interface.
43	<code>Raisecom#show dhcp-server-profile { all profile-list }</code>	Show configurations of the DHCP server template.
44	<code>Raisecom#show version epon-onu slot-id/olt-id/onu-list</code> <code>Raisecom#show version epon-onu epon-olt slot-id/olt-list</code> <code>Raisecom#show version epon-onu slot slot-list</code> <code>Raisecom#show version epon-onu ten-giga-epon-olt slot-id/olt-list</code>	Show the ONU version.
45	<code>Raisecom(config)#show epon-onu eoc</code>	Show the status of EOC ONU resource synchronization.

4.2 Configuring GPON ONU

4.2.1 Default configurations

Function	Default values
ONU access control mode	Allow LAN access.
UNI alarm suppression	Disabled
UNI flow control	Disabled
ONU UNI interface loopback status	Non-loopback

Function	Default values
Default VLAN ID of the ONU interface	VLAN 1
Alarm threshold of ONU Rx optical power	The high alarm threshold is 0. The low alarm threshold is -80 (namely, -80×0.5 dBm).
Alarm threshold of ONU Tx optical power	The high alarm threshold is 12 (namely, 12×0.5 dBm). The low alarm threshold is 0.
Circuit ID padding mode	user-define
PPPoE proxy	Disabled
Remote ID padding mode	user-define
UNI interface status	Enabled
UNI rate and duplex mode	Auto-negotiation

4.2.2 Basic configurations

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# gpon-onu slot-id/olt-id/onu-id	Enter GPON ONU management configuration mode.
3	Raisecom(config-gpon-onu-*/*:*)# reboot [now]	(Optional) restart the ONU.  Note The system also supports rebooting the ONU using the reboot gpon-onu [all slot-id/olt-id/onu-id] [now] command in privileged mode.

4.2.3 Configuring user interface

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# gpon-onu uni ethernet slot-id/olt-id/onu-id/uni-id example: Raisecom(config)#gpon-onu uni ethernet 3/2/1/1	Enter GPON ONU UNI configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface - uni-id: ONU UNI ID
3	Raisecom(config-gpon-onu-ethernet-*/*:*)# shutdown	(Optional) disable the interface.

Step	Command	Description
4	<pre>Raisecom(config-gpon-onu-ethernet-*/*/*:*)#speed auto</pre> <pre>Raisecom(config-gpon-onu-ethernet-*/*/*:*)#speed { 10 100 1000 } duplex { half full }</pre> example: <pre>Raisecom(config-gpon-onu-ethernet-3/1/1:1)#speed 100 duplex full</pre>	(Optional) configure the interface rate and duplex mode. • auto: auto-negotiation of rate and duplex mode • 10: the rate is forced 10 Mbit/s. • 100: the rate is forced 100 Mbit/s. • 1000: the rate is forced 1000 Mbit/s. • full: full duplex mode • half: half duplex mode
5	<pre>Raisecom(config-gpon-onu-ethernet-*/*/*:*)#loopback { enable disable }</pre>	(Optional) enable/disable interface loopback.
6	<pre>Raisecom(config-gpon-onu-ethernet-*/*/*:*)#flowcontrol { enable disable }</pre>	(Optional) enable/disable interface flow control.
7	<pre>Raisecom(config-gpon-onu-ethernet-*/*/*:*)#alarm-control { enable interval { time always } disable }</pre> example: <pre>Raisecom(config-gpon-onu-ethernet-3/1/1:1)#alarm-control enable interval 10</pre>	(Optional) enable/disable interface alarm suppression. • enable: enable UNI alarm suppression. • disable: disable UNI alarm suppression. • interval time: alarm suppression time, an integer, ranging from 0 to 254 where 0 indicates suppression for one time, in units of second • always: always
8	<pre>Raisecom(config-gpon-onu-ethernet-*/*/*:*)#pppoe-filter { enable disable }</pre>	(Optional) enable/disable PPPoE packet suppression on the interface.  Note When this function is enabled, the interface only allows PPPoE packets to pass.
9	<pre>Raisecom(config-gpon-onu-ethernet-*/*/*:*)#poe pse { enable disable }</pre>	(Optional) enable/disable interface PPPoE.

4.2.4 Configuring PPPoE proxy

PPoE Proxy is mainly used to process a specific tag in a PPPoE packet. The tag contains two fields: Circuit ID and Remote ID.

- The circuit ID is filled with the VLAN ID, interface number, and host name information of the interface that receives the client request packet.
- The remote ID is filled with the MAC address of the client or the MAC address of the ONU.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)# gpon-onu <i>slot-id/olt-id/onu-id</i> example: Raisecom(config)#gpon-onu 1/3/1	Enter GPON ONU management configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-gpon-onu-*/*:*)# pppoe-agent { enable disable }	Enable/Disable PPPoE Agent.
4	Raisecom(config-gpon-onu-*/*:*)# pppoe-agent circuit-id <i>string string</i> example: Raisecom(config-gpon-onu-1/3:1)#pppoe-agent circuit-id string pppoe-0-8-1-1	Configure the customized value of PPPoE Agent Circuit_ID Option. You can use the no pppoe-agent circuit-id string command to restore the default value of the interface customized value. string: interface customized value, a string of 1 to 64 characters
5	Raisecom(config-gpon-onu-*/*:*)# pppoe-agent circuit-id <i>mode { onu-eth-id onu-mac client-mac user-define }</i> example: Raisecom(config-gpon-onu-1/3:1)#pppoe-agent circuit-id mode onu-mac	Configure the padding mode of PPPoE Agent Circuit_ID. You can use the no pppoe-agent circuit-id mode command to restore the Remote_ID to the default value. - onu-eth-id: ONU Ethernet interface ID - onu-mac: ONU MAC address - client-mac: client MAC address - user-define: user-defined
6	Raisecom(config-gpon-onu-*/*:*)# pppoe-agent remote-id <i>string string</i> example: Raisecom(config-gpon-onu-1/3:1)#pppoe-agent remote-id string pppoe-0-8-1-1	Configure the user-defined value of PPPoE Agent Remote_ID. You can use the no pppoe-agent circuit-id string command to restore the customized value to the default one. string: user-defined Remote ID, a string of 1 to 64 characters
7	Raisecom(config-gpon-onu-*/*:*)# pppoe-agent remote-id <i>mode { onu-eth-id onu-mac client-mac user-define }</i> example: Raisecom(config-gpon-onu-1/3:1)#pppoe-agent remote-id mode onu-eth-id	Configure the padding mode of PPPoE Agent Remote_ID. You can use the no pppoe-agent remote-id mode command to restore the default value of Remote_ID. - onu-eth-id: ONU Ethernet interface ID - onu-mac: ONU MAC address - client-mac: client MAC address - user-define: user-defined

4.2.5 Configuring rate-limit profile on ETH interface

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# gpon-onu uni ethernet <i>slot-id/olt-id/onu-id/uni-id</i> example: Raisecom(config)#gpon-onu uni ethernet 3/2/1/1	Enter GPON ONU UNI configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface - uni-id: ONU UNI ID

Step	Command	Description
3	<pre>Raisecom(config-gpon-onu-ethernet-*/*/*:*)#policing-profile-name { ingress egress } name example: Raisecom(config-gpon-onu-ethernet-3/2/1:1)#policing-profile-name ingress raisecom</pre>	Configure rate limiting in the uplink and downlink of the ETH interface based on rate-limit profile name. • ingress: uplink • egress: downlink • name: profile name, a string of 1 to 16 characters

4.2.6 Configuring ONU access control mode

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#gpon-onu slot-id/olt-id/onu-id example: Raisecom(config)#gpon-onu 1/3/1</pre>	Enter GPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-gpon-onu-*/*:*)#access-control { http telnet ping https } mode { blockall allowwan allowlan allowall } example: Raisecom(config-gpon-onu-3/1:1)#access-control http mode allowwan</pre>	Configure the ONU access control mode. • http: HTTP access control • telnet: Telnet access control • ping: PING access control • https: HTTPS access control • blockall: deny all types of accesses • allowwan: allow WAN access. • allowlan: allow LAN access. • allowall: allow all accesses.

4.2.7 Configuring ONU IPHost interface

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#gpon-onu slot-id/olt-id/onu-id example: Raisecom(config)#gpon-onu 1/3/1</pre>	Enter GPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-gpon-onu-*/*:*)#iphost iphost-id dhcp example: Raisecom(config-gpon-onu-1/3:1)#iphost 2 dhcp</pre>	(Optional) configure the uplink IPHost interface mode to DHCP. • iphost-id: IPHost interface index, an integer, ranging from 1 to 8

Step	Command	Description
	Raisecom(config-gpon-onu-*/:*)#iphost <i>iphost-id</i> pppoe username <i>name</i> password <i>password</i> example: Raisecom(config-gpon-onu-1/3:1)#iphost 1 pppoe username name password 123	(Optional) configure the uplink IPHost interface mode to PPPoE and configure the user name and password. • iphost-id: IPHost interface index, an integer, ranging from 1 to 8 • name: user name • password: password
	Raisecom(config-gpon-onu-*/:*)#iphost <i>iphost-id</i> static address <i>ip-address</i> [mask <i>ip-address</i>] default-gw <i>ip-address</i> { primary-dns <i>ip-address</i> secondary-dns <i>ip-address</i> }* example: Raisecom(config-gpon-onu-1/3:1)#iphost 1 static address 10.0.0.2 default-gw 10.0.0.1 primary-dns 10.0.0.3	(Optional) configure the static IP address, gateway, and DNS server IP address of the uplink IPHost interface. • iphost-id: IPHost interface index, an integer, ranging from 1 to 8 • ip-address: management IP address, in dotted decimal notation, such as 10.10.10.10 • ip-mask: management IP mask, in dotted decimal notation, such as 255.0.0.0 • default-gw ip-address: default gateway IP address, in dotted decimal notation, such as 10.0.0.1 • primary-dns ip-address: primary DNS server address, in dotted decimal notation, such as 10.10.10.1 • secondary-dns ip-address: secondary DNS server address, in dotted decimal notation, such as 10.10.10.2
4	Raisecom(config-gpon-onu-*/:*)#iphost <i>iphost-id</i> service { internet iptv voip-sinalling voip-media management }* example: Raisecom(config-gpon-onu-1/3:1)#iphost 2 service internet	(Optional) configure the service type of IPHost interface. • iphost-id: IPHost interface index, an integer, ranging from 1 to 8 • internet: Internet access channel. The WAN interface can only automatically generate a static route. • iptv: IPTV channel. It only appears on the device supporting IPTV. • voip-sinalling: voice signaling channel. It only appears on the device supporting voice functions. • voip-media: voice media channel. It only appears on the device supporting voice functions. • management: management channel. The WAN interface can automatically generate a policy route.
5	Raisecom(config-gpon-onu-*/:*)#iphost <i>iphost-id</i> service mode { bridge hybrid route } cos <i>cos</i> [portlist <i>list</i>] [ssidlist <i>list</i>] example: Raisecom(config-gpon-onu-1/3:1)#iphost 2 service mode route cos 1	(Optional) configure ONU IPHost interface mode. • iphost-id: IPHost interface index, an integer, ranging from 1 to 8 • bridge: bridge mode • hybrid: hybrid mode • route: routing mode • cos: priority, an integer, ranging from 0 to 7 • portlist list: interface list • ssidlist list: SSID list

Step	Command	Description
6	<pre>Raisecom(config-gpon-onu- */:*)#iphost iphost-id service mode { hybrid route } nat enable example: Raisecom(config-gpon-onu- 1/3:1)#iphost2 service mode route nat enable</pre>	(Optional) enable NAT on ONU IPHost interface • iphost-id: IPHost interface index, an integer, ranging from 1 to 8 • hybrid: hybrid mode • route: routing mode • enable: enable NAT. • disable: disable NAT.
7	<pre>Raisecom(config-gpon-onu- */:*)#iphost iphost-id vlan vlan-id [priority priority] example: Raisecom(config-gpon-onu- 3/1:1)#iphost 1 vlan 10 priority 0</pre>	(Optional) configure VLAN partitions based on IPHost interface and configure the priority of the partitioned VLAN. • iphost-id: ONU IPHost interface ID, an integer, ranging from 1 to 8 • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • priority: priority of VLAN partitions, an integer, ranging from 0 to 7



Note

- The WAN interface in Internet Management mode can generate static routes and polity routes automatically.
- The WAN interface in Manangement mode can only generate policy routes automatically.
- The WAN interface in Internet mode can only generate static routes automatically.
- The Voip-sinalling Management, Voip-media Management, Voip-media, Voip-sinalling, Voip-sinalling Internet, and Voip-media Internet are supported by devices that support VoIP only. Devices in these modes can automatically generate policy routes.

4.2.8 Checking configurations

No.	Command	Description
1	Raisecom#show gpon-onu slot-id/olt-id/onu-id information	Show basic information about the ONU.
2	Raisecom#show gpon-onu slot-id/olt-id/onu-id detail-information	Show details of the ONU.
3	<pre>Raisecom#show version gpon-onu [slot- id/olt-id/onu-id list] Raisecom#show version gpon-onu slot slot- list Raisecom#show version gpon-onu gpon-olt slot-id/olt-list Raisecom#show version gpon-onu xgspon-olt slot-id/olt-list</pre>	Show the ONU version.
4	Raisecom#show gpon-onu slot-id/olt-id/onu-id capability	Show ONU capability.
5	Raisecom#show gpon-onu slot-id/olt-id/onu-id uni ethernet [uni-id] information	Show ONU UNI configurations.

No.	Command	Description
6	Raisecom#show gpon-onu slot-id/olt-id/onu-id spanning-tree	Show global spanning tree configurations of the ONU.
7	Raisecom#show gpon-onu slot-id/olt-id/onu-id uni ethernet [uni-id] spanning-tree	Show spanning tree configurations on the ONU UNI.
8	Raisecom#show onu-remote vlan translation-rule-gpon	Show configurations of VLAN mapping created on the ONU.
9	Raisecom#show onu-remote vlan aggregation-rule-gpon	Show configurations of VLAN aggregation created on the ONU.
10	Raisecom#show gpon-onu slot-id/olt-id/onu-id uni ethernet [uni-id] { statistics statistics-15min }	Show ONU UNI statistics.
11	Raisecom#show gpon-onu slot-id/olt-id/onu-id gemindex [gem-index] statistics-15min	Show ONU GEM Port statistics.
12	Raisecom#show interface gpon-olt [slot-id/olt-list] transceiver rx-onu-power	Show the Rx optical power of the OLT PON interface.
13	Raisecom#show gpon-onu [slot-id/olt-id] device statistics	Show statistics on ONU types.
14	Raisecom#show gpon-onu slot-id/olt-id/onu-id pppoe-agent	Show PPPoE configurations of the ONU.
15	Raisecom#show gpon-onu slot-id/olt-id/onu-id access-control-mode	Show the ONU access control mode.
16	Raisecom#show gpon-onu slot-id/olt-id/onu-id iphost [iphost-id] [service]	Show ONU IPHost port configurations.
17	Raisecom#show interface gpon-onu slot-id/olt-id/onu-list tcont [tcont-id] information	Show TCONT information about the GPON ONU.
18	Raisecom#show gpon-onu slot-id/olt-id/onu-list iphost [iphost-id] [access-control-mode]	Show the access control mode of the ONU IPHost interface.

4.3 Wi-Fi (EPON)

4.3.1 Configuring Wi-Fi access point

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id	Enter EPON ONU management configuration mode.
3	Raisecom(config-epon-onu-*//*:*)# wifi id admin { enable disable }	Enable Wi-Fi access point management status. You can use the disable form of this command to disable this function.

Step	Command	Description
4	<code>Raisecom(config-epon-onu-*//*:*)# wifi id countrycode code</code>	Configure the country code of the Wi-Fi access point.
5	<code>Raisecom(config-epon-onu-*//*:*)# wifi id standard { 802.11ac 802.11b 802.11bg 802.11bgn 802.11g 802.11n 802.11gn }</code>	Configure the standard of the Wi-Fi access point.
6	<code>Raisecom(config-epon-onu-*//*:*)# wifi id channel channelid</code>	Configure the channel of the Wi-Fi access point.
7	<code>Raisecom(config-epon-onu-*//*:*)# wifi id power power</code>	Configure the power of the Wi-Fi access point.
8	<code>Raisecom(config-epon-onu-*//*:*)# wifi id type { 2.4g 5g }</code>	Configure the type of the Wi-Fi access point.

4.3.2 Configuring virtual Wi-Fi access point

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</code>	Enter EPON ONU management configuration mode.
3	<code>Raisecom(config-epon-onu-*//*:*)# wifi id wifi-vir-ap vir-id admin { enable disable }</code>	Enable the management status of the virtual Wi-Fi access point. You can use the disable form of this command to disable this function.
4	<code>Raisecom(config-epon-onu-*//*:*)# wifi id wifi-vir-ap vir-id auth mode { unauth wep-open wep-share wpa wpa2 wpa2-mixed }</code>	Configure the authentication mode of the virtual WIFI access point.
5	<code>Raisecom(config-epon-onu-*//*:*)# wifi id wifi-vir-ap vir-id client isolate { enable disable }</code>	Configure user isolation of the virtual Wi-Fi access point.
6	<code>Raisecom(config-epon-onu-*//*:*)# wifi id wifi-vir-ap vir-id client max num</code>	Configure the maximum number of client accesses to the virtual WIFI access point.
7	<code>Raisecom(config-epon-onu-*//*:*)# wifi id wifi-vir-ap vir-id hide { enable disable }</code>	Enable the hidden status of the virtual Wi-Fi access point. You can use the disable form of this command to disable this function.
8	<code>Raisecom(config-epon-onu-*//*:*)# wifi id wifi-vir-ap vir-id ssid-name name</code>	Configure the SSID name of the virtual Wi-Fi access point.

Step	Command	Description
9	<pre>Raisecom(config-epon-onu-*//*:*)# wifi id wifi-vir-ap vir-id wep key key Raisecom(config-epon-onu-*//*:*)# wifi id wifi-vir-ap vir-id wepdefkey key length { 128bit 64bit } Raisecom(config-epon-onu-*//*:*)# wifi id wifi-vir-ap vir-id wpa encryptionmode { aes mixed tkip } Raisecom(config-epon-onu-*//*:*)# wifi id wifi-vir-ap vir-id wpa key key</pre>	Configure the authentication mode of the virtual Wi-Fi access point.
10	<pre>Raisecom(config-epon-onu-*//*:*)# wifi id wifi-vir-ap vir-id rate { 11m 12m 18m 1m 24m 2m 36m 48m 5.5m 54m 6m 9m auto mcs0 mcs1 mcs10 mcs11 mcs12 mcs13 mcs14 mcs15 mcs2 mcs3 mcs4 mcs5 mcs6 mcs7 mcs8 mcs9 }</pre>	Configure the working rate of the virtual Wi-Fi access point.

4.3.3 Checking configurations

No.	Command	Description
1	<pre>Raisecom# show epon-onu slot-id/olt-id/onu-id wifi id information</pre>	Show EPON ONU Wi-Fi configurations.
2	<pre>Raisecom# show epon-onu slot-id/olt-id/onu-id wifi id wifi-vir-ap vir-id information</pre>	Show EPON ONU virtual Wi-Fi configurations.

4.4 Wi-Fi (GPON)

4.4.1 Configuring Wi-Fi

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#gpon-onu slot-id/olt-id/onu-id example: Raisecom(config)#gpon-onu 1/3/1</pre>	Enter GPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-gpon-onu-*//*:*)#wifi admin enable</pre>	Enable Wi-Fi management status. You can use the wifi admin disable command to disable this function.

Step	Command	Description
4	Raisecom(config-gpon-onu-*//*:*)# wifi country code <i>id</i> example: Raisecom(config-gpon-onu-1/1:1)#wifi country code 1	Configure the Wi-Fi country code. • id: country code, an integer, ranging from 1 to 2000
5	Raisecom(config-gpon-onu-*//*:*)# wifi standard { 802.11b 802.11bg 802.11bgn 802.11g 802.11n 802.11ng } example: Raisecom(config-gpon-onu-1/1:1)#wifi standard 802.11b	Configure the Wi-Fi standard. • 802.11b: wireless standard 802.11b • 802.11bg: wireless standard 802.11bg • 802.11bgn: wireless standard 802.11bgn • 802.11g: wireless standard 802.11g • 802.11n: wireless standard 802.11n • 802.11ng: wireless standard 802.11ng

4.4.2 Configuring 5G Wi-Fi

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# gpon-onu <i>slot-id/olt-id/onu-id</i>	Enter GPON ONU remote management configuration mode.
3	Raisecom(config-gpon-onu-*//*:*)# wifi-5g admin enable	Enable Wi-Fi administrative status. You can use the wifi-5g admin disable command to disable this function.
4	Raisecom(config-gpon-onu-*//*:*)# wifi-5g country code <i>id</i>	Configure the 5G Wi-Fi country code.
5	Raisecom(config-gpon-onu-*//*:*)# wifi-5g standard { 802.11a 802.11acna 802.11na }	Configure the 5G Wi-Fi standard.

4.4.3 Configuring Wi-Fi access point

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# gpon-onu <i>slot-id/olt-id/onu-id</i> example: Raisecom(config)#gpon-onu 1/3/1	Enter GPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-gpon-onu-*//*:*)# wifi-ap <i>id</i> admin enable example: Raisecom(config-gpon-onu-1/3:1)#wifi-ap 1 admin enable	Enable Wi-Fi access point management. You can use the wifi-ap id admin disable command to disable this function. • id: wireless access point ID, an integer, ranging from 1 to 8

Step	Command	Description
4	<pre>Raisecom(config-gpon-onu-*//*:*)#wifi-ap id auth mode { unauth wep-open wep-share wpa wpa2 wpa2-mixed } example: Raisecom(config-gpon-onu-1/3:1)#wifi-ap 1 auth mode unauth</pre>	Configure the authentication mode of the Wi-Fi access point. • unauth: unauthenticated • wep-open: WEP open mode • wep-share: WEP shared mode • wpa: WPA mode • wpa2: WPA2 mode • wpa2-mixed: WPA2 hybrid mode
5	<pre>Raisecom(config-gpon-onu-*//*:*)#wifi-ap id client isolate enable example: Raisecom(config-gpon-onu-1/1:1)#wifi-ap 1 client isolate enable</pre>	Enable Wi-Fi access point user isolation. You can use the wifi-ap id client isolate disable command to disable this function. • id: wireless access point ID, an integer, ranging from 1 to 8
6	<pre>Raisecom(config-gpon-onu-*//*:*)#wifi-ap id client max num example: Raisecom(config-gpon-onu-1/3:1)#wifi-ap id client max 20</pre>	Configure the maximum access clients of the Wi-Fi access point. • id: wireless access point ID, an integer, ranging from 1 to 8 • num: the number of clients, an integer, ranging from 1 to 32
7	<pre>Raisecom(config-gpon-onu-*//*:*)#wifi-ap id hidden enable example: Raisecom(config-gpon-onu-1/1:1)#wifi-ap 1 hidden enable</pre>	Configure the Wi-Fi access point to hidden status. You can use the wifi-ap id hidden disable command to disable this function. • id: wireless access point ID, an integer, ranging from 1 to 8
8	<pre>Raisecom(config-gpon-onu-*//*:*)#wifi-ap id ssid-name name example: Raisecom(config-gpon-onu-1/1:1)#wifi-ap 1 ssid-name raisecom</pre>	Configure the SSID name of the Wi-Fi access point. • id: wireless access point ID, an integer, ranging from 1 to 8 • name: SSID name, a string of 1 to 32 characters
9	<pre>Raisecom(config-gpon-onu-*//*:*)#wifi-ap id wep key key example: Raisecom(config-gpon-onu-1/1:1)#wifi-ap 1 wep key 4</pre>	(Optional) configure the authentication mode of the Wi-Fi access point to WEP and configure its secret key node. • id: wireless access point ID, an integer, ranging from 1 to 8 • key key: secret key node in wep authentication mode, an integer, ranging from 1 to 4

Step	Command	Description
10	<pre>Raisecom(config-gpon-onu-*//*:*)#wifi-ap id wepdefkey key { key key keyformat { ascii hex } keylength { 128bit 64bit } } example: Raisecom(config-gpon-onu-1/1:1)#wifi-ap 1 wepdefkey key 4</pre>	(Optional) configure the default key of the WEP authentication mode of the Wi-Fi access point. • id: wireless access point ID, an integer, ranging from 1 to 8 • key key: secret node in wep authentication mode, an integer, ranging from 1 to 4 • wepdefkey key: default key of wep authentication mode, an integer, ranging from 1 to 4 • key key: secret key, a string of 1 to 13 characters • ascii: ASCII secret key padding mode • hex: HEX secret key padding mode • 128bit: the length of the secret key ID is 128bit. • 64bit: the length of the secret key ID is 64bit.
11	<pre>Raisecom(config-gpon-onu-*//*:*)#wifi-ap id wpa encryptionmode { aes mixed tkip } example: Raisecom(config-gpon-onu-1/1:1)#wifi-ap 1 wpa encryptionmode aes</pre>	(Optional) configure the WPA authentication mode of the Wi-Fi access point. • key key: wpa key information, a string of 8 to 63 characters
12	<pre>Raisecom(config-gpon-onu-*//*:*)#wifi-ap id wpa key key example: Raisecom(config-gpon-onu-1/1:1)#wifi-ap 1 wpa key asd</pre>	(Optional) configure the WPA secret key of the Wi-Fi access point. • key key: wpa key, a string of 8 to 63 characters
13	<pre>Raisecom(config-gpon-onu-*//*:*)#wifi-ap id workrate { 11m 12m 18m 1m 24m 2m 36m 48m 5.5m 54m 6m 9m auto mcs0 mcs1 mcs10 mcs11 mcs12 mcs13 mcs14 mcs15 mcs2 mcs3 mcs4 mcs5 mcs6 mcs7 mcs8 mcs9 } example: Raisecom(config-gpon-onu-1/1:1)#wifi-ap 1 workrate 11m</pre>	(Optional) configure the working rate of the Wi-Fi access node. • id: wireless access point ID, an integer, ranging from 1 to 8 • 11m: the working rate of the access point is 11 M. • auto: the working rate of the access point is automatic. • mcs0: the working rate of the access point is the rate corresponding to the modulation and coding strategy index 0.

4.4.4 Configuring 5G Wi-Fi access point

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#gpon-onu slot-id/olt-id/onu-id	Enter GPON ONU remote management configuration mode.

Step	Command	Description
3	<code>Raisecom(config-gpon-onu-*//*:*)#wifi-ap-5g id admin enable</code>	Enable the administrative status of the 5G Wi-Fi access point. You can use the wifi-ap-5g id admin disable command to disable this function.
4	<code>Raisecom(config-gpon-onu-*//*:*)#wifi-ap-5g id auth mode { unauth wep-open wep-share wpa wpa2 wpa2-mixed }</code>	Configure the authentication mode of the 5G-Wi-Fi access point.
5	<code>Raisecom(config-gpon-onu-*//*:*)#wifi-ap-5g id client isolate enable</code>	Enable user isolation of the 5G Wi-Fi access point. You can use the wifi-ap-5g id client isolate disable command to disable this function.
6	<code>Raisecom(config-gpon-onu-*//*:*)#wifi-ap-5g id client max num</code>	Configure the maximum client accesses to the 5G Wi-Fi access point.
7	<code>Raisecom(config-gpon-onu-*//*:*)#wifi-ap-5g id hidden enable</code>	Enable the hidden status of the 5G Wi-Fi access point. You can use the wifi-ap id hidden disable command to disable this function.
8	<code>Raisecom(config-gpon-onu-*//*:*)#wifi-ap-5g id ssid-name name</code>	Configure the SSID name of the 5G Wi-Fi access point.
9	<code>Raisecom(config-gpon-onu-*//*:*)#wifi-ap-5g id wep key key</code>	(Optional) configure the 5G Wi-Fi access point authentication mode to WEP and configure its key node.
10	<code>Raisecom(config-gpon-onu-*//*:*)#wifi-ap-5g id wedefkey key { key key keyformat { ascii hex } keylength { 128bit 64bit } }</code>	(Optional) configure the default key for the WEP authentication mode of the 5G Wi-Fi access point.
11	<code>Raisecom(config-gpon-onu-*//*:*)#wifi-ap-5g id wpa encryptionmode { aes mixed tkip }</code>	(Optional) configure the WPA authentication mode of the 5G Wi-Fi access point.
12	<code>Raisecom(config-gpon-onu-*//*:*)#wifi-ap-5g id wpa key key</code>	(Optional) configure the WPA key of the 5G Wi-Fi access point.
13	<code>Raisecom(config-gpon-onu-*//*:*)#wifi-ap-5g id workrate { 12m 18m 24m 36m 48m 54m 6m 9m auto mcs0 mcs0-nss1 mcs0-nss2 mcs1 mcs1-nss1 mcs2-nss2 mcs2 mcs2-nss1 mcs2-nss2 mcs3 mcs3-nss1 mcs3-nss2 mcs4 mcs4-nss1 mcs4-nss2 mcs5 mcs5-nss1 mcs5-nss2 mcs6 mcs6-nss1 mcs6-nss2 mcs7 mcs7-nss1 mcs7-nss2 mcs8-nss1 mcs8-nss2 mcs9-nss1 mcs9-nss2 }</code>	(Optional) configure the working rate of the 5G Wi-Fi access point.

4.4.5 Checking configurations

No.	Command	Description
1	Raisecom# show gpon-onu slot-id/olt-id/onu-id wifi information	Show GPON ONU Wi-Fi parameters.
2	Raisecom# show gpon-onu slot-id/olt-id/onu-id wifi-5g information	Show GPON ONU 5G Wi-Fi configurations.

5

Configuring multicast services

This chapter describes multicast services and configuration process of the device, including the following sections:

- Introduction
- Quick configurations of multicast services
- Configuring static multicast
- Configuring IGMP Snooping
- Configuring IGMP Proxy
- Configuring MVR
- Configuring dynamic controllable multicast
- Configuring MLD Snooping
- Configuring MLD Proxy
- Configuring multicast VLAN
- Maintenance

5.1 Introduction

5.1.1 Multicast

Multicast is a point to multipoint data transmission method. The method can effectively solve the single point sending and multipoint receiving problems. During the network packet transmission, it can save network resources and improve information security.

Comparisons among unicast, broadcast, and multicast

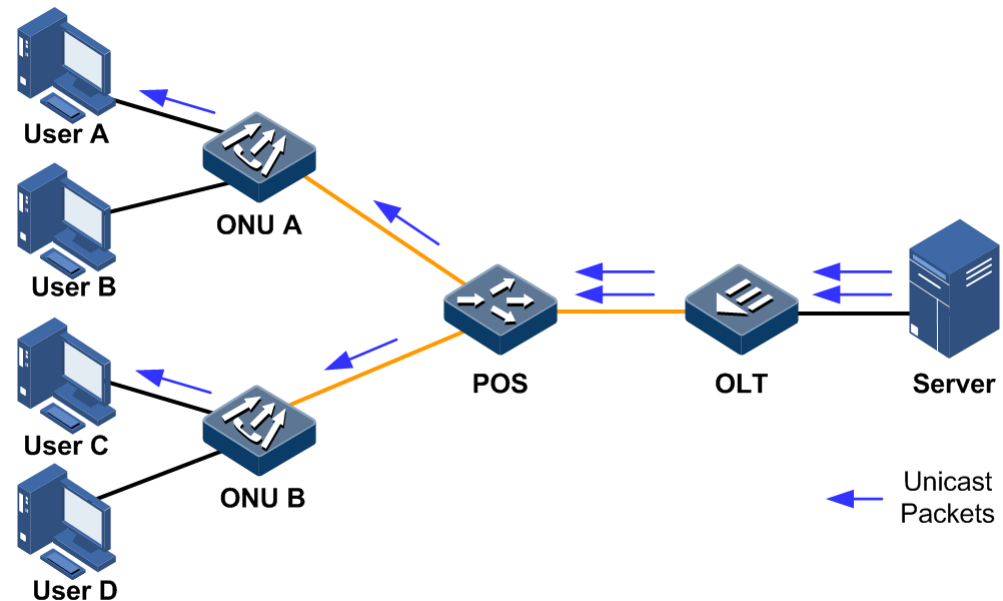
In Ethernet network, packets are transmitted in forms of unicast, broadcast, and multicast.

- Unicast: the system establishes a packet transmission path for each user who needs this packet and sends an independent copy of the packet to the user.

As shown in Figure 5-1, assume that User A and User C need a certain type of packets. In the unicast transmission mode, the Server establishes a transmission path with User A and User C respectively. Because the number of transmitted packets depends on the number of users, when there are more users need a certain packet, multiple identical packet flows will be

transmitted through the network. Therefore, the bandwidth hits a bottleneck. In the unicast transmission mode, packets cannot be transmitted in a large scale.

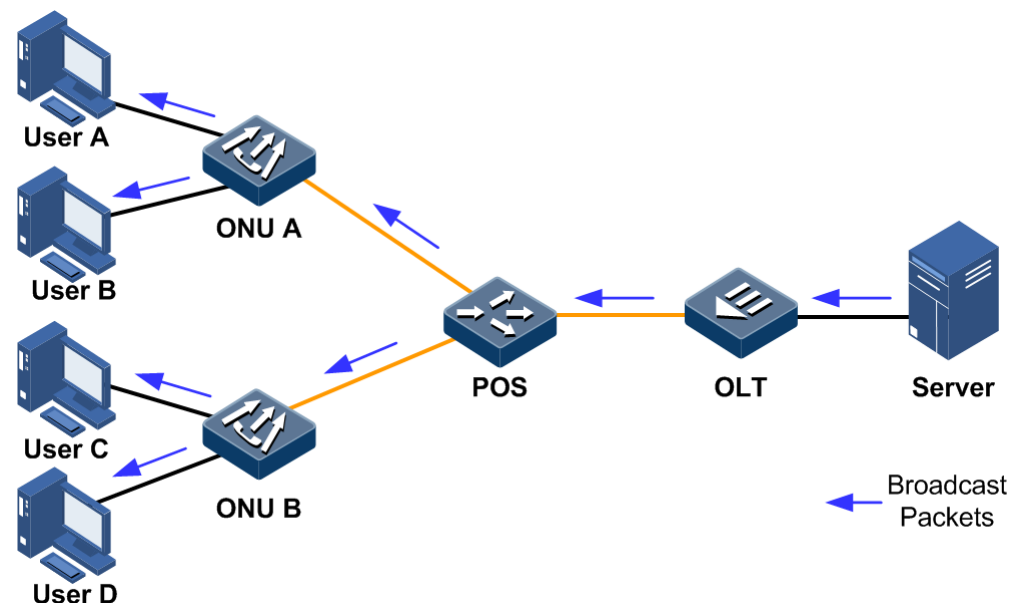
Figure 5-1 Unicast transmission mode



- **Broadcast:** the system sends a packet to all users in the network, regardless whether they need it or not. All users will receive a broadcast packet.

As shown in Figure 5-2, assume that User A and User C need a certain type of packets. In the broadcast transmission mode, the Server floods this type of packets through a router and all users (including User B) will also receive these packet. The security and non-gratuitousness of the packets cannot be ensured. In addition, network resources cannot be well utilized when few users need this type of packets.

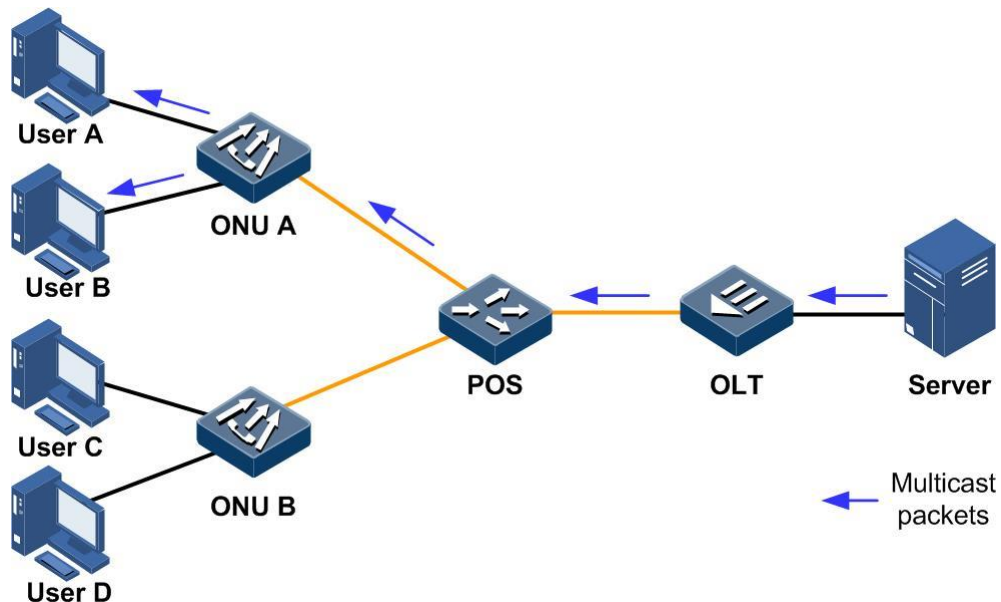
Figure 5-2 Broadcast transmission mode



- Multicast: when some users need a specified packet, the multicast packet sender (multicast source) sends this packet once. This packet is copied and forwarded at the furthest port.

As shown in Figure 5-3, assume that User A and User C need a certain packet. In the multicast transmission mode, User A and User C makes up a group. The ISCOM6800 and ISCOM6860 and ONU devices in the network establish a multicast forwarding table based on its own Internet Group Management Protocol (IGMP) packet. Therefore, the packet is transmitted to receivers who need it.

Figure 5-3 Multicast transmission mode



As described above, the unicast transmission mode fits for a network with few users while the broadcast transmission mode fits for a network with many users. Both the unicast and the broadcast transmission modes work inefficiently when the number of users in a network is not confirmed. In the multicast mode, when the number of users increases exponentially, packets can be transmitted to the specific user without increasing the backbone bandwidth. This makes multicast become one research hotspot of the current network technologies.

Basic concepts

Basic concepts involved in the multicast service are shown as below.

- Multicast source: the device used to send multicast packets. It is the server that sends packets by taking the multicast address as the destination address. A multicast source can send packets to multiple multicast groups simultaneously. In addition, multiple multicast sources can send packets to a multicast group.
- Multicast group: the device used to receive multicast packets. The device uses a multicast IP address to identify a multicast group. A user host (or other receiving devices) becomes a member of a multicast group once it is added to the group. And then the host can recognize and receive packets with the specified IP multicast address. Hosts in a multicast group can be located in any place.
- Multicast router: the router supporting multicast in a network. The multicast router locates at the end network segment that is connected with the user host, to manage multicast members, implement multicast routing, and to conduct forwarding multicast packets.

- Router interface: an interface on the device, which is used to connect the multicast router and the user host. The interface is used to connect the multicast router and receive IGMP packets.
- Member interface: an interface on the device. The interface is used to connect to the user host and send multicast packets.

You must note that the multicast source may (or may not) belong to a multicast group. In addition, multiple multicast sources may send identical packets to a multicast group.

Multicast address

To make the multicast source and the multicast group communicate with each other across the Internet, you must provide a network-layer multicast, using IP multicast addresses.

To make multicast packets transmitted across the local physical network properly, you must provide a link-layer multicast (hardware cast). When the link layer adopts Ethernet technologies, the hardware multicast uses multicast MAC addresses.

To make multicast packet traverse the network layer and the link layer properly, there must be a technology used to map IP multicast addresses to multicast MAC addresses.

- IP multicast address

Internet Assigned Numbers Authority (IANA) takes Class D IPv4 addresses as multicast addresses. The IPv4 multicast address ranges from 224.0.0.0 to 239.255.255.255.

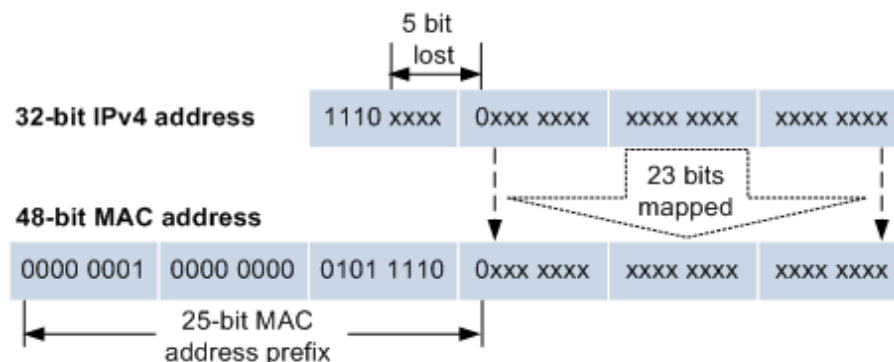
IPv6 multicast addresses are preceded with FF. The first 8 bits are set to 1. If the third hexadecimal number is set to 0, it indicates the IPv6 multicast address is a commonly-used multicast address. If it is set to 1, it indicates the IPv6 multicast address is a temporary multicast address. The fourth hexadecimal number indicates the multicast range. The remaining hexadecimal numbers indicate specific multicast groups.

- Multicast MAC address

When a unicast packet is transmitted through Ethernet network, the MAC address of the receiver is used. However, when a multicast packet is transmitted, the destination is not a specified receiver but a group with multiple members. Therefore, a multicast MAC address must be adopted.

As formulated by IANA, the first 24 bits of a multicast MAC address is fixed to 0x01005E; the twenty fifth bit is set to 0. The last 23 bits are related to the last 23 bits of an IPv4 multicast address. Figure 5-4 shows the mapping between an IPv4 multicast address and a multicast MAC address.

Figure 5-4 Mapping between an IPv4 multicast address and a multicast MAC address



Because the first 4 bits of an IP multicast address is 1110, and only the last 23 bits of the IP multicast address is mapped to a multicast MAC address. The lost 5 bits will make 32 IP multicast addresses mapped to an identical MAC address. Therefore, during Layer 2 processing, besides the related IPv4 multicast, the device will receive other multicast data. These redundant multicast data will be filtered on the upper layer of the device.

IPv6 multicast MAC addresses are preceded with 0x3333. The last 32 bits is related to the last 32 bits of an IPv6 multicast address. Finally, a 48-bit multicast MAC address is formed. For example, the IPv6 multicast address FF1E::F30E:101 is related to the multicast MAC address 33-33-F3-0E-01-01.

Advantages and applications of multicast

Compared with the unicast and broadcast transmission modes, the multicast transmission mode has the following advantages:

- Improve efficiency, reduce network traffic, and reduce server and CPU load.
- Optimize performance and reduce redundant traffic.
- Make multipoint application available with distribution applications.

With increasingly development of Internet, more and more data, voice, and video information are exchanged in the Internet. Emerging services, such as electronic commerce, online conference, online auction, Video on Demand (VOD), and remote education, are become more popular. These services bring requirements on information security and non-gratuitousness. However, traditional unicast and broadcast transmission modes cannot meet these requirements.

Supported Multicast features

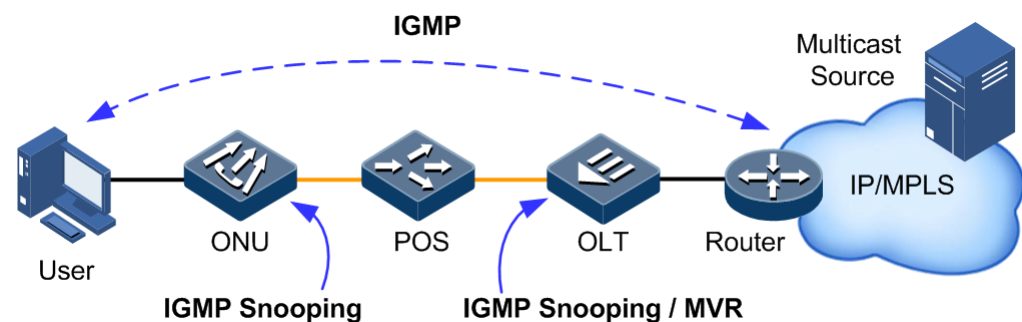
For a network that needs to implement multicast services, you need to deploy various multicast protocols at different nodes of the network. These multicast protocols cooperate with each other to implement network-based multicast services.

In general, based on layers of the Open System Interconnect (OSI), multicast is divided into 2 types:

- Layer 3 multicast: IP multicast working in the network layer. And related multicast protocols are called Layer 3 multicast protocols, such as IGMP.
- Layer 2 multicast: IP multicast working in the data link layer. And related multicast protocols are called Layer 2 multicast protocols, including Internet Group Management Protocol Snooping (IGMP Snooping), Multicast VLAN Registration (MVR), and so on.

Figure 5-5 shows operating positions of the IGMP and Layer 2 multicast protocols.

Figure 5-5 Operating positions of the IGMP and Layer 2 multicast protocols



IGMP is an integrated part of the TCP/IP protocol suite, used for managing IPv4 multicast members. It is a communications protocol used by hosts and adjacent routers on IP networks to establish and maintain multicast group memberships. IGMP manages multicast groups by sending and receiving IGMP packets between the host and the multicast router. IGMP packets are encapsulated in IP packets. IGMP packets are in a form of Query packet, Report packet, or a Leave packet.

The implementation process of the IGMP is shown as below:

- A host is added to a multicast group by sending a Report packet to the multicast router and leave from the multicast group by sending a Leave packet. The host can decide which packets to receive.
- The multicast router sends Query packets periodically and receives Report packets and Leave packets sent by hosts to learn multicast groups in a network segment. If a multicast group is in a network segment, the multicast router forwards multicast data to the network segment. Otherwise, no multicast data is forwarded to the network segment.

At present, there are 3 IGMP versions, IGMPv1, IGMPv2, and IGMPv3. The new version is compatible to old versions. Currently, IGMPv2 is the most commonly-used version. The Leave packet fits for IGMPv2 and IGMPv3 only.

5.1.2 IGMP Snooping

IGMP Snooping is a Layer 2 multicast function. It maintains port information of multicast packets, manages and controls forwarding of multicast packets by listening to multicast packets between multicast groups and hosts.

When the device listens to an IGMP Report packet sent to a multicast group by a host, the device will add the interface, which is connected to the host, to the forwarding table of the multicast group. Similarly, when the device is enabled with immediate-leave, it will delete the interface from the forwarding table of the multicast group after it listens to an IGMP Leave packet. If no packet of a multicast group is listened, the device will delete the interface from the multicast group.

IGMP Snooping forwards multicast data through Layer 2 multicast forwarding table. When the device receives multicast data, it forwards the multicast data to related Tx interface based on the multicast forwarding table instead of flooding the data to all interfaces. Therefore, it helps save bandwidth efficiently.

IGMP Snooping can establish the Layer 2 multicast forwarding table through dynamic learning or manual configuration.

5.1.3 IGMP Proxy

IGMP Proxy is an IGMP agent mechanism, which runs on a Layer 2 device to help manage and control multicast groups. IGMP Proxy processes IGMP packets. For multicast sources, it acts as a host; while for the downlink network, it acts as a multicast router.

A Layer 2 device, where IGMP Proxy is enabled, has 2 roles:

- Querier: at the user side, it acts as a server. It queries user information by sending Query packets periodically and processes Report and Leave packets sent by users.
- Host: at the network router side, it acts as a client. It responds to Query packets sent by multicast routers, sends Report and Leave packets, and sends current user information to the network as required.

This agent mechanism can efficiently obtain and control user information. In addition, it helps to reduce number of protocol packets at the network side and network load.

IGMP Proxy establishes the multicast forwarding table by intercepts IGMP packets between users and multicast routers.



Note

IGMP Proxy can work with MVR.

Concepts related to IGMP Proxy are as below.

- IGMP Querier

If the multicast mode is configured to IGMP Proxy, the device periodically sends IGMP query packets to query information about multicast members on the interface.

- Query interval

After you configure the interval for general query packets in IGMP Proxy mode, IGMP Proxy query timeout will be recounted, and TTL of all online member interfaces in this mode will be reset to "general query interval+maximum response time". By default, the query interval is set to 125s.

- Maximum response time of Query packets

The maximum response time for query packets is used to control the deadline for reporting member relations by a host. When the host receives query packets, it starts a timer for each multicast group. The value of the timer is between 0 and maximum response time. When the timer expires, the host sends the Report packet to the multicast group. The maximum response time of the query packets of the ISCOM6800 and ISCOM6860 is 10s by default.

- Interval for last member to respond

The device sends Query packets continuously to a specified multicast group after it receives IGMP Leave packets of the specified multicast group.

The query packet for the specified multicast group is sent to query whether the group has members on the interface. If yes, the members must send Report packets within the maximum response time; after the device receives Report packets in a specie period, it continues to maintain multicast forwarding entries of the group. If the members fail to send Report packets within the maximum response time, it is believed that the last member of the multicast group has left, and multicast forwarding entries of the multicast group will be deleted. The interval of the last member response time of the ISCOM6800 and ISCOM6860 is 2s by default

5.1.4 MVR

MVR is a multicast restriction mechanism running on Layer 2 devices. It is used to manage and control multicast groups, and implement Layer 2 multicast.

By configuring multicast VLANs, MVR adds member ports of different Customer VLAN (CVLAN) of the device to multicast VLANs. Therefore, users in different VLANs can share the same multicast VLAN. Multicast flows are transmitted across a multicast VLAN. You do not need to copy multicast flows for each VLAN. In this way, bandwidth is saved. In addition, security is enhanced by isolating multicast VLANs and CVLANs.

The differences of MVR and IGMP Snooping are as below.

- Multicast VLANs and CVLANs in IGMP Snooping are identical.

- Multicast VLANs and CVLANs in MVR are different.

5.1.5 Dynamic controllable multicast

In the EPON system, dynamic controllable multicasts forward multicast services in a form of SCB+IGMP. The ISCOM6800 and ISCOM6860 support CTC OAM-based dynamic controllable multicast.

Dynamic controllable multicast refers than an Optical Line Terminal (OLT) identifies a user based on the IGMP control packet carried by the user, and then controls Optical Network Units (ONUs) to forward multicast data by extending Operation Administration, and Maintenance (OAM) information. The main process is shown as below.

- OLT process
 - At the OLT side, you should maintain a user multicast service authority control table, facilitating centralized management users' multicast service access authorities.
 - The OLT uses the Logical Link Identifiers (LLID) and the VLAN IDs carried by uplink the IGMP Report packets to identify ports (users).
 - Based on the multicast service authority control list, the OLT judges whether a port (user) has the access authority and its parameters of the related multicast services. The OLT uses extended multicast control OAM packets to send access authority of a port (user) to ONUs. And then ONUs decides to forward or discard multicast services from the port (user).
- ONU process
 - The ONU maintains a multicast address filtering table and a multicast forwarding table. The ONU dynamically refreshes these 2 tables based on multicast control OAM packets sent by the OLT.
 - The ONU adds a VLAN tag of the port (user) to received IGMP Report/Leave packets and then sends them to the OLT.
 - After receiving multicast control OAM packets sent by the OLT, the ONU adds or deletes ONU local multicast filtering entries and multicast forwarding entries based on the contents of the packets. And then the ONU decides to forward or discard related multicast traffic.
 - The ONU supports removing VLAN IDs for downlink multicast traffic.

5.2 Quick configurations of multicast services

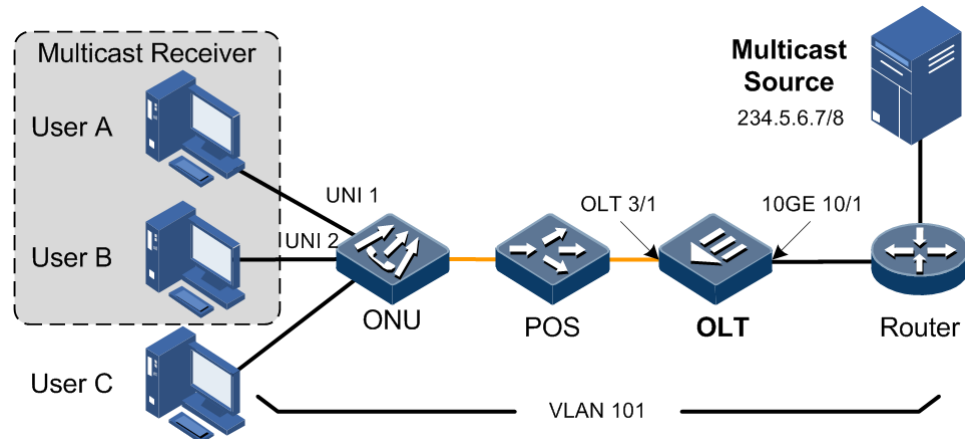
The configuration of multicast services is complex and involves many configuration items. This section provides configuration examples for several typical applications to facilitate users quickly provisioning multicast services.

5.2.1 Example for configuring IGMP Snooping

Networking requirements

As shown in Figure 5-6, the uplink port 10GE 10/1 of the OLT device is connected to the multicast router, and the PON port OLT 3/1 is connected to the ONU. The two Ethernet ports UNI 1 and UNI 2 on the ONU are connected to two users. All multicast users belong to the same VLAN 101. You need to configure IGMP Snooping and immediate leave on the OLT and the ONU respectively to enable the user to receive multicast data.

Figure 5-6 IGMP Snooping networking



Configuration steps

- Configure the OLT.

Step 1 Create a multicast VLAN and configure the interface attribute.

```
Raisecom#config
Raisecom(config)#create vlan 101 active
Raisecom(config)#multicast-vlan 101
Raisecom(config)#interface ten-gigabitethernet 10/1
Raisecom(config-if-ten-gigabitetherne-10:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitetherne-10:1)#switchport trunkallowed vlan
101
Raisecom(config-if-ten-gigabitetherne-10:1)#exit
Raisecom(config)#interface epon-olt 3/1
Raisecom(config-if-epon-olt-3:1)#switchport mode trunk
Raisecom(config-if-epon-olt-3:1)#switchport trunkallowed vlan 101
Raisecom(config-if-epon-olt-3:1)#exit
```

Step 2 Configure the role of the multicast VLAN interface and enable immediate leave.

```
Raisecom#config
Raisecom(config)#interface ten-gigabitethernet 10/1
Raisecom(config-if-ten-gigabitethernet-10:1)#multicast-vlan 101 router
Raisecom(config-if-ten-gigabitethernet-10:1)#exit
Raisecom(config)#interface epon-olt 3/1
Raisecom(config-if-epon-olt-3:1)#multicast-vlan 101 member
Raisecom(config-if-epon-olt-3:1)#igmp snooping immediate-leave multicast-
vlan 101
Raisecom(config-if-epon-olt-3:1)#exit
```

Step 3 Enable global IGMP.

```
Raisecom(config)#igmp
```

- Configure the ONU.

Step 4 Create a multicast VLAN and configure the interface attribute.

```
Raisecom#config
Raisecom(config)#epon-onu uni ethernet 3/1/1/1
Raisecom(config-epon-onu-ethernet-3/1/1:1)#vlan mode tagged
Raisecom(config-epon-onu-ethernet-3/1/1:1)#native vlan 101
Raisecom(config-epon-onu-ethernet-3/1/1:1)#multicast vlan 101
Raisecom(config-epon-onu-ethernet-3/1/1:1)#multicat vlan stripped
Raisecom(config-epon-onu-ethernet-3/1/1:1)#exit
Raisecom(config)#epon-onu uni ethernet 3/1/1/2
Raisecom(config-epon-onu-ethernet-3/1/1:2)#vlan mode tagged
Raisecom(config-epon-onu-ethernet-3/1/1:2)#native vlan 101
Raisecom(config-epon-onu-ethernet-3/1/1:2)#multicast vlan 101
Raisecom(config-epon-onu-ethernet-3/1/1:2)#multicat vlan stripped
Raisecom(config-epon-onu-ethernet-3/1/1:2)#exit
```

Step 5 Enable IGMP Snooping and configure immediate leave.

```
Raisecom(config-epon-onu-3/1:1)#ip igmp mode snooping
Raisecom(config-epon-onu-3/1:1)#ip igmp immediate-leave
```

Step 6 Configure the forwarding mode of multicast service traffic.

```
Raisecom(config-epon-onu-3/1:1)#ip igmp vlan-aware enable
```

Checking results

- Check OLT configurations.

Check whether IGMP configurations on the OLT are correct.

```
Raisecom#show igmp
igmp: enable
igmp snooping timeout: 300s
igmp proxy version: v3
igmp proxy query interval: 125s
igmp proxy query max response: 5s
igmp proxy last query interval: 1s
igmp proxy last query count: 2
igmp proxy source-ip: 192.168.1.100
```

Check whether IGMP configurations are correct on the ONU.

```
Raisecom#show epon-onu 3/1/1 ip igmp
ONU ID: 3/1/1
  IGMP Mode           : snooping
  Last Member Query Count : 2
  Last Member Query Interval : 2s
  Aging Time          : 300s
  VLAN Aware          : enable
  Immediate-leave Administrative : enable
```

Check whether multicast VLAN configurations on the ONU are correct.

```
Raisecom#show multicast-vlan
multicast-vlan mode  cvlan forward  upstream-priority  downstream-priority
-----
1                   snooping  disable           keep                keep
```

Check whether routing interface configurations of IGMP multicast VLAN are correct.

```
Raisecom#show multicast-vlan 10 router
Multicast vlan      Router
-----
101                 ten-gigabitethernet10/1
```

Check whether member interface configurations of IGMP multicast VLAN are correct.

```
Raisecom#show multicast-vlan 10 member
Multicast vlan      Member      immediate-leave
-----
101                 epon-olt 3/1      enable
```

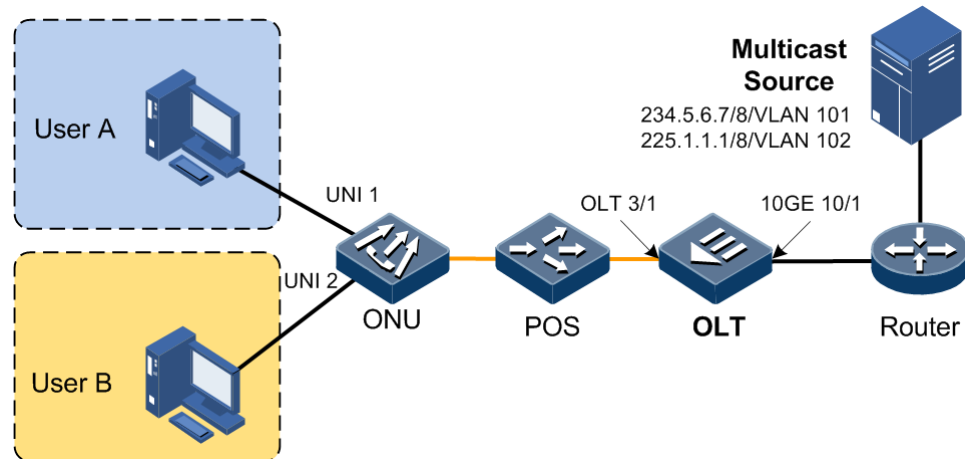
5.2.2 Example for configuring dynamic controllable multicast

Networking requirements

As shown in Figure 5-7, port 10GE 10/1 of the OLT device is connected to the multicast router, and PON port OLT 3/1 is connected to the user through the ONU. By configuring the dynamic controllable multicast, you can enable User 1 and User 2 with different access rights to channel 1 (234.5.6.7) and channel 2 (225.1.1.1).

- User A: it is allowed to watch channel 1 and has 10 minutes of preview permission for channel 2.
- User B: it is allowed to watch channel 2 but not channel 1.

Figure 5-7 Dynamic controllable multicast networking



Configuration steps

- Configuring the OLT.

Step 1 Create a multicast VLAN and configure unknown multicast filtering.

```
Raisecom#config
Raisecom(config)#creat vlan 1,2,101,102 active
Raisecom(config)#multicast-vlan 101
Raisecom(config)#multicast-vlan 102
Raisecom(config)#multicast-vlan 1
Raisecom(config)#multicast-vlan 2
Raisecom(config)#mac-address-table unknown-multicast filter vlanlist
1,2,101,102
```

Step 2 Enable IGMP.

```
Raisecom(config)#igmp
```

Step 3 Create a multicast channel.

```
Raisecom(config)#multicast-ctrl
Raisecom(config)#multicast-ctrl channel id 1 name channel1 group-ip
234.5.6.7
Raisecom(config)#multicast-ctrl package packag1
Raisecom(config)#multicast-ctrl package packag1 channel channel1 permit
Raisecom(config)#multicast-ctrl package package1 channel channel2 preview
preview-profile profile1
Raisecom(config)#multicast-ctrl channel id 2 name channel2 group-ip
225.1.1.1
Raisecom(config)#multicast-ctrl package packag2
Raisecom(config)#multicast-ctrl package packag2 channel channel2 permit
```

```
Raisecom(config)#multicast-ctrl package packag2 channel channel1 deny
```

Step 4 Enable global preview and configure a preview template.

```
Raisecom(config)#multicast-ctrl preview
Raisecom(config)#multicast-ctrl peview-profile profile1
Raisecom(config)#multicast-ctrl peview-profile profile1 duration 10
```

Step 5 Create a dynamic controllable multicast user and specify the channel package of the user.

```
Raisecom(config)#multicast-ctrl user user1 source 1/1/1 cvlan 1
Raisecom(config)#multicast-ctrl user user1 package package1
Raisecom(config)#multicast-ctrl user user2 source 1/1/2 cvlan 2
Raisecom(config)#multicast-ctrl user user2 package package2
```

Step 6 Configure multicast VLAN and MVR.

```
Raisecom(config)#mvr
Raisecom(config)#multicast-vlan 101 group 234.5.6.7
Raisecom(config)#multicast-vlan 102 group 225.1.1.1
Raisecom(config)#interface epon-olt 3/1
Raisecom(config-if-epon-olt-3:1)#multicast-vlan 101 member
Raisecom(config-if-epon-olt-3:1)#multicast-vlan 102 member
Raisecom(config-if-epon-olt-3:1)#exit
```

Step 7 Configure information about the OLT interface.

```
Raisecom(config)#interface epon-olt 3/1
Raisecom(config-if-epon-olt-3:1)#switchport mode trunk
Raisecom(config-if-epon-olt-3:1)#switchport trunk allowed vlan
1,2,101,102
Raisecom(config-if-epon-olt-3:1)#exit
Raisecom(config)#interface ten-gigabitethernet 10/1
Raisecom(config-if-ten-gigabitethernet-10:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-10:1)#switchport trunk allowed
vlan 101,102
Raisecom(config-if-ten-gigabitethernet-10:1)#end
```

- Configure the ONU.

Step 8 Configure the ONU multicast mode to dynamic controllable multicast.


```
Raisecom#config
Raisecom(config)#epon-onu 3/1/1
Raisecom(config-epon-onu-3/1/1)#ip igmp mode ctrl-multicast
Raisecom(config-epon-onu-3/1/1)#exit
```

Step 9 Configure information about the ONU interface.

```
Raisecom(config)#epon-onu uni ethernet 3/1/1/1
Raisecom(config-epon-onu-ethernet-3/1/1/1)#multicast vlan stripped
Raisecom(config-epon-onu-ethernet-3/1/1/1)#exit
Raisecom(config)#epon-onu uni ethernet 3/1/1/2
Raisecom(config-epon-onu-ethernet-3/1/1/2)#multicast vlan stripped
```

Checking results

- Check OLT configurations.

Check configurations of the dynamic controllable multicast channel.

```
Raisecom#show multicast-ctrl channel
```

ID	Channel	cdr	group ip
1	RaisecomChenable	255.1.1.1-255.1.1.1	
2	RaisecomChenable	234.5.6.7-234.5.6.7	

Show user configurations.

```
Raisecom#show multicast-ctrl user
```

Total user number: 2

User source cvlanpackagestate

```
-----
user1vport 1/1/11package1online
```

```
User2vport 1/1/22package1online
```

- Show ONU configurations.

Show the processing mode of ONU IGMP packets.

```
Raisecom#show epon-onu 3/1/1 ip igmp
```

ONU ID: 3/1/1

IGMP Mode : ctrl-multicast

Last Member Query Count : 2

Last Member Query Interval : 2s

Aging Time : 300s

Immediate-leave Administrative : enable

5.3 Configuring static multicast

5.3.1 Preparing for configurations

Scenario

The device support static multicast, permitting you to configure the static multicast group, specify the corresponding relationship among the multicast MAC address, multicast VLAN, and multicast interface, and add/remove a specify interface to/from a static multicast group.

If the multicast members and corresponding interfaces are fixed, you can configure static multicast to lower performance waste caused by monitoring multicast packets.

Prerequisite

N/A

5.3.2 Default configurations

N/A

5.3.3 Configuring static multicast

The device adds the member interface to the multicast routing table by identifying the IGMP packet sent by the host automatically. You can manually configure the device to add member interfaces for a specified multicast routing table.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#mac-address- table static multicast mac- address vlan vlan-id interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet port- channel group-id } slot- id/olt-id example: Raisecom(config)#mac-address- table static multicast 0100.5E00.0001 vlan 1 interface gigabitethernet 1/1</pre>	Configure static Layer 2 multicast MAC address entries. • mac-address: multicast MAC address, in dotted hexadecimal notation, such as 0100.5E00.0001 • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • epon-olt slot-id/port-id: EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gpon-olt slot-id/port-id: GPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gigabitethernet slot-id/port-id: 1000 Mbit/s Ethernet interface. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-gigabitethernet slot-id/port-id: 10 Gbit/s Ethernet interface. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-giga-epon-olt slot-id/port-id: 10G EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • port-channel group-id: aggregation group interface ID. The group-list refers to the aggregation group interface ID, ranging from 1 to 32.
3	<pre>Raisecom(config)#mac-address- table static multicast mac- address vlan vlan-id { add remove } interface { epon-olt gpon-olt ten-giga-epon-olt gigabitethernet port- channel group-id } slot- id/olt-id example: Raisecom(config)#mac-address- table static multicast 0100.5E00.0001 vlan 1 add interface gigabitethernet 3/1</pre>	(Optional) configure the add/remove L2 multicast address of the interface. • mac-address: multicast MAC address, in dotted hexadecimal notation, such as 0100.5E00.0001 • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • add: add a MAC address entry. • remove: delete the MAC address entry. • epon-olt slot-id/port-id: EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gpon-olt slot-id/port-id: GPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gigabitethernet slot-id/port-id: 1000 Mbit/s Ethernet interface. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-gigabitethernet slot-id/port-id: 10 Gbit/s Ethernet interface. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-giga-epon-olt slot-id/port-id: 10G EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • port-channel group-id: aggregation group interface ID. The group-list refers to the aggregation group interface ID, ranging from 1 to 32.
4	<pre>Raisecom(config)#mac-address- table unknown-multicast filter vlanlist vlan-list example: Raisecom(config)#mac-address- table unknown-multicast filter vlanlist 10-20</pre>	(Optional) configure the VLAN list for unknown multicast filtering • vlan-list: VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

5.3.4 Checking configurations

No.	Command	Description
1	Raisecom# show mac-address-table multicast [statistics]	Show configurations of the multicast MAC address forwarding table.

5.4 Configuring IGMP Snooping

5.4.1 Preparing for configurations

Scenario

If multiple ONU users need to receive data from the multicast source, you can enable IGMP Snooping on the device and ONU respectively, and create and maintain 2 multicast forwarding tables respectively by monitoring multicast packets between the router and host, to achieve Layer 2 multicast.

- Create a multicast forwarding table recording the corresponding relationship between the multicast packet and PON interface on the device to achieve multicast information distribution based on PON interface.
- Create a multicast forwarding table recording the corresponding relationship between the multicast packet and UNI on the ONU to achieve multicast information distribution based on UNI.

Prerequisite

Create and configure the related VLAN.

5.4.2 Default configurations

Default configurations of IGMP Snooping on the device are as below.

Function	Default value
Global multicast VLAN mode	IGMP Snooping
Global IGMP Snooping	Disable
IGMP Snooping under VLAN	Disable
Aging time of multicast routing entries	300s
Multicast router interface	N/A
Immediate-leave	Disable
Static multicast routing table	N/A

Default configurations of IGMP Snooping on the ONU devices are as below.

Function	Default value
IGMP mode	IGMP Snooping
Timeout times for the last member to send IGMP query packets	2
Interval for the last member to send IGMP query packets	2s
Aging time of multicast route entries	300s
Forwarding mode of multicast service traffic	VLAN+MAC
Immediate leave	disable

5.4.3 Configuring IGMP Snooping

Configuring IGMP on OLT

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# igmp	Enable global IGMP. You can use the no igmp command to disable this function.



Note

If the current multicast VLAN mode is IGMP Snooping, you can use the **igmp** command to enable global IGMP features; if the current multicast VLAN mode is IGMP Proxy, you need to use the **multicast-vlan mode** command to switch the multicast VLAN mode to IGMP Snooping, and then use the **igmp** command to enable global IGMP features.

Configuring IGMP Snooping on ONU

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/1/1	Enter EPON ONU management mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*//*:*)# ip igmp mode { snooping ctrl-multicast transparent proxy } example: Raisecom(config-epon-onu-service-profile:1)#ip igmp mode ctrl-multicast	Configure IGMP mode. • ctrl-multicast: controllable multicast • proxy: Proxy mode • snooping: Snooping mode • transparent: transparent transmission mode
4	Raisecom(config-epon-onu-*//*:*)# ip igmp vlan-aware{ enable disable }	(Optional) enable/disable vlan-aware of multicast service traffic forwarding mode.

Step	Command	Description
5	<pre>Raisecom(config-epon-onu-*//*:*)#ip igmp last-member-query-count count example: Raisecom(config-epon-onu-3/1:1)#ip igmp last-member-query-count 5</pre>	(Optional) timeout times of Last-Member query packets triggered by leave packets. You can use the no ip igmp last-member-query-count command to restore default configurations. count: timeout times, an integer, ranging from 1 to 16
6	<pre>Raisecom(config-epon-onu-*//*:*)#ip igmp last-member-query-interval second example: Raisecom(config-epon-onu-3/1:1)#ip igmp last-member-query-interval 10</pre>	(Optional) response timeout time of Last-Member query packets triggered by leave packets. You can use the no ip igmp last-member-query-interval command to restore to default configurations. second: interval, an integer, ranging from 1 to 25, in units of second
7	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#multicast vlan { stripped no- stripped } example: Raisecom(config-epon-onu-ethernet- 3/1/1:1)#multicast vlan stripped</pre>	(Optional) configure the mode of the UNI to process the VLAN Tags of the multicast service packets. - stripped: enable the ONU Ethernet interface to remove the VLAN Tags of multicast service packets. - no-stripped: disable the ONU Ethernet service interface from removing the VLAN Tags of multicast service packets.
8	<pre>Raisecom(config-epon-onu-ethernet- *//*:*)#multicast vlan vlan-list example: Raisecom(config-epon-onu-ethernet- 3/1/1:1)#multicast vlan 1</pre>	(Optional) configure the multicast VLAN list of UNI. You can use the no multicast vlan command to restore default configurations. vlan-id: VLAN ID, an integer, ranging from 1 to 4094

5.4.4 (Optional) configuring aging time of multicast routing entries

In IGMP Snooping, when the device does not receive the IGMP packet about Layer 2 multicast routing in a period of time, maybe the relevant host or router has left from the multicast group without sending the leave packet. You can configure the aging time of multicast routing entries to delete these entries from the multicast routing table automatically when the aging time expires.

Configuring aging time of OLT multicast routes

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#igmp snooping timeout { period infinite }</pre> example: <pre>Raisecom(config)#igmp snooping timeout 100</pre>	Configure the aging time of multicast routing entries. You can use the no igmp snooping timeout command to restore default configuration. • period: timeout value, an integer, ranging from 30 to 3600, in units of second • infinite: the multicast forwarding entry does not time out.

Configuring aging time of ONU multicast routes

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu slot- id/olt-id/onu-id</pre> example: <pre>Raisecom(config)#epon-onu 3/1/1</pre>	Enter EPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	<pre>aisecom(config-epon-onu- */*:*)#ip igmp aging-time period</pre> example: <pre>Raisecom(config-epon-onu- 3/1:1)#ip igmp aging-time 600</pre>	Configure the aging time of multicast routes. You can use the no ip igmp aging-time command to restore default configurations. • time: aging time, an integer, ranging from 30 to 3600, in units of second

5.4.5 (Optional) configuring immediate leave

When the user host sends the IGMP leave packet, the device does not delete multicast route automatically, but wait for a while before deletion. When there are a lot of downstream users, and the operation of adding or leaving is frequent, you can configure the immediate-leave feature. Then multicast route will be deleted automatically when the user host sends the IGMP leave packet.

This function is only applied to IGMPv2/v3.

Configuring OLT immediate leave

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet port-channel group-id} slot-id/olt-id</pre> example: <pre>Raisecom(config)#interface gigabitethernet 3/1</pre>	Enter physical interface configuration mode. Enter interface configuration mode. • epon-olt slot-id/port-id: enter EPON interface configuration mode. • ten-giga-epon-olt slot-id/port-id: enter 10G EPON interface configuration mode. • gpon-olt slot-id/port-id: enter GPON interface configuration mode. • gigabitethernet slot-id/port-id: enter 1000 Mbit/s Ethernet interface configuration mode. • ten-gigabitethernet slot-id/port-id: enter 10 Gbit/s Ethernet interface configuration mode. • port-channel channel-id: enter link aggregation group configuration mode.

Configuring ONU immediate leave

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</pre>	Enter EPON ONU management configuration mode.
3	<pre>Raisecom(config-epon-onu-*//*:*)#ip igmp immediate-leave</pre>	Configure immediate leave on the ONU.

5.4.6 Checking configurations

Checking configurations of OLT

No.	Command	Description
1	<pre>Raisecom#show igmp</pre>	Show IGMP global configurations.
2	<pre>Raisecom#show igmp statistics</pre>	Show statistics on IGMP packets.
3	<pre>Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet port-channel group-id } slot-id/olt-id igmp statistics</pre>	Show statistics on IGMP packets on a specified interface.

Checking ONU configurations

No.	Command	Description
1	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id ip igmp</pre>	Show configurations of ONU IGMP Snooping.

5.5 Configuring IGMP Proxy

5.5.1 Preparing for configurations

Scenario

In a network where the multicast routing protocol is widely applied, there are multiple hosts or client subnets receiving multicast information. Configure IGMP Proxy on a multicast router and device connected to the host to block IGMP packets between the host and router to reduce the network load.

IGMP Proxy can reduce the task of configuring and managing the client subnet through a multicast router and achieve client subnet multicast connection at the same time.

IGMP Proxy and IGMP Snooping cannot be used concurrently in the same multicast VLAN.

Prerequisite

Create a VLAN and add related interfaces to the VLAN.

5.5.2 Default configurations

Default configurations of IGMP Proxy on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
IGMP version	v2
IGMP query interval	125s
Maximum response time of Tx Query packets	10s
Query interval of the last member	2s
Query times of the last member	2
Source IP address of IGMP Proxy packet sent by IGMP querier	192.168.1.100
IGMP Proxy robustness coefficient	2

5.5.3 Configuring IGMP Proxy

Configuring OLT IGMP Proxy



Note

When you use the **igmp** command to enable global IGMP features, the default working mode of the multicast VLAN is IGMP Snooping. If you need to enable IGMP Proxy, use the **multicast-vlan mode** command to switch the multicast VLAN mode to IGMP Proxy.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#igmp proxy query-interval <i>seconds</i> example: Raisecom(config)#igmp proxy query-interval 100	(Optional) configure the IGMP query interval. You can use the no igmp proxy query-interval command to restore default configuration. • seconds: interval, an integer, ranging from 10 to 65535, in units of second
3	Raisecom(config)#igmp proxy query-max-response <i>seconds</i> example: Raisecom(config)#igmp proxy query-max-response-interval 15	(Optional) configure the maximum response time of IGMP query. You can use the no igmp proxy query-max-response command to restore default configuration. • seconds: query response time, an integer, ranging from 1 to 25, in units of second
4	Raisecom(config)#igmp proxy last-query-interval <i>seconds</i> example: Raisecom(config)#igmp proxy last-query-interval 10	(Optional) configure the query interval of the last member in the multicast group. You can use the no igmp proxy last-query-interval command to restore default configuration. • seconds: interval, an integer, ranging from 1 to 25, in units of second
5	Raisecom(config)#igmp proxy last-query-count <i>count</i> example: Raisecom(config)#igmp proxy last-query-count 5	(Optional) configure the query times of the last member in the multicast group. You can use the no igmp proxy last-query-count command to restore default configuration. • count: query counts, an integer, ranging from 2 to 5
6	Raisecom(config)#igmp proxy source-ip <i>ip-address</i> example: Raisecom(config)#igmp proxy source-ip 10.0.0.1	(Optional) configure the source IP address of the IGMP Proxy packet sent by the IGMP querier. You can use the no igmp proxy source-ip command to restore default configuration. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1
7	Raisecom(config)#igmp proxy robustness <i>robustness</i> example: Raisecom(config)#igmp proxy robustness 3	Configure the IGMP Proxy robustness coefficient. You can use the no igmp proxy robustness command to restore default configuration. • robustness: robustness coefficient, an integer, ranging from 1 to 5

Configuring ONU IGMP Proxy

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu <i>slot-id/olt-id/onu-id</i> example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-list: ONU ID under the PON interface

Step	Command	Description
3	<pre>Raisecom(config-epon-onu-*//*:*)#ip igmp proxy ip-address address</pre> example: <pre>Raisecom(config-epon-onu-3/2:1)#ip igmp proxy ip-address 10.10.10.1</pre>	Configure IGMP Proxy IP address. You can use the no ip igmp proxy ip-address command to delete the configuration. ip-address: ONU multicast proxy IP address, in dotted decimal notation, such as 10.10.10.1
4	<pre>Raisecom(config-epon-onu-*//*:*)#ip igmp proxy vlan vlan-id</pre> example: <pre>Raisecom(config-epon-onu-3/1:1)#ip igmp proxy vlan 10</pre>	(Optional) configure IGMP Proxy VLAN. You can use the no ip igmp proxy vlan command to delete this configuration. vlan-id: tag VLAN ID to the frame. The VLAN ID is an integer ranging from 0 to 4094.

Checking configurations

No.	Command	Description
1	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet multicast</pre>	Show multicast service configurations on the ONU UNI.
2	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id mac-address-table multicast [uni ethernet uni]</pre>	Show the multicast address and VLAN learned by the ONU UNI.

5.6 Configuring MVR

5.6.1 Preparing for configurations

Scenario

When multiple user hosts need to receive data from the multicast source, and different user hosts, host and multicast router belong to different VLANs, you can configure MVR on the multicast router and the device connected to the user host, to enable users in different VLANs to receive the same multicast packet and reduce bandwidth waste.

Prerequisite

Create a VLAN and add related interfaces to the VLAN.

5.6.2 Default configurations

Default configurations of MVR on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Global MVR	Disable

5.6.3 Configuring basic MVR

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# mvr	Enable global MVR. You can use the no mvr command to disable this function.

5.6.4 Checking configurations

No.	Command	Description
1	Raisecom# show mvr	Show MVR configurations.

5.7 Configuring dynamic controllable multicast

5.7.1 Preparing for configurations

Scenario

Multicast data features heavy traffic and numerous receivers. So you must strictly manage the multicast source and receivers, and control the transmission direction and range of multicast data, in order to implement transmission of multicast services on the IP network.

Otherwise, operating multicast services not only affects the current IP network but also fails to provide services of the expected quality for receivers.

Prerequisite

You must configure the dynamic controllable multicast feature on the OLT and ONU simultaneously to implement this function in the EPON system.

5.7.2 Default configurations

Default configurations of dynamic controllable multicast on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Dynamic controllable multicast	Disable
Channel preview	Enable
Auto-reset period of preview	weekly
Aware time of preview	4s

Function	Default value
CDR	Enable
IP address of CDR Rx server	0.0.0.0
Maximum number of CDR	65535
Maximum duration when there is no on-demand packet	5 minutes

5.7.3 Configuring global parameters

5.7.4 Parameters

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#multicast-ctrl	Enable global dynamic controllable multicast.
3	Raisecom(config)#multicast-ctrl max-non-igmp-report-duration time example: Raisecom(config)#multicast-ctrl max-non-igmp-report-duration 10	Configure the maximum duration when there is no on-demand packet. You can use the no multicast-ctrl max-non-igmp-report-duration command to restore default configuration. period: time value, an integer, ranging from 1 to 65535, in units of minute

5.7.5 Configuring user management

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#multicast-ctrl user username source slot-id/port-id/vport-id cvlan vlan-id example: Raisecom(config)#multicast-ctrl user aa source 1/1/1 cvlan 10	Create a dynamic controllable multicast user. - username: VoD user name - slot-id/port-id/vport-id: slot ID/interface ID/virtual interface ID - vlan-id: CVLAN ID, an integer, ranging from 1 to 4094
3	Raisecom(config)#multicast-ctrl user username package packagename example: Raisecom(config)#multicast-ctrl user aa package sports	Configure channel package for users. - username: user name - packagename: channel package name

5.7.6 Configuring multicast channel management

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	raisecom(config)#multicast-ctrl channel id id name channel-name vlan vlan-id group-ip ip-address example: Raisecom(config)#multicast-ctrl channel id 1 name music vlan 2000 group-ip 240.0.0.1	Create a multicast channel. You can use the no multicast-ctrl channel name command to delete the channel. - channel-id: channel ID, an integer, ranging from 1 to 1024 - channel-name: name of the new channel, a string of 1 to 16 characters - vlan-id: VLAN ID, an integer, ranging from 1 to 4094 - group-ip ip-address: channel IP address, in dotted decimal notation, such as 224.0.0.1
3	Raisecom(config)#multicast-ctrl channel channelname cdr example: Raisecom(config)#multicast-ctrl channel sports cdr	Enable channel CDR. You can use the no multicast-ctrl channel channelname cdr command to disable this function. name: channel name, a string of 1 to 16 characters (cannot be empty)
4	Raisecom(config)#multicast-ctrl package packagename example: Raisecom(config)#multicast-ctrl package music	Create a channel package. You can use the no multicast-ctrl package packagename command to delete the channel. packagename: package name
5	Raisecom(config)#multicast-ctrl package packagename channel channelname { deny permit preview } [perview-profile profile] example: Raisecom(config)#multicast-ctrl package music channel popular permit	Add channels to the package. You can use the no multicast-ctrl package packagename channel channelname command to restore default configuration. - packagename: channel package name - channelname: add a channel name to the channel package. - deny: deny the view right. - permit: permit the view right. - preview: permit the preview right. - perview-profile profile: preview template, with the name of profile

5.7.7 Configuring preview rules

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#multicast-ctrl preview	Enable the preview function. You can use the no multicast-ctrl preview command to disable this function.

Step	Command	Description
3	<code>Raisecom(config)#multicast-ctrl preview reset</code>	Reset the preview manually.
4	<code>Raisecom(config)#multicast-ctrl preview auto-reset-period { daily weekly monthly custom } example: Raisecom(config)#multicast-ctrl preview auto-reset-period weekly</code>	Configure the auto-reset period of preview. You can use the no multicast-ctrl preview auto-reset-period command to restore default configuration. • daily: reset at 0:00 every day • monthly: reset at 0:00 on 1st of every month • weekly: reset at 0:00 every Sunday • custom: customized resetting time
5	<code>Raisecom(config)#multicast-ctrl preview auto-reset-time time example: Raisecom(config)#multicast-ctrl preview auto-reset-time 23:23:23</code>	Configure the auto-reset time of preview. You can use the no multicast-ctrl preview auto-reset command to restore default configuration. • time: reset time, in format of HH:MM:SS
6	<code>Raisecom(config)#multicast-ctrl preview aware-time time example: Raisecom(config)#multicast-ctrl preview aware-time 10</code>	Configure the aware time of preview. You can use the no multicast-ctrl preview aware-time command to restore default configuration. • time: preview recognition time, an integer, ranging from 1 to 60, in units of second
7	<code>Raisecom(config)#multicast-ctrl preview-profile { profile-name profile-id } example: Raisecom(config)#multicast-ctrl preview-profile preview</code>	Create a preview profile. You can use the nomulticast-ctrl preview-profile profile command to delete the profile. • profile-name: preview profile name • profile-id: preview profile ID
8	<code>Raisecom(config)#multicast-ctrl preview-profile { profile-name profile-id } total-time time example: Raisecom(config)#multicast-ctrl preview-profile preview total- time 4000</code>	Configure the total time for previewing a profile. You can use the no multicast-ctrl preview-profile profile total-time command to restore default configuration. • profile-name: template name • profile-id: profile ID • time: maximum counts of preview, an integer, ranging from 1 to 100
9	<code>Raisecom(config)#multicast-ctrl preview-profile { profile-name profile-id } count count example: Raisecom(config)#multicast-ctrl preview-profile preview count 100</code>	Configure the maximum times for previewing a profile. You can use the no multicast-ctrl preview-profile profile count command to restore default configuration. • profile-name: template name • profile-id: profile ID • time: maximum counts of preview, an integer, ranging from 1 to 100
10	<code>Raisecom(config)#multicast-ctrl preview-profile { profile-name profile-id } duration time example: Raisecom(config)#multicast-ctrl preview-profile preview duration 100</code>	Configure the maximum duration for previewing a profile at one time. You can use the no multicast-ctrl preview-profile profile duration command to restore default configuration. • profile-name: template name • profile-id: profile ID • period: maximum time of single preview, an integer, ranging from 1 to 6000, in units of second

Step	Command	Description
11	<pre>Raisecom(config)#multicast-ctrl preview-profile <i>profile</i> interval <i>time</i> example: Raisecom(config)#multicast-ctrl preview-profile preview interval 600</pre>	Configure the interval for previewing a profile for a second time. You can use the no multicast-ctrl preview-profile <i>profile</i> interval command to restore default configuration. • profile-name: template name • profile-id: profile ID • interval: preview interval, an integer, ranging from 1 to 6000, in units of second

5.7.8 Configuring CDR management

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#multicast-ctrl cdr	Enable CDR management. You can use the no multicast-ctrl cdr command to disable this function.
3	<pre>Raisecom(config)#multicast-ctrl cdr max-records <i>number</i> example: Raisecom(config)#multicast-ctrl cdr max-records 65530</pre>	Configure the maximum number of CDR. You can use the no multicast-ctrl cdr max-records command to restore default configuration. • max: maximum number of CDR records, an integer, ranging from 500 to 65535
4	Raisecom(config)#multicast-ctrl cdr report	Report CDR manually.
5	<pre>Raisecom(config)#multicast-ctrl cdr report-interval <i>interval</i> example: Raisecom(config)#multicast-ctrl cdr report-interval 10</pre>	Configure the interval for reporting CDR manually. You can use the no multicast-ctrl cdr report-interval command to restore default configuration. • interval: interval of CDR reporting, an integer, ranging from 1 to 30, in units of minute
6	<pre>Raisecom(config)#multicast-ctrl cdr report-threshold <i>value</i> example: Raisecom(config)#multicast-ctrl cdr report-threshold 500</pre>	Configure the threshold for reporting CDR manually. You can use the no multicast-ctrl cdr report-threshold command to restore default configuration. • value: threshold or CDR records reported to the NMS, an integer, ranging from 300 to 65535

5.7.9 Checking configurations

No.	Command	Description
1	Raisecom#show multicast-ctrl	Show configurations of dynamic controllable multicast.
2	Raisecom#show multicast-ctrl channel [<i>channelname</i>] online-user	Show channel online users.

No.	Command	Description
3	Raisecom# show multicast-ctrl channel [<i>channel-name</i> <i>channel-id</i> all]	Show channel configurations.
4	Raisecom# show multicast-ctrl user [<i>username</i>]	Show user configurations.
5	Raisecom# show multicast-ctrl user [<i>username</i>] online-channel	Show channel package of users.
6	Raisecom# show multicast-ctrl package [<i>package-name</i> <i>package-id</i> all]	Show information about the channel package.
7	Raisecom# show multicast-ctrl cdr	Show CDR configurations.
8	Raisecom# show multicast-ctrl cdr-content	Show the current CDR.
9	Raisecom# show multicast-ctrl preview	Show preview configurations.
10	Raisecom# show multicast-ctrl preview-profile [<i>profile</i>]	Show preview profile configurations.

5.8 Configuring MLD Snooping

5.8.1 Preparing for configurations

Scenario

Multicast Listener Discover (MLD) is a network protocol used by multicast technology. It is used to discover multicast listeners for the IPv6 device in its directly-connected network segment, namely the host nodes that expect to receive multicast data.

To implement the multicast function in an IPv6 network, you need to configure the MLD multicast function.

Prerequisite

N/A

5.8.2 Default configurations

Default configurations of MLD on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Global MLD multicast	Disable
Aging time of MLD Snooping	300s

5.8.3 Configuring MLD Snooping

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mld	Enable MLD multicast. You can use the no mld command to disable this function.
3	Raisecom(config)#mld snooping timeout { period infinite } example: Raisecom(config)#mld snooping timeout 100	(Optional) configure the aging time of MLD Snooping. You can use the no mld snooping timeout command to restore default configurations. • period: timeout value, an integer, ranging from 30 to 3600, in units of second • infinite: the multicast forwarding entry does not age out.

5.8.4 Checking configurations

No.	Command	Description
1	Raisecom#show mld statistics	Show MLD packet statistics.
2	Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet port-channel group-id } slot-id/olt-id mld statistics	Show MLD packet statistics on a specified interface.

5.9 Configuring MLD Proxy

5.9.1 Preparing for configurations

Scenario

MLD is a network protocol used by multicast technology. It is used to discover multicast listeners for the IPv6 device in its directly-connected network segment, namely the host nodes that expect to receive multicast data.

To implement the multicast function in an IPv6 network, you need to configure the MLD multicast function.

Prerequisite

N/A

5.9.2 Default configurations

Default configurations of MLD Proxy on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Global MLD multicast	Disable
MLD multicast IP address	Local link address, namely, the address generated by the local MAC address and starting with FE80, such as fe80::2a0:1eff:fea0:aaa0
MLD Proxy query interval	125s
Maximum response time of MLD Proxy query	10s
Query interval of MLD Proxy last member	2s
Number of query packets of MLD Proxy last member	2
MLD Proxy robustness coefficient	2
MLD Proxy version	v2

5.9.3 Configuring MLD Proxy

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mld	Enable MLD Proxy. You can use the no mld command to disable this function.
3	Raisecom(config)#mld proxy source-ip ipv6-address example: Raisecom(config)#mld proxy source-ip 3001::1	Configure the MLD Proxy multicast IPv6 address. You can use the no mld proxy source-ip command to delete the configuration. • ipv6-address: IPv6 address, in colon hexadecimal notation, such as 3001::1
4	Raisecom(config)#mld proxy query-interval seconds example: Raisecom(config)#mld proxy query-interval 100	(Optional) configure the MLD Proxy query interval. You can use the no mld proxy query-interval command to restore default configurations. • seconds: interval, an integer, ranging from 10 to 65535, in units of second
5	Raisecom(config)#mld proxy query-max-response seconds example: Raisecom(config)#mld proxy query-max-response 15	(Optional) configure the maximum response time of MLD Proxy query. You can use the no mld proxy query-max-response command to restore default configurations. • seconds: query response time, an integer, ranging from 1 to 25, in units of second

Step	Command	Description
6	<pre>Raisecom(config)#mld proxy last-query-interval seconds</pre> example: <pre>Raisecom(config)#mld proxy last-query-interval 10</pre>	(Optional) configure the query interval of MLD Proxy last member. You can use the no mld proxy last-query-interval command to restore default configurations. seconds: interval, an integer, ranging from 1 to 25, in units of second
7	<pre>Raisecom(config)#mld proxy last-query-count count</pre> example: <pre>Raisecom(config)#mld proxy last-member-query-count 5</pre>	(Optional) configure the times to query the MLD Proxy last member. You can use the no mld proxy last-query-count command to restore default configurations. count: query times, an integer, ranging from 2 to 5
8	<pre>Raisecom(config)#mld proxy source-ip ipv6-address</pre> example: <pre>Raisecom(config)#mld proxy source-ip 3001::1</pre>	(Optional) configure the source IPv6 address of the query packet sent by the MLD Proxy querier. You can use the no mld proxy source-ip command to restore default configurations. ipv6-address: IPv6 address, in colon hexadecimal notation, such as 3001::1
9	<pre>Raisecom(config)#mld proxy robustness robustness</pre> example: <pre>Raisecom(config)#mld proxy robustness 3</pre>	Configure the robustness coefficient of MLD Proxy. You can use the no mld proxy robustness command to restore default configurations. robustness: robustness coefficient, an integer, ranging from 1 to 5

5.9.4 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show mld statistics</pre>	Show MLD packet statistics.
2	<pre>Raisecom#show interface { epon-olt ten-giga- epon-olt gpon-olt gigabitethernet port- channel group-id } slot-id/olt-id mld statistics</pre>	Show MLD packet statistics on a specified interface.

5.10 Configuring multicast VLAN

5.10.1 Preparing for configurations

Scenario

In the traditional on-demand multicast mode, when hosts in different VLANs request the same multicast group at the same time, Layer 3 devices need to copy multicast data to each

VLAN. This not only wastes the bandwidth, but also increases the burden of the Layer 3 device.

You can use the multicast VLAN to solve the problem. After you configure the multicast VLAN on the Layer 2 device, the Layer 3 device only needs to make a copy of multicast data in the multicast VLAN and sent it to the Layer 2 device, without making a copy in each VLAN. In this case, it saves the network bandwidth and reduces the burden of the Layer 3 device.

Prerequisite

N/A

5.10.2 Default configurations

Default configurations of multicast VLAN on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Multicast VLAN	Disable
Working mode of multicast VLAN	Snooping
CVLAN transparent transmission	Disable
Priority of multicast VLAN uplink protocol packets	keep
Priority of multicast VLAN downlink protocol packets	keep

5.10.3 Configuring multicast VLAN

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#multicast-vlan vlan-id example: Raisecom(config)#multicast-vlan 10	Create a multicast VLAN. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
3	Raisecom(config)#multicast-vlan vlan-id mode { snooping proxy } example: Raisecom(config)#multicast-vlan 10 mode proxy	Configure the working mode of the multicast VLAN. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • snooping: configure the working mode of multicast VLAN to Snooping. • proxy: configure the working mode of multicast VLAN to Proxy.

Step	Command	Description
4	<pre>Raisecom(config)#multicast-vlan vlan-id group address [count] example: Raisecom(config)#multicast-vlan 10 group 224.1.1.1</pre>	Configure binding the multicast VLAN with the group address. You can use the no multicast-vlan vlan-id group { group-address [count] any } command to restore default configuration. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • address: group address, in dotted decimal notation, such as 224.0.0.1 • count: configure the number of multiple consecutive group addresses, an integer, ranging from 1 to 1024
5	<pre>Raisecom(config)#multicast-vlan vlan-id cvlan-forward example: Raisecom(config)#multicast-vlan 10 cvlan-forward</pre>	Configure CVLAN transparent transmission. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
6	<pre>Raisecom(config)#multicast-vlan vlan-id upstream-priority pri example: Raisecom(config)#multicast-vlan 10 upstream-priority 6</pre>	Configure the priority of multicast VLAN uplink protocol packets. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • priority: protocol packet priority, an integer, ranging from 0 to 7
7	<pre>Raisecom(config)#multicast-vlan vlan-id downstream-priority pri example: Raisecom(config)#multicast-vlan 10 downstream-priority 6</pre>	Configure the priority of multicast VLAN downlink protocol packets. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • priority: protocol packet priority, an integer, ranging from 0 to 7
8	<pre>Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten- gigabitethernet port-channel group-id } slot-id/olt-id example: Raisecom(config)#interface gigabitethernet 2/1</pre>	Enter physical interface configuration mode. • epon-olt slot-id/port-id: EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gpon-olt slot-id/port-id: GPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gigabitethernet slot-id/port-id: 1000 Mbit/s Ethernet interface. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-gigabitethernet slot-id/port-id: 10 Gbit/s Ethernet interface. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-giga-epon-olt slot-id/port-id: 10G EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • port-channel group-id: aggregation group interface ID. The group-list refers to the aggregation group interface ID, ranging from 1 to 32.

Step	Command	Description
9	Raisecom(config-if-*-*:*)# multicast-vlan <i>vlan-id</i> router example: Raisecom(config-if-gigabitethernet-2:1)#multicast-vlan 10 router	Configure the multicast VLAN router interface. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
10	Raisecom(config-if-*-*:*)# multicast-vlan <i>vlan-id</i> member example: Raisecom(config-if-gigabitethernet-2:1)#multicast-vlan 10 member	Configure the multicast VLAN member interface. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094



Note

- The system supports automatic learning of the multicast VLAN router port. The auto-learned multicast router port does not support manual deletion. By default, the aging time is not configurable.
- The system supports automatic learning of member ports of multicast VLANs. The member ports that are automatically learned cannot be deleted manually. When member ports are not referenced, the system automatically deletes the member ports.

5.10.4 Checking configurations

No.	Command	Description
1	Raisecom(config)# show multicast-vlan <i>vlan-id</i>	Show multicast VLAN configurations.
2	Raisecom(config)# show multicast-vlan <i>vlan-id</i> group	Show multicast VLAN group address.
3	Raisecom(config)# show multicast-vlan <i>vlan-id</i> router	Show the multicast VLAN router interface.
4	Raisecom(config)# show multicast-vlan <i>vlan-id</i> member	Show the member interfaces of a specified IGMP multicast VLAN.

5.11 Maintenance

No.	Command	Description
1	Raisecom(config)# clear igmp statistics	Clear IGMP packet statistics.

No.	Command	Description
2	Raisecom(config)#clear interface { epon-olt slot-id/port-id ten-giga-epon-olt slot-id/port-id gpon-olt slot-id/port-id gigabitethernet slot-id/port-id ten-gigabitethernet slot-id/port-id port-channel group-id } igmp statistics example: Raisecom(config)#clear interface gigabitethernet 2/1 igmp	Clear IGMP packet statistics on a specified interface. • epon-olt slot-id/port-id: EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gpon-olt slot-id/port-id: GPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gigabitethernet slot-id/port-id: 1000 Mbit/s Ethernet interface. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-gigabitethernet slot-id/port-id: 10 Gbit/s Ethernet interface. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-giga-epon-olt slot-id/port-id: 10G EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • port-channel group-id: aggregation group interface ID. The group-list refers to the aggregation group interface ID, ranging from 1 to 32.
3	Raisecom(config)# clear mld statistics	Clear MLD packet statistics.
4	Raisecom(config)#clear interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet port-channel group-id } slot-id/port-id mld statistics example: Raisecom(config)#clear interface gigabitethernet 2/1 mld statistics	Clear MLD packet statistics on a specified interface. • epon-olt slot-id/port-id: EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gpon-olt slot-id/port-id: GPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gigabitethernet slot-id/port-id: 1000 Mbit/s Ethernet interface. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-gigabitethernet slot-id/port-id: 10 Gbit/s Ethernet interface. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-giga-epon-olt slot-id/port-id: 10G EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • port-channel group-id: aggregation group interface ID. The group-list refers to the aggregation group interface ID, ranging from 1 to 32.
5	Raisecom(config)# multicast-ctrl cdr clear	Clear CDR information.

No.	Command	Description
6	Raisecom(config)#clear mac-address-table multicast dynamic vlan <i>vlan-id</i> example: Raisecom(config)#clear mac-address-table multicast dynamic vlan 1	Clear the VLAN-based multicast dynamic learning entry. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
7	Raisecom(config)#clear interface { gigabitethernet ten-gigabitethernet epon-olt } mac-address-table multicast dynamic vlan <i>vlan-id</i> example: Raisecom(config)#clear interface gigabitethernet mac-address-table multicast dynamic vlan 1	Clear interface-based multicast dynamic learning entries. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • epon-olt slot-id/port-id: PON interface ID. The slot-id refers to the slot ID; the olt-id refers to the PON interface ID. • gpon-olt slot-id/olt-id: GPON interface ID. The slot-id refers to the slot ID; the olt-id refers to the PON interface ID. • gigabitethernet slot-id/port-id: GE interface ID. The slot-id refers to the slot ID; the port-id refers to the GE interface ID. • ten-gigabitethernet slot-id/port-id: 10 Gbit/s Ethernet interface. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-giga-epon-olt slot-id/olt-id: 10G EPON interface ID. The slot-id refers to the slot ID; the olt-id refers to the PON interface ID.
8	Raisecom(config)#clear mac-address-table dynamic multicast <i>mac-address</i> example: Raisecom(config)#clear mac-address-table dynamic multicast 000E.5E12.3456	Clear the MAC-based multicast dynamic learning entries. • mac-address: mac-address, in dotted hexadecimal notation, such as 000E.5E12.3456

6 Configuring VoIP services

This chapter describes VoIP services and configuration process of the device, and provides related configurations examples, including the following sections:

- Overview of VoIP services
- Quick configuration of VoIP services
- Configuring VoIP
- Configuring POTS interface
- Configuring SIP
- Configuring H.248
- Configuring second dialing
- Configuring fax
- Configuring call emulation test
- Configuring SIP server profile

6.1 Overview of VoIP services

6.1.1 VoIP

Voice over IP (VoIP) is the technology to transmit traditional TDM digital voice signals in packets through the IP network in real time so as to realize voice communication. Compared with traditional voice services, VoIP can make use of the extensive Internet environment to provide more, better, and cheaper services.

VoIP can use multiple signalling protocols to realize voice call. The ISCOM6800 and ISCOM6860 support Session Initiation Protocol (SIP) and H.248 protocol.

6.1.2 SIP

Overview of SIP

SIP is an application-layer control protocol which is used to perform media communication over Internet Protocol (IP) network. The protocol can be used for creating, modifying, and terminating interactive sessions, such as video, voice, and instance communication.

SIP is a text-based protocol. It can run on IP, Transmission Control Protocol (TCP), and User Datagram Protocol (UDP), with UDP as a preference, over the IP network.

Basic concepts of SIP

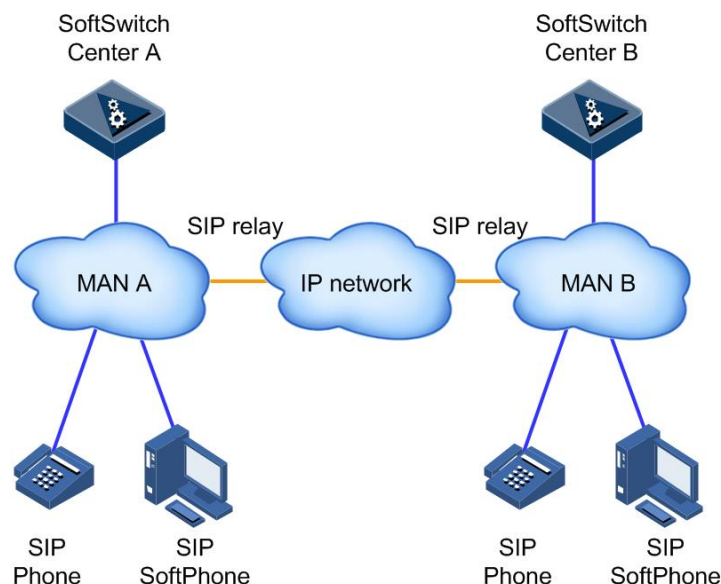
Related concepts involved in the operating environment of SIP are shown as below.

- Location Server: provides possible location information for the Redirect Server or the Proxy Server.
- Proxy Server: forwards SIP requests for other users. The Proxy Server parses and modifies (if necessary) requests before forwarding them.
- Redirect Server: receives SIP requests, maps addresses of SIP requests to 0 or more new addresses, and sends the result to the customer.
- Register Server: receives registration requests and registers user information. In general, it is located at the same place with the Proxy Server/Redirect Server for providing location services.
- User Agent Client: initiates SIP requests.
- User Agent Server: contacts and replies users after receiving SIP requests. It can receive, refuse, or redirect these requests.

Typical application of SIP

Figure 6-1 shows a typical application of SIP in the Next Generation Network (NGN).

Figure 6-1 Typical application of SIP in NGN



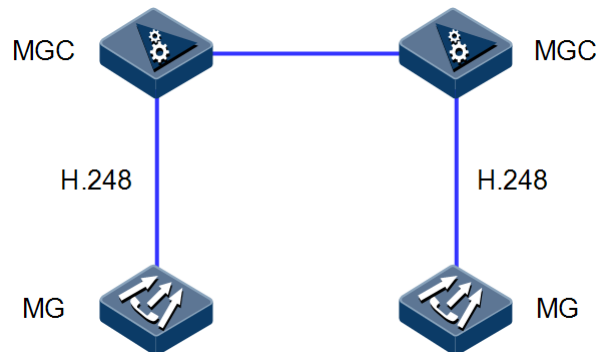
6.1.3 H.248

Overview of H.248

H.248 or Media Gateway Control Protocol (Megaco) is a media gateway control protocol defined by Internet Engineering Task Force (IETF) and ITU Telecommunication

Standardization Sector (ITU-T). It is used for communication between Media Gateway Controller (MGC) and Media Gateway (MG), as shown in Figure 6-2.

Figure 6-2 Position of H.248 in the network



H.248 packets can be transmitted across multiple packet networks, such as IP, ATM, and MTP.

H.248 protocol information coding can adopt binary/text format. At present, it supports text-based coding only.

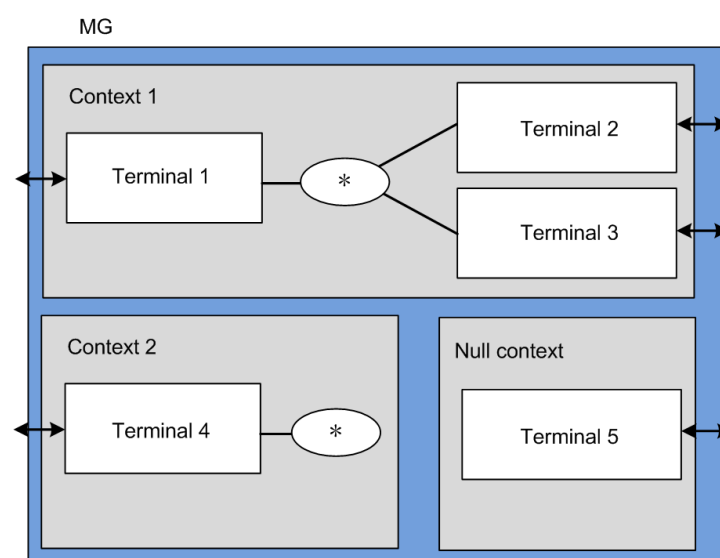
Currently, H.248 packets are transmitted through UDP. When H.248 protocol is adopted, the port number is related with the coding type. By default, port 2934 is used for text-based coding while port 2945 is used for binary coding.

H.248 connection model

The H.248 connection model contains the logical entities, or objects, within the MGs that can be controlled by the MGC. It is the core for the MGC and MGs communicating messages. The MGC controls connection objects within MGs. MGs report various state information about connection objects, such as parameters and capability.

The H.248 connection model contains Terminal and Context, as shown in Figure 6-3.

Figure 6-3 H.248 H.248 connection model



The terminal is a logical entity that can send/receive one or multiple types of media traffic, including the following 3 types:

- Physical terminal: also known as semi-permanent terminal. Its entity can be a trunk interface of the Trunk Gateway (TG), or a telephone interface/PBX interface of the Access Gateway (AG).
- Virtual terminal: also known as ephemeral terminal. It is used to deal with some data flow, such as a RTP voice stream. It depends on calls. Once a call is finished, the terminal is dead.
- Root terminal: represents the whole MG. when the ROOT is entered as the parameter of a command, the command takes effect on the whole gateway instead of a terminal on the gateway.

In real application, once a terminal is created, the system will assign a unique Terminal ID (TID) for the terminal identification.

The context is made up by a collection of terminals and their connection topology. One context contains a terminal at least. Otherwise, this context is deleted. A terminal cannot coexist in two or more contexts. If a context contains two or more terminals, the context should describe the topology structure and other media hybrid/exchanging parameters.

Null context is a special context. It contains one terminal which is not associated with other terminals.

The context has the following features:

- Context ID: a 32-bit integer selected by a MG, which is unique within the MG
- Topology: describes the direction of media traffic among terminals within a context. It mainly refers to directions of media traffic on both ingress and egress interfaces of the MG.
- Priority: indicates the sequence for a MG dealing with contexts. In some cases where the system needs to co-process multiple contexts, the MGC can use the priority to control the sequence for a MG processing these contexts. According to H.248, 0 refers to the lowest priority and 15 refers to the highest priority.
- Indicator for Emergency Call: a MG prioritizes processing calls with Indicator for Emergency Call.

6.2 Quick configuration of VoIP services

Configurations of VoIP voice services are complicated involving many functional configuration items. This section provides you a typical configuration example to facilitate you to enable VoIP voice services quickly.

If you need to configure more VoIP voice service functions or have a more detailed understanding of VoIP service configurations, see other sections in this chapter.

6.2.1 Example for configuring SIP voice service (Proxy call)

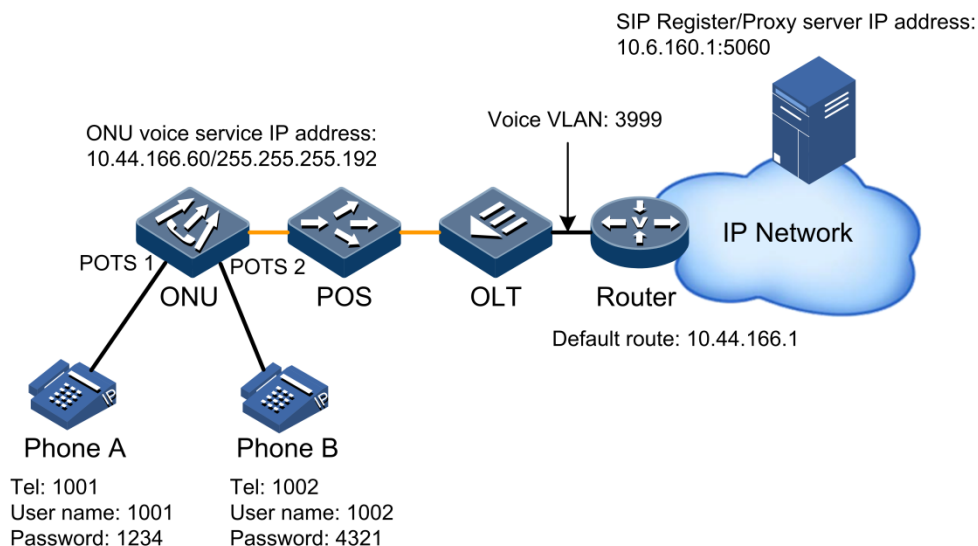
Networking requirements

As shown in Figure 6-4, configure SIP voice service (Proxy call) on the OLT as below:

- See section 6.5 Configuring SIP for data service configuration involved in enabling the SIP voice service.
- Voice service VLAN: 3999

- Configure two phone numbers on the ONU, that is, POTS 1: 1001 and POTS 2: 1002.

Figure 6-4 Configuring SIP voice service (Proxy call)



Configuration steps

Step 1 Configure the VoIP signalling protocol.

```
Raisecom#config
Raisecom(config)#epon-onu 3/1/1 voice
Raisecom(config-epon-onu-voice-3/1:1)#voip-protocol sip
Raisecom(config-epon-onu-voice-3/1:1)#exit
Raisecom(config)#epon-onu 3/1/1
Raisecom(config-epon-onu-3/1:1)#write
Raisecom(config-epon-onu-3/1:1)#reboot
```

Caution

After you save configurations by using the **write** command, you need to wait 10s and then use the **reboot** command to reboot the ONU since it takes time for the OLT to distribute configurations to the ONU. Otherwise, the OLT may fail to distribute configurations to the ONU.

Step 2 Configure the voice service VLAN.

```
Raisecom#config
Raisecom(config)#epon-onu 3/1/1 voice
Raisecom(config-epon-onu-voice-3/1:1)#vlan mode tagged
Raisecom(config-epon-onu-voice-3/1:1)#vlan 3999 cos 6
```

Step 3 Configure the IP address for the voice service.

```
Raisecom(config-epon-onu-voice-3/1:1)#ip address 10.44.166.60
255.255.255.192
Raisecom(config-epon-onu-voice-3/1:1)#ip route default 10.44.166.1
```

Step 4 Configure the phone number of POTS.

```
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 1001 1
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 1002 2
```

Step 5 Configure the Proxy server and Register server (both servers have the same IP address).

```
Raisecom(config-epon-onu-voice-3/1:1)#sip primary proxy-server ip
10.6.160.1
Raisecom(config-epon-onu-voice-3/1:1)#sip primary register-server ip
10.6.160.1
```

Step 6 (Optional) configure user authentication information only when the SIP server requires to authenticate users

```
Raisecom(config-epon-onu-voice-3/1:1)#sip pots authentication 1001
password 1234 1
Raisecom(config-epon-onu-voice-3/1:1)#sip pots authentication 1002
password 4321 2
```

Checking results

Check whether the route between the ONU voice node and soft switch is available. You need to configure the in-band management IP address of the OLT and default gateway in advance.

```
Raisecom#config
Raisecom(config)#ip route 0.0.0.0 0.0.0.0 10.44.166.1
Raisecom(config)#interface vlanif 3999
Raisecom(config-vlanif-3999)#ip address 10.44.166.61 255.255.255.192
Raisecom(config-vlanif-3999)#end
Raisecom#ping 10.6.160.1
Type CTRL+C to abort.
Sending 5, 72-byte ICMP Echos to 10.6.160.1 , timeout is 1 seconds:
!!!!
Success rate is 100 percent(5/5)
round-trip (ms) min/avg/max = 0/3/16
```

Show information about the POTS phone number.

```
Raisecom#config
Raisecom(config)#epon-onu 3/1/1 voice
Raisecom(config-epon-onu-voice-3/1:1)#show epon-onu 3/1/1 voice pots
Pots ID   Admin Status  Port Status   Service Status CodecType
-----
3/1/1/1   enable    registerSucceed normal    G.711A
3/1/1/2   enable    registerSucceed normal    G.711A
```

Show POTS registration information.

```
Raisecom(config-epon-onu-voice-3/1:1)#show epon-onu 3/1/1 voice sip pots
1 service
Port ID: 3/1/1:1
  Register state : registerSucceed
  Call state    : hookon
  Caller ID state : enable
  Call wait state : disable
  Three way conference: disable
```

```
Raisecom(config-epon-onu-voice-1/1:1)#show epon-onu 3/1/1 voice sip pots
2 service
Port ID: 3/1/1:2
  Register state : registerSucceed
  Call state    : hookon
  Caller ID state : enable
  Call wait state : disable
  Three way conference: disable
```

Show IP information about the voice service.

```
Raisecom(config-epon-onu-voice-3/1:1)#show epon-onu 3/1/1 voice ip
ONU ID: 3/1/1
  IP mode      : static
  IP address   : 10.44.166.60
  Subnet mask  : 255.255.255.192
  Default route : 10.44.166.1
  DNS server IP address: 0.0.0.0
  Vlan mode    : tagged
  VID         : 3999
  Cos         : 6
  Outter VID   : 0
  MAC address  : 000e.5e07.7ac0
  IP QoS trust policy : None
  QoS default-dscp : 0
  QoS default-tos  : 0
  QoS default-priority : 0
```

Show address information about the SIP Proxy/Register server.


```
Raisecom(config-epon-onu-voice-1/1:1)#show epon-onu 3/1/1 voice sip
primary proxy-server
```

ONU ID	Proxy IP	Udp Port	Tcp Port	Transport
3/1/1	10.6.160.1	5060	5060	udp

```
Raisecom(config-epon-onu-voice-1/1:1)#show epon-onu 3/1/1 voice sip
primary register-server
```

ONU ID	Server IP	Udp Port	Tcp Port	Transport	Fresh Period(s)
3/1/1	10.6.160.1	5060	5060	udp	3600

Show user authentication information.

```
Raisecom(config-epon-onu-voice-1/1:1)#show epon-onu 3/1/1 voice sip pots
authentication
```

Pots ID	Authentication Name	Authentication Password
3/1/1:1	1001	1234
3/1/1:2	1002	4321
3/1/1:3	N/A	*
3/1/1:4	N/A	*
3/1/1:5	N/A	*
3/1/1:6	N/A	*
3/1/1:7	N/A	*
3/1/1:8	N/A	*
3/1/1:9	N/A	*
3/1/1:10	N/A	*
3/1/1:11	N/A	*
3/1/1:12	N/A	*
3/1/1:13	N/A	*
3/1/1:14	N/A	*
3/1/1:15	N/A	*
3/1/1:16	N/A	*

Service verification: telephones under the ONU can communicate with each other if the SIP registration is successful after configurations.

- The calling party picks up the phone and hears the dial tone.
- When the calling party dials the phone number of the called party, the phone of the called party rings and the calling party hears the ringback tone.
- The calling party communicates with the called party normally.
- The calling party hears the busy tone if the called party hangs up.

6.2.2 Example for configuring SIP voice service (Direct call)

Networking requirements

As shown in Figure 6-5, configure SIP voice service (Direct call) on the OLT as below:

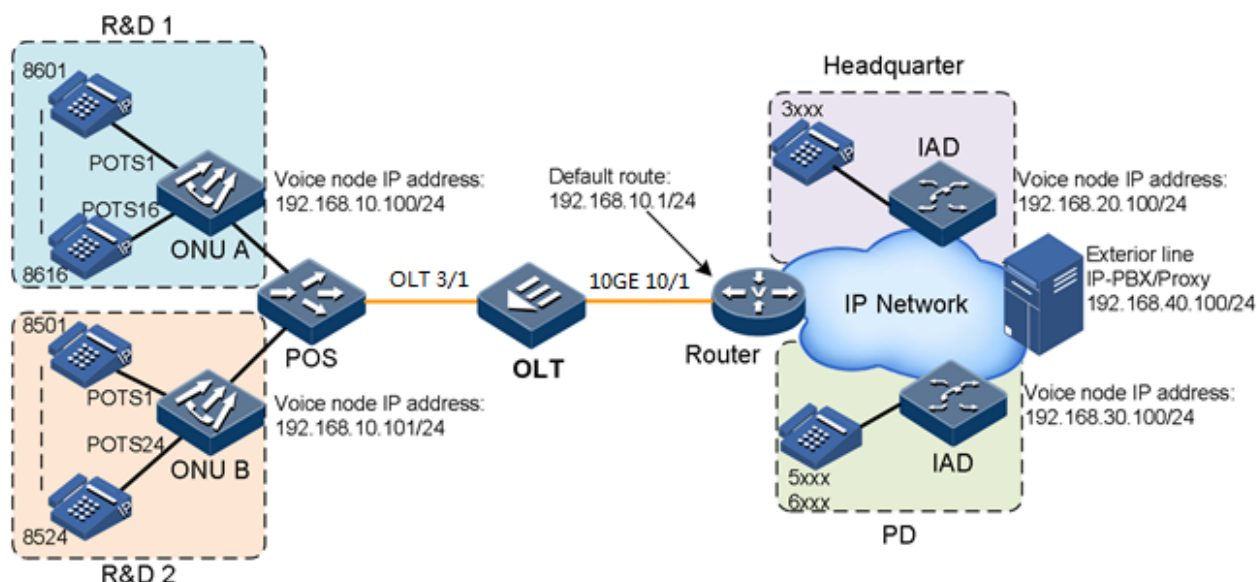
- The IP route among headquarter, R&D 1, R&D 2, production department and exterior line station is available, and there is no VLAN in network.
- Extension number of headquarter: 3xxx; IP address of IAD SIP voice device: 192.168.20.100
- Extension number of R&D 1: 86xx; IP address of ONU A voice device: 192.168.10.100
- Extension number of R&D 2: 85xx; IP address of ONU B voice device: 192.168.10.101
- Extension number of production department: 5xxx or 6xxx; IP address of IAD SIP voice device: 192.168.30.100
- IP address of exterior line station: 192.168.40.100; the first number for exterior line: 0; # is used in the end to accelerate the dial-up.
- Dialing rule configurations are the same on all devices. Take R&D 1 for example.
- The SIP routing table is shown as below:

```

1 86xx 192.168.10.100
2 85xx 192.168.10.101
3 3xxx 192.168.20.100
4 [5-6]xxx 192.168.30.100
5 0x.# 192.168.40.100

```

Figure 6-5 Configuring SIP voice service (Direct call)



Configuration steps

Take R&D 1 SIP voice service as an example to configure ONU A. Configurations on ONU B in R&D 2 are the same.

Step 1 Configure the VoIP signalling protocol.

```

Raisecom#config
Raisecom(config)#epon-onu 3/1/1 voice

```

```
Raisecom(config-epon-onu-voice-3/1:1)#voip-protocol sip
Raisecom(config-epon-onu-voice-3/1:1)#exit
Raisecom(config)#epon-onu 3/1/1
Raisecom(config-epon-onu-3/1:1)#write
Raisecom(config-epon-onu-3/1:1)#reboot
```



After you save configurations by using the **write** command, you need to wait 10s and then use the **reboot** command to reboot the ONU since it takes time for the OLT to distribute configurations to the ONU. Otherwise, the OLT may fail to distribute configurations to the ONU.

Step 2 Configure the IP address for the voice service.

```
Raisecom#config
Raisecom#epon-onu 3/1/1 voice
Raisecom(config-epon-onu-voice-3/1:1)#ip address 192.168.10.100
Raisecom(config-epon-onu-voice-3/1:1)#ip route default 192.168.10.1
```

Step 3 Configure the POTS phone number.

```
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8601 1
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8602 2
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8603 3
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8604 4
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8605 5
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8606 6
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8607 7
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8608 8
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8609 9
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8610 10
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8611 11
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8612 12
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8613 13
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8614 14
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8615 15
Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 8616 16
```

Step 4 Configure the mapping rule of SIP phone numbers.

```
Raisecom(config-epon-onu-voice-3/1:1)#sip dial-map-rule 1 86xx
192.168.10.100
Raisecom(config-epon-onu-voice-3/1:1)#sip dial-map-rule 2 85xx
192.168.10.101
Raisecom(config-epon-onu-voice-3/1:1)#sip dial-map-rule 3 3xxx
192.168.20.100
```

```
Raisecom(config-epon-onu-voice-3/1:1)#sip dial-map-rule 4 [5-6]xxx
192.168.30.100
Raisecom(config-epon-onu-voice-3/1:1)#sip dial-map-rule 5 0x.#
192.168.40.100
```

Checking results

Show dialling rule configurations.

```
Raisecom#config
Raisecom(config)#epon-onu 3/1/1 voice
Raisecom(config-epon-onu-voice-3/1:1)#show epon-onu 3/1/1 voice sip dial-
map-rule
ONU ID: 3/1/1
```

Rule ID	Phone Number	SIP URI
1	86xx	192.168.10.100
2	85xx	192.168.10.101
3	3xxx	192.168.20.100
4	[5-6]xxx	192.168.30.100
5	0x.#	192.168.40.100

Show the running configuration file of the ONU.

```
Raisecom(config-epon-onu-voice-3/1:1)#show running-config
!Voice current configuration:
sip dial-map-rule 1 86xx 192.168.10.100
sip dial-map-rule 2 85xx 192.168.10.101
sip dial-map-rule 3 3xxx 192.168.20.100
sip dial-map-rule 4 [5-6]xxx 192.168.30.100
sip dial-map-rule 5 0x.# 192.168.40.100
pots phone-number 8601 1
pots phone-number 8602 2
pots phone-number 8603 3
pots phone-number 8604 4
pots phone-number 8605 5
pots phone-number 8606 6
pots phone-number 8607 7
pots phone-number 8608 8
pots phone-number 8609 9
pots phone-number 8610 10
pots phone-number 8611 11
pots phone-number 8612 12
pots phone-number 8613 13
pots phone-number 8614 14
pots phone-number 8615 15
pots phone-number 8616 16
ip address 192.168.10.100 255.255.255.0
ip route default 192.168.10.1
!
```

Check whether the route between the voice node and the gateway is reachable. You need to configure the in-band management IP address and default gateway in advance.

```
Raisecom(config-epon-onu-voice-3/1:1)#end
Raisecom#config
Raisecom(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.1
Raisecom(config)#interface vlanif 1
config-vlanif-Raisecom(1)#ip address 192.168.10.253 255.255.255.0
Raisecom(config-vlanif-1)#end
Raisecom#ping 192.168.10.1
Sending 5, 72-byte ICMP Echos to 192.168.10.1 , timeout is 1 seconds:
!!!!
Success rate is 100 percent(5/5)
round-trip (ms) min/avg/max = 0/24/110
```

After you configure other devices correctly, use the telephone in R&D 1 to perform dial-up authentication:

- The calling party picks up the phone and hears the dial tone.
- When the calling party dials the four-digit long phone numbers beginning with 86, 85, 3, 5, 6, or more than two-digit long numbers beginning with 0, the phone of the called party rings and the calling party hears ringback tone.
- The calling party communicates with the called party normally.
- The calling party hears the busy tone if the called party hangs up.

6.2.3 Example for configuring H.248 voice service

Networking requirements

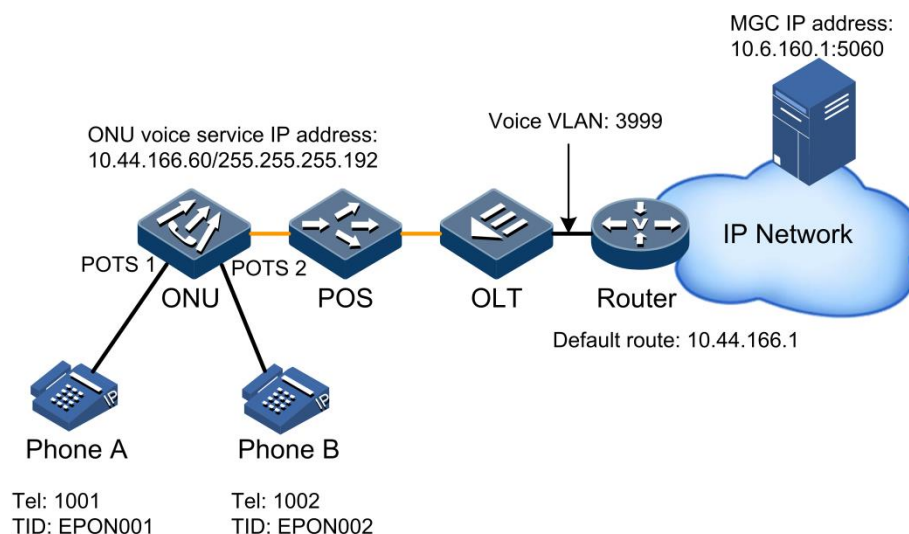
As shown in Figure 6-6, configure the H.248 voice service to realize communication between 2 ways of voice services on the ONU. The example in this section is suitable for the quick configuration of the H.248 voice service. For details, see section 6.6 Configuring H.248.

You need to obtain the following information from the central office so as to ensure the consistency between the configuration and default configurations of the central office as well as activation of voice services. Default values in the table below are applicable to this example only. You should refer to the default configurations of the central office in practice

Parameter	Default value
IP address and mask of ONU voice node	• IP address: 10.44.166.60 • Mask: 255.255.255.192
Routing gateway of voice node	10.44.166.1
Voice VLAN and service priority	• Voice VLAN: 3999 • Service priority: 6
MG registration mode	domain-name
MG name (which is not needed in IP or MAC registration mode)	raisecom
MG transmission interface ID	2944

Parameter	Default value
Coding mode of H.248 protocol signalling	text
IP address of MGC server	10.6.160.1
Generation mode of MG POTS TID	line
MG POTS TID	• POTS 1 TID: EPON001 • POTS 2 TID: EPON002
Prefix and digital length of MG RTP TID	• Prefix: RTP • Digital length: 5
Phone number	You just need to configure the POTS TID without the phone number, which is generated by the MGC configuration of the central office.

Figure 6-6 H.248 Configuring H.248 voice service



Configuration steps

Step 1 Choose the VoIP signalling protocol type.

```
Raisecom#config
Raisecom(config)#epon-onu 3/1/1 voice
Raisecom(config-epon-onu-voice-3/1:1)#voip-protocol h248
Raisecom(config-epon-onu-voice-3/1:1)#exit
Raisecom(config)#epon-onu 3/1/1
Raisecom(config-epon-onu-3/1:1)#write
Raisecom(config-epon-onu-3/1:1)#reboot
```



After you save configurations by using the write command, you need to wait 10s and then use the **reboot** command to reboot the ONU since it takes time for the OLT to distribute configurations to the ONU. Otherwise, the OLT may fail to distribute configuration

Step 2 Configure the voice VLAN

```
Raisecom(config-epon-onu-voice-3/1:1)#vlan mode tagged  
config-epon-onu-voice-3/1:1#vlan 3999 cos 6
```

Step 3 Configure the IP address for the ONU voice service.

```
Raisecom(config-epon-onu-voice-3/1:1)#ip address 10.44.166.60  
255.255.255.192  
Raisecom(config-epon-onu-voice-3/1:1)#ip route default 10.44.166.1
```

Step 4 Configure MG information.

```
Raisecom(config-epon-onu-voice-3/1:1)#h248 mg register-mode domain-name  
Raisecom(config-epon-onu-voice-3/1:1)#h248 mg name raisecom  
Raisecom(config-epon-onu-voice-3/1:1)#h248 mg encode text  
Raisecom(config-epon-onu-voice-3/1:1)#h248 mg transport port 2944
```

Step 5 Configure POTS TID and RTP TID.

```
Raisecom(config-epon-onu-voice-3/1:1)#h248 mg tid mode line  
Raisecom(config-epon-onu-voice-3/1:1)#h248 pots tid name EPON001 1  
Raisecom(config-epon-onu-voice-3/1:1)#h248 pots tid name EPON002 2  
Raisecom(config-epon-onu-voice-3/1:1)#h248 mg tid rtp prefix RTP length 5
```

Step 6 Configure the MGC server.

```
Raisecom(config-epon-onu-voice-3/1:1)#h248 primary mgc ip 10.6.160.1 port  
2944  
Raisecom(config-epon-onu-voice-3/1:1)#no h248 primary mgc authentication
```

Step 7 Save configurations.

```
Raisecom(config-epon-onu-voice-3/1:1)#exit
Raisecom(config)#epon-onu 3/1/1
Raisecom(config-epon-onu-3/1:1)#write
```

Checking results

Check whether the route between the ONU voice node and the MGC is available. You need to configure the in-band management IP address of the OLT in advance.

```
Raisecom#config
Raisecom(config)#ip route 0.0.0.0 0.0.0.0 10.44.166.1
Raisecom(config)#interface vlanif 3999
Raisecom(config-vlanif-3999)#ip address 10.44.166.61 255.255.255.192
Raisecom(config-vlanif-3999)#end
Raisecom#ping 10.6.160.1
Type CTRL+C to abort.
Sending 5, 72-byte ICMP Echos to 10.6.160.1 , timeout is 1 seconds:
!!!!!!
Success rate is 100 percent(5/5)
round-trip (ms) min/avg/max = 0/3/16
```

Show MG registration status.

```
Raisecom#config
Raisecom(config)#epon-onu 3/1/1 voice
Raisecom(config-epon-onu-voice-3/1:1)#show epon-onu 1/1/1 voice h248 mg
ONU ID: 1/1/1
  Transport Port   : 2944
  Encode Mode     : text
  Register Mode    : IP
  Name            : raisecom
  Long Timer      : 20s
  Short Timer     : 5s
  Start Timer     : 10s
  State           : registered
  Maximum waiting delay: 180s
```

Show POTS interface registration status.

```
Raisecom(config-epon-onu-voice-3/1:1)#show epon-onu 3/1/1 voice h248 pots
Pots ID  TID Name          Status
-----
3/1/1/1  EPON001                inservice
3/1/1/2  EPON002                inservice
```

Service verification: telephones under the ONU can communicate with each other if the H.248 registration is successful after configurations.

- The calling party picks up the phone and hears the dial tone.
- When the calling party dials the phone number (for the phone number, refer to the MGC configuration) of the called party, the phone of the called party rings and the calling party hears the ringback tone.
- The calling party communicates with the called party normally.
- The calling party hears the busy tone if the called party hangs up.

6.3 Configuring VoIP

6.3.1 Preparing for configurations

Scenario

Before enabling the voice service, you need to configure the VoIP signalling protocol (SIP or H.248 protocol) and choose the transmission mode of voice signalling, thus realizing the voice call.

Prerequisite

N/A

6.3.2 Default configurations

Default configurations of VoIP and network parameters on the ONU are as below.

Function	Default value
VoIP protocol type	H.248
IP address of ONU voice service	• IP address: 0.0.0.0 • Mask: 0.0.0.0
Default route of ONU voice service	0.0.0.0
DHCP Client feature of ONU voice service	disable
DHCP Client host name of ONU voice service	RaisecomFTTX
DHCP Client classification identifier of ONU voice service	RaisecomFTTX
DHCP Client Client-ID of ONU voice service	null
VLAN mode of ONU voice service	transparent
Signalling traffic and media traffic VLAN of ONU voice service	0
Signalling traffic and media traffic CoS of ONU voice service	6
QoS trust mode of ONU voice service	none
QoS trusted DSCP value of ONU voice service	0
QoS trusted ToS value of ONU voice service	0
QoS trusted default priority of ONU voice service	0

6.3.3 Configuring VoIP protocol type

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 2/3/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*//*:*)# voip-protocol { sip h248 } example: Raisecom(config-epon-onu-voice-3/1:1)# voip-protocol sip	Configure the VoIP protocol type. • sip: SIP • h248: H.248



Note

- After choosing different VoIP protocol types, you need to save configurations, and then use the **reboot** or **reload** command to re-load the ONU configuration file to make the configuration take effect. Based on the chosen VoIP protocol, you can perform the protocol configuration and service configuration and so on.
- After you save configurations by using the **write** command, you need to wait 10s and then use the **reboot** command to reboot the ONU since it takes time for the OLT to distribute configurations to the ONU. Otherwise, the OLT may fail to distribute configurations to the ONU.

6.3.4 Configuring VoIP network parameters

For the IP address of the ONU voice service, you can manually configure a static IP address or enable DHCP Client to obtain a dynamic IP address.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 2/3/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*//*:*)# ip address ip-address [mask] example: Raisecom(config-epon-onu-voice-3/1:1)#ip address 10.0.0.1 255.0.0.0	Configure the IP address and mask for the voice service. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • mask: subnet mask, in dotted decimal notation, such as 255.0.0.0

Step	Command	Description
4	<pre>Raisecom(config-epon-onu-voice-*//*:*)#ip route default ip-address example: Raisecom(config-epon-onu-voice-3/1:1)#ip route default 192.168.1.100</pre>	Configure the default route for the voice service. You can use the no ip route default command to restore default configurations. ip-address: media default route, in dotted decimal notation, such as 10.10.10.1
5	<pre>Raisecom(config-epon-onu-voice-*//*:*)#ip dhcp client</pre>	(Optional) enable DHCP Client of voice service. You can use the no ip dhcp client command to disable this function.
6	<pre>Raisecom(config-epon-onu-voice-*//*:*)#ip dhcp client hostname string example: Raisecom(config-epon-onu-voice-3/1:1)#ip dhcp client hostname raisecom</pre>	(Optional) configure the DHCP Client host name of voice service. You can use the no ip dhcp client hostname command to restore default configurations. string: host name, a string of 1 to 32 characters
7	<pre>Raisecom(config-epon-onu-voice-*//*:*)#vlan mode { transparent tagged stacking } example: Raisecom(config-epon-onu-voice-3/1:1)#vlan mode tagged</pre>	Configure the VLAN mode of voice services. - transparent: transparent transmission mode - tagged: Tag mode - stacking: double Tag mode
8	<pre>Raisecom(config-epon-onu-voice-*//*:*)#ip dhcp client class-id class-id example: Raisecom(config-epon-onu-voice-3/1:1)#ip dhcp client class-id raisecom</pre>	(Optional) configure the ClassID of voice service DHCP Client. You can use the no ip dhcp client class-id command to restore default configurations. class-id: CLASS ID, a string of 1 to 32 characters
9	<pre>Raisecom(config-epon-onu-voice-*//*:*)#ip dhcp client client-id client-id example: Raisecom(config-epon-onu-voice-3/1:1)#ip dhcp client client-id raisecom</pre>	(Optional) configure the ClientID of voice service DHCP Client. You can use the no ip dhcp client client-id command to restore default configurations. client-id: Client-ID, a string of 1 to 32 characters

Step	Command	Description
10	<pre>Raisecom(config-epon-onu-voice-*//*:*)#vlan vlan-id [cos cos-value] example: Raisecom(config-epon-onu-voice-3/1:1)#vlan 30 cos 7</pre>	Configure the VLAN ID and CoS priority of the ONU voice signaling traffic. You can use the no vlan command to restore default configurations.  Note Voice services are sensitive to time delay. We recommend configuring the voice service with higher priority to ensure that voice packets are preferentially scheduled. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • cos cos-value: CoS value. The cos-value is an integer ranging from 0 to 7.
11	<pre>Raisecom(config-epon-onu-voice-*//*:*)#ip qos trust { dscp priority tos none } example: Raisecom(config-epon-onu-voice-3/1:1)#ip qos trust priority</pre>	Configure QoS trust mode of voice services. • dscp: the QoS trusting policy is trusting DSCP. • priority: the QoS trusting policy is trusting priority. • tos: the QoS trusting policy is trusting ToS. • none: disable QoS.
12	<pre>Raisecom(config-epon-onu-voice-*//*:*)#ip qos default-dscp dscp-value example: Raisecom(config-epon-onu-voice-3/1:1)#ip qos default-dscp 30</pre>	configure the value of DSCP trusted by voice QoS. • default-dscp dscp: DSCP default value. The dscp is an integer ranging from 0 to 63.
13	<pre>Raisecom(config-epon-onu-voice-*//*:*)#ip qos default-priority priority-value example: Raisecom(config-epon-onu-voice-3/1:1)#ip qos default-priority 2</pre>	Configure the QoS trusted IP precedence of voice services. • default-priority priority: default priority. The priority is an integer ranging from 0 to 7.
14	<pre>Raisecom(config-epon-onu-voice-*//*:*)#ip qos default-tos tos-value example: Raisecom(config-epon-onu-voice-*//*:*)#ip qos default-tos 200</pre>	Configure the QoS trusted ToS of voice services. • default-tos tos: ToS default value. The tos is an integer ranging from 0 to 255.

Step	Command	Description
15	<pre>Raisecom(config-epon-onu-voice-*//*:*)#pppoe mode { auto chap pap } example: Raisecom(config-epon-onu-voice-3/1:1)#pppoe mode chap</pre>	Configure the PPPoE mode of voice services. You can use the no pppoe mode command to restore default configurations. • auto: AUTO mode • chap: CHAP mode pap: PAP mode
16	<pre>Raisecom(config-epon-onu-voice-*//*:*)#pppoe username username example: Raisecom(config-epon-onu-voice-3/1:1)#pppoe username pppoename</pre>	Configure the PPPoE user name of voice services. You can use the no pppoe username command to restore default configurations. name: PPPoE user name, a string of 1 to 12 characters
17	<pre>Raisecom(config-epon-onu-voice-*//*:*)#pppoe password password example: Raisecom(config-epon-onu-voice-3/1:1)#pppoe password pppoepsw</pre>	Configure PPPoE password of the voice service. You can use the no pppoe password command to restore default configurations. • password: PPPoE user password, a string of 1 to 12 characters
18	<pre>Raisecom(config-epon-onu-voice-*//*:*)#voip register</pre>	(Optional) configure the ONU to re-register to the soft switch system.
19	<pre>Raisecom(config-epon-onu-voice-*//*:*)#voip deregister</pre>	(Optional) configure the ONU to deregister to the soft switch system.
20	<pre>Raisecom(config-epon-onu-voice-*//*:*)#voip reset</pre>	(Optional) reset the IAD module in the ONU.

6.3.5 Configuring network parameters of media traffic

By default, signalling and media traffic of the voice service use the same network parameters, such as VLAN and IP address. However, in actual network topologies, you need to configure VLANs for the signalling and media traffic of voice services.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice</pre>	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface

Step	Command	Description
3	<pre>Raisecom(config-epon-onu-voice-*/*:*)#media vlan <i>vlan-id</i> [cos <i>cos-value</i>]</pre> example: <pre>Raisecom(config-epon-onu-voice-3/1:1)#media vlan 1</pre>	Configure the VLAN ID and CoS priority of the voice service media traffic. You can use the no media vlan command to restore default configurations.  Note - Media traffic VLAN is inconsistent with the signalling traffic VLAN. - When configuring network parameters of media traffic, you need to configure the VLAN before configuring the IP address. - vlan-id: VLAN ID, an integer, ranging from 1 to 4094 - cos cos-value: CoS value, an integer, ranging from 0 to 7
4	<pre>Raisecom(config-epon-onu-voice-*/*:*)#media ip address <i>ip-address</i> [<i>mask</i>]</pre> example: <pre>Raisecom(config-epon-onu-voice-3/1:1)#media ip address 192.168.1.1 255.255.255.0</pre>	Configure the IP address and mask of the voice service media traffic. You can use the no media ip address command to restore default configurations. - ip-address: media IP address, in dotted decimal notation, such as 10.10.10.1 - mask: media IP address mask, in dotted decimal notation, such as 255.0.0.0
5	<pre>Raisecom(config-epon-onu-voice-*/*:*)#media ip route default <i>ip-address</i></pre> example: <pre>Raisecom(config-epon-onu-voice-3/1:1)#media ip route default 192.168.1.100</pre>	Configure the default route of the voice service media traffic. You can use the no media ip route default command to restore default configurations. ip-address: media default route, in dotted decimal notation, such as 10.10.10.1
6	<pre>Raisecom(config-epon-onu-voice-*/*:*)#media ip qos trust { dscp priority tos none}</pre> example: <pre>Raisecom(config-epon-onu-voice-3/1:1)#media ip qos trust priority</pre>	Configure the QoS trust mode of the voice service media traffic. - dscp: the QoS trusting policy is trusting DSCP. - priority: the QoS trusting policy is trusting priority. - tosQoS: the trusting policy is trusting ToS. - none: disable QoS.

Step	Command	Description
7	Raisecom(config-epon-onu-voice-*//*:*)# media ip qos default-dscp <i>dscp-value</i> example: Raisecom(config-epon-onu-voice-3/1:1)#media ip qos default-priority 5	Configure the QoS trusted DSCP value of the voice service media traffic. default-dscp dscp: DSCP default value. The dscp is an integer ranging from 0 to 63.
8	Raisecom(config-epon-onu-voice-*//*:*)# media ip qos default-priority <i>priority-value</i> example: Raisecom(config-epon-onu-voice-3/1:1)#media ip qos default-priority 6	Configure the QoS trusted IP precedence of the voice service media traffic. default-priority priority: default priority. The priority is an integer ranging from 0 to 7.
9	Raisecom(config-epon-onu-voice-*//*:*)# media ip qos default-tos <i>tos-value</i> example: Raisecom(config-epon-onu-voice-3/1:1)#media ip qos default-tos 200	Configure the QoS trusted ToS priority of the voice service media traffic. default-tos tos: ToS default value. The tos is an integer ranging from 0 to 255.

6.3.6 Configuring call process tone parameters

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# epon-onu <i>slot-id/olt-id/onu-id</i> voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter voice service configuration mode of the EPON ONU. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*//*:*)# call-progress-tone { busy congestion dial ringback waiting } { high-frequency low-frequency } <i>frequency</i> example: Raisecom(config-epon-onu-voice-3/1:1)#call-progress-tone dial low-frequency 400	Configure the low frequency and high frequency of ONU call process tone. - dial: dial tone - ringback: ring back tone - busy: busy tone - congestion: congestion tone - waiting: call waiting tone - low-frequency frequency: low frequency. Frequency is an integer ranging from 0 to 65535, in units of Hz. - high-frequency frequency: high frequency. Frequency is an integer ranging from 0 to 65535, in units of Hz.

Step	Command	Description
4	<pre>Raisecom(config-epon-onu-voice-*//*:*)#call- progress-tone { busy congestion dial ringback waiting } { high-frequency low- frequency } volume <i>volume</i></pre> example: <pre>Raisecom(config-epon-onu-voice-3/1:1)#call- progress-tone dial low-frequency volume 50</pre>	Configure the low-frequency volume gain and high-frequency volume gain of ONU call process tone. • dial: dial tone • ringback: ring back tone • busy: busy tone • congestion: congestion tone • waiting: call waiting tone • low-frequency: low frequency • high-frequency: high frequency • volume: volume, an integer, ranging from 0 to 100, in units of dB
5	<pre>Raisecom(config-epon-onu-voice-*//*:*)#call- progress-tone { busy congestion dial ringback waiting } { first-signal second- signal } on-time <i>value</i> off-time <i>value</i></pre> example: <pre>Raisecom(config-epon-onu-voice-3/1:1)#call- progress-tone dial first-signal on-time 300 off- time 500</pre>	Configure the start time and end time of the first ring and second ring of ONU call process tone. • dial: dial tone • ringback: ringback tone • busy: busy tone • congestion: congestion tone • waiting: call waiting tone • first-signal: first ring • second-signal: second ring • on-time: start time of the ring, an integer, ranging from 0 to 65535, in units of millisecond • off-time: end time of the ring, an integer, ranging from 0 to 65535, in units of millisecond



Note

After parameters of the call process tone are modified, only when you save them and restart the ONU can they take effect.

6.3.7 Checking configurations

Step	Command	Description
1	<pre>Raisecom#show epon-onu slot-id/olt- id/onu-id voice voip-protocol</pre>	Show ONU VoIP protocol type.
2	<pre>Raisecom#show epon-onu slot-id/olt- id/onu-id voice ip</pre>	Show configurations of ONU VoIP network parameters.
3	<pre>Raisecom#show epon-onu slot-id/olt- id/onu-id voice ip dhcp client</pre>	Show configurations of DHCP Client for the ONU voice service.
4	<pre>Raisecom#show epon-onu slot-id/olt- id/onu-id voice media ip</pre>	Show configurations of network parameters for ONU voice service media traffic.

Step	Command	Description
5	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice pppoe</code>	Show PPPoE configurations of ONU voice services.
6	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice statistics error-code</code>	Show statistics of ONU VoIP error codes.
7	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice statistics sdp</code>	Show ONU VoIP SDP statistics.
8	<code>Raisecom# show epon-onu slot-id/olt-id/onu-list voice call-progress-tone [busy congestion dial ringback waiting] information</code>	Show configurations of ONU call process tones.
9	<code>Raisecom#show epon-onu slot-id/olt-id/onu-list voice dtmf</code>	Show configurations of ONU second dialing.

6.4 Configuring POTS interface

6.4.1 Preparing for configurations

Scenario

POTS interfaces are used for voice call. When using the SIP to transmit VoIP signalling, you need to configure the phone number of the POTS interface. When you connect to the POTS interface, you will obtain the phone number, through which you can dial up and realize voice call.

Prerequisite

You need to plan the phone number by yourself. The phone number of the POTS interface should be unique across the whole network. Since the ONU cannot detect whether the phone number of its POTS interface conflicts with that of the POTS interface on other ONUs, uniqueness of the POTS interface phone number should be ensured when configured.

6.4.2 Default configurations

Default configurations of the POTS interface on the ONU are as below.

Function	Default value
Phone number of ONU POTS interface	N/A
User name of ONU POTS interface	pots-uni-line No.
Packet encapsulation mode of ONU POTS interface	BellCore
Management status of ONU POTS interface	Enable

Function	Default value
Echo cancellation feature of ONU POTS interface	Enable
Silence compression feature of ONU POTS interface	Disable
Comfort noise feature of ONU POTS interface	Enable
Preferred coding/decoding type of ONU line	G.711A

6.4.3 Configuring POTS interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 2/3/1 voice	Enter EPON ONU voice service configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*/*:*)#pots phone-number number pots-id example: Raisecom(config-epon-onu-voice-3/1:1)#pots phone-number 1234567 1	Configure the phone number of the ONU POTS interface, which can be digits from 0 to 9 in the length of no more than 16 digits.  Note You can use the no pots phone-number command to delete configurations.  Note When you configure the SIP, the phone number is a required item; when you configure the H.248 protocol, the phone number is an optional one. - number: phone number, a string of 1 to 32 characters. The character contents comply with the E.164 standard. - pots-id: POTS interface ID, an integer, ranging from 1 to 24
4	Raisecom(config-epon-onu-voice-*/*:*)#pots name string pots-id example: Raisecom(config-epon-onu-voice-3/1:1)#pots name raisecom 1	(Optional) configure user names of the POTS interfaces for distinguishing interfaces. You can use the no pots name command to restore default configurations. - name: user name, a character string - pots-id: POTS interface ID, an integer, ranging from 1 to 24

Step	Command	Description
5	<pre>Raisecom(config-epon-onu-voice- /*:*)#pots { enable disable } pots-list example: Raisecom(config-epon-onu-voice- 3/1:1)#pots enable 1,2</pre>	Enable/Disable the POTS interface.  Note When the POTS interface is disabled, the current communication will be interrupted. At this time, the interface cannot initiate a call or receive a new call. • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • enable: enable ONU POTS. • disable: disable ONU POTS.
6	<pre>Raisecom(config-epon-onu-voice- /*:*)#pots echo-cancellation { enable disable } pots-list example: Raisecom(config-epon-onu-voice- 3/1:1)#pots echo-cancellation enable 1</pre>	Enable/Disable the echo cancellation feature of the POTS interface. • pots-list: POTS interface list, an integer, ranging from 1 to 24 • enable: enable echo cancellation on the ONU POTS interface. • disable: disable echo cancellation on the ONU POTS interface.
7	<pre>Raisecom(config-epon-onu-voice- /*:*)#pots silence-compression { enable disable } pots-list example: Raisecom(config-epon-onu-voice- 3/1:1)#pots silence-compression enable 1</pre>	Enable/Disable the silence compression feature of the POTS interface. • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • enable: enable silence compression on the ONU POTS interface. • disable: disable silence compression on the ONU POTS interface.
8	<pre>Raisecom(config-epon-onu-voice- /*:*)#pots cng { enable disable } pots-list example: Raisecom(config-epon-onu-voice- 3/1:1)#pots cng enable 1</pre>	Enable/Disable the comfort noise generation feature of the POTS interface. • enable: enable comfort noise generation on the ONU POTS interface. • disable: disable comfort noise generation on the ONU POTS interface. • pots-list: POTS interface list, an integer, ranging from 1 to 24
9	<pre>Raisecom(config-epon-onu-voice- /*:*)#pots prefer-codec { g711a g729 g711u g723 g726 } pots- list example: Raisecom(config-epon-onu-voice- 3/1:1)#pots prefer-codec g729 1</pre>	Configure the preferred coding/decoding type of the ONU line. You can use the no pots prefer-codec command to restore default configurations. • g711a: G711A • g729: G729 • g711u: G711U • g723: G723 • g726: G726 • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

Step	Command	Description
10	<pre>Raisecom(config-epon-onu-voice- */*:*)#pots caller-id mode { bellcore / etsi / ntt } pots-list example: Raisecom(config-epon-onu-voice- 3/1:1)#pots caller-id mode bellcore 1</pre>	(Optional) configure the encapsulation mode of CID packets for ONU call services. • bellcore: bellcore • etsi: European code • ntt: Japanese code • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
11	<pre>Raisecom(config-epon-onu-voice- */*:*)#pots circuit-test pots-id example: Raisecom(config-epon-onu-voice- 3/1:1)#pots circuit-test 1</pre>	(Optional) configure performing circuit test on the POTS interface. • pots-id: POTS interface ID, an integer, ranging from 1 to 24
12	<pre>Raisecom(config-epon-onu-voice- */*:*)#pots loop-line-test pots-id example: Raisecom(config-epon-onu-voice- 3/1:1)#pots loop-line-test 1</pre>	(Optional) configure performing loop test on the POTS interface. • pots-id: POTS interface ID, an integer, ranging from 1 to 24

6.4.4 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice pots [pots-id]</pre>	Show the management status of the ONU POTS interface.
2	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice statistics call pots [pots-id]</pre>	Show call statistics of the ONU POTS interface.
3	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-list voice pots [pots-id] service</pre>	Show feature information about the ONU POTS interface.
4	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-list voice pots [pots-id] session</pre>	Show the session status of the ONU POTS interface.

6.5 Configuring SIP

6.5.1 Preparing for configurations

Scenario

When VoIP uses SIP as the signalling transmission protocol, you can realize ONU SIP voice services through configurations, and configure multiple service features, such as Caller Identification (CID), call waiting, and three-way calling.

SIP is one of the VoIP signalling protocols, proposed by IETF. It is used to create, modify, or terminate interactive user sessions containing multimedia elements, such as video, voice, and instant communication. It pushes services and control information to the terminal to achieve terminal intellectualization.

Prerequisite

N/A

6.5.2 Default configurations

Default configurations of the SIP on the ONU are as below.

Function	Default value
Monitor port of SIP	5060
TCP transmission function	Disable
IP address of primary/secondary SIP Proxy server registered by ONU	0.0.0.0
Monitor port of primary/secondary SIP Proxy server registered by ONU	5060
Transmission protocol type of primary/secondary SIP Proxy server registered by ONU	UDP
IP address of primary/secondary SIP Register server registered by ONU	0.0.0.0
Monitor port of primary/secondary SIP Register server registered by ONU	5060
Transmission protocol type of primary/secondary SIP Register server registered by ONU	UDP
Refresh interval for the ONU to send registration packets to the SIP Register server	3600 seconds
SIP primary/secondary proxy swap	Enable
IP address of Outbound Proxy server registered by ONU	0.0.0.0
UDP port ID of Outbound Proxy server registered by ONU	5060
Heartbeat cycle of ONU SIP	60 seconds
Heartbeat timeout times of ONU SIP	3
Detection mode of ONU SIP	send-option
Heartbeat switch of ONU SIP	off
CID of ONU POTS	Enable
Encapsulation mode of CID packets on the ONU POTS interface	BELLCORE
Echo cancellation status on the ONU POTS interface	Enable

Function	Default value
Silence compression status on the ONU POTS interface	Disable
Comfort noise generation status on the ONU POTS interface	Enable
Call waiting service	Disable
Three-way calling	Disable
SIP Modem transparent transmission service	Enable
Polarity reversal service	Enable
Hotline service	Disable
SIP numbers matching rules	min
Voice protocol type of the ONU SIP server	

6.5.3 Configuring SIP transmission protocol

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*/*:*)#sip transport { udp tcp } port port-id example: Raisecom(config-epon-onu-voice-3/1:1)#sip transport udp port 5600	Configure the monitor port of ONU SIP. You can use the no sip transport { udp tcp } port command to restore default configurations. - udp: UDP - tcp: TCP - port-id: interface ID, an integer, ranging from 1 to 65535
4	Raisecom(config-epon-onu-voice-*/*:*)#sip transport tcp { enable disable }	Enable/Disable TCP transmission.



Note

Pay attention to the following matters when configuring parameters, such as SIP monitor protocol and monitor port:

- Keep consistent with the peer Proxy/Register server, and do not modify randomly.
- By default, use the UDP protocol. The interface ID is 5060, which does not need to be modified in practice.
- RTP/RTCP media traffic of the ONU adopts the UDP with the interface ID starting from 60000. The configured SIP monitor port should not conflict with each other; otherwise, SIP cannot work properly.

6.5.4 Configuring SIP Proxy/Register server

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*//*:*)#sip { primary secondary } proxy-server ip ip-address [{ udp tcp } port port-number] example: Raisecom(config-epon-onu-voice-3/1:1)#sip primary proxy-server ip 10.0.0.1 udp port 5600	Configure the IP address and monitor port of the primary/secondary SIP Proxy server. You can use the no sip { primary secondary } proxy-server ip command to restore default configurations. • primary: primary server • secondary: backup server • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • udp: UDP • tcp: TCP • port port-id: interface ID • port-id: an integer, ranging from 0 to 65535
4	Raisecom(config-epon-onu-voice-*//*:*)#sip { primary secondary } proxy-server transport { udp tcp } example: Raisecom(config-epon-onu-voice-3/1:1)#sip primary proxy-server transport tcp	Configure the transmission protocol type of the primary/secondary SIP Proxy server. You can use the no sip { primary secondary } proxy-server transport command to restore default configurations. • primary: primary Proxy server • secondary: backup Proxy server • udp: UDP • tcp: TCP
5	Raisecom(config-epon-onu-voice-*//*:*)#sip { primary secondary } register-server ip ip-address [{ udp tcp } port port-number] example: Raisecom(config-epon-onu-voice-3/1:1)#sip primary register-server ip 10.0.0.1 udp port 5600	Configure the IP address and monitor port of the primary/secondary SIP Register server. You can use the no sip { primary secondary } register-server ip command to restore default configurations. • primary: primary server • secondary: backup server • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • udp: UDP • tcp: TCP • port port-id: monitor interface ID, an integer, ranging from 0 to 65535

Step	Command	Description
6	<pre>Raisecom(config-epon-onu-voice-*//*:*)#sip { primary secondary } register-server transport { udp tcp } example: Raisecom(config-epon-onu-voice-3/1:1)#sip primary register-server transport tcp</pre>	Configure the transmission protocol type of the primary/secondary SIP Register server. You can use the sip { primary secondary } register-server transport command to restore default configurations. • primary: primary register server • secondary: backup register server • udp: UDP • tcp: TCP
7	<pre>Raisecom(config-epon-onu-voice-*//*:*)#sip proxy-swap { enable disable }</pre>	Enable/Disable SIP primary/secondary proxy swap.
8	<pre>Raisecom(config-epon-onu-voice-*//*:*)#sip register fresh-period period example: Raisecom(config-epon-onu-voice-3/1:1)#sip regiser fresh-period 120</pre>	Configure the refresh interval for the ONU to send registration packets to the SIP Register server. You can use the no sip register fresh-period command to restore default configurations. • time: interval, an integer, ranging from 60 to 65535, in units of second
9	<pre>Raisecom(config-epon-onu-voice-*//*:*)#sip realm string example: Raisecom(config-epon-onu-voice-3/1:1)#sip regiser fresh-period 120</pre>	Configure the SIP domain name. You can use the no sip realm command to restore default configurations. time: interval, an integer, a string of 60 to 65535 characters, in units of second
10	<pre>Raisecom(config-epon-onu-voice-*//*:*)#sip outbound proxy-server ip ip-address [udp port port-number] example: Raisecom(config-epon-onu-voice-3/1:1)#sip outbound proxy-server ip 10.10.10.2 udp port 5061</pre>	Configure the IP address and monitor port of the Outbound Proxy server. You can use the no sip outbound proxy-server ip command to restore default configurations. • ip-address: IP address of the Outbound Proxy server, in dotted decimal notation, such as 10.10.10.1 • udp port port-id: UDP monitor port of the Outbound Proxy server. The port-id refers to the interface ID, which is an integer ranging from 1 to 65535.
11	<pre>Raisecom(config-epon-onu-voice-*//*:*)#sip uri [phonenumber username] example: Raisecom(config-epon-onu-voice-3/1:1)#sip uri username</pre>	Configure the information type of URI in the FROM header when performing SIP registration or calling. You can use the no sip uri command to restore default configurations. • phonenumber: phone number • username: user name



Note

- We recommend you to configure the refresh interval of registration packets to more than 300s to prevent multiple POTS users on multiple ONUs from frequently sending SIP Register packets to the SIP Register server, which causes great burden on the SIP Register server.
- If the SIP Proxy/Register server adopts TCP, the device should adopt TCP.

6.5.5 Registering and re-registering phone users

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*/*:*)#sip pots { register deregister } pots-list example: Raisecom(config-epon-onu-voice-3/1:1)#sip pots register 1	Deregister a user or initiate a new registration.  Note Both operations are mainly used for testing. You can use the deregister command to delete registration information about a telephone user on the Register server; you can use the register command to make the telephone user to initiate a new registration. • register: register • deregister: deregister • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

6.5.6 Configuring SIP heartbeat

To detect whether the ONU is connected with the SIP Proxy/Register server properly, the server sends SIP message to the ONU regularly or the ONU sends message to server regularly. The information is called "heartbeat message".

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface

Step	Command	Description
3	Raisecom(config-epon-onu-voice-*/*:*)# sip heartbeat cycle <i>period</i> example: Raisecom(config-epon-onu-voice-3/1:1)#sip heartbeat cycle 100	(Optional) configure the heartbeat cycle of ONU SIP. You can use the no sip heartbeat cycle command to restore default configurations. • time: heartbeat cycle, an integer, ranging from 10 to 43200, in units of second
4	Raisecom(config-epon-onu-voice-*/*:*)# sip heartbeat timeout count <i>number</i> example: Raisecom(config-epon-onu-voice-3/1:1)#sip heartbeat timeout count 10	(Optional) configure the heartbeat timeout counts of ONU SIP. You can use the no sip heartbeat timeout command to restore default configurations. • number: heartbeat timeout counts, an integer, ranging from 1 to 100
5	Raisecom(config-epon-onu-voice-*/*:*)# sip heartbeat mode { send-option receive-option send-info receive-info } example: Raisecom(config-epon-onu-voice-3/1:1)#sip heartbeat mode receive-option	(Optional) configure the heartbeat mode of ONU SIP. You can use the no sip heartbeat mode command to restore default configurations. • send-option: sending Option mode • receive-option: receiving Option mode • send-info: sending Information mode • receive-info: receiving Information mode
6	Raisecom(config-epon-onu-voice-*/*:*)# sip heartbeat { on off } example: Raisecom(config-epon-onu-voice-3/1:1)#sip heartbeat on	(Optional) enable/disable ONU SIP heartbeat. • on: enable ONU SIP heartbeat. • off: disable ONU SIP heartbeat.



Note

- We recommend configuring the heartbeat cycle more than 60s; otherwise, it will affect the performance of the ONU and server.
- The heartbeat mode and cycle should cooperate with the server. If the server does not support heartbeat, you need to disable the heartbeat feature of the ONU.

6.5.7 Configuring SIP user authentication

To avoid illegal user access, the SIP Proxy/Register server or SIP peer device should be authenticated before accessing the network. The ONU supports two registration modes: authentication based on user name and authentication based on user name+password.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface

Step	Command	Description
3	<pre>Raisecom(config-epon-onu-voice- /*:*)#sip pots authentication name [password password] pots-list example: Raisecom(config-epon-onu-voice- 3/1:1)#sip pots authentication user password raisecom 1</pre>	Configure authentication information about POTS users. You can use the no sip pots authentication { all pots-list } command to delete the configuration. • name: user name, a string of 1 to 32 characters • password password: password, a string of 1 to 16 characters • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

6.5.8 Configuring SIP DigitMap

CID refers to displaying the number of the caller when the phone of the called party rings.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu slot- id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 2/3/1 voice</pre>	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-epon-onu-voice- /*:*)#sip digitmap string example: Raisecom(config-epon-onu-voice- 3/1:1)#sip digitmap map</pre>	Configure SIP DigitMap. • name: digitmap name, a character string, ranging from 1 to 200, in units of byte

6.5.9 Configuring CID services

Caller ID services refer to that the calling party number is displayed during the ringing process of the called party user.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu slot- id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice</pre>	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-epon-onu-voice- /*:*)#sip pots caller-id { enable disable } pots-list example: Raisecom(config-epon-onu-voice- 3/1:1)#sip pots caller-id enable 1</pre>	Enable/Disable CID services. • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • Enable: enable ONU CID services. • Disable: disable OUN CID services.

6.5.10 Configuring call waiting services

If a calling party places a call to a called party which is otherwise engaged, and the called party has the call waiting feature enabled, the called party is able to make the new calling party to wait until the original communication ends.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*/*:*)#sip pots call-wait { enable disable } pots-list example: Raisecom(config-epon-onu-voice-3/1:1)#sip pots caller-wait enable 1	Enable/Disable call waiting services. • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • Enable: enable ONU call waiting services. • Disable: disable OUN call waiting services.



Note

If it is a soft switch in the central office and you need to configure the call waiting service, you should enable call waiting on the soft switch in advance.

6.5.11 Configuring three-way calling services

Three-way calling, also known as Multi-Party telecommunication (MPTY) or teleconference, is a new service based on the call waiting and holding. Simply, it means that you can have a conversation with two people simultaneously. When you are communicating with someone, you can make a new phone call without hanging up the original one, or answer the call from a third party. In this case, it avoids the inconvenience that the third party cannot be put through when the called party is communicating with others.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface

Step	Command	Description
3	<pre>Raisecom(config-epon-onu-voice- */*:*)#sip pots 3-way-conference { enable disable } pots-list example: Raisecom(config-epon-onu-voice- 3/1:1)#sip pots 3-way-conference enable 1</pre>	Enable/Disable three-way calling. • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • Enable: enable three-way calling services on the ONU. • Disable: disable three-way calling services on the ONU.



Note

If it is a soft switch in the central office and you need to configure the three-way calling service, you should enable three-way calling on the soft switch in advance.

6.5.12 Configuring Modem transparent transmission services

Modem transparent transmission refers that traditional Modem data services are transmitted through the IP network.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu slot- id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice</pre>	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-epon-onu-voice- */*:*)#sip modem { enable disable }</pre>	Enable/Disable SIP Modem.  Note When Modem transparent transmission is enabled, traditional Modem data services can be transmitted through the IP network.
4	<pre>Raisecom(config-epon-onu-voice- */*:*)#modem transparent redundancy value example: Raisecom(config-epon-onu-voice- 3/1:1)#modem transparent redundancy 4</pre>	(Optional) configure the redundancy for the ONU to transparently transmit Modem services. You can use the no modem transparent redundancy command to restore default configurations. • value: redundancy, an integer, ranging from 0 to 7

6.5.13 Configuring polarity reversal service

Polarity reversal refers to the polarity (the positive and negative terminals of the telephone A/B wire) is reversed. Polarity reversal is configured under the following two conditions:

- Pickup for communication

- Hangup when communication ends

Polarity reversal will generate a pulse to enable the telephone meter to record the start time and end time of the calling for charging fees. This function is mainly used for public telephones.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*/*:*)#sip pots polarity-reverse { enable disable } pots-list example: Raisecom(config-epon-onu-voice-3/1:1)#sip pots polarity-reverse enable 1	Enable/Disable polarity reversal services. • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • Enable: enable polarity reversal services on the ONU POTS interface. • Disable: disable polarity reversal services on the ONU POTS interface.

6.5.14 Configuring hotline service

Hotline service is a service for which the calling party and called party share the call charges. The called party has a nationally unique phone number. A call to this phone number will be automatically directed to the preset destination (a phone number or call center). Call charges of the hotline service are shared by the calling and called parties. The calling party pays the city charges and the called party pays the charges for answering incoming calls.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*/*:*)#sip pots hot-line { disable instant delay } pots-list example: Raisecom(config-epon-onu-voice-3/1:1)#sip pots hot-line instant 1	Configure hotline services on the POTS interface. You can use the no sip pots hot-line { all pots-list } command to restore default configurations. • disable: disable hotline. • instant: instant hotline • delay: delay hotline. • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

Step	Command	Description
4	<pre>Raisecom(config-epon-onu-voice- /*:*)#sip pots hot-line phone- number number pots-id example: Raisecom(config-epon-onu-voice- 3/1:1)#sip pots hot-line phone- number 12345678 1</pre>	Configure the hotline number on the POTS interface. You can use the no sip pots hot-line phone-number { all pots-list } command to restore default configurations. • number: phone number character string • pots-id: POTS interface ID, an integer, ranging from 1 to 24

6.5.15 Configuring mapping rule of SIP phone numbers

Mapping rule of SIP phone numbers refers how to map the phone number of the called party to the corresponding SIP URI format of "sip:user@host IP", namely, map the phone number of the called party to the IP address of the SIP voice device. Through this IP address, the peer device can be connected and the called party can be contacted.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu slot- id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice</pre>	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-epon-onu-voice- /*:*)#digitmap match-mode { min max } example: Raisecom(config-epon-onu-voice- 3/1:1)#digitmap match-mode max</pre>	Configure the matching mode of the digitmap. You can use the no digitmap match-mode command to restore default configurations. • Min: minimum matching mode. If the current receiving number matches one of the dialling rules, it will be immediately reported and the number receiving ends. • Max: max match mode. If the current receiving number matches one of the dialling rules, but it is also possible to receive more numbers to match other different dialling rules, the number receiving does not end but continues.
4	<pre>Raisecom(config-epon-onu-voice- /*:*)#sip digitmap digitmap example: Raisecom(config-epon-onu-voice- 3/1:1)#sip digitmap map</pre>	Configure the digitmap. You can use the no sip digitmap command to delete the configuration. • name: digitmap name, a string of 1 to 200 bytes



Note

The ONU with the voice function supports adding, deleting, and querying the mapping rule of SIP phone numbers. The mapping rule of SIP phone numbers defines how to map the phone number of the called party to the corresponding SIP URI format of "sip:user@host IP", including the following two parts:

- Receive the phone number: the ONU receives the phone number dialed by the calling party and then initiates the calling process after determines that it is a complete phone number.
- Map the phone number: according to the mapping rule, map the received phone number to the corresponding SIP URI format and then start the call.

The phone number of the called party supports 'x', '.', '#', '*', '[]', '-', and digits from 0 to 9.

- 'x': indicate a digit.
- '.': repeat the previous character 0 time or multiple times.
- '-': indicate a continuous value, such as [2-8], which means supporting any digit in the range of 2 to 8.

Moreover, the phone number supports '#' and '*' for supplementary services.

The mapping rule cannot begin with '.'.

Phone numbers for different mapping rules cannot be identical.

Some configuration examples are as below:

- [2-8]xxxxxxx: a 8-digit local phone number, each digit of which ranges from 2 to 8, such as 50158293
- 13xxxxxxxx: a 11-digit mobile phone number beginning with 13, such as 13810292839
- 0xxxxxxxxxxxx: a 15-digit long-distance phone number beginning with 0, such as 057182882492123
- 9xxxx: a 5-digit special service number beginning with 9, such as 95555
- x#: a phone number ends with '#'
- 1[0124-9]x: a 3-digit phone number with 1 at the beginning and a non-3 digit in the middle, such as 110, 114, and 120
- [0-9*#]: any phone number, including '*' and '#'
- x: any phone number, excluding '*' and '#'

SIP URI supports the IP:PORT format.

- IP should be the IPv4 address of the called party. If it is not configured, the calling is switched to the SIP Proxy (already configured) by default.
- PORT is optional, the value of which is 5060 by default.

6.5.16 Configuring voice protocols of SIP server

The SIP server supports the following voice protocols:

- SIP
- IMS-SIP

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON port ID • onu-id: PON port ONU ID
3	Raisecom(config-epon-onu-voice-*/*:*)#sip-agent voip-protocol { sip ims-sip } example: Raisecom(config-epon-onu-voice-3/1:1)#sip-agent voip-protocol sip	Configure the voice protocol type of the ONU SIP server. You can use the no sip-agent command to restore to the default condition. • sip: SIP • ims-sip: IMS-SIP



Note

After configuring the protocol type, you need to write and then reload. If a Trap prompting "Successfully reloaded!" is received, it indicates that the protocol switching succeeds.

6.5.17 Configuring SIP user parameters

Perform the following configuration on the device that needs to configure the SIP user parameters corresponding to the ONU voice port.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON port ID • onu-id: PON port ONU ID
3	Raisecom(config-epon-onu-voice-*/:*)#sip-user aor user-aor username username password password pots-list example: Raisecom(config-epon-onu-voice-3/1:1)#sip-user aor sip1 username user1 password raisecom 1-3	Configure the voice protocol type of the ONU SIP server. You can use the no sip-agent command to restore to the default condition. • user-aor: user telephone number, a string of 1 to 16 characters • username: user name, a string of 1 to 32 characters • password: password, a string of 1 to 16 characters • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

6.5.18 Checking configurations

No.	Command	Description
1	Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip transport	Show information about the ONU SIP transmission protocol.
2	Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip { primary secondary } proxy-server	Show configurations of the ONU SIP primary/secondary SIP Proxy server.
3	Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip { primary secondary } register-server	Show configurations of the ONU SIP primary/secondary SIP Register server.
4	Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip active proxy-server	Show the type of the currently active/standby ONU SIP server.
5	Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip proxy-swap	Show configurations of ONU SIP proxy swap.
6	Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip realm	Show information about ONU SIP domain names.

No.	Command	Description
7	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip outbound proxy-server</code>	Show configurations of the ONU Outbound Proxy server.
8	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip pot service</code>	Show the SIP service information on the ONU POTS interface.
9	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip heartbeat</code>	Show SIP heartbeat configurations on the ONU POTS interface.
10	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip pots authentication</code>	Show user authentication information on the ONU POTS interface.
11	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice pots service</code>	Show feature information about the ONU POTS interface.
12	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip dial-map-rule</code>	Show information about the ONU SIP phone number mapping rules.
13	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice modem</code>	Show ONU Modem information.
14	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip modem</code>	Show ONU SIP Modem status.
15	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip uri</code>	Show the type of URI in the FROM header when performing SIP registration or calling.
16	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice digitmap</code>	Show matching information about the ONU digitmap.
17	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip digitmap</code>	Show the SIP digitmap.
18	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice statistics call pots [pots-id]</code>	Show calling statistics on the ONU POTS interface.
19	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice statistics sip</code>	Show ONU SIP performance statistics.
20	<code>Raisecom#show epon-onu slot-id/olt-id/onu-list uni pots [pots-id] sip-user</code>	Show SIP user information about the ONU voice port.

6.6 Configuring H.248

6.6.1 Preparing for configurations

Scenario

H.248 is one of VoIP signalling protocols, used between MG and MGC. Through MGC coordination control, the MG users can achieve voice call and communication.

H.248 is one of VoIP signalling protocols supported by the Raisecom ONU. If you use the H.248 as the signalling protocol, you can achieve the voice service through the following configurations.

Prerequisite

N/A

6.6.2 Default configurations

Default configurations of the H.248 protocol are as below.

Function	Default value
Registration mode of MG	ip
Transmission interface ID of MG	2944
Coding type of H.248 protocol signalling	text
IP address of primary/secondary MGC server	0.0.0.0
Transmission interface ID of primary/secondary MGC server	2944
Generation mode of MG TID	line
Prefix of MG TID	null
MG TID	null
Prefix of RTP	rtp/
Digital length of RTP	1
Starting TID of RTP	0
Total amount of RTP resources	2 ×POTS interface quantity
Maximum waiting delay of MG	180s
MG heartbeat duration	60s
MG heartbeat mode	ITO
Timeout times of MG fault judgement	3
H.248 digitmap matching mode	min
Long timer of H.248 digitmap	20s
Short timer of H.248 digitmap	5s
Start timer of H.248 digitmap	10s
MGC type authenticated by H.248 protocol	national
Authentication parameters of H.248 protocol	• g: 2 • p: null • ki: null
MGC initial retransmission timeout	2000ms
MGC minimum retransmission timeout	100ms
MGC maximum retransmission timeout	4000ms

Function	Default value
Deregistration delay of H.248 POTS interface	60s
TID of H.248 POTS interface	null

6.6.3 Configuring H.248 authentication

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*/*:*)#h248 create authentication auth-id type { national hw zte } example: Raisecom(config-epon-onu-voice-3/1:1)#h248 create authentication 2 type national	Add the MGC type in H.248 voice gateway authentication. You can use the no h248 create authentication { auth-id all } to delete the configuration. - auth-id: authentication ID, integer, with the value of 1 or 2 - national: national standard - hw: Huawei - zte: ZTE
4	Raisecom(config-epon-onu-voice-*/*:*)#h248 create authentication auth-id [g g] [p p] [ki ki] [mginfo mg-info] example: Raisecom(config-epon-onu-voice-3/1:1)#h248 create authentication 1 g 3 p 4 ki pwd12345678 mginfo [192.168.10.55]:2944	Add parameter G to H.248 voice gateway authentication parameters. You can use the no h248 create authentication { auth-id all } to delete the configuration. - auth-id: authentication ID, an integer, ranging from 1 or 2 - g g: radix; g is a string of 1 to 4 characters. - p p: modulus; p is a string of 1 to 256 characters. - ki ki: initial secret key ki is a string of 1 to 128 characters. - mginfo mginfo: media gateway identification - mginfo: a string of 1 to 64 characters
5	Raisecom(config-epon-onu-voice-*/*:*)#h248 authentication auth-id type { national hw zte } example: Raisecom(config-epon-onu-voice-3/1:1)#h248 authentication 2 type zte	Modify the MGC type of H.248 voice gateway authentication. - auth-id: authentication ID, an integer, with the value of 1 or 2 - national: national standard - hw: Huawei - zte: ZTE

Step	Command	Description
6	<pre>Raisecom(config-epon-onu-voice- /*:*)#h248 authentication auth-id [g g] [p p] [ki ki] [mginfo mg-info] example: Raisecom(config-epon-onu-voice- 3/1:1)#h248 authentication 1 g 3 p 4 ki pwd12345678 mginfo [192.168.10.55]:2944</pre>	Modify H.248 voice gateway authentication parameters. • auth-id: authentication ID, an integer, with the value of 1 or 2 • g g: radix; g: a string of 1 to 4 characters • p p: modulus; p: a string of 1 to 256 characters • ki ki: initial secret key ki: a string of 1 to 128 characters • mginfo mginfo: media gateway identification • mginfo: a string of 1 to 64 characters



Caution

When the device is connected with the MGC, configure authentication information about the voice gateway if the MGC requires.

6.6.4 Configuring MG

MG is a H.248 media gateway unit. All ONUs with the voice function can be MG objects.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu slot- id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice</pre>	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-epon-onu-voice- /*:*)#h248 mg name name example: Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg name raisecom</pre>	(Optional) configure the MG name. Note If the registration name is domain-name, device-name, or mid, the MG name should be configured. You can refer to the specified name provided by the central office. • name: MG name, a string of 1 to 64 characters

Step	Command	Description
4	<pre>Raisecom(config-epon-onu-voice- /*:*)#h248 mg register-mode { ip domain-name device-name mac mid } example: Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg register-mode domain- name</pre>	(Optional) configure MG registration mode. You can use the no h248 mg register-mode command to restore default configurations.  Note If the central office specifies the MG registration mode, you need to configure this item; otherwise, you do not. • ip: IP address • domain-name: domain name • device-name: device name • mac: MAC address • mid: message identifier
5	<pre>Raisecom(config-epon-onu-voice- /*:*)#h248 mg max-waiting-delay time example: Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg max-waiting-delay 360</pre>	(Optional) configure the maximum delay. You can use the no h248 mg max-waiting-delay command to restore default configurations. • time: maximum delay, an integer, ranging from 0 to 1200, in units of second
6	<pre>Raisecom(config-epon-onu-voice- /*:*)#h248 mg transport port port- number example: Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg transport port 100</pre>	(Optional) configure the transmission interface ID of the MG. You can use the no h248 mg transport port command to restore default configurations. • port: interface ID, an integer, ranging from 1 to 65535
7	<pre>Raisecom(config-epon-onu-voice- /*:*)#h248 mg encode { text compact-text bin } example: Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg encode text</pre>	(Optional) configure the H.248 signaling coding mode. You can use the no h248 mg encode command to restore default configurations. • text: text • compact-text: compact text • bin: binary
8	<pre>Raisecom(config-epon-onu-voice- /*:*)#h248 mg encryption { password password authentication } example: Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg encryption authentication</pre>	(Optional) configure the encryption mode of H.248 MG signaling. • password password: password, a string of 1 to 128 characters • authentication: authentication mode



Note

- Basic parameters of the MG should be consistent with those of the MGC server, and they are not allowed to be modified.
- RTP/RTCP media traffic of the ONU uses the UDP with interface ID starting from 60000. The configured MG transmission interface ID should not conflict with each other; otherwise, the H.248 protocol cannot work properly.
- If the MG name is not configured, perform registration according to "local IP address: interface ID" by default.

6.6.5 Configuring MGC

MGC is a H.248 media gateway control unit. MGC is usually used in softswitch network.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*/*:*)#h248 { primary secondary } mgc ip ip-address [port port-number] example: Raisecom(config-epon-onu-voice-3/1:1)#h248 primary mgc ip 10.0.0.1 port 100	Configure the IP address and transmission interface ID of the primary/secondary MGC server. You can use the no h248 { primary secondary } mgc ip command to restore default configurations. - primary: primary MGC server - secondary: secondary MGC server - ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 - port port-number: interface ID, an integer, ranging from 0 to 65535
4	Raisecom(config-epon-onu-voice-*/*:*)#h248 { primary secondary } mgc name string example: Raisecom(config-epon-onu-voice-3/1:1)#h248 primary mgc name raisecom	(Optional) configure the name of the primary/secondary MGC server. You can use the no h248 { primary secondary } mgc name command to restore default configurations.  Note Names of the primary and secondary MGC servers should be different. - primary: primary - secondary: secondary - name: MGC name, a string of 1 to 64 characters
5	Raisecom(config-epon-onu-voice-*/*:*)#h248 { primary secondary } mgc authentication auth-id example: Raisecom(config-epon-onu-voice-3/1:1)#h248 primary mgc authentication 1	(Optional) configure authentication information about the primary/secondary MGC server. You can use the no h248 { primary secondary } mgc authentication command to delete the configuration. - primary: primary - secondary: secondary - auth-id: authentication ID, an integer, ranging from 1 or 2
6	Raisecom(config-epon-onu-voice-*/*:*)#h248 mgc-swap { enable disable }	(Optional) enable/disable ONU primary/secondary MGC server swap.

Step	Command	Description
7	<pre>Raisecom(config-epon-onu-voice- */*:*)#h248 mgc { initial max min } timeout time example: Raisecom(config-epon-onu-voice- 3/1:1)#h248 mgc max retrains timeout 300</pre>	(Optional) configure the H.248 MGC retransmission timeout. You can use the h248 mgc { initial max min } timeout command to restore default configurations. time: minimum timeout retransmission time, an integer, ranging from 1 to 1000, in units of millisecond



Note

- When configuring H.248 basic services, you should configure basic parameters of the MGC on the ONU, including IP address, interface ID, and MGC name. These parameters must correspond to MGC configurations.
- When configuring primary and secondary MGC, you need to enable heartbeat detection for primary/secondary MGC swap.

6.6.6 Configuring TID

H.248 uses the TID to identify the endpoints on the MG. TID can be divided into POTS TID and RTP TID. POTS TID is the unique identifier of MG interface on the MGC, and is bound with the specific phone number.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu slot- id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice</pre>	Enter EPON ONU voice service configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-epon-onu-voice- */*:*)#h248 mg tid mode { auto line multilayer } example: Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg tid mode auto</pre>	Configure the generation mode of POTS interface TID. You can use the no h248 mg tid mode command to restore default configurations. - line: line mode - auto: automatic accumulation mode - multilayer: multilayer mode

Step	Command	Description
4	<pre>Raisecom(config-epon-onu-voice- */*:*)#h248 mg tid prefix <i>prefix name</i> example: Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg tid prefix a name 001</pre>	(Optional) configure the prefix and name of the POTS interface TID. You can use the no h248 mg tid prefix command to restore default configurations.  Note If the POTS interface TID mode is auto, you need to configure this item; otherwise, you do not. • prefix: prefix, a string of 1 to 16 characters • name: digital part, a string of 1 to 16 characters
5	<pre>Raisecom(config-epon-onu-voice- */*:*)#h248 mg tid rtp prefix <i>prefix length length</i> example: Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg tid rtp prefix abcd length 2</pre>	(Optional) configure the length of RTP TID prefix and numerical part.  Note If the local office gives an RTP name and it is different from the default value, you need to configure this item. Otherwise, no configuration is required. • Prefix: prefix, a string of 1 to 16 characters • Length: numerical part, a string of 1 to 16 characters
6	<pre>Raisecom(config-epon-onu-voice- */*:*)#h248 mg tid rtp begin <i>value</i> example: Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg tid rtp begin 2</pre>	Configure the start value of RTP TID numerical part. You can use the no h248 mg tid rtp begin command to restore default configurations. • Value: start value of the numerical part, an integer, ranging from 0 to 20000 000
7	<pre>Raisecom(config-epon-onu-voice- */*:*)#h248 mg tid rtp number <i>value</i> example: Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg tid rtp number 2</pre>	Configure the number of RTP TID. You can use the no h248 mg tid rtp number command to restore default configurations. • Value: number of RTP resources, an integer, ranging from 1 to 2 × POTS interfaces



Note

- The prefix of RTP TID should not be empty.
- There is no limit for the quantity of RTP resources on the MGC. By default, the total number of RTP resources should be two times of the number of interfaces (default).
- The user interface unused does not need to be configured with TID.
- Values of TID for different user interfaces should be different.

6.6.7 Configuring MG heartbeat

To detect the connectivity between the MG and MGC, they may send information to each other regularly. The information is called "heartbeat information".

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*/*:*)#h248 mg heartbeat cycle period example: Raisecom(config-epon-onu-voice-3/1:1)#h248 mg heartbeat cycle 100	Configure the MG heartbeat cycle. You can use the no h248 mg heartbeat cycle command to restore default configurations. time: heartbeat cycle, an integer, ranging from 10 to 43200, in units of second
4	Raisecom(config-epon-onu-voice-*/*:*)#h248 mg heartbeat mode { disable svc ito audit } example: Raisecom(config-epon-onu-voice-3/1:1)#h248 mg heartbeat mode audit	Configure the MG heartbeat cycle. You can use the no h248 mg heartbeat mode command to restore default configurations. - disable: disabled - Svc: mode of sending ServiceChange messages - ito: ITO mode - audit: auditing mode
5	Raisecom(config-epon-onu-voice-*/*:*)#h248 mg heartbeat timeout count number example: Raisecom(config-epon-onu-voice-3/1:1)#h248 mg heartbeat timeout count 10	Configure timeout times of MG fault judgement. You can use the no h248 mg heartbeat timeout count command to restore default configurations. number: heartbeat timeout times, an integer, ranging from 1 to 100



Note

- We recommend configuring the timeout of MG heartbeat less than that of MGC heartbeat.
- The heartbeat mode and cycle should cooperate with the server. If the server does not support heartbeat, you need to disable heartbeat detection.

6.6.8 Configuring H.248 digitmap

In softswitch, digitmap is in the MGC, used to detect and report Digit events received by the endpoint. The digitmap is distributed to the MG along with the dial tone when you pick up the phone. When you dial up, the MG uses the digitmap to determine whether the dialled number is a valid one. When the MG detects that the phone number is matched, it will report the number to the MGC.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#epon-onu slot- id/olt-id/onu-id voice</pre> example: <pre>Raisecom(config)#epon-onu 3/1/1 voice</pre>	Enter EPON ONU voice service configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-epon-onu-voice- */*:*)#h248 digitmap dm-id name string</pre> example: <pre>Raisecom(config-epon-onu-voice- 3/1:1)#h248 digitmap 1 dm1 ([2- 8]xxxxxx 13xxxxxxxx 0xxxxxxxx 9xxx E F x.F 1[0124-9]x [0-9EF])</pre>	Configure H.248 DigitMap. - dm-id: digitmap ID, an integer, ranging from 1 to 5. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". - Name: digitmap name, a string of 1 to 32 characters - String: digitmap number string, an integer, ranging from 1 to 1024
4	<pre>Raisecom(config-epon-onu-voice- */*:*)#digitmap match-mode { min max }</pre> example: <pre>Raisecom(config-epon-onu-voice- 3/1:1)#digitmap match-mode max</pre>	Configure the digitmap matching mode. You can use the no digitmap match-mode command to restore default configurations. - Min: minimum matching mode. If the current receiving number matches one of the dialling rules, it will be immediately reported and the number receiving ends. - Max: max match mode. If the current receiving number matches one of the dialling rules, but it is also possible to receive more numbers to match other different dialling rules, the number receiving does not end but continues.
5	<pre>Raisecom(config-epon-onu-voice- */*:*)#h248 mg digitmap long-timer longtime</pre> example: <pre>Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg digitmap long-timer 30</pre>	Configure the long timer used in DigitMap. You can use the no h248 mg digitmap long-timer command to restore default configurations. longtime: long timer time, an integer, ranging from 0 to 99, in units of second
6	<pre>Raisecom(config-epon-onu-voice- */*:*)#h248 mg digitmap short-timer shorttime</pre> example: <pre>Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg digitmap short-timer 10</pre>	Configure the short timer used in DigitMap. You can use the no h248 mg digitmap short-timer command to restore default configurations. shorttime: short timer time, an integer, ranging from 0 to 99, in units of second
7	<pre>Raisecom(config-epon-onu-voice- */*:*)#h248 mg digitmap start-timer starttime</pre> example: <pre>Raisecom(config-epon-onu-voice- 3/1:1)#h248 mg digitmap start-timer 20</pre>	Configure the start timer used in DigitMap. You can use the no h248 mg digitmap start-timer command to restore default configurations. starttime: start timer time, an integer, ranging from 0 to 99, in units of second



Caution

In general, you do not need to configure the digitmap. The digitmap issued by the MGC is used preferentially.

6.6.9 Configuring H.248 service management

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*//*:*)#h248 mg forced-deregister	Forcedly deregister the MG.
4	Raisecom(config-epon-onu-voice-*//*:*)#h248 mg register	Register the MG.
5	Raisecom(config-epon-onu-voice-*//*:*)#h248 mg delay-deregister delay-time example: Raisecom(config-epon-onu-voice-3/1:1)#h248 mg delay-deregister 20	Deregister the MG after a delay. • delay-deregister delay-time: delay registration. The delay-time is an integer ranging from 0 to 65535, in units of second.
6	Raisecom(config-epon-onu-voice-*//*:*)#h248 pots forced-deregister pots-list example: Raisecom(config-epon-onu-voice-3/1:1)#h248 pots forced-deregister 2	Forcedly deregister the POTS interface. • pots-list: POTS interface ID list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
7	Raisecom(config-epon-onu-voice-*//*:*)#h248 pots register pots-list example: Raisecom(config-epon-onu-voice-*//*:*)#h248 pots register 10	Register the POTS interface. • pots-list: POTS interface ID list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
8	Raisecom(config-epon-onu-voice-*//*:*)#h248 pots delay-deregister delay-time pots-list example: Raisecom(config-epon-onu-voice-*//*:*)#h248 pots delay-deregister 1000 10	Deregister the POTS interface after a delay. • delay-deregister delay-time: delay deregistration. The delay-time is an integer, ranging from 0 to 65535 where 0 indicates that deregistration starts after the call ends, in units of second. • pots-list: POTS interface ID list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

Step	Command	Description
9	<pre>Raisecom(config-epon-onu-voice-*/*:*)#h248 pots tid name name pots-id example: Raisecom(config-epon-onu-voice-3/1:1)#h248 pots tid name raisecom 1</pre>	Configure the TID of the POTS interface. You can use the no h248 pots tid name { all pots-list } command to restore default configurations. • name: name, a string of 1 to 32 characters • pots-id: POTS interface ID, an integer, ranging from 1 to 24

6.6.10 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 mg</pre>	Show parameters of H.248 voice gateway.
2	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 mg heartbeat</pre>	Show heartbeat information about the H.248 voice gateway.
3	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 pots [pots-id]</pre>	Show TID of the POTS interface.
4	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 mgc</pre>	Show configurations of H.248 MGC.
5	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 { primary secondary } mgc</pre>	Show configurations of the H.248 primary/secondary MGC server.
6	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 mgc-swap</pre>	Show information about H.248 primary/secondary MGC server swap.
7	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 digitmap [dm-id]</pre>	Show H.248 digitmap.
8	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 authentication</pre>	Show H.248 authentication information.
9	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 mg encryption</pre>	Show configurations of H.248 voice gateway signaling encryption.
10	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice statistics h248</pre>	Show H.248 performance statistics.
11	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 mg tid</pre>	Show configurations of H.248 POTS interface TID.
12	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id voice statistics rtp pots [pots-id]</pre>	Show configurations of H.248 RTP TID statistics.

6.7 Configuring second dialing

6.7.1 Preparing for configurations

Scenario

Second dialling refers to dialling again after being put through, such as dialling an extension or entering the card password.

Second dialling supports transmitting dialling information through the following four modes:

- Voice transparent transmission mode
- RFC 2833 mode
- RFC 2833 redundancy mode (use RFC 2198 protocol)
- SIP-INFO mode

The SIP-INFO mode takes effect only when the SIP is used, and cannot be configured when the H.248 protocol is used.

Prerequisite

The transmission mode of second dialling should be consistent with that of the connected device.

6.7.2 Default configurations

Default configurations of second dialling are as below.

Function	Default value
Transmission mode of second dialing	transparent

6.7.3 Configuring second dialing

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*/*:*)#dtmf { rfc2833-relay rfc2833-redundancy sip-info transparent } example: Raisecom(config-epon-onu-voice-3/1:1)#dtmf rfc2833-relay	Configure the transmission type of second dialing. You can use the no dtmf command to restore default configurations. • rfc2833-relay: RFC2833 relay mode • rfc2833-redundancy: RFC2833 redundancy mode • sip-info: message mode • transparent: transparent transmission mode

Step	Command	Description
4	<pre>Raisecom(config-epon-onu-voice- */*:*)#dtmf volume volume example: Raisecom(config-epon-onu-voice- 3/1:1)#dtmf volume -10</pre>	(Optional) configure DTMF volume. You can use the no dtmf volume command to restore default configurations. • volume: volume, an integer, ranging from -31 to 0, in units of dB
5	<pre>Raisecom(config-epon-onu-voice- */*:*)#dtmf payload-type type example: Raisecom(config-epon-onu-voice- 3/1:1)#dtmf payload-type 100</pre>	(Optional) configure DTMF loading type. You can use the dtmf payload-type command to restore default configurations. • payload-type type: loading type, an integer, ranging from 96 to 127

6.7.4 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-list voice dtmf</pre>	Show configurations of secondary dialing.

6.8 Configuring fax

6.8.1 Preparing for configurations

Scenario

The ONU supports two fax transmission modes: voice transparent transmission and T.38 protocol. When using the T.38 protocol, you can choose two error correction modes: Forward Error Correction (FEC) and redundancy transmission.

When the transmission mode is configured to T.38 protocol, it does not mean that you should use the configurations for voice and fax switching. Whether to use the T.38 protocol and T38 fax depends on the actual negotiation result of Session Description Protocol (SDP). If T.38 protocol switching fails, it will automatically switch to voice transparent transmission mode to fax.

Prerequisite

N/A

6.8.2 Default configurations

Default configurations of the fax service on the ONU are as below.

Function	Default value
Transmission mode of fax	transparent
ONU T.38 fax error correction mode	redundancy
T.38 fax rate on POTS interface	14400 bit/s

6.8.3 Configuring fax

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*/*:*)#fax transport { transparent t38 } example: Raisecom(config-epon-onu-voice-3/1:1)#fax transport t38	Configure the transmission mode of fax. You can use the no fax transport command to restore default configurations. - transparent: transparent transmission - t38: T.38 fax protocol
4	Raisecom(config-epon-onu-voice-*/*:*)#fax control mode { negotiation auto-vbd } example: Raisecom(config-epon-onu-voice-3/1:1)#fax control-mode negotiation	Configure the fax control mode. You can use the no fax control-mode command to restore default configurations. - negotiation: negotiation mode - auto-vbd: Auto VBD
5	Raisecom(config-epon-onu-voice-*/*:*)#fax error-correction-mode { redundancy fec } example: Raisecom(config-epon-onu-voice-3/1:1)#fax error-correction-mode redundancy	Configure T.38 fax error correction mode. You can use the no fax error-correction-mode command to restore default configurations. - redundancy: redundancy mode - fec: FEC mode
6	Raisecom(config-epon-onu-voice-*/*:*)#pots fax relay rate { 2400 4800 7200 9600 12000 14400 } pots-list example: Raisecom(config-epon-onu-voice-3/1:1)#pots fax relay rate 9600 1	Configure the T.38 fax rate on the POTS interface. You can use the no pots fax relay rate { all pots-list } command to restore default configurations. 2400: the fax rate is 2400 bit/s. 4800: the fax rate is 4800 bit/s. 7200: the fax rate is 7200 bit/s. 9600: the fax rate is 9600 bit/s. 12000: the fax rate is 12000 bit/s. 14400: the fax rate is 14400 bit/s. - pots-list: POTS interface list, an integer, ranging from 1 to 24

Step	Command	Description
7	Raisecom(config-epon-onu-voice-*/*:*)# fax t38 data redundancy <i>value</i> example: Raisecom(config-epon-onu-voice-3/1:1)#fax t38 data redundancy 2	(Optional) configure T.38 data redundancy. You can use the no fax t38 data redundancy command to restore default configurations. • redundancy: redundancy, an integer, ranging from 0 to 3
8	Raisecom(config-epon-onu-voice-*/*:*)# fax transparent redundancy <i>value</i> example: Raisecom(config-epon-onu-voice-3/1:1)#fax transparent redundancy 2	(Optional) configure the fax transparent transmission redundancy. You can use the no transparent redundancy to restore default configurations. • redundancy: redundancy, an integer, ranging from 0 to 5
9	Raisecom(config-epon-onu-voice-*/*:*)# fax t38 signal redundancy <i>value</i> example: Raisecom(config-epon-onu-voice-3/1:1)#fax t38 signal redundancy 2	(Optional) configure fax T.38 signalling redundancy. You can use the no fax t38 signal redundancy command to restore default configurations. • redundancy: redundancy, an integer, ranging from 0 to 7

6.8.4 Checking configurations

No.	Command	Description
1	Raisecom# show epon-onu slot-id/olt-id/onu-id voice fax	Show fax service configurations on the ONU.
2	Raisecom# show epon-onu slot-id/olt-id/onu-id voice pots [pots-id] fax	Show fax service configurations on the ONU POTS interface.

6.9 Configuring call emulation test

6.9.1 Preparing for configurations

Scenario

Call emulation is an important method for the VoIP device to troubleshoot network faults. It uses the program to emulate operations and events in the calling and called process to complete the call without the involvement of users.

Call emulation contains incoming emulation and outgoing emulation. Incoming emulation is used to locate voice called failure; outgoing emulation is used to locate the voice calling failure. You can use obtain the current interface status and detect the emulation test process through querying commands. You can make the interface on-hook to stop the test and obtain the test result through related commands. If the test fails, you cannot obtain the test result.

Prerequisite

N/A

6.9.2 Preparing for configurations

The default configuration of the call emulation service on the Raisecom ONU device is as below.

Function	Default value
Low frequency of call process tone	450 Hz
High frequency of call process tone	0 Hz
Low-frequency volume of call process tone	40 dB
High-frequency volume of call process tone	0 dB

Default configurations of the start and end time of the first ring and second ring are as below.

Ring time	Dial	Ringback	Busy	Congestion	Waiting
Start time of the first ring	0	1000	350	350	400
End time of the first ring	0	4000	350	350	4000
Start time of the second ring	0	0	0	0	0
End time of the second ring	0	0	0	0	0

6.9.3 Configuring call emulation test

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*/:*)#pots call-test start pots-id caller [timeout timeout] media { tone loopback } phone-number number example: Raisecom(config-epon-onu-voice-3/1:1)#pots call-test start 1 caller media tone phone-number 1001	Start the outgoing call emulation test. • pots-id: POTS interface ID, an integer, ranging from 1 to 24 • timeout timeout: test timeout time, timeout: an integer, ranging from 60 to 300, in units of second • tone: test tone • loopback: voice loopback • number: number of the phone under test

Step	Command	Description
4	<pre>Raisecom(config-epon-onu-voice- /*:*)#pots call-test start pots-id callee [timeout timeout] media { tone loopback } example: Raisecom(config-epon-onu-voice- 3/1:1)#pots call-test start 1 callee media tone phone-number 1001</pre>	Start the incoming call emulation test. • pots-id: POTS interface ID, an integer, ranging from 1 to 24 • timeout timeout: test timeout time, timeout: an integer, ranging from 60 to 300, in units of second • tone: test tone • loopback: voice loopback • number: number of the phone under test
5	<pre>Raisecom(config-epon-onu-voice- /*:*)#pots call-test stop pots-id example: Raisecom(config-epon-onu-voice- 3/1:1)#pots call-test stop</pre>	End the call emulation test. • pots-id: POTS interface ID, an integer, ranging from 1 to 24
6	<pre>Raisecom(config-epon-onu-voice- /*:*)#pots call-test query { all pots- list } example: Raisecom(config-epon-onu-voice- 3/1:1)#pots call-test query</pre>	Query the call emulation test. • all: query all POTS interfaces. • pots-id: query the ID of the specified POTS interface, which is an integer, ranging from 1 to 24.
7	<pre>Raisecom(config-epon-onu-voice- /*:*)#call-progress-tone { dial ringback busy congestion waiting }{ low-frequency high- frequency } frequency example: Raisecom(config-epon-onu-voice- 3/1:1)#call-progress-tone dial low- frequency 400</pre>	(Optional) configure the low frequency and high frequency of the call process tone. You can use the no call-progress-tone { dial ringback busy congestion waiting }{ low-frequency high-frequency } command to restore default configurations. • dial: dialing tone • ringback: ringback tone • busy: busy tone • congestion: congestion tone • waiting: call waiting tone • low-frequency frequency: low frequency rate. The frequency is an integer ranging from 0 to 65535, in units of Hz. • high-frequency frequency: high frequency rate. The frequency is an integer ranging from 0 to 65535, in units of Hz.

Step	Command	Description
8	<pre>Raisecom(config-epon-onu-voice- /*:*)#call-progress-tone { dial ringback busy congestion waiting }{ low-frequency high- frequency } volume <i>volume</i> example: Raisecom(config-epon-onu-voice- 3/1:1)#call-progress-tone dial low- frequency volume 50</pre>	(Optional) configure the low frequency and high frequency value of the call process tone. You can use the no call-progress-tone { dial ringback busy congestion waiting }{ low-frequency high-frequency } volume command to restore default configurations. • dial: dialing tone • ringback: ringback tone • busy: busy tone • congestion: congestion tone • waiting: call waiting tone • low-frequency: low frequency • high-frequency: high frequency • volume: volume, an integer, ranging from 0 to 100, in units of dB
9	<pre>Raisecom(config-epon-onu-voice- /*:*)#call-progress-tone { dial ringback busy congestion waiting } { first-signal second-signal } on-time <i>value</i> off-time <i>value</i> example: Raisecom(config-epon-onu-voice- 3/1:1)#call-progress-tone dial first- signal on-time 300 off-time 500</pre>	(Optional) configure the start time and end time of the first ring and second ring of call process tone. You can use the no call-progress-tone { dial ringback busy congestion waiting }{ first-signal second-signal } command to restore default configurations. • dial: dialing tone • ringback: ringback tone • busy: busy tone • congestion: congestion tone • waiting: call waiting tone • first-signal: first ring • second-signal: second ring • on-time: ring start tone, an integer, ranging from 0 to 65535, in units of ms • off-time: ring end tone, an integer, ranging from 0 to 65535, in units of ms



Note

When the POTS interface is transmitting voice service or being tested, you cannot perform call emulation. Each ONU supports one-way call emulation test, which excludes with the circuit/loop test, so they cannot be performed simultaneously.

6.9.4 Checking configurations

Step	Command	Description
1	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-list voice call-progress-tone [dial ringback busy congestion waiting] information</pre>	Show configurations of call process tone.

6.10 Configuring SIP server profile

6.10.1 Preparing for configurations

Scenario

It is used to configure a SIP server template on the OLT, configure the parameters of the SIP server, generate a template, and apply the template to the ONU configuration.

Prerequisite

N/A

6.10.2 Default configurations

N/A

6.10.3 Configuring SIP server profile

Creating SIP server profile

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#create sip-agent-profile-id <i>profile-id</i> name <i>profile-name</i> example: Raisecom(config)#create sip-agent-profile-id 1 name raisecom	(Optional) create a SIP server profile according to the profile ID. You can use the no form of this command to delete the profile. • profile-id: SIP server profile ID, an integer, ranging from 1 to 24 • profile-name: SIP server profile name, a string of 1 to 64 characters
3	Raisecom(config)#create sip-agent-profile-name <i>profile-name</i> example: Raisecom(config)#create sip-agent-profile-name raisecom	(Optional) create a SIP server profile based on profile name. You can use the no form of this command to delete the profile. • profile-name: SIP server profile name, a string of 1 to 64 characters
4	Raisecom(config)#sip-agent-profile-id <i>profile-id</i> name <i>profile-name</i> example: Raisecom(config)#sip-agent-profile-id 1 name abc	(Optional) modify the name of the SIP server profile according to the SIP server profile ID. • profile-id: SIP server profile ID, an integer, ranging from 1 to 24 • profile-name: SIP server profile name, a string of 1 to 64 characters

Configuring SIP server profile according to SIP server profile ID

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#sip-agent-profile-id <i>profile-id</i> proxy <i>proxy-serve-name</i> outbound <i>outbound proxy-serve-name</i> registrar <i>registrar server-name</i> example: Raisecom(config)#sip-agent-profile-id 1 proxy a outbound outbound b registrar c	(Optional) modify the proxy server, outbound server, and registration server name of the SIP server profile according to the SIP server profile ID. • profile-id: SIP server profile ID, an integer, ranging from 1 to 24 • proxy-serve-name: SIP proxy server name, a string of 1 to 50 characters • proxy-serve-nam: name of the SIP outbound proxy server, a string of 1 to 50 characters • server-name: SIP registration server name, a string of 1 to 50 characters
3	Raisecom(config)#sip-agent-profile-id <i>profile-id</i> primary-dns <i>ip-address</i> secondary-dns <i>ip-address</i> example: Raisecom(config)#sip-agent-profile-id 1 profile-id primary-dns 192.168.2.2 secondary-dns 192.168.3.2	(Optional) configure the primary and secondary DNS server addresses of the SIP server according to the SIP server profile ID. • profile-id: SIP server profile ID, an integer, ranging from 1 to 24 • primary-dns ip-address: primary DNS address, in dotted decimal notation, such as 10.10.10.1 • secondary-dns ip-address: secondary DNS, in dotted decimal notation, such as 10.10.10.1
4	Raisecom(config)#sip-agent-profile-id <i>profile-id</i> user-domain <i>domain</i> example: Raisecom(config)#sip-agent-profile-id 1 user-domain raisecom	Configure the user domain name according to the SIP server profile ID. • profile-id: SIP server profile ID, an integer, ranging from 1 to 24 • domain: SIP user domain name, in dotted decimal notation, ranging from 1 to 75
5	Raisecom(config)#sip-agent-profile-id <i>profile-id</i> register-expire-time <i>time</i> example: Raisecom(config)#sip-agent-profile-id 1 register-expire-time 120	(Optional) configure the registration expiration time according to the SIP server profile ID. You can use the no form of this command to delete the configuration. • profile-id: SIP server profile ID, an integer, ranging from 1 to 24 • time: registration expiration time, an integer, in units of second, ranging from 60 to 65535
6	Raisecom(config)#sip-agent-profile-id <i>profile-id</i> re-register-time <i>time</i> example: Raisecom(config)#sip-agent-profile-id 1 register-expire-time 120	(Optional) configure the re-registration expiration time according to the SIP server profile ID. You can use the no form of this command to delete this configuration. • profile-id: SIP server profile ID, an integer, ranging from 1 to 24 • time: registration expiration time, an integer, in units of second, ranging from 60 to 3600

Step	Command	Description
7	Raisecom(config)# sip-agent-profile-id <i>profile-id</i> uri-format { tel sip } example: Raisecom(config)#sip-agent-profile-id uri-format sip	(Optional) configure the URI format according to the SIP server profile ID. You can use the no form of this command to delete this configuration. • tel: Tel format • sip: SIP format
8	Raisecom(config)# sip-agent-profile-id <i>profile-id</i> option-transmit-control { enable disable } example: Raisecom(config)#sip-agent-profile-id 1 option-transmit-control enable	(Optional) enable option transmission control according to the SIP server profile ID. You can use the no form of this command to delete this configuration. • profile-id: SIP server profile ID, an integer, ranging from 1 to 24 • enable: enable option transmission control. • disable: disable option transmission control.
9	Raisecom(config)# sip-agent-profile-id <i>profile-id</i> digitmap <i>digitmap</i> example: Raisecom(config)#sip-agent-profile-id 1 digitmap abc	(Optional) configure the registration expiration time according to the SIP server template ID. You can use the no form of this command to delete this function. • profile-id: SIP server template ID, an integer, ranging from 1 to 24 • digitmap: digitmap, a string of 1 to 1024 characters
10	Raisecom(config)# sip-agent-profile-name <i>profile-name</i> digitmap <i>digitmap</i> example: Raisecom(config)#sip-agent-profile-name 11 digitmap abc	(Optional) configure the registration expiration time according to the SIP server template name. You can use the no form of this command to delete the configuration. • profile-name: SIP server template name, a string of 1 to 64 characters • digitmap: digitmap, a string of 1 to 1024 characters

Configuring SIP server profile according to SIP server profile name

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# sip-agent-profile-name <i>profile-name</i> proxy <i>proxy-serve-name</i> outbound <i>outbound</i> proxy-serve-name <i>proxy-serve-name</i> registrar <i>registrar</i> server-name <i>server-name</i> example: Raisecom(config)#sip-agent-profile-name raisecom proxy a outbound outbound b registrar c	(Optional) modify the proxy server, outbound proxy server, and registration server name of the SIP server profile according to the SIP server profile ID. • profile-name: SIP server profile name, a string of 1 to 64 characters • proxy-serve-name: SIP proxy server name, a string of 1 to 50 characters • proxy-serve-nam: name of the SIP outbound proxy server, a string of 1 to 50 characters • server-name: SIP registration server name, a string of 1 to 50 characters

Step	Command	Description
3	<pre>Raisecom(config)#sip-agent-profile-name profile-name primary-dns ip-address secondary-dns ip-address example: Raisecom(config)#sip-agent-profile-name raisecom primary-dns 192.168.2.2 secondary-dns 192.168.3.2</pre>	(Optional) configure the primary and secondary DNS server addresses of the SIP server according to the SIP server profile name. • profile-name: SIP server profile name, a string of 1 to 64 characters • primary-dns ip-address: primary DNS address, in dotted decimal notation, such as 10.10.10.1 • secondary-dns ip-address: secondary DNS address, in dotted decimal notation, such as 10.10.10.1
4	<pre>Raisecom(config)#sip-agent-profile-name profile-name user-domain domain example: Raisecom(config)#sip-agent-profile-name user-domain abc</pre>	(Optional) Configure the user domain name according to the SIP server profile name. • profile-name: SIP server profile name, a string of 1 to 64 characters • domain: SIP user domain name, in dotted decimal notation, ranging from 1 to 75
5	<pre>Raisecom(config)#sip-agent-profile-name profile-name register-expire-time time example: Raisecom(config)#sip-agent-profile-name raisecom register-expire-time 120</pre>	(Optional) configure the registration expiration time according to the SIP server profile name. You can use the no form of this command to delete the configuration. • profile-name: SIP server profile name, a string of 1 to 64 characters • time: registration expiration time, an integer, ranging from 60 to 3600, in units of second
6	<pre>Raisecom(config)#sip-agent-profile-name profile-name re-register-time time example: Raisecom(config)#sip-agent-profile-name raisecom register-expire-time 120</pre>	(Optional) configure the URI format according to the SIP server profile name. You can use the no form of this command to delete this configuration. • profile-name: SIP server profile name, a string of 1 to 64 characters • time: registration expiration time, an integer, ranging from 60 to 3600, in units of second
7	<pre>Raisecom(config)#sip-agent-profile-name profile-name uri-format { tel sip } example: Raisecom(config)#sip-agent-profile-name raisecom uri-format sip</pre>	(Optional) configure the URI format according to the SIP server profile ID. You can use the no form of this command to delete this configuration. • tel: Tel format • sip: SIP format
8	<pre>Raisecom(config)#sip-agent-profile-name profile-name option-transmit-control { enable disable } example: Raisecom(config)#sip-agent-profile-name raisecom option-transmit-ctrl enable</pre>	(Optional) enable option transmission control according to the SIP server profile name. You can use the no form of this command to delete this configuration. • profile-name: SIP server profile name, a string of 1 to 64 characters • enable: enable option transmission control. • disable: disable option transmission control.

6.10.4 Referencing SIP server profile

Referencing SIP server profile in GPON ONU service profile configuration mode

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#gpon-onu-service-profile <i>profile-id</i> example: Raisecom(config)#gpon-onu-service-profile 10	Enter GPON ONU service profile configuration mode. • profile-id: service profile ID, an integer, ranging from 1 to 1024
3	Raisecom(config-gpon-onu-service-profile:profile-id)#uni pots <i>pots-list</i> { sip-agent-profile-id <i>profile-id</i> secondary sip-agent-profile-id <i>profile-id</i> } example: Raisecom(config-gpon-onu-service-profile-1)#uni pots 1 sip-agent-profile-id 1	(Optional) reference primary and secondary SIP server profiles based on SIP server ID on the voice interface. You can use the no form of this command to delete this command. • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • sip-agent-profile-id profile-id: primary SIP server profile ID, an integer, ranging from 1 to 24 • secondary sip-agent-profile-id profile-id: secondary SIP server profile ID, an integer, ranging from 1 to 24
4	Raisecom(config-gpon-onu-service-profile:profile-id)#uni pots <i>pots-list</i> { sip-agent-profile-name <i>profile-name</i> secondary sip-agent-profile-name <i>profile-name</i> } example: Raisecom(config-gpon-onu-service-profile-1)#uni pots 1 sip-agent-profile-name raisecom	(Optional) reference primary and secondary SIP server profiles based on SIP server name on the voice interface. You can use the no form of this command to delete this command. • pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • sip-agent-profile-name profile-name: primary SIP server profile name, a string of 1 to 64 characters • secondary sip-agent-profile-name profile-name: secondary SIP server profile name, a string of 1 to 64 characters

Referencing SIP server profile in GPON ONU POTS interface configuration mode

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)# gpon-onu uni pots slot-id/olt-id/onu-id/pots-id example: Raisecom(config)#gpon-onu uni pots 3/2/1/1	Enter GPON ONU POTS interface configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface - pots-id: ONU UNI ID
3	Raisecom(config-gpon-onu-pots-*/*/*:*)# sip-agent-profile-id profile-id example: Raisecom(config-gpon-onu-pots-3/2/1:1)#sip-agent-profile-id 1	(Optional) reference the primary SIP server profile based on SIP server ID on the voice interface. You can use the no form of this command to delete this command. profile-id: SIP server profile ID, an integer, ranging from 1 to 24
4	Raisecom(config-gpon-onu-pots-*/*/*:*)# sip-agent-profile-name profile-name example: Raisecom(config-gpon-onu-pots-3/2/1:1)#sip-agent-profile-name raisecom	(Optional) reference the primary SIP server profile based on SIP server name on the voice interface. You can use the no form of this command to delete this command. profile-name: SIP server profile name, a string of 1 to 64 characters
5	Raisecom(config-gpon-onu-pots-*/*/*:*)# secondary sip-agent-profile-id profile-id example: Raisecom(config-gpon-onu-3/2/1:1)#sip-agent-profile-id 1	(Optional) reference the secondary SIP server profile based on SIP server ID on the voice interface. You can use the no form of this command to delete this command. profile-id: primary SIP server profile ID, an integer, ranging from 1 to 24
6	Raisecom(config-gpon-onu-pots-*/*/*:*)# secondary sip-agent-profile-name profile-name example: Raisecom(config-gpon-onu-3/1/1:1)#secondary sip-agent-profile-name raisecom	(Optional) reference the secondary SIP server profile based on SIP server name on the voice interface. You can use the no form of this command to delete this command. profile-name: primary SIP server profile name, a string of 1 to 64 characters
7	Raisecom(config-gpon-onu-pots-*/*/*:*)# sip-agent reg-exp-time time example: Raisecom(config)#sip-agent reg-exp-time 120	(Optional) configure the registration expiration time of the SIP server. You can use the no form of this command to delete the configuration. time: registration expiration time, an integer, in units of second, ranging from 60 to 3600
8	Raisecom(config-gpon-onu-pots-*/*/*:*)# sip-agent uri-format { tel sip } example: Raisecom(config)#sip-agent uri-format sip	(Optional) configure the URI format of the SIP server. You can use the no form of this command to delete the configuration. - tel: Tel format - sip: SIP format

Referencing SIP server profile in GPON ONU POTS interface configuration mode

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id/pots-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-voice-*/*:*)#secondary sip-agent-profile-id profile-id example: Raisecom(config-epon-onu-voice-3/1:1)#secondary sip-agent-profile-id 1	(Optional) reference the standby SIP server template of the ONU based on the SIP server ID. You can use the no form of this command to delete the configuration. profile-id: SIP server template ID, an integer, ranging from 1 to 24
4	Raisecom(config-epon-onu-voice-*/*:*)#secondary sip-agent-profile-name profile-name example: Raisecom(config-gpon-onu-pots-3/2/1:1)#secondary sip-agent-profile-name profile1	(Optional) reference the standby SIP server template of the ONU based on the SIP server name. You can use the no form of this command to delete the configuration. profile-name: SIP server template name, an integer, ranging from 1 to 64
5	Raisecom(config-epon-onu-voice-*/*:*)#sip-agent-profile-id profile-id [secondary sip-agent-profile-id profile-id] example: Raisecom(config-gpon-onu-3/2/1:1)# sip-agent-profile-id 1 secondary sip-agent-profile-id 2	(Optional) reference the primary/standby SIP server template of the ONU based on the SIP server ID. You can use the no form of this command to delete the configuration. profile-id: primary SIP server template ID, an integer, ranging from 1 to 24
6	Raisecom(config-epon-onu-voice-*/*:*)#sip-agent-profile-name profile-name [secondary sip-agent-profile-name profile-name] example: Raisecom(config-gpon-onu-3/2/1:1)#sip-agent-profile-name profile1 secondary sip-agent-profile-name profile2	(Optional) reference the primary/standby SIP server template of the ONU based on the SIP server name. You can use the no form of this command to delete the configuration. profile-name: SIP server profile name, a string of 1 to 64 characters

6.10.5 Checking configurations

Step	Command	Description
1	Raisecom#show sip-agent-profile all	Show information about all SIP server profiles.
2	Raisecom#show sip-agent-profile-id profile-id	Show information about the specified SIP server profile according to the ID.
3	Raisecom#show sip-agent-profile-name profile-name	Show information about the specified SIP server profile according to the name.

Step	Command	Description
4	Raisecom# show gpon-onu slot-id/olt-id/onu-id uni pots [uni-id] { information line-status media sip-agent sip-user statistics rtp }	Show configurations of the ONU POTS interface.
5	Raisecom# show epon-onu slot-id/olt-id/onu-list sip-agent	Show SIP server information about the ONU.

7 Configuring VoIP services (applicable to EPON POL scenario)

This chapter describes the VoIP service and the configuration process of the EPON device in the POL scenario, and provides the corresponding configuration examples:

- Introduction
- Configuring VoIP
- Configuring SIP user parameters
- Configuring SIP server template
- Examples for configuring MSG

7.1 Introduction

7.1.1 VoIP

Voice over IP (VoIP) is a technology that transmits the traditional TDM digitalized voice signals over an IP network in real time in the form of data packets to realize voice communication. The advantage of VoIP over traditional voice services is that it utilizes a wide range of Internet environments and can provide more, better, and cheaper services.

VoIP uses multiple signaling protocols to implement voice calls. The device supports SIP and IMS-SIP.

7.1.2 SIP

SIP overview

Session Initiation Protocol (SIP) is an application layer control protocol for multimedia communication on an IP network. It is used to establish, modify and terminate interactive user sessions including multimedia elements such as video, voice, and instant messaging.

SIP is based on text encoding and decoding, and can be carried on an IP network. The network layer protocol used is IP, and the transport layer protocol can be TCP or UDP, with UDP being preferred.

SIP basic concepts

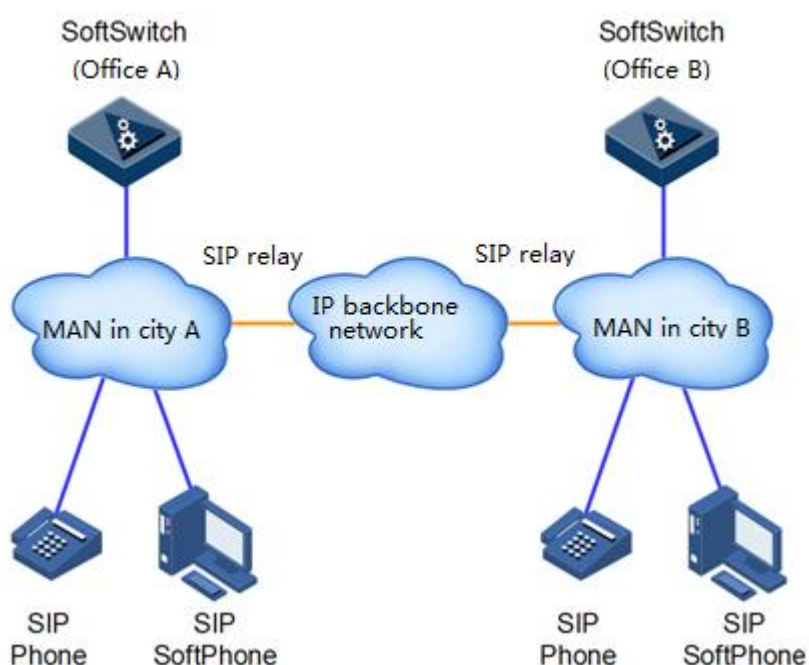
The operating environment of SIP involves the following related concepts:

- Location server: provide possible location information of the called user for the redirect server or proxy server.
- Proxy server: forward SIP requests on behalf of other users. The proxy server parses the message before forwarding the request, and rewrites the request if necessary.
- Redirect server: receive SIP requests, map their addresses to 0 or more new addresses, and return the results to the client.
- Registrar server: receive registration requests and register user information. It is often located at the same place as the proxy server or redirect server to provide location services together.
- User agent client: initiate SIP requests.
- User agent server): contact users and send back responses on behalf of users after receiving SIP requests. The response can indicate acceptance, rejection, or redirection of the request message.

SIP typical application

Figure 7-1 show typical application of SIP in the next generation network.

Figure 7-1 Typical application SIP in NGN



7.1.3 IMS-SIP

IMS-SIP overview

IP Multimedia Core Subsystem (IMS) is a sub-system that supports IP multimedia services proposed by the Third Generation Partnership Project (3GPP). It uses Session Initiation Protocol (SIP), and communication has nothing to do with access modes. It provides a variety of media services, and features separation of control functions and bearing capabilities, separation of calls and sessions, separation of applications and services, separation of services and networks, and integration of mobile networks and Internet services. IMS conforms to the trend of convergence and development of communication networks. Due to the flexibility of SIP, SIP, as a session control protocol, is adopted in the 3GPP R5 to design IMS 3GPP. It did not define a new SIP, but only used SIP defined by IETF in a certain way.

7.2 Configuring VoIP

7.2.1 Preparing for configurations

Scenario

When provisioning the voice service, you must first configure the VoIP signaling protocol (SIP or IMS-SIP) and select the transmission mode of voice signaling to realize the voice call process.

Prerequisite

N/A

7.2.2 Default configurations

Default configurations of the VoIP on the ONU (MSG) are as below:

Function	Default value
VoIP type	IMS-SIP

7.2.3 Configuring VoIP type

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice	Enter EPON ONU voice service configuration mode.
3	Raisecom(config-epon-onu-voice-*//*:*)#sip-agent voip-protocol { sip ims-sip }	Configure the VoIP type.



Note

After configuring the protocol type, you need to perform a **write** operation and then a **reload** operation. After the device receives the Trap report "reload succeeded", it means that the protocol switching is actually completed.

7.2.4 Checking configurations

Step	Command	Description
1	Raisecom(config)# show epon-onu slot-id/olt-id/onu-list sip-agent	Show SIP server information of the ONU.

7.3 Configuring SIP user parameters

7.3.1 Configuring SIP user parameters

Please perform the following configuration on the device that needs to configure the SIP user parameters corresponding to the ONU voice port.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# epon-onu slot-id/olt-id/onu-id voice example: Raisecom(config)#epon-onu 3/1/1 voice	Enter EPON ONU voice service configuration mode. - slot-id: Slot ID - olt-id: PON port ID - onu-id: ONU ID under the PON port
3	Raisecom(config-epon-onu-voice-*/*:*)# sip-user aor user-aor username username password password pots-list example: Raisecom(config-epon-onu-voice-3/1:1)# sip-user aor sip1 username user1 password raisecom 1-3	Configure the voice protocol type of the ONU SIP server. You can use the no sip-agent command to restore to the default status. - user-aor: user phone number, a string of 1 to 16 characters - username: user name, a string of 1 to 32 characters - password: password, a string of 1 to 16 characters - pots-list: POTS list, an integer, ranging from 1 to 24. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

7.3.2 Checking configurations

No.	Command	Description
1	Raisecom# show epon-onu slot-id/olt-id/onu-list uni pots [pots-id] sip-user	Show SIP user information on the ONU voice interface.

7.4 Configuring SIP server template

7.4.1 Preparing for configurations

Scenario

It is used to configure the SIP server template on the OLT, configure the parameters of the SIP server, and generate the template.

Prerequisite

N/A

7.4.2 Default configurations

N/A

7.4.3 Configuring SIP server template

Creating SIP server template

No.	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# create sip-agent-profile-id <i>profile-id</i> example: Raisecom(config)#create sip-agent-profile-id 1	(Optional) create a SIP server template based on the template ID. You can use the no form of this command to delete the template. • profile-id: SIP server template ID, an integer, ranging from 1 to 24
3	Raisecom(config)# create sip-agent-profile-name <i>profile-name</i> example: Raisecom(config)#create sip-agent-profile-name raisecom	(Optional) create a SIP server template based on the template name. You can use the no form of this command to delete the template. • profile-name: SIP server template name, a string of 1 to 64 characters

No.	Command	Description
4	Raisecom(config)#sip-agent-profile-id <i>profile-id</i> name <i>profile-name</i> example: Raisecom(config)#sip-agent-profile-id 1 name raisecom	(Optional) modify the SIP server template name based on the SIP server template. • profile-id: SIP server template ID, an integer, ranging from 1 to 24 • profile-name: SIP server template name, an integer, ranging from 1 to 64

Configuring SIP server template based on SIP server template ID

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)#sip-agent-profile-id <i>profile-id</i> name <i>profile-name</i> example: Raisecom(config)#sip-agent-profile-id 1 name abc	(Optional) modify the SIP server template name based on SIP server template ID. • profile-id: SIP server template ID, an integer, ranging from 1 to 24 • profile-name: SIP server template name, a string of 1 to 64 characters
3	Raisecom(config)#sip-agent-profile-id <i>profile-id</i> proxy <i>proxy-serve-name</i> outbound <i>outbound proxy-serve-name</i> registrar <i>registrar server-name</i> example: Raisecom(config)#sip-agent-profile-id 1 proxy a outbound outbound b registrar c	(Optional) modify the proxy server name, outbound proxy server name, and registration server name of the SIP server template according to the SIP server template ID. • profile-id: SIP server template ID, an integer, ranging from 1 to 24 • proxy-serve-name: SIP proxy server name, a string of 1 to 50 characters • outbound proxy-serve-nam: SIP outbound proxy server name, a string of 1 to 50 characters • registrar server-name: SIP registration server name, a string of 1 to 50 characters
4	Raisecom(config)#sip-agent-profile-id <i>profile-id</i> register-expire-time <i>time</i> example: Raisecom(config)#sip-agent-profile-id 1 register-expire-time 120	(Optional) Configure the registration expiration time according to the SIP server template ID. You can use the no form of this command to delete the configuration. • profile-id: SIP server profile ID, an integer, ranging from 1 to 24 • time: registration expiration time, an integer, in units of second, ranging from 60 to 65535
5	Raisecom(config)#sip-agent-profile-id <i>profile-id</i> digitmap <i>digitmap</i> example: Raisecom(config)#sip-agent-profile-id 1 digitmap abc	(Optional) modify the digitmap content according to the SIP server template ID. • profile-id: SIP server profile ID, an integer, ranging from 1 to 24 • digitmap: digitmap, a string of 1 to 1024 characters

Configuring the SIP server template according to the SIP server template name

Step	Command	Description
1	raisecom#config	Enter global configuration mode.
2	Raisecom(config)#sip-agent-profile-name <i>profile-name proxy proxy-serve-name</i> outbound <i>outbound proxy-serve-name</i> registrar <i>registrar server-name</i> example: Raisecom(config)#sip-agent-profile-name raisecom proxy a outbound outbound b registrar c	(Optional) modify the proxy server name, outbound proxy server name, and registration server name of the SIP server template according to the SIP server template name. • profile-name: SIP server profile name, a string of 1 to 64 characters • proxy-serve-name: SIP proxy server name, a string of 1 to 50 characters • outbound proxy-serve-name: SIP outbound proxy server name, a string of 1 to 50 characters • registrar server-name: SIP registration server name, a string of 1 to 50 characters
3	Raisecom(config)#sip-agent-profile-name <i>profile-name register-expire-time time</i> example: Raisecom(config)#sip-agent-profile-name raisecom register-expire-time 120	(Optional) configure the registration expiration time according to the SIP server template name. You can use the no form of this command to delete the configuration. • profile-name: SIP server profile name, a string of 1 to 64 characters • time: registration expiration time, an integer, ranging from 60 to 65535, in units of second
4	Raisecom(config)#sip-agent-profile-name <i>profile-name digitmap digitmap</i> example: Raisecom(config)#sip-agent-profile-name 11 digitmap abc	(Optional) modify the digitmap content according to the SIP server template name. • profile-name: SIP server template name, a string of 1 to 64 characters • digitmap: digitmap, a string of 1 to 1024 characters

7.4.4 Referencing SIP server template

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice	Enter EPON ONU voice service configuration mode.
3	Raisecom(config-epon-onu-voice- */*:*)#sip-agent-profile-id <i>profile-id</i> [secondary sip-agent-profile-id <i>profile-id]</i>	(Optional) reference the primary and secondary SIP server template based on the SIP server ID of the ONU. You can use the no sip-agent-profile [secondary] form of this command to delete the configuration.

Step	Command	Description
4	<code>Raisecom(config-epon-onu-voice- */*:*)#sip-agent-profile-name <i>profile- name</i> [secondary sip-agent-profile-name <i>profile-name</i>]</code>	(Optional) reference the primary and secondary SIP server template based on the SIP server name of the ONU. You can use the no sip-agent-profile [secondary] command to delete the configuration.
5	<code>Raisecom(config-epon-onu-voice- */*:*)#secondary sip-agent-profile-name <i>profile-name</i></code>	(Optional) reference the secondary SIP server template based on the SIP server name of the ONU. You can use the no sip-agent-profile secondary command to delete the configuration.
6	<code>Raisecom(config-epon-onu-voice- */*:*)#secondary sip-agent-profile-id <i>profile-id</i></code>	(Optional) reference the secondary SIP server template based on the SIP server ID of the ONU. You can use the no sip-agent-profile secondary command to delete the configuration.

7.4.5 Checking configurations

Step	Command	Description
1	<code>Raisecom#show sip-agent-profile all</code>	Show information about all SIP server templates.
2	<code>Raisecom#show sip-agent-profile-id <i>profile-id</i></code>	Check information about the specified SIP server template based on ID.
3	<code>Raisecom#show sip-agent-profile-name <i>profile-name</i></code>	Check information about the specified SIP server template based on name.

7.5 Examples for configuring MSG

7.5.1 Provisioning IMS-SIP voice services

Configuring template type

Step 1 Configure the sip-agent template (primary/secondary template).

Create the primary template.

```
Raisecom(config)#create sip-agent-profile-id 2 name ims-sip
Raisecom(config)#sip-agent-profile-id 2 proxy sbc.chinamobile.com
outbound sbc.chinamobile.com registrar sbc.chinamobile.com//if the voice
server is an IP address, you need to modify the domain name to the IP
format: X.X.X.X.
```

Create the secondary voice template.

```
Raisecom(config)#create sip-agent-profile-id 5 name ims-sip-secondary
Raisecom(config)#sip-agent-profile-id 5 proxy sbc.chinamobile1.com
outbound sbc.chinamobile1.com registrar sbc.chinamobile1.com
```

- Step 2 Create a VoIP template, modify the voice protocol to IMS-SIP, and bind the sip-agent template.

```
Raisecom(config)#create voip-profile 2 name ims-sip pots 2 //fill in the
number of pots according to the actual situation. For example, fill in 2
if there are 2 ports.
Raisecom(config)#voip-profile 2
Raisecom(config-epon-onu-voip-profile:2)#voip-protocol ims-sip
Raisecom(config-epon-onu-voip-profile:2)#sip-agent-profile-id 2 secondary
sip-agent-profile-id 5
Raisecom(config-epon-onu-voip-profile:2)#quit
```

- Step 3 Create a service template and bind the VoIP template.

```
Raisecom(config)#epon-onu-service-profile 2
Raisecom(config-epon-onu-service-profile:2)#name ims-sip
Raisecom(config-epon-onu-service-profile:2)#port-num ethernet 4
Raisecom(config-epon-onu-service-profile:2)#voip-profile 2
Raisecom(config-epon-onu-service-profile:2)#quit
```

- Step 4 Create an ONU and bind the service template.

```
Raisecom(config)#interface epon-olt 3/4
Raisecom(config-if-epon-olt-1:1)#create epon-onu mac 000e.5e5b.2db1 line-
profile-id 1024 service-profile-id 2
Raisecom(config-if-epon-olt-1:1)#exit
```

- Step 5 Configure the voice account and password.

```
Raisecom(config)#epon-onu 1/1/1 voice
Raisecom(config-epon-onu-voice-1/1:1)#sip-user aor 1001 username 1001
password 1001 1//account and password of pots1
Raisecom(config-epon-onu-voice-1/1:1)#sip-user aor 2001 username 2001
password 2001 2 //account and password of pots2
Raisecom(config-epon-onu-voice-1/1:1)#quit
```

Step 6 Configure the WAN connection of the voice service (select one mode from DHCP or static).

Configure the voice WAN connection in DHCP mode:

```
Raisecom(config)#epon-onu 1/1/1  
Raisecom(config-epon-onu-1/1:1)#wan 2 mode dhcp  
Raisecom(config-epon-onu-1/1:1)#wan 2 vlan 2000  
Raisecom(config-epon-onu-1/1:1)#wan 2 service voip-media  
Raisecom(config-epon-onu-1/1:1)#wan 2 service mode route cos 6
```

Configure the voice WAN connection in static mode:

```
Raisecom(config)#epon-onu 1/1/1  
Raisecom(config-epon-onu-1/1:1)#wan 2 mode static  
Raisecom(config-epon-onu-1/1:1)#wan 2 static ip-address 172.16.91.215  
255.255.255.0 default-gw 172.16.91.1 primary-dns 172.16.8.8 secondary-dns  
172.16.8.6  
Raisecom(config-epon-onu-1/1:1)#wan 2 vlan 2000  
Raisecom(config-epon-onu-1/1:1)#wan 2 service voip-media  
Raisecom(config-epon-onu-1/1:1)#wan 2 service mode route cos 6  
Raisecom(config-epon-onu-1/1:1)#quit
```

Step 7 Create and configure a VLAN and configure the corresponding port to allow the VLAN to pass.

Create an outer VLAN 2000, and configure the uplink port and PON port to allow the VLAN to pass.

```
Raisecom(config)#create vlan 2000 active
```

Configure the uplink port VLAN.

```
Raisecom(config)#interface ten-gigabitethernet 19/1  
Raisecom(config-if-ten-gigabitethernet-19:1)#switchport trunk allowed  
vlan add 2000  
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
```

Configure the PON port VLAN.

```
Raisecom(config)#interface epon-olt 1/1  
Raisecom(config-if-epon-olt-1:1)#switchport trunk allowed vlan add 2000  
Raisecom(config-if-epon-olt-1:1)#vlan-mapping ingress outer 2000  
translate outer 2000 inner copy-from-outer //(optional, no need to  
configure this command for a single-layer VLAN)
```

```
Raisecom(config-if-epon-olt-1:1)#switchport trunk untagged vlan add 2000  
//(optional, no need to configure this command for a single-layer VLAN)  
Raisecom(config-if-epon-olt-1:1)#exit
```

Step 8 Save configurations.

```
Raisecom#write startup-config
```

Manual configuration

Step 1 Configure the sip-agent template (primary/secondary template)

The configuration step is the same as step 1 of configuring template type in 7.5.1 provisioning IMS-SIP services.

Step 2 Bind a voice template for ONU remote management.

```
Raisecom(config)#epon-onu 1/1/1 voice  
Raisecom(config-epon-onu-voice-1/1:1)#sip-agent-profile-id 2 secondary  
sip-agent-profile-id 5 //bind the primary and secondary voice server.  
Raisecom(config-epon-onu-voice-1/1:1)#sip-agent voip-protocol ims-sip  
//modify the voice protocol to ims-sip.
```

Step 3 Configure the account and password of voice dial.

```
Raisecom(config)#epon-onu 1/1/1 voice  
Raisecom(config-epon-onu-voice-1/1:1)#sip-user aor 1001 username 1001  
password 1001 1 //account and password of pots 1  
Raisecom(config-epon-onu-voice-1/1:1)#sip-user aor 2001 username 2001  
password 2001 2 //account and password of pots2  
Raisecom(config-epon-onu-voice-1/1:1)#quit
```

Step 4 Configure the WAN connection of the voice service (select one mode from DHCP or static).

The configuration step is the same as step 6 of configuring template type in 7.5.1 provisioning IMS-SIP services.

Step 5 Create and configure a VLAN and configure the corresponding port to allow the VLAN to pass.

The configuration step is the same as step 7 of configuring template type in 7.5.1 provisioning IMS-SIP voice services.

Step 6 Save configurations.

```
Raisecom#write startup-config
```

7.5.2 Provisioning SIP voice service

Configuring template type

Step 1 Configure the sip-agent template (primary/secondary template).

Configure the primary voice server.

```
Raisecom(config)#create sip-agent-profile-id 6 name sip
Raisecom(config)#sip-agent-profile-id 6 proxy 172.16.91.224 outbound
172.16.91.224 registrar 172.16.91.224
```

Configure the secondary voice server.

```
Raisecom(config)#create sip-agent-profile-id 7 name sip-secondary
Raisecom(config)#sip-agent-profile-id 7 proxy 172.16.91.228 outbound
172.16.91.228 registrar 172.16.91.228
```

Step 2 Create a VoIP template, modify the voice protocol to SIP, and bind the sip-agent template.

```
Raisecom(config)#create voip-profile 5 name sip pots 2// fill in the
number of pots according to the actual situation. For example, fill in 2
if there are 2 ports.
Raisecom(config)#voip-profile 5
Raisecom(config-epon-onu-voip-profile:5)#voip-protocol sip
Raisecom(config-epon-onu-voip-profile:5)#sip-agent-profile-id 6 secondary
sip-agent-profile-id 7
Raisecom(config-epon-onu-voip-profile:5)#quit
```

Step 3 Create a service template and bind the VoIP template.

```
Raisecom(config)#epon-onu-service-profile 3
Raisecom(config-epon-onu-service-profile:3)#name sip
Raisecom(config-epon-onu-service-profile:3)#port-num ethernet 4
Raisecom(config-epon-onu-service-profile:3)#voip-profile 5
Raisecom(config-epon-onu-service-profile:3)#quit
```

Step 4 Create an ONU and bind the service template.

```
Raisecom(config)#interface epon-olt 1/1
Raisecom(config-if-epon-olt-1:1)#create epon-onu mac 000e.5e5b.2db1 line-
profile-id 1024 service-profile-id 3
Raisecom(config-if-epon-olt-1:1)#exit
```


Step 5 Configure the voice account and password.

The configuration step is the same as step 5 of configuring template type in 7.5.1 provisioning IMS-SIP voice services.

Step 6 Configure the WAN connection of the voice service (select one mode from DHCP or static).

The configuration step is the same as step 6 of configuring template type in 7.5.1 provisioning IMS-SIP voice services.

Step 7 Create and configure a VLAN and configure the corresponding port to allow the VLAN to pass.

The configuration step is the same as step 7 of configuring template type in 7.5.1 provisioning IMS-SIP voice services.

Step 8 Save configurations.

```
Raisecom#write startup-config
```

Manual configuration

Step 1 Configure the sip-agent template (primary/secondary template)

The configuration step is the same as step 1 of configuring template type in 7.5.2 provisioning SIP services.

Step 2 Bind a voice template for ONU remote management.

```
Raisecom(config)#epon-onu 1/1/1 voice
Raisecom(config-epon-onu-voice-1/1:1)#sip-agent-profile-id 6 secondary
sip-agent-profile-id 7 //bind the primary and secondary voice servers.
Raisecom(config-epon-onu-voice-1/1:1)#sip-agent voip-protocol sip
//modify the voice protocol to SIP.
```

Step 3 Configure the account and password of voice dial.

```
Raisecom(config)#epon-onu 1/1/1 voice
Raisecom(config-epon-onu-voice-1/1:1)#sip-user aor 1001 username 1001
password 1001 1 //account and password of pots1
Raisecom(config-epon-onu-voice-1/1:1)#sip-user aor 2001 username 2001
password 2001 2 //account and password of pots2
Raisecom(config-epon-onu-voice-1/1:1)#quit
```

Step 4 Configure the WAN connection of the voice service (select one mode from DHCP or static).

The configuration step is the same as step 6 of configuring template type in 7.5.1 provisioning IMS-SIP voice services.

Step 5 Create a VLAN and configure it. Configure the corresponding port to allow the VLAN to pass.

The configuration step is the same as step 7 of configuring template type in 7.5.1 provisioning IMS-SIP voice services.

Step 6 Save configurations.

Raisecom#**write startup-config**

8 Configuring CATV services

This chapter describes CATV services and configuration process of the device, and provides related configurations examples, including the following sections:

- Overview of CATV services
- Quick configuration of CATV services
- Configuring CATV services

8.1 Overview of CATV services

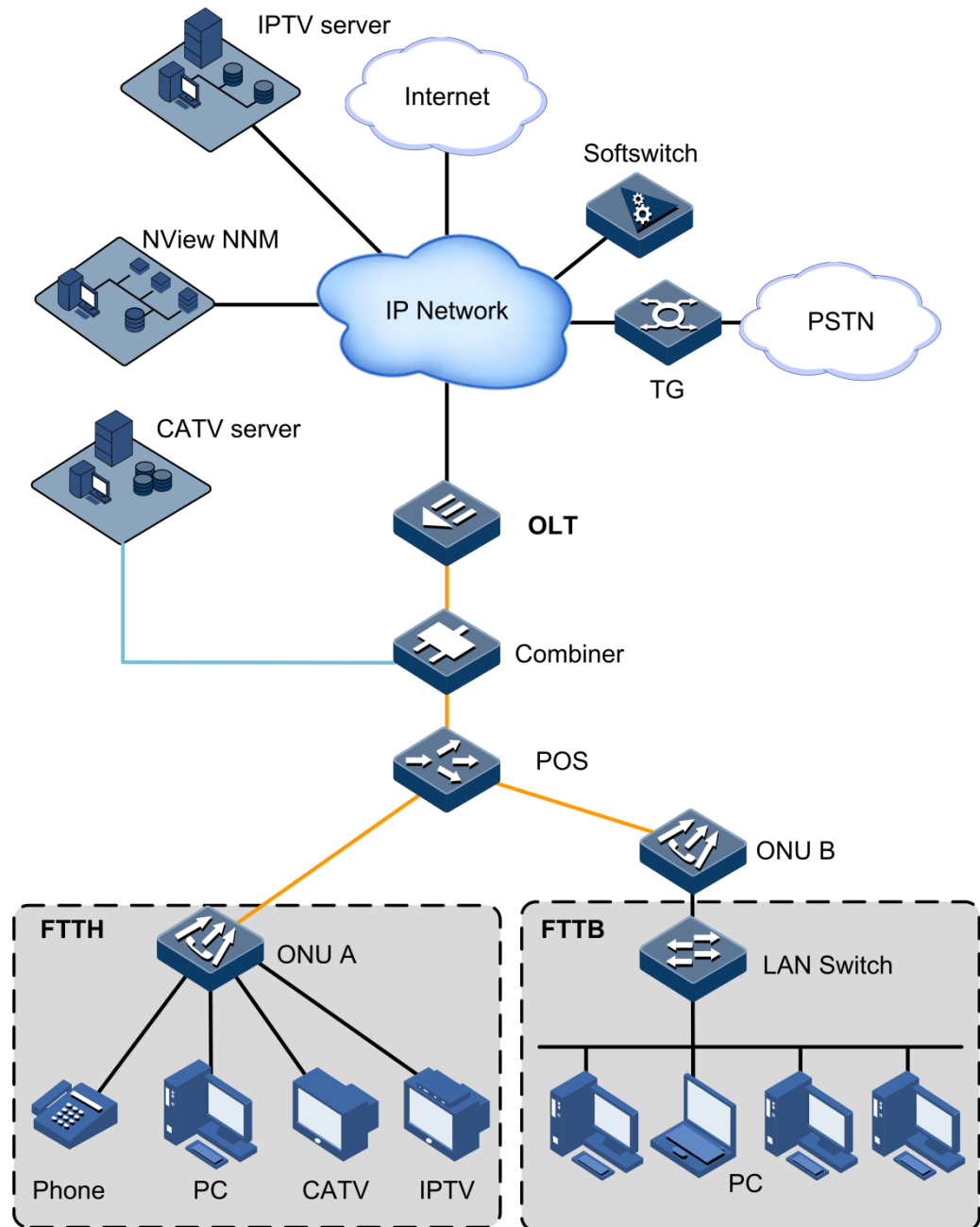
Community Antenna Television (CATV) is a cable TV system of transmitting multichannel TV signals through coaxial cables.

CAVT network, also known as cable TV network, is an analog network, which adopts the analog transmission mode. The CATV system can divide the frequency band into various frequency segments, which are used to transmit TV programs of different channels. Because each channel occupies a frequent segment, they are independent from each other.

Against the triple-play background, you can use the EPON system to transmit traditional CATV services. CATV services are transmitted in the Optical Distribution Network (ODN) through the combiner with 1550 nm wavelength. Therefore, you can configure CATV services on ONUs that support them.

Figure 8-1 shows the typical triple-play networking.

Figure 8-1 Typical triple-play networking



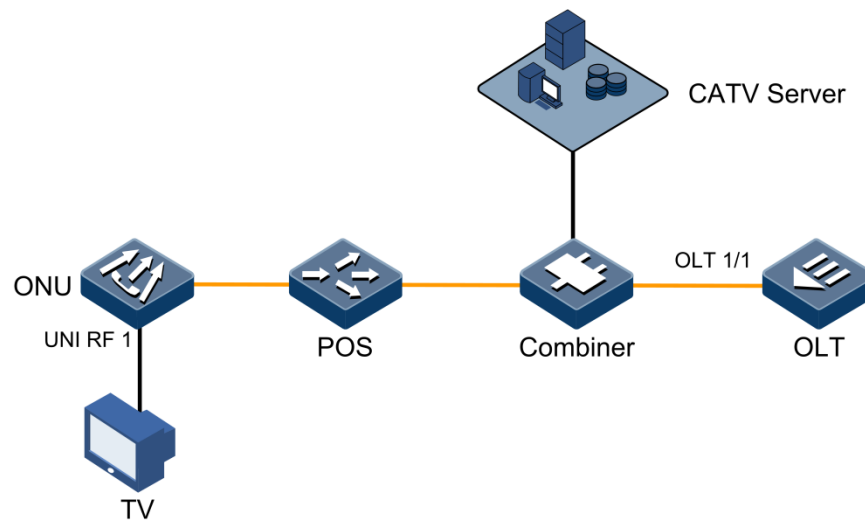
8.2 Quick configuration of CATV services

CATV service configuration is simple. You just need to enable the corresponding interface on the ONU which supports CATV services.

8.2.1 Networking requirements

As shown in Figure 8-2, the OLT is connected to the ONU through its PON interface OLT 3/1. The ONU connects the user through the UNI RF 1. Configure CATV services on the ONU to enable the user to receive CATV signals.

Figure 8-2 Configuring CATV services



8.2.2 Configuration steps

Step 1 Enable CATV on the RF interface.

```
Raisecom#config
Raisecom(config)#epon-onu 3/1/1
Raisecom(config-epon-onu-3/1:1)#uni rf 1 enable
```

8.2.3 Checking results

Show configurations of CATV services on the ONU.

```
Raisecom#show epon-onu 3/1/1 uni rf 1 information
RF UNI ID Admin State
-----
3/1/1/1 enable
```

8.3 Configuring CATV services

8.3.1 Preparing for configurations

Scenario

As shown in Figure 8-1, in triple-play networking, you need to configure CATV services on the ONU to realize transmission of CATV services through the ODN.

Prerequisite

Ensure that the ONU supports CATV services.

8.3.2 Configuring CATV services

Configuring EPON CATV services

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU remote management configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-list: ONU ID under the PON interface
3	Raisecom(config-epon-onu-1/1:1)#uni rf uni-id { enable disable } example: Raisecom(config-epon-onu-3/1:1)#uni rf 1 enable	Enable/Disable CATV services - rf-id: RF interface ID, an integer, ranging from 1 to 4 - enable: enable the RF user interface. - disable: disable the RF user interface.

Configuring GPON CATV services

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#gpon-onu uni catv [range] slot-id/olt-id/onu-id/uni-id example: Raisecom(config)#gpon-onu uni catv 8/1/4/1	Enter the CATV interface of the GPON ONU user. slot-id/olt-id/onu-id/uni-id: slot-id refers to the slot ID; the olt-id refers to the PON interface ID; the onu-id refers to the ONU ID under the PON interface; the uni-id refers to UNI ID. It is an integer ranging from 1 to 10/1 to 16/1 to 64/1 to 24.
3	Raisecom(config-gpon-onu-catv-*/*/*:*)#shutdown	Disable the CATV interface of the GPON ONU user.

8.3.3 Checking configurations

No.	Command	Description
1	Raisecom#show epon-onu slot-id/olt-id/onu-id uni rf [uni-id] information	Show configurations of ONU RF interface.
2	Raisecom#show epon-onu slot-id/olt-id/onu-id nni catv [uni-id] information	Show ONU CATV services.

No.	Command	Description
3	Raisecom# show gpon-onu slot-id/olt-id/onu-id uni catv information	Show information about the ONU UNI CATV interface.

9 Configuring MAC address

This chapter describes basic principles and configuration process of the MAC address table for the device, and provides related configuration examples, including the following sections:

- Introduction
- Configuring dynamic MAC address
- Configuring static MAC address
- Maintenance and search
- Configuration examples

9.1 Introduction

The ISCOM6800 and ISCOM6860 support forwarding packets at the data link layer. It forwards packets to related interfaces based on destination MAC addresses of these packets. The MAC address is a Layer 2 forwarding table that records the relationship between MAC addresses and forwarding interfaces. The MAC address table is the basis for the ISCOM6800 and ISCOM6860 to quickly forward Layer 2 packets.

MAC address entries in the MAC address table consist of following information:

- Destination MAC address
- Interface ID corresponding to the destination MAC address
- VLAN ID to which an interface belongs
- Static/Dynamic flags

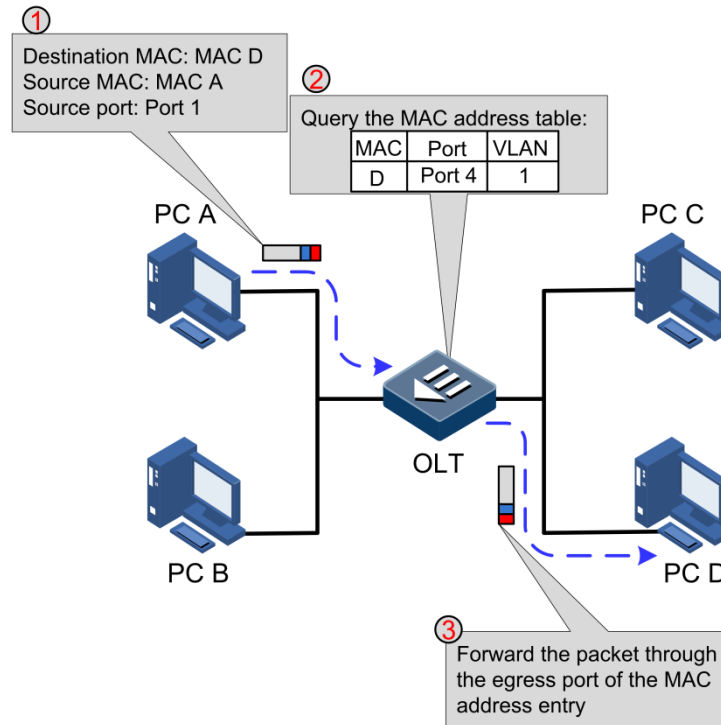
The MAC address table on the ISCOM6800 and ISCOM6860 consists of two kinds of address entries:

- Static MAC address entries: also termed as permanent addresses, you can add and remove them manually. It does not age with time. For a small network, by manually adding static addresses, you can reduce the broadcast traffic across the network.
- Dynamic MAC address entries: refers to MAC addresses that can be added through MAC address learning mechanism. Dynamic MAC addresses can be deleted when the configured aging time expires.

When forwarding packets, based on the information about MAC address entries, the ISCOM6800 and ISCOM6860 adopt following modes:

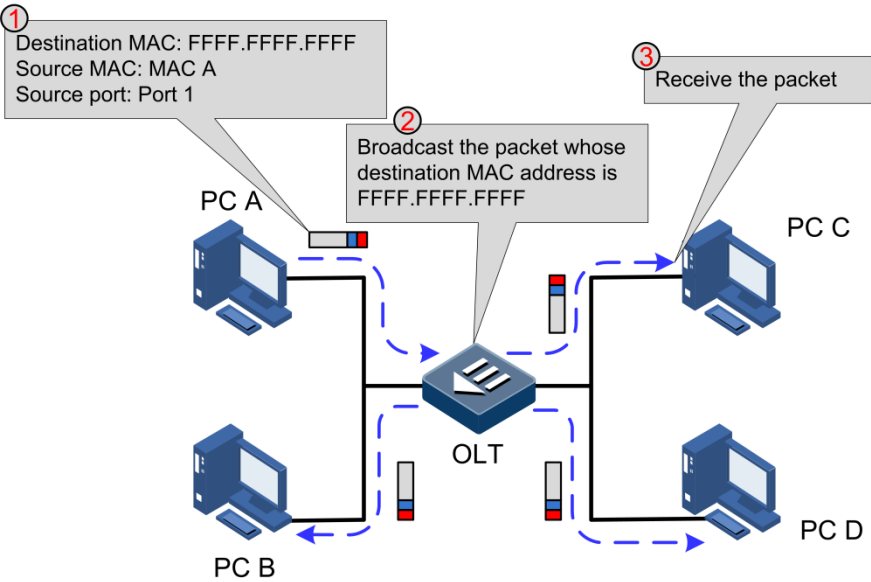
- Unicast: when a MAC address entry, which is related to the destination MAC address of a packet, is listed in the MAC address table, the device will directly forward the packet through the egress interface. Otherwise, the device will broadcast the packet, as shown in Figure 9-1.

Figure 9-1 Unicast forwarding mode of MAC address



- Multicast: when the device receives a packet whose destination address is a multicast MAC address, if the MAC address table contains an entry that is related to the destination MAC address of the packet, the device will forward the packet through the egress interface. Otherwise, the device will broadcast this packet.
- Broadcast: when the device receives an all-F packet, or when the device receives a packet whose MAC address is not listed in the MAC address table, it will flood the packet to all interfaces in the same VLAN except for the interface that receives this packet, as shown in Figure 9-2.

Figure 9-2 Broadcast forwarding mode of MAC address



9.2 Configuring dynamic MAC address

9.2.1 Preparing for configurations

Scenario

Dynamic MAC address entries can be added through the MAC address learning mechanism. You can limit the number of MAC addresses to be learnt. Dynamic MAC address entries will be deleted when the configured aging time expires, and can also be deleted manually. Dynamic MAC address entries will be cleared when the device is restarted.

Prerequisite

N/A

9.2.2 Default configurations

Default configurations of dynamic MAC address entries on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
MAC address learning	Enable
Aging time of MAC address	300s
MAC address limit	Unlimited

Default configurations of dynamic MAC address entries on the Raisecom ONU devices are as below.

Function	Default value
MAC address learning	Enable
Aging time of MAC address	300s
MAC address limit	Unlimited

9.2.3 Configuring MAC address learning

When the network scale is large or positions of hosts change frequently, using static MAC addresses will increase maintenance workload. Thus, you need to configure MAC address learning to make the device learn MAC address dynamically to implement Layer 2 forwarding.

Configuring MAC address learning of OLT

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#mac-address-table learning	Enable MAC address learning on the interface. You can use the no mac-address-table learning command to disable this function.

Configuring ONU MAC address learning

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id	Enter EPON ONU UNI configuration mode.
3	Raisecom(config-epon-onu-ethernet-*/*/*:*)#mac-address-table learning { enable disable }	Enable/Disable MAC address learning on the ONU UNI.

9.2.4 (Optional) configuring aging time of MAC address

To avoid explosive increase of the MAC address table, you need to configure the aging time for the dynamic MAC address table. The timer starts when a MAC address is added to the MAC address table, if no interface receives the frame whose source address is the MAC address in the aging time, the MAC address will be deleted from the dynamic MAC address table. Otherwise, the aging time timer will be updated and start timing again.

Configuring MAC address aging time of OLT

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# mac-address-table aging-time { 0 <i>period</i> } example: Raisecom(config)# mac-address-table aging-time 500	Configure the aging time of dynamic MAC addresses. You can use the no mac-address-table aging-time command to restore default configuration.  Note The value 0 refers to that the dynamic MAC address is not aged. • 0: aging time, the value 0 indicates no aging for dynamic MAC address entries • period: aging time, in units of second, an integer. The OLT MAC address table ranges from 10 to 1000000; the ONU MAC address table ranges from 5 to 57600.

Configuring aging time of ONU MAC address

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# epon-onu slot-id/olt-id/onu-id example: Raisecom(config)# epon-onu 3/2/1	Enter EPON ONU remote management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-list: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*/*:*)# mac-address-table aging-time { 0 <i>period</i> } example: Raisecom(config-epon-onu-3/1:1)# mac-address-table aging-time 500	Configure the aging time of the ONU dynamic MAC address. You can use the no mac-address-table aging-time command to restore default configurations.  Note The value 0 indicates that the MAC address does not age out. • 0: aging time, the parameter 0 indicates that the dynamic MAC address does not age out. • period: aging time, in units of second, an integer. The OLT MAC address table ranges from 10 to 1000000; the ONU MAC address table ranges from 5 to 57600.

9.2.5 (Optional) configuring MAC address limit

To avoid explosive increase of the MAC address table, you need to configure the MAC address limit.

Configuring OLT MAC address limit

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id example: Raisecom(config)#interface gigabitethernet 2/1	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: 1000 Mbit/s Ethernet interface configuration mode • ten-gigabitethernet: 10 Gbit/s Ethernet interface configuration mode
3	Raisecom(config-if-*-*:*)#mac-address-table threshold threshold example: Raisecom(config-if-gigabitethernet-2:1)#mac-address-table threshold 200	Configure the threshold of MAC addresses allowed to be learnt by the interface. You can use the no mac-address-table threshold command to restore default configuration. • number: MAC address learning threshold, an integer. The OLT ranges from 1 to 16000; the ONU ranges from 1 to 8190.

Configuring ONU MAC address limit

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#interface epon-onu 3/2/1	Enter EPON ONU virtual interface mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-if-epon-onu-*/*:*)#mac-address-table threshold threshold example: Raisecom(config-if-epon-onu-3/1:1)#mac-address-table threshold 100	Configure the number of MAC addresses earned by the ONU. You can use the no mac-address-table threshold command to restore default configurations. • number: MAC address learning threshold, an integer. The OLT ranges from 1 to 16000; the ONU ranges from 1 to 8190.

Configuring ONU UNI MAC address limit

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</pre> example: <pre>Raisecom(config)#epon-onu uni ethernet 3/1/1/1</pre>	Enter EPON ONU UNI configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • uni-id: ONU UNI ID
3	<pre>Raisecom(config-epon-onu-ethernet-*/*/*:*)#mac-address-table threshold { unlimited number }</pre> example: <pre>Raisecom(config-epon-onu-ethernet-3/1/1:1)#mac-address-table threshold 64</pre>	Configure the number of MAC addresses allowed to be learnt by the ONU UNI. You can use the no mac-address-table threshold command to restore default configurations. • number: the maximum number of MAC addresses allowed to be learned, an integer, ranging from 0 to 128 • unlimited: the number of MAC addresses learned is unlimited.

9.2.6 Configuring MAC address flapping

No.	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id</pre> example: <pre>Raisecom(config)#interface gigabitethernet 2/1</pre>	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode
3	<pre>Raisecom(config-if-*/*:*)#mac-address-table station move</pre>	Configure MAC address flapping.

9.2.7 Checking configurations

Checking OLT configurations

No.	Command	Description
1	<pre>Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-list mac-address-table</pre>	Show configurations of the MAC address.

No.	Command	Description
2	Raisecom#show mac-address-table 12-address [vlan <i>vlan-id</i> interface { epon-olt ten-giga-epon-olt epon-onu <i>slot-id/olt-id/onu-list</i> gpon-olt gigabitethernet ten-gigabitethernet port-channel <i>group-id</i> } <i>slot-id/port-id</i>]	Show L2 MAC address entries.
3	Raisecom#show mac aging-time	Show the aging time of MAC addresses.

Checking ONU configuraitons

No.	Command	Description
1	Raisecom#show { gpon-onu epon-onu } slot-id/olt-id/onu-id mac-address-table 12-address [uni ethernet <i>uni-id</i>] { all dynamic static } [count]	Show configurations of MAC address table on the ONU UNI.
2	Raisecom#show { gpon-onu epon-onu } slot-id/olt-id/onu-list mac-address-table aging-time	Show aging time of the ONU MAC address.
3	Raisecom#show interface epon-onu slot-id/olt-id/onu-list mac-address-table threshold	Show the number of MAC addresses that can be learned by the ONU.
4	Raisecom#show epon-onu slot-id/olt-id/onu-id mac-address-table 12-address [uni ethernet <i>uni-id</i>] { all dynamic static } [count]	Show MAC address entries of the ONU or the specified ONU UNI.
5	Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet [<i>uni-id</i>] mac-address-table	Show configurations of the MAC address tabled on the ONU UNI.

9.3 Configuring static MAC address

9.3.1 Preparing for configurations

Scenario

Static MAC address entries, also termed as permanent addresses, can be added or removed manually, and do not age with time. For a network with small changes of devices, you can add static MAC address entries manually to decrease broadcast traffic on the network.

Prerequisite

N/A

9.3.2 Default configurations

N/A

9.3.3 Configuring static unicast MAC address

Static MAC address can be set for fixed servers, special persons (manager, financial staff, and so on) fixed and important hosts to make sure all data traffic to the MAC address are forwarded from the interface related to the static MAC address related preferentially.

Configuring static unicast MAC addresses of OLT

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)#mac-address-table static unicast <i>mac-address</i> vlan <i>vlan-id</i> interface { { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } <i>slot-id/port-id</i> port-channel <i>group-id</i> epon-onu <i>slot-id/port-id/onu-id</i> } example: Raisecom(config)#mac-address-table static multicast 0100.5E00.0001 vlan 1 interface gigabitethernet 3/1	Configure static unicast MAC addresses. You can use the no mac-address-table static unicast mac-address vlan vlan-id command to delete the configuration. • mac-address: MAC address, in dotted hexadecimal notation, such as 0100.5E00.0001 • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • epon-olt slot-id/port-id: EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gpon-olt slot-id/port-id: GPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gigabitethernet slot-id/port-id: GE interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-gigabitethernet slot-id/port-id: 10GE interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-giga-epon-olt slot-id/port-id: 10G EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • port-channel group-id: aggregation group interface ID. The group-list refers to the aggregation group interface ID, ranging from 1 to 32.

Configuring static unicast MAC address of ONU

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</pre> example: <pre>Raisecom(config)#epon-onu 3/1/1</pre>	Enter EPON ONU management configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-epon-onu-*//*:*)#mac-address-table static unicast mac-address uni ethernet uni-id</pre> example: <pre>Raisecom(config-epon-onu-3/1:1)#mac-address-table static unicast 000e.5e12.3456 uni ethernet 1</pre>	Configure the static unicast address entry of the ONU. You can use the no mac-address-table static unicast mac-address command to delete the entry. - mac-address: MAC address, in hexadecimal notation, such as 000E.5E12.3456 - uni-id: UNI ID, an integer, ranging from 1 to 24

9.3.4 Configuring static multicast MAC address

Multicast mode is suitable for online video conferencing and online video on demand. If unicast is used, packets are transmitted on a node-by-node basis, which means that the times of transmission corresponds with the number of destination nodes. This mode is obviously inefficient and undesirable; if a broadcast mode that does not distinguish between targets and transmits all packets is adopted, although the data can be transmitted at one time, it is obviously impossible to distinguish the objects receiving the specified data. By means of multicast, it is possible to transfer data of all target nodes at a time and only to specific objects

Configuring static multicast MAC address of OLT.

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#mac-address-table static multicast mac-address vlan vlan-id { add remove } interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet port-channel group-id } slot-id/port-id example: Raisecom(config)#mac-address-table static multicast 0100.5E00.0001 vlan 1 interface gigabitethernet 3/1</pre>	Configure static multicast MAC address entries. You can use the no mac-address-table static multicast mac-address vlan vlan-id port-list port-list command to delete the configuration. • mac-address: multicast MAC address, in dotted hexadecimal notation, such as 0100.5E00.0001 • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • add: adding a MAC address entry • remove: deleting a MAC address entry • epon-olt slot-id/ port-id: EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gpon-olt slot-id/ port-id: GPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • gigabitethernet slot-id/ port-id: GE interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-gigabitethernet slot-id/ port-id: 10GE interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • ten-giga-epon-olt slot-id/port-id: 10G EPON interface ID. The slot-id refers to the slot ID; the port-id refers to the interface ID. • port-channel group-id: aggregation group interface ID. The group-list refers to the aggregation group interface ID, ranging from 1 to 32.

Configuring static multicast MAC address of ONU

No.	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/1/1</pre>	Enter EPON ONU management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface

No.	Command	Description
3	<pre>Raisecom(config-epon-onu-*//*:*)#mac-address-table static multicast mac-address vlan vlan-id uni ethernet uni-list</pre> <pre>Raisecom(config-epon-onu-*//*:*)#exit</pre> example: <pre>Raisecom(config-epon-onu-3/1:1)#mac-address-table static multicast 0100.5e00.0001 vlan 10 uni ethernet 1</pre>	Configure the static multicast MAC address of the ONU. You can use the no mac-address-table static multicast { mac-address all } command to delete the configuration. - mac-address: multicast MAC address, in hexadecimal notation, such as 0100.5E00.0001 - vlan-id: local VLAN of the UNI, an integer, ranging from 1 to 4094 - uni-list: UNI ID, an integer, ranging from 1 to 24
4	<pre>Raisecom(config)#mac-address-table unknown-multicast filter vlanlist vlan-list</pre> example: <pre>Raisecom(config)#mac-address-table unknown-multicast filter vlanlist 10-20</pre>	Configure the filtering VLANs of OLT unknown multicast packets. vlan-list: VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

9.3.5 Checking configurations

Checking OLT configurations

No.	Command	Description
1	<pre>Raisecom#show mac-address-table static unicast [vlan vlan-id interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet port-channel group-id } slot-id/port-id]</pre>	Show static unicast MAC addresses.
2	<pre>Raisecom#show mac-address-table statistics unicast [vlan vlan-id interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet port-channel group-id } slot-id/port-id]</pre>	Show statistics on static unicast MAC addresses.
3	<pre>Raisecom#show mac-address-table multicast [statistics]</pre>	Show static multicast MAC addresses.

Checking ONU configurations

No.	Command	Description
1	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id mac-address-table static [uni ethernet uni-id]</pre>	Show the static MAC address table of the ONU UNI.
2	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id mac-address-table multicast [uni ethernet uni-id]</pre>	Show the multicast MAC address table of the ONU.

No.	Command	Description
3	Raisecom#show epon-onu slot-id/olt-id/onu-id mac-address-table static multicast [vlan vlan-id]	Show the specified VLAN or all static multicast MAC addresses of the ONU.

9.4 Maintenance and search

9.4.1 Preparing for configurations

Scenario

The ISCOM6800 and ISCOM6860 support clearing the Layer 2 MAC address table, including:

- Clear all MAC address entries.
- Clear dynamically-learned MAC address entries.
- Clear statically-configured MAC address entries.

You can use the **search** command to search for the content of the MAC address entry and related information of the OLT or ONU.

Prerequisite

N/A

9.4.2 Default configurations

N/A

9.4.3 Clearing MAC address

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#clear [interface { epon-olt gpon-olt gigabitethernet ten-gigabitethernet ten-giga-epon- olt port-channel } slot-id/port-id] mac-address-table unicast [dynamic static] [vlan vlan-id] example: Raisecom(config)#clear interface gpon- olt 1/1 mac-address-table unicast dynamic vlan 1</pre>	Clear entries in the unicast MAC address table. • epon-olt slot-id/ port-id: EPON interface ID • gpon-olt slot-id/ port-id: GPON interface ID • gigabitethernet slot-id/ port-id: GE interface ID • ten-gigabitethernet slot-id/ port-id: 10GE interface ID • ten-giga-epon-olt slot-id/port-id: 10GEPON interface ID • port-channel group-id: aggregation group interface ID. The group-id refers to the aggregation group ID. • dynamic: clear dynamic MAC address entries. • static: clear static MAC address entries. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
3	<pre>Raisecom(config)#clear epon-onu slot- id/olt-id/onu-id mac-address-table { all dynamic static } example: Raisecom(config)#clear epon-onu 3/1/1 mac-address-table dynamic</pre>	Clear the MAC address entries in the ONU MAC address table. • slot-id/olt-id/onu-id: ONU ID. The slot-id refers to the slot ID, which is an integer; the olt-id refers to the PON ID, which is an integer; the onu-id refers to the ONU ID under the PON interface, which is an integer. • all: clear all MAC address entries. • dynamic: clear dynamic MAC address entries. • static: clear static MAC address entries.

9.4.4 Searching MAC address

Step	Command	Description
1	<pre>Raisecom#search mac-address mac-address example: Raisecom#search mac-address F04D.A22D.7B05</pre>	Search for a MAC address entry. • mac-address: MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456
2	<pre>Raisecom#search epon-onu slot- id/olt-id/onu-id mac-address- table mac-address example: Raisecom#search epon-onu 1/1/1 mac-address-table 111.1111.1111</pre>	Check ONU MAC address entries. • slot-id/olt-id/onu-id: ONU ID. The slot-id refers to the slot ID, which is an integer; the olt-id refers to the PON ID, which is an integer; the onu-id refers to the ONU ID under the PON interface, which is an integer. • mac-address: MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456

9.4.5 Tracing MAC address

Step	Command	Description
1	Raisecom#trace mac-address <i>mac-address</i> example: Raisecom#trace mac-address 000E.5E12.3456	Trace a specified MAC address. • <i>mac-address</i>: MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456

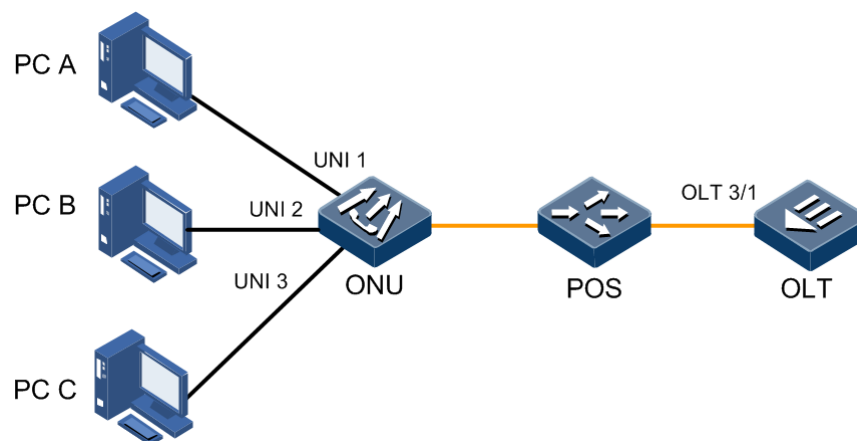
9.5 Configuration examples

9.5.1 Example for configuring dynamic MAC address

Networking requirements

As shown in Figure 9-3, the ONU is connected downstream to multiple hosts. To avoid explosive increase of the MAC address table on the ONU, you can configure the aging time of dynamic MAC address table to 100s (which takes effect only after dynamic MAC address learning is enabled), the maximum MAC addresses learned by ONU UNI2 to 128, and the aging time of the dynamic MAC address table on the OLT to 500s.

Figure 9-3 Configuring dynamic MAC address



Configuration steps

- Configure the dynamic MAC address on the OLT.

Step 1 Enable MAC address learning on OLT PON interface 3/1.

```

Raisecom#config
Raisecom(config)#interface epon-olt 3/1
Raisecom(config-if-epon-olt-3:1)#mac-address-table learning
Raisecom(config-if-epon-olt-3:1)#exit
  
```

Step 2 Configure the aging time of MAC addresses on the OLT.

```
Raisecom(config)#mac-address-table aging-time 500
Raisecom(config)#end
```

- Configure the dynamic MAC address on the ONU.

Step 3 Enable MAC address learning on the ONU.

```
Raisecom#config
Raisecom(config)#epon-onu uni ethernet 3/1/1/1
Raisecom(config-epon-onu-ethernet-3/1/1:1)#mac-address-table learning
enable
Raisecom(config-epon-onu-ethernet-3/1/1:1)#exit
Raisecom(config)#epon-onu uni ethernet 3/1/1/2
Raisecom(config-epon-onu-ethernet-3/1/1:2)#mac-address-table learning
enable
Raisecom(config-epon-onu-ethernet-3/1/1:2)#exit
Raisecom(config)#epon-onu uni ethernet 3/1/1/3
Raisecom(config-epon-onu-ethernet-3/1/1:3)#mac-address-table learning
enable
Raisecom(config-epon-onu-ethernet-3/1/1:3)#end
```

Step 4 Configure the MAC address aging time on the ONU.

```
Raisecom#config
Raisecom(config)#epon-onu 3/1/1
Raisecom(config-epon-onu-3/1:1)#mac-address-table aging-time 500
Raisecom(config-epon-onu-3/1:1)#exit
```

Step 5 Configure the MAC address limits on ONU UNI2 to 128.

```
Raisecom(config)#epon-onu uni ethernet 3/1/1/2
Raisecom(config-epon-onu-ethernet-3/1/1:2)#mac-address-table threshold
128
```

Checking results

- Checking OLT results.

Show the MAC address learning status and aging time on the OLT.

```
Raisecom#show interface epon-olt 3/1 mac-address-table
Port ID  MAC-learning  MAC-threshold
```

```
-----
epon-olt3/1      Enable      0
```

```
Raisecom#show mac aging-time
Aging time: 500 seconds
```

- Checking ONU results.

Show the configured MAC address learning status and aging time on the OLT.

```
Raisecom#show epon-onu 3/1/1 uni ethernet mac-address-table
```

```
Port ID      Learning Threshold
-----
3/1/1/1      enable      no limit
3/1/1/2      enable      128
3/1/1/3      enable      no limit
```

```
Raisecom#config
```

```
Raisecom(config)#show epon-onu 3/1/1 mac-address-table aging-time
```

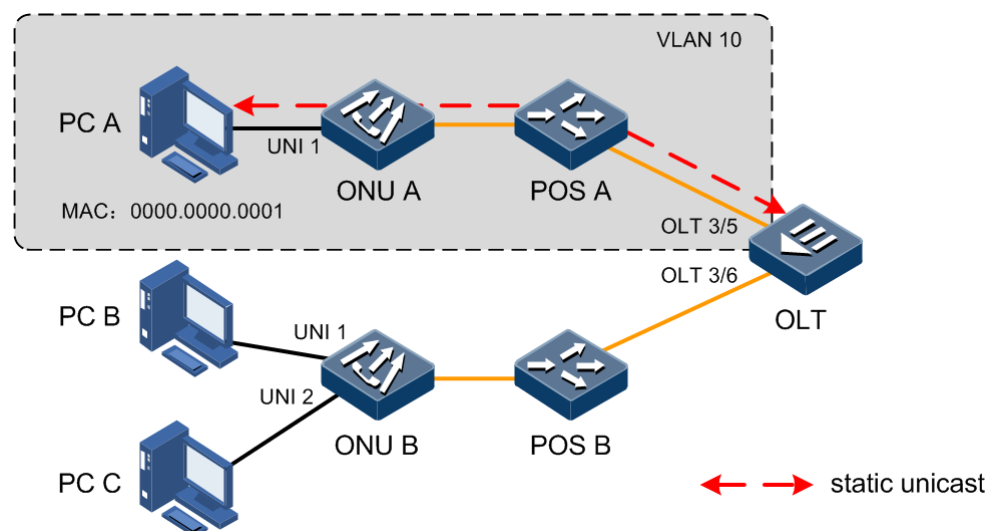
```
ONU ID      AgingTime(s)
-----
3/1/1      100
```

9.5.2 Example for configuring static MAC address

Networking requirements

As shown in Figure 9-4, PC A is in a fixed and important position. Configure a static unicast MAC address for PC A on the connected OLT and ONU. The MAC address of PC A is 0000.0000.0001. PC A belongs to VLAN 10.

Figure 9-4 Configuring static MAC address



Configuration steps

- Configure a static unicast MAC address on the OLT.

Step 1 Create a VLAN and configure the interface mode on the OLT.

```
Raisecom#config
Raisecom(config)#create vlan 10 active
Raisecom(config)#interface epon-olt 3/5
Raisecom(config-if-epon-olt-3:5)#switchport mode trunk
Raisecom(config-if-epon-olt-3:5)#switchport trunk allowed vlan 10
Raisecom(config-if-epon-olt-3:5)#exit
```

Step 2 Configure a static unicast MAC address on the OLT.

```
Raisecom(config)#mac-address-table static unicast 0000.0000.0001 vlan 10
interface epon-olt 1/5
Raisecom(config)#end
```

- Configure a static unicast MAC address on the ONU.

Step 3 Create a VLAN on the ONU and configure interface mode.

```
Raisecom#config
Raisecom(config)#epon-onu uni ethernet 3/5/1/1
Raisecom(config-epon-onu-ethernet-3/5/1:1)#vlan mode tagged
Raisecom(config-epon-onu-ethernet-3/5/1:1)#native vlan 10
Raisecom(config-epon-onu-ethernet-3/5/1:1)#exit
Raisecom(config)#epon-onu uplink
Raisecom(config-epon-onu-uplink)#vlan mode transparent
Raisecom(config-epon-onu-uplink)#exit
```

Step 4 Configure a static unicast MAC address on the ONU.

```
Raisecom(config)#epon-onu 3/5/1
Raisecom(config-epon-onu-3/5:1)#mac-address-table static unicast
0000.0000.0001 uni ethernet 1
```

Checking results

- Check OLT results.

Show information about the MAC address under a VLAN on the OLT.

```
Raisecom#show mac-address-table 12-address vlan 10
Mac Address      Port          Vlan  Flags
-----
0000.0000.0001   epon-olt3/5   10    Static
```

- Check ONU results.

Show information about the static unicast MAC address on the ONU.

```
Raisecom#show epon-onu 3/5/1 mac-address-table static uni ethernet 1
Port ID      Static Mac Address
-----
3/5/1/1      0000.0000.0001
```

10 Configuring VLAN

This chapter describes the VLAN features and configuration process of the device, and provides related configuration examples, including the following sections:

- Introduction
- Configuring VLAN
- Configuring QinQ
- Configuring VLAN ACL
- Configuring VLAN partitioning
- Configuring VLAN mapping
- Configuring virtual interface
- Configuration examples

10.1 Introduction

10.1.1 VLAN

Overview

When too many PCs work in a network, a number of broadcast traffic will be generated. This will reduce network performance, even worse, making the network collapsed. To ensure PCs work at a high speed in the network, you must partition broadcast domains to reduce broadcast traffic. That is why Virtual Local Area Network (VLAN) technology is introduced.

VLAN is a Layer 2 isolation technology that is used to partition devices in a Local Area Network (LAN) logically instead of physically to network segments. Therefore multiple distinct virtual broadcast domains are created. By partitioning the VLAN, you can isolate hosts that do not need to communicate with others. Therefore, the broadcast traffic is reduced and fewer broadcast storms are generated.

A VLAN is a logical subnet or a broadcast domain. PCs in a VLAN can be located at different places. You can add any PC to a VLAN as required.

Hosts in a VLAN can receive data frames sent by other hosts in the same VLAN. However, they cannot receive data frames sent by hosts in other VLANs. Hosts in different VLANs can communicate through a router or a Layer 3 switch.



Note

Broadcast domain refers to a collection of devices that can receive broadcast packets sent by any device in a network. If the broadcast domain and broadcast traffic are over great, network performance will be reduced. What's worse, the network will collapse. Therefore, you must partition broadcast domain to improve network performance when establishing a network. You can partition a broadcast domain either by routers or by partitioning VLANs on a switch.

Advantages of VLAN

By partitioning VLANs, you can realize:

- Portioning broadcast domains and reducing broadcast storms
- Improving network security
- Simplifying network management

Working principle of VLAN

After you partition VLANs on a switching device, the device will be virtualized as multiple switching devices. The switching devices learn MAC addresses and forwarding packets based on VLAN. Each VLAN has an independent MAC address table.

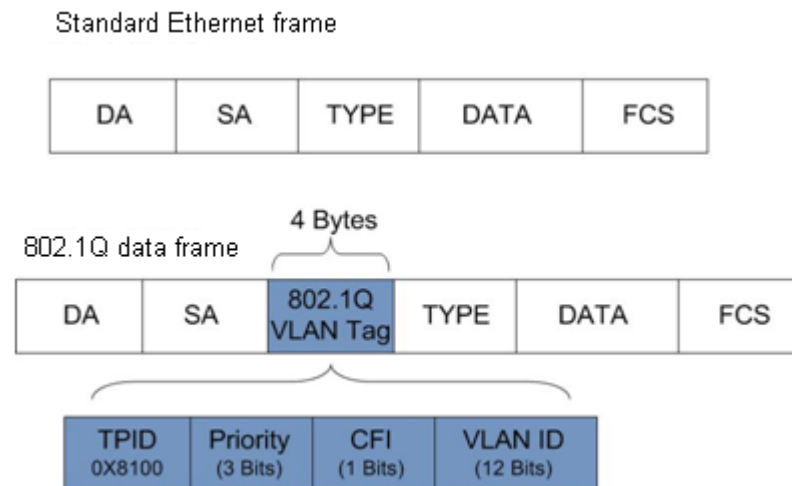
When a frame is sent to the ingress interface of a device, the device will query the VLAN where the ingress interface is and then query the MAC address table to which the VLAN is related. If the destination MAC address of the frame is listed in the MAC address table, the frame will be forwarded. Otherwise, the frame is discarded.

802.1Q protocol and VLAN Tag

After partitioning VLANs, to identify frames from different VLANs, you can use 802.1Q protocol to add VLAN Tags to them.

The 802.1Q protocol defines a new Ethernet field. Compared with the Ethernet frame, 802.1Q frame has a 4-Byte 802.1Q VLAN Tag field, which is added after the SA field. Figure 10-1 shows structures of Ethernet frame and 802.1Q frame.

Figure 10-1 Structures of Ethernet frame and 802.1Q frame



- Tag Protocol Identifier (TPID): a new type defined by IEEE to identify the frame as an IEEE 802.1Q-tagged frame. The 802.1Q TPID is 0x8100.
- VLAN Identifier (VID): a 12-bit field specifying the VLAN to which the frame belongs. The value ranges from 0 to 4095. VLAN 0 and VLAN 4095 are reserved VLANs. So the general range is 1 to 4094.
- Canonical Format Indicator (CFI): a 1-bit field used for compatibility among bus Ethernet, FDDI, and Token Ring networks.
- Priority Code Point (PCP): a 3-bit field which indicates the frame priority. Values are from 0 (best effort) to 7 (highest). The bigger the number is, the higher the priority is. When the network is congested, the device sends packets with higher priorities first.

VLAN mode of OLT interface

The interface on the ISCOM6800 and ISCOM6860 support two modes: Access mode and Trunk mode.

Table 10-1 lists comparison of VLAN modes and packet processing modes.

Table 10-1 VLAN modes and packet processing modes

Interface type	Processing ingress packets		Processing egress packets
	Untagged packet	Tagged packet	
Access	Add the Tag of the Access VLAN to the packet.	• If the VLAN ID for a packet is identical to the Access VLAN, receive the packet. • If the VLAN ID for a packet is not identical to the Access VLAN, discard the packet.	If the VLAN ID for a packet is identical to the Access VLAN ID, send the packet after removing the Tag.

Interface type	Processing ingress packets		Processing egress packets
	Untagged packet	Tagged packet	
Trunk	If the Native VLAN is in the VLAN ID list on an interface, receive the packet after adding the Tag of the Native VLAN to the packet.	• If the VLAN ID for a packet is in the VLAN ID list on an interface, receive the packet. • If the VLAN ID for a packet is not in the VLAN ID list on an interface, discard the packet.	• If the VLAN ID for a packet is identical to the Native VLAN ID, send the packet after removing the Tag. • If the VLAN ID for a packet is not identical to the Native VLAN ID, send the packet with its original Tag. Otherwise, discard the packet.

VLAN modes of ONU interface

Raisecom ONUs supports the following VLAN modes:

- VLAN Transparent mode
- VLAN Tagged mode
- VLAN Translation mode
- VLAN Trunk mode

Specific behaviours of various VLAN modes are shown as below.

Table 10-2 lists how ONU interfaces to process Ethernet frames in VLAN Transparent mode.

Table 10-2 Processing modes of Ethernet frames in VLAN Transparent mode

Direction	With/Without Tag	Processing mode
Uplink	With VLAN Tag	Forward Ethernet packets without any change (reserve the original VLAN Tag).
	Without VLAN Tag	Forward Ethernet packets without any change.
Downlink	With VLAN Tag	Forward Ethernet packets without any change (reserve the original VLAN Tag).
	Without VLAN Tag	Forward Ethernet packets without any change.

Table 10-3 lists how ONU interfaces to process Ethernet frames in VLAN Tagged mode.

Table 10-3 Processing modes of Ethernet frames in VLAN Tagged mode

Direction	With/Without Tag	Processing mode
Uplink	With VLAN Tag	Discard Ethernet packets.
	Without VLAN Tag	Forward Ethernet packets by adding new VLAN Tags (Native VLAN of the interface).

Direction	With/Without Tag	Processing mode
Downlink	With VLAN Tag	Forward Ethernet packets to related UNI based on VID and remove their VLAN Tags. If VLAN IDs of downlink Tagged packets are not identical to the configured ones, these packets are discarded.
	Without VLAN Tag	Discard Ethernet packets.

Table 10-4 lists the mode used by the ONU to process Ethernet frames in VLAN Translation mode.

Table 10-4 Processing modes of Ethernet frames in VLAN Translation mode

Direction	With/Without Tag	Processing mode
Uplink	With VLAN Tag	If VIDs of the original Tags have related entries (input VIDs) in VLAN Translation list of the related interface, forward Ethernet packets after translating VIDs into related VIDs (output VIDs). Otherwise, Ethernet packets are discarded.
	Without VLAN Tag	Forward Ethernet packets by adding native VLANs to Untagged packets.
Downlink	With VLAN Tag	If VIDs of the original Tags have related entries (input VIDs) in VLAN Translation list of the related interface, forward Ethernet packets after translating VIDs into related VIDs (output VIDs). Otherwise, Ethernet packets are discarded. If VIDs of the original Tags are native VIDs, forward Ethernet packets after removing their Tags.
	Without VLAN Tag	Discard Ethernet packets.

Table 10-5 lists the mode used by the ONU to process Ethernet frames in VLAN Trunk mode.

Table 10-5 Processing modes of Ethernet frames in VLAN Trunk mode

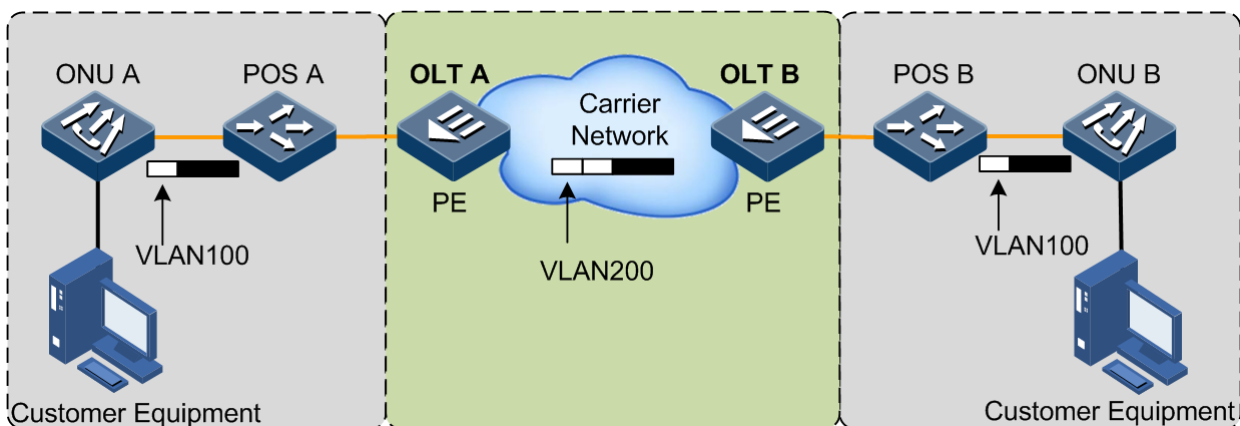
Direction	With/Without Tag	Processing mode
Uplink	With VLAN Tag	If VLANs carried by Ethernet packets are in allowed VLAN list of the interface, forward these Ethernet packets. Otherwise, discard these Ethernet packets.
	Without VLAN Tag	Forward Ethernet packets by adding native VLANs to Untagged packets.
Downlink	With VLAN Tag	If VLANs carried by Ethernet packets are in allowed VLAN list of the interface, forward these Ethernet packets. Otherwise, discard these Ethernet packets. If VLAN IDs carried by Ethernet packets are native VLANs, forward these Ethernet packets.
	Without VLAN Tag	Discard Ethernet packets.

10.1.2 QinQ

QinQ technology is an extension of 802.1Q, which is defined in the 802.1ad standard defined by the IEEE.

Basic QinQ is a simple Layer 2 VPN tunnel technique, which encapsulates outer VLAN Tag for user private network packet at the carrier access end. The packet takes double VLAN Tag to transmit through backbone network (public network) of carrier. In the public network, the packet is transmitted according to the outer VLAN Tag (public VLAN Tag). And the private VLAN Tag is transmitted as the data in the packet.

Figure 10-2 Basic QinQ networking



As shown in Figure 10-2, the OLT is the Provider Edge (PE). Its uplink interface is connected to the Carrier network and the PON interface is connected to the user network through ONUs.

A packet is sent to the PE by a customer equipment, carrying a Tag VLAN 100. When passing through the uplink interface of the PE, the packet is added with an outer Tag VLAN 200. And then the packet is sent to the Carrier network through the uplink interface of the PE.

When the packet with the outer Tag is sent to the peer PE, this PE will remove the outer Tag of the packet and then send the packet to the customer equipment. In this case, the packet only carries the Tag VLAN 100.

10.1.3 VLAN mapping

VLAN mapping is mainly used to replace the private VLAN Tags of Ethernet packets with Carrier's VLAN Tags, so that packets will be transmitted according to Carrier's VLAN forwarding rules. When packets are sent to the peer private network from the Carrier network, these VLAN Tags recover to the original private VLAN Tags, according to the same VLAN forwarding rules. Therefore, packets are correctly sent to the destination.

When two or more user networks, which connect the Carrier network, communicate with each other, these user networks define different service access requirements and various VLAN Tags for all packets. When the Carrier network performs Layer 2 switching on packets, with VLAN mapping, the Carrier's access device will replace VLAN Tags of these packets with VLAN Tags defined by the Carrier. According to the switching mode and route defined by the Carrier, packets are forwarded to the destination. When packets are sent to the peer user network from the Carrier network, the Carrier defined VLAN Tags are replaced with VLAN Tags that can be recognized by the user network. Then the peer user network performs the Layer 2 addressing among the VLAN Tags to access to destination hosts.

When the OLT receives packets with private VLAN Tags, it will match the private VLAN Tags according to configured VLAN mapping rules. If success, the private VLAN Tags are replaced according to configured VLAN mapping rules. VLAN mapping provides the following modes:

- 1:1 VLAN mapping: the VLAN Tag carried by a packet from a specified VLAN is replaced with a new VLAN Tag.
- N:1 VLAN mapping: different VLAN Tags carried by packets from two or more VLANs are replaced with the same VLAN Tag

10.2 Configuring VLAN

10.2.1 Preparing for configurations

Scenario

The main function of VLAN is to divide logic network segments. There are 2 typical application modes:

- In a small-scale LAN, you can partition multiple VLANs on a Layer 2 device, separating hosts logically. In this case, hosts in the same VLAN can communicate with each other, while hosts in different VLANs cannot.
- In a large-scale LAN or enterprise network, there are many hosts. The hosts in the same department are located at different places but they need to communicate with each other. You can configure VLANs on multiple interconnected Layer 2 devices to make hosts in the same VLAN communicate with each other and hosts in different VLANs unable to communicate. If hosts in different VLANs need to communicate, use a Layer 3 device, such as a router.

Prerequisite

N/A

10.2.2 Default configurations

Default configurations of VLAN on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Interface TPID	0x8100
Filter type of uplink data packets on interface	All (allow all packets to pass)
VLAN processing mode on interface	• Uplink: Access • Downlink: Access
New priority used by the interface to add VLAN Tag to data	• Uplink: 0 • Downlink: 0
Enable/Disable the interface to use a new priority when adding VLAN Tag to data	• Uplink: disable • Downlink: disable

Function	Default value
VLAN ID used by the interface to add VLAN Tag to data	• Uplink: 1 • Downlink: 1

Default configurations of VLAN on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
UNI VLAN processing mode	Transparent
UNI default VLAN	1
UNI default priority	0
VLAN processing mode of the uplink interface	Transparent

10.2.3 Configuring OLT interface VLAN

Creating VLAN

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# create vlan <i>vlan-id</i> { active suspend } example: Raisecom(config)#create vlan 10 active	Create a VLAN. You can use the no vlan { all <i>vlan-id</i> } command to delete the VLAN. • vlan-id: VLAN ID, an integer, ranging from 2 to 4094. Multiple VLANs can be created concurrently. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • active: VLAN is active. Packets are allowed to pass. • suspend: VLAN is suspended. Packets are not allowed to pass.
3	Raisecom(config)# vlan <i>vlan-id</i> example: Raisecom(config)#vlan 1	Enter VLAN configuration mode.  Note If the VLAN has not been created, the system creates a VLAN automatically when you use this command, and the VLAN is in suspended status. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094. Enter the configuration mode of the VLAN to configure the VLAN. The VLAN will be automatically created if it is not created.
4	Raisecom(config-vlan-*)# name <i>name</i> example: Raisecom(config-vlan-*)#name product	(Optional) configure the VLAN name. You can use the no name command to restore default configuration. • name: VLAN name, a string of 1 to 15 characters

Step	Command	Description
5	Raisecom(config-vlan-*)# state { active suspend } example: Raisecom(config-vlan-*)#state active	(Optional) configure the VLAN status. • active: VLAN is active and available. Packets are allowed to pass. • suspend: VLAN is suspended and unavailable. Packets are not allowed to pass.
6	Raisecom(config-vlan-*)# p2p { enable disable }	(Optional) enable/disable VLAN intercommunication.



Note

- VLAN 1 is the default VLAN. All interfaces in Access mode belong to the default VLAN. VLAN 1 cannot be created and deleted.
- By default, VLANs are named by "VLAN + 4-digit VLAN ID". For example, VLAN 1 is named VLAN 0001 by default, and VLAN 4094 is named as VLAN 4094 by default.
- All configurations of VLAN are not effective until the VLAN is activated. When the VLAN is in suspended status, you can configure the VLAN, such as deleting/adding interfaces and setting VLAN name. The configurations will be saved by the system. Once the VLAN is activated, the configurations will take effect in the system.

Configuring interface VLAN mode

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } <i>slot-id/port-id</i> example: Raisecom(config)#interface gigabitethernet 2/1	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: 1000 Mbit/s Ethernet interface configuration mode • ten-gigabitethernet: 10 Gbit/s Ethernet interface configuration mode
3	Raisecom(config-if-*-*)# switchport mode { access trunk } example: Raisecom(config-if-gigabitethernet-2/1)#switchport mode trunk	Configure the VLAN mode. You can use the no switchport mode command to restore default configurations. • access: configure the interface to Access mode. • trunk: configure the interface to Trunk mode.

Configuring interface VLAN of Access mode

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)# interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } <i>slot-id/port-id</i> example: Raisecom(config)#interface gigabitethernet 2/1	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: 1000 Mbit/s Ethernet interface configuration mode • ten-gigabitethernet: 10 Gbit/s Ethernet interface configuration mode
3	Raisecom(config-if- <i>*-*</i> :*)# switchport mode access	Configure the VLAN mode of the interface to Access.
4	Raisecom(config-if- <i>*-*</i> :*)# switchport access vlan <i>vlan-id</i> example: Raisecom(config-if-gigabitethernet-2/1)#switchport access vlan 10	Configure the default VLAN for the interface in Access mode. You can use the no switchport access vlan command to restore default configuration. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
5	Raisecom(config-if- <i>*-*</i> :*)# vlan drop-untagged	(Optional) configure the interface to discard the untagged packet. You can use the no vlan drop-untagged command to restore default configuration.



Note

- If the VLAN is not created and activated when you configure the default VLAN for the Access interface, the system will create and activate the VLAN automatically.
- If the Access VLAN is deleted or suspended by users manually, the system will configure the Access VLAN of the interface as default VLAN 1 automatically.
- The Access interface-allowed VLAN list is only effective to the static VLAN.

Configuring interface VLAN of Trunk mode

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } <i>slot-id/port-id</i> example: Raisecom(config)#interface gigabitethernet 2/1	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode
3	Raisecom(config-if- <i>*-*</i> :*)# switchport mode trunk	Configure the VLAN mode of the interface to Trunk.

Step	Command	Description
4	<pre>Raisecom(config-if-*-*:*)#switchport trunk native vlan <i>vlan-id</i> example: Raisecom(config-if-gigabitethernet-3/1)#switchport trunk native vlan 10</pre>	Configure the Native VLAN of the interface. You can use the no switchport trunk native vlan command to restore default configuration. • vlan-id:VLAN ID, an integer, ranging from 1 to 4094
5	<pre>Raisecom(config-if-*-*:*)#switchport trunk allowed vlan { all [add remove] <i>vlan-list</i> } [confirm] example: Raisecom(config-if-gigabitethernet-3/1)#switchport trunk allowed vlan 10,20</pre>	Configure the VLAN ID allowed to pass by the Trunk interface. You can use the no switchport trunk allowed vlan command to restore default configuration.  Note By default, the Trunk interface allows all VLANs to pass. • all: the Trunk interface allows all VLANs to pass. • vlan-list: VLAN list allowed to pass by the Trunk interface, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • confirm: confirmed. After configuration, there is no prompt for entering the confirmation information. • add add-vlan-list: add VLANs allowed to pass to the original VLAN list. • add-vlan-list: added VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • remove remove-vlan-list: delete the VLANs that are allowed to pass from the original VLAN list. • remove-vlan-list: deleted VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

Step	Command	Description
6	<pre>Raisecom(config-if-*-*:*)#switchport trunk untagged vlan { all [add remove] vlan-list } [confirm] example: Raisecom(config-if- gigabitethernet-3/1)#switchport trunk untagged vlan 10,20</pre>	(Optional) configure the Trunk egress interface to remove the tagged VLAN ID. You can use the no switchport trunk untagged vlan command to restore default configuration. • all: the VLAN tags of all tagged packets sent by all Trunk interfaces will be removed and become untagged frames. • vlan-list: the tag should be removed when the Trunk interface sends frames. An integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • confirm: confirmed • add add-vlan-list: add VLANs allowed to pass to the original VLAN list. • add-vlan-list: added VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • remove remove-vlan-list: delete the VLANs that are allowed to pass from the original VLAN list. • remove-vlan-list: deleted VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
7	<pre>Raisecom(config-if-*-*:*)#vlan drop-untagged</pre>	(Optional) configure the interface to discard the untagged packet. You can use the no vlan drop-untagged command to restore default configuration.



Note

- The Trunk interface allows Native VLAN packets to pass regardless of configurations on Trunk interface allowed VLAN list and Untagged VLAN list. The forwarded packets do not carry VLAN TAG.
- When you configure the Native VLAN, the system will create and activate the VLAN automatically if the VLAN is not created and activated in advance.
- The system will configure the Trunk Native VLAN as the default VLAN if the Native VLAN is deleted or blocked manually.
- The Trunk interface allowed VLAN list and Trunk Untagged VLAN list are only effective to the static VLAN.

10.2.4 Configuring VLAN on ONU UNI

Configuring VLAN mode

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</pre> example: <pre>Raisecom(config)#epon-onu uni ethernet 3/1/1/1</pre>	Enter ONU UNI Ethernet interface configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface - uni-id: ONU UNI interface ID
3	<pre>Raisecom(config-epon-onu-ethernet- *//*/*)#vlan mode { tagged translation transparent trunk aggregation }</pre> example: <pre>Raisecom(config-epon-onu-ethernet- 3/1/1:1)#vlan mode tagged</pre>	Configure the VLAN mode. You can use the no vlan mode command to restore default configurations. - aggregation: VLAN aggregation mode - tagged: VLAN tagging mode - translation: VLAN translation mode - transparent: transparent transmission mode - trunk: Trunk mode

Configuring VLAN translation rules

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#vlan translation-rule rule-id old vlan-id priority new vlan-id priority</pre> example: <pre>Raisecom(config)#vlan translation-rule 1 old 10 1 new 20</pre>	Create a VLAN translation rule. You can use the no vlan translation-rule { rule-id all } command to delete the VLAN translation rule. - rule-id: VLAN translation rule ID, an integer, ranging from 1 to 1024 - old: old VLAN - new: new VLAN - vlan-id: VLAN ID, an integer, ranging from 1 to 4094 - priority: VLAN priority, an integer, ranging from 0 to 7
3	<pre>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu- id/uni-id</pre> example: <pre>Raisecom(config)#epon-onu uni ethernet 3/1/1/1</pre>	Enter ONU UNI Ethernet interface configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface - uni-id: ONU UNI ID
4	<pre>Raisecom(config-epon-onu- ethernet-*//*/*)#vlan translation-rule rule-list</pre> example: <pre>Raisecom(config-epon-onu- ethernet-3/1/1:1)#vlan translation-rule 1</pre>	Apply the VLAN translation rule to the ONU UNI. You can use the no vlan translation-rule command to restore default configurations. rule-list: VLAN translation rule list, an integer, ranging from 1 to 1024. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".



Note

- The rule ID created and the rule contents must be unique.

- The rule after being created cannot be modified. If you need to modify it, you have to delete it and recreate one.
- The rule which is referenced by the UNI cannot be deleted. If you need to delete it, you should cancel the reference relationship first.

Configuring VLAN aggregation rules

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# vlan aggregation-rule <i>rule-id</i> [name <i>name</i>] vlan-list <i>vlan-list</i> target <i>vlan-id</i> example: Raisecom(config)#vlan aggregation-rule 1	Create a VLAN aggregation rule. You can use the no vlan aggregation-rule { all rule-list } command to delete the configurations. • rule-id: aggregation rule ID, an integer, ranging from 1 to 2048 • name: aggregation rule name, a string of 1 to 4 characters
3	Raisecom(config)# vlan aggregation-rule <i>rule-id</i> name <i>name</i> [vlan-list <i>vlan-list</i> target <i>vlan-id</i>] example: Raisecom(config)#vlan aggregation-rule 1 name rule	(Optional) configure the VLAN aggregation rule name. You can use the no vlan aggregation-rule { all rule-list } command to delete the configurations. • rule-id: aggregation rule ID, an integer, ranging from 1 to 2048 • name: aggregation rule name, a string of 1 to 4 characters
4	Raisecom(config)# epon-onu uni ethernet <i>slot-id/olt-id/onu-id/uni-id</i> example: Raisecom(config)#epon-onu uni ethernet 3/1/1/1	Enter ONU UNI Ethernet interface configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • uni-id: ONU UNI ID
5	Raisecom(config-epon-onu-ethernet-*/*//*:*)# vlan aggregation-rule <i>rule-list</i> example: Raisecom(config-epon-onu-ethernet-3/1)#vlan aggregation-rule 1	Apply VLAN aggregation rules to the ONU UNI. You can use the no vlan aggregation-rule command to restore default configurations. • rule-list: aggregation rule ID, an integer, ranging from 1 to 2048. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".



Note

- The rule ID created and the rule contents must be unique.
- The rule after being created cannot be modified. If you need to modify it, you have to delete it and recreate one.
- The rule which is referenced by the UNI cannot be deleted. If you need to delete it, you should cancel the reference relationship first.

Configuring default VLAN on UNI

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id example: Raisecom(config)#epon-onu uni ethernet 3/2/1/1	Enter ONU UNI Ethernet interface configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • uni-id: ONU UNI ID
3	Raisecom(config-epon-onu-ethernet-*/*/*:*)#native vlan vlan-id [priority] example: Raisecom(config-epon-onu-ethernet-3/2/1:1)#native vlan 10	Configure the default VLAN and priority of the ONU UNI. You can use the no native vlan command to restore default configurations.  Note This command takes effect only in Tag, Trunk, and Translation interface VLAN modes. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • priority: VLAN priority, an integer, ranging from 0 to 7

Configuring Trunk VLAN

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id example: Raisecom(config)#epon-onu uni ethernet 3/2/1/1	Enter ONU UNI Ethernet interface configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • uni-id: ONU UNI ID
3	Raisecom(config-epon-onu-ethernet-*/*/*:*)#vlan trunk allowed vlan-list example: Raisecom(config-epon-onu-ethernet-3/1/1:1)#vlan trunk allowed 10	Configure the VLAN ID allowed to pass by the ONU UNI in Trunk mode. You can use the no vlan trunkd allowed command to restore default configurations. • vlan-list: VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

Configuring QinQ on UNI

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)# epon-onu <i>slot-id/olt-id/onu-id</i> example: Raisecom(config)#epon-onu 2/1/1	Enter EPON ONU remote management configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*//*:*)# vlan double-tagging { enable disable }	Enable/Disable ONU QinQ.
4	Raisecom(config-epon-onu-*//*:*)# vlan double-tagging tpid <i>tpid</i> example: Raisecom(config-epon-onu-2/1:1)#vlan double-tagging tpid 9101	Configure the TPID of the external label. tpid: TPID, in hexadecimal notation, ranging from 0x0600 to 0xFFFF

10.2.5 Configuring VLAN on ONU SNI

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# epon-onu <i>slot-id/olt-id/onu-id sni</i> example: Raisecom(config)#epon-onu 2/1/1 sni	Enter EPON ONU SNI configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-sni-*//*:*)# vlan mode { transparent trunk } example: Raisecom(config-epon-onu-sni-1/5:1)#vlan mode trunk	Configure the VLAN mode of the SNI. You can use the no vlan mode command to restore default configurations. - transparent: transparent transmission mode - trunk: Trunk mode
4	Raisecom(config-epon-onu-sni-*//*:*)# vlan trunk allowed <i>vlan-list</i> example: Raisecom(config-epon-onu-ethernet-3/1/1:1)#vlan trunk allowed 10	Configure the VLAN ID allowed to pass by the SNI in Trunk mode. You can use the no vlan trunkd allowed command to restore default configurations. vlan-list: VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

10.2.6 Checking configurations

No.	Command	Description
1	Raisecom# show vlan [<i>vlan-list</i> static dynamic]	Show VLAN configurations.
2	Raisecom# show vlan [<i>vlan-list</i>] member-port	Show information about the VLAN member interface and untagged interface.

No.	Command	Description
3	Raisecom# show epon-onu slot-id/olt-id/onu-list vlan	Show configurations of ONU VLAN.
4	Raisecom# show onu-remote vlan translation-rule [rule-list]	Show the created VLAN translation rules of the ONU.
5	Raisecom# show onu-remote vlan aggregation-rule [rule-list]	Show the created VLAN aggregation rules of the ONU.
6	Raisecom# show epon-onu slot-id/olt-id/onu-id uplink vlan	Show VLAN configurations on the ONU SNI.
7	Raisecom# show epon-onu slot-id/olt-id/onu-id uni ethernet [uni-id] vlan	Show VLAN configurations of the ONU UNI.
8	Raisecom# show interface { epon-olt slot-id/olt-id gpon-olt slot-id/olt-id gigabitethernet slot-id/olt-id ten-giga-epon-olt slot-id/olt-id } switchport vlan-access-list	Show configurations of the VLAN ACL on the physical interface.
9	Raisecom# show epon-onu slot-id/olt-id/onu-list lan-vlan information	Show configurations of the VLAN, IP address, and DHCP server of the EPON ONU.

10.3 Configuring QinQ

10.3.1 Preparing for configurations

Scenario

With application of basic QinQ, you can add outer VLAN Tag to plan the VLAN ID freely for the private network so as to make the data at both ends of carrier network transmitted transparently without conflicting with the VLAN ID in the Internet Service Provider's (ISP) network.

Prerequisite

N/A

10.3.2 Default configurations

Default configurations of QinQ on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
TPID of outer Tag	0x8100
Basic QinQ	Disable

10.3.3 Configuring basic QinQ

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } <i>slot-</i> <i>id/port-id</i> example: Raisecom(config)#interface gigabitethernet 2/1	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode
3	Raisecom(config-if-*:*:*)#vlan dot1q-tunnel	Enable basic QinQ on the interface. You can use the no vlan dot1q-tunnel to disable this function.
4	Raisecom(config-if-*:*:*)#vlan tpid tpid example: Raisecom(config-if- gigabitethernet-2/1)#vlan tpid 8101	Configure the outer TPID. You can use the no vlan tpid command to restore default configuration. • tpid: TPID, in hexadecimal notation, such as FFFF, ranging from 0x0600 to 0xFFFF



Note

- After QinQ is enabled, the interface processes the received tagged packets as untagged packets, namely, adding outer VLAN Tags to original packets.
- After QinQ is enabled, configurations for the outer VLAN are the same with those for the general VLAN. For details, refer to section 10.2.3 Configuring OLT interface VLAN.

10.3.4 Checking configurations

No.	Command	Description
1	Raisecom#show interface [ten-gigabitethernet gigabitethernet epon-olt ten-giga-epon-olt gpon-olt] <i>slot-id/olt-id</i> vlan-mapping	Show QinQ configurations.

10.4 Configuring VLAN ACL

10.4.1 Preparing for configurations

Scenario

With VLAN ACL, you can flexibly match the source MAC address, SVLAN, CVLAN, CoS, and Ethernet type in Layer 2 packets, and the source IPv4 address, destination IPv4 address and IP type in Layer 3 packets by configuring matching rules, and configure actions on different packets according to the matching situation, such as adding outer VLANs, modifying inner VLANs, and so on.

Prerequisite

N/A

10.4.2 Default configurations

N/A

10.4.3 Creating ACL

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#vlan-access-list <i>list-number</i>	Create a VLAN ACL and enter the VLAN ACL configuration mode. You can use the no vlan-access-list <i>acl-number</i> command to delete the ACL.
3	Raisecom(config-vlan-acl)#description <i>desc-string</i>	(Optional) configure the VLAN ACL description. You can use the no description command to restore to the default condition.
4	Raisecom(config-vlan-acl)#rule <i>rule-number</i>	Create a VLAN ACL sub-rule and enter sub-rule configuration mode. You can use the no rule <i>rule-number</i> command to delete the sub-rule.
5	Raisecom(config-vlan-acl-*<i>-rule</i>-*)#access-type { permit deny }	Configure the access type of the sub-rule.

10.4.4 Configuring matching contents

Configuring IPv4 matching contents

Step	Command	Description
1	Raisecom(config-vlan-acl-*<i>-rule</i>-*)#match mac source <i>mac-address</i> [<i>mask</i>]	(Optional) match the source MAC address.

Step	Command	Description
2	Raisecom(config-vlan-acl-* <i>-rule</i> -*)# match svlan <i>vlan-id</i> [mask <i>mask-value</i>]	(Optional) match the SVLAN ID.
3	Raisecom(config-vlan-acl-* <i>-rule</i> -*)# match cvlan <i>vlan-id</i>	(Optional) match the CVLAN ID.
4	Raisecom(config-vlan-acl-* <i>-rule</i> -*)# match ethertype { <i>frame-type frame-type-mask</i> arp eapol flowcontrol ip loopback mpls mpls-mcast pppoe pppoedisc x25 x75 }	(Optional) match the protocol type in the Layer 2 frame header.
5	Raisecom(config-vlan-acl-* <i>-rule</i> -*)# match ip { destination-address source-address } <i>ip-address</i> [mask]	(Optional) match the source and destination IP address.
6	Raisecom(config-vlan-acl-* <i>-rule</i> -*)# match ip protocol { <i>protocol-num</i> ahp esp gre icmp igmp igrp ipinip ospf pcp pim tcp udp }	(Optional) match the IP upper-layer protocol type.
7	Raisecom(config-vlan-acl-* <i>-rule</i> -*)# match ip tcp destination-port { <i>port-id</i> bgp domain echo exec finger ftp ftp-data gopher hostname ident irc klogin kshell login lpd nntp pim-auto-rp pop2 pop3 smtp sunrpc tacacs talk telnet time uucp whois www }	(Optional) match the destination port ID of TCP packets. You can use the no match ip tcp destination-port command to delete the configuration.
8	Raisecom(config-vlan-acl-* <i>-rule</i> -*)# match ip udp destination-port { <i>port-id</i> biff bootpc bootps domain echo mobile-ip netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip smtp snmptrap sunrpc syslog tacacs talk tftp time who }	(Optional) match the destination port ID of UDP packets. You can use the no match ip udp destination-port command to delete the configuration.

Configuring IPv6 matching contents

Step	Command	Description
1	Raisecom(config-vlan-acl-* <i>-rule</i> -*)# match ipv6 { destination-address <i>ipv6-address/prefix</i> source-address <i>ipv6-address/prefix</i> }	(Optional) match the source and destination IPv6 addresses.
2	Raisecom(config-vlan-acl-* <i>-rule</i> -*)# match ipv6 protocol <i>protocol-num</i>	(Optional) match the IPv6 ID.
3	Raisecom(config-vlan-acl-* <i>-rule</i> -*)# match ipv6 traffic-class <i>class-value</i>	(Optional) define ACL matching rules. Match the IPv6 Traffic-class. If the attribute of the packet is the same as the defined rule, the packet will be processed (permit or deny). You can use the no match ipv6 traffic-class command to delete the rule.

10.4.5 Configuring actions for matched packets

Step	Command	Description
1	<code>Raisecom(config-vlan-acl-* rule-*)#add { outer inner } vlan-id</code>	(Optional) add a VLAN. You can use the no add { outer inner } command to delete the configuration.
2	<code>Raisecom(config-vlan-acl-* rule-*)#remove inner</code>	(Optional) remove the VLAN. You can use the no remove inner command to delete the configuration.
3	<code>Raisecom(config-vlan-acl-* rule-*)#translate { outer inner } vlan to vlan-id</code>	(Optional) configure VLAN mapping. You can use the no translate { outer inner } vlan command to delete the configuration.
4	<code>Raisecom(config-vlan-acl-* rule-*)#translate outer cos to cos</code>	(Optional) modify the CoS value. You can use the no translate outer cos command to delete the configuration.



Note

The XEP8 (B) card does not support VLAN ACL in the egress direction.

10.4.6 Applying VLAN-ACL

Step	Command	Description
1	<code>Raisecom(config)#interface { ten-gigabitethernet epon-olt gpon-olt } slot- id/port-id</code>	Enter physical interface configuration mode.
2	<code>Raisecom(config-if-* :*)#vlan-access-list list- num</code>	Apply VLAN ACL rules to the interface. You can use the no vlan-access-list list-num command to delete VLAN ACL rules. Note Applying a VLAN ACL to an interface actually only processes incoming interface packets and has no effect on outgoing interface packets.

10.4.7 Checking configurations

No.	Command	Description
1	<code>Raisecom#show vlan-access-list [acl-num]</code>	Show VLAN ACL configurations.

No.	Command	Description
2	<code>Raisecom#show interface [ten-gigabitethernet epon-olt gpon-olt] slot-id/olt-id vlan-access-list</code>	Show VLAN ACL rules applied to the port.

10.5 Configuring VLAN partitioning

10.5.1 Preparing for configurations

Scenario

- VLAN partitioning by MAC address

After MAC-VLAN is enabled on an interface, MAC-VLAN association on the interface becomes invalid. When the interface receives packets, it matches the source MAC address of these packets with the MAC-VLAN. If the matching is successful, the interface forwards packets according to matched VLAN ID and priority. If the matching fails, the interface matches packets according to other matching rules.

- VLAN partitioning by IP subnet

If the device is enabled with IP subnet VLAN, it will match the source IP address of received packets with the ip-subnet-vlan entry after receiving packets. If the matching is successful, it forwards packets according to the matched VLAN and priority.

- VLAN partitioning by Ethernet type

Partitioning VLANs by Ethernet type associates the specified protocol type with VLANs, and determines the VLAN, to which the packets of different protocol types belong to, according to the association relation, and automatically assigns packet with the VLAN for transmission. It is used on the network which uses different transmission paths according to different protocol types.

Prerequisite

N/A

10.5.2 Default configurations

Default configurations of VLAN partitioning on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
MAC-VLAN	Disable
VLAN partitioning based on IP subnet	Disable
VLAN partitioning based on protocol	Disable

10.5.3 Configuring VLAN based on MAC address

Configure the VLAN based on MAC address for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mac-vlan <i>mac-address [mask] vlan vlan-id [priority value]</i>	Associate a MAC address with a VLAN
3	Raisecom(config)#mac-vlan enable	Enable MAC-VLAN.

Caution

- If the MAC address is a multicast MAC address, all-0 or all-F address, the configuration will fail.
- If you associate a created MAC address to a VLAN but this association conflict with an existing association (for example, the MAC address is associated with different VLANs), the association will fail.

10.5.4 Configuring VLAN based on IP subnet

Configure the VLAN based on IP subnet for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip-subnet-vlan { <i>ip-address/prefix-length ipv6-address/prefix-length</i> } vlan <i>vlan-id</i> [priority value]	Associate a VLAN with an IP subnet.
3	Raisecom(config)#ip-subnet-vlan enable	Enable VLAN partitioning based on IP subnet.

Caution

- If the IP address or subnet mask is invalid, the configuration will fail.
- If you associate a created IP subnet to a VLAN but this association conflict with an existing association (for example, the IP subnet is associated with different VLANs), the association will fail.

10.5.5 Configuring VLAN based on protocol

Configure the VLAN based on protocol for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)# protocol-vlan { <i>ethertype</i> ipv4 ipv6 arp pppoe pppoedisc } vlan <i>vlan-id</i> [priority <i>value</i>]	Configure the rule for associating the protocol VLAN with Ethernet packets.
3	Raisecom(config)# protocol-vlan enable	Enable VLAN partitioning based on protocol.

10.5.6 Checking configurations

No.	Command	Description
1	Raisecom# show mac-vlan { all vlan <i>vlan-id</i> <i>mac-address</i> [<i>mask</i>] }	Show configurations of MAC-VLAN.
2	Raisecom# show ip-subnet-vlan { all vlan <i>vlan-id</i> <i>ip-address</i> <i>ip-address/prefix-length</i> <i>ipv6-address</i> <i>ipv6-address/prefix-length</i> }	Show configurations of the IP subnet VLAN.
3	Raisecom# show protocol-vlan { <i>ethertype</i> ipv4 ipv6 arp pppoe pppoedisc all vlan <i>vlan-id</i> }	Show configurations of all protocol VLANs.

10.6 Configuring VLAN mapping

10.6.1 Preparing for configurations

Scenario

Different from QinQ, VLAN mapping changes the VLAN Tag without encapsulating multilayer VLAN Tags so that packets are transmitted according to the carrier's VLAN forwarding rules. VLAN mapping does not increase the length of the original packet. It can be used in the following scenarios:

- Translate the VLAN ID of user service to the VLAN ID of the carrier.
- Translate VLAN IDs of multiple user services to the VLAN ID of the carrier.

Prerequisite

- Connect the interface, configure its physical parameters, and make it Up at the physical layer.
- Create a VLAN.

10.6.2 Default configurations

Default configurations of VLAN mapping on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
VLAN mapping	Enable

10.6.3 Configuring VLAN mapping mode

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { epon-olt ten-giga- epon-olt gpon-olt gigabitethernet ten- gigabitethernet } slot- id/port-id example: Raisecom(config)#interface gigabitethernet 2/1	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode
3	Raisecom(config-if-* *)#vlan-mapping cos- aware	Configure CoS-aware VLAN mapping, that is, VLAN+CoS translation. You can use the no vlan-mapping cos-aware command to disable this function.
4	Raisecom(config-if-* *)#vlan-mapping { egress ingress } drop-unmatched example: Raisecom(config-if- gigabitethernet-3:1)#vlan- mapping ingress drop- unmatched	Drop packets which mismatch VLAN mapping rules. You can use the no vlan-mapping { egress ingress } drop-unmatched command to disable this function. • egress: discard the packets which mismatch the VLAN translation rules in the egress direction. • ingress: discard the packets which mismatch the VLAN translation rules in the ingress direction.

10.6.4 Configuring 1:1 VLAN mapping

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { epon-olt ten-giga-epon- olt gpon-olt gigabitethernet ten- gigabitethernet } slot- id/port-id example: Raisecom(config)#interface gigabitethernet 2/1	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode

Step	Command	Description
3	<pre>Raisecom(config-if-*-*:*)#vlan-mapping { ingress egress } outer before- outer translate outer after- outer inner { add vlan-id remove vlan-id unchange } example: Raisecom(config-if- gigabitethernet-3:1)#vlan- mapping ingress outer 1 translate outer 2 inner remove</pre>	Configure VLAN mapping rules based on the ingress/egress interface (translate the outer VLAN Tag only). • before-outer: old outer VLAN, an integer, ranging from 1 to 4094 • after-outer: new outer VLAN, an integer, ranging from 1 to 4094 • inner-vlan-id: new inner VLAN ID, an integer, ranging from 1 to 4094 • remove: deleted VLAN • add vlan-id: add a VLAN. The vlan-id is an integer, ranging from 1 to 4094. • unchanged: untranslated
4	<pre>Raisecom(config-if-*-*:*)#vlan-mapping { ingress egress } outer before- outer inner before-inner translate outer after-outer inner { vlan-id remove } example: Raisecom(config-if- gigabitethernet-3:1)#vlan- mapping ingress outer 1 inner 2 translate outer 3 inner remove</pre>	Configure VLAN mapping rules based on the ingress/egress interface (translate both outer and inner VLAN Tags). • before-outer: old outer VLAN, an integer, ranging from 1 to 4094 • before-inner: old inner VLAN ID list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • after-outer: new outer VLAN, an integer, ranging from 1 to 4094 • inner vlan-id: new inner VLAN ID, an integer, ranging from 1 to 4094 • remove: deleted VLAN

10.6.5 Configuring N:1 VLAN mapping

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#interface { epon-olt ten-giga-epon- olt gpon-olt gigabitethernet ten- gigabitethernet } slot- id/port-id example: Raisecom(config)#interface gigabitethernet 2/1</pre>	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode

Step	Command	Description
3	<pre>Raisecom(config-if-*-*:*)#vlan-mapping outer before-vlan aggregate outer after-vlan inner { add vlan-id unchange }</pre> example: <pre>Raisecom(config-if-gigabitethernet-2:1)#vlan-mapping outer 1 aggregate outer 2 inner add 4</pre>	Configure N:1 VLAN mapping rules based on interface (translate outer VLAN Tag and add inner VLAN Tag). • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • unchanged: untranslated • port-id: GEM interface range, an integer, ranging from 1 to 8 • vlan-list: VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
	<pre>Raisecom(config-if-*-*:*)#vlan-mapping outer before-outer inner before-innerlist aggregate outer after-outer inner { vlan-id remove }</pre> example: <pre>Raisecom(config-if-gigabitethernet-2:1)#vlan-mapping outer 1 inner 2 aggregate outer a3 inner remove</pre>	Configure N:1 VLAN mapping rules based on interface (translate both outer and inner VLAN Tags). • before-outer: old outer VLAN, an integer, ranging from 1 to 4094 • before-inner: old inner VLAN ID list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • after-outer: new outer VLAN, an integer, ranging from 1 to 4094 • inner vlan-id: new outer VLAN ID, an integer, ranging from 1 to 4094 • remove: deleted VLAN

10.6.6 Configuring translation rules based on VLAN+CoS

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id</pre> example: <pre>Raisecom(config)#interface gigabitethernet 2/1</pre>	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode

Step	Command	Description
3	<pre>Raisecom(config-if-*-*:*)#vlan-mapping ingress cos-aware outer before-outer before-cos translate outer after-outer inner { vlan-id add vlan-id remove unchange } example: Raisecom(config-if- gigabitethernet-2:1)#vlan- mapping ingress cos-aware outer 1 2 translate outer 3 inner unchange</pre>	Configure VLAN mapping rules based on VLAN+CoS on the ingress interface. You can use the no vlan-mapping { ingress egress } cos-aware outer before-outer before-cos translate command to cancel this application. • before-outer: old outer VLAN, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • before-cos: old outer VLAN COS, an integer, ranging from 0 to 7 • after-outer: new outer VLAN, an integer, ranging from 1 to 4094 • inner vlan-id: new inner VLAN ID, an integer, ranging from 1 to 4094 • add vlan-id: added VLAN. The vlan-id is an integer, ranging from 1 to 4094. • remove: deleted VLAN • unchange: untranslated

10.6.7 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id vlan-mapping { ingress egress } translate</pre>	Show 1:1 VLAN mapping rules.
2	<pre>Raisecom#show interface { epon-olt ten-giga-epon-olt gigabitethernet ten-gigabitethernet gpon-olt } slot-id/port-id vlan-mapping aggregate</pre>	Show N:1 VLAN mapping rules.
3	<pre>Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id vlan-mapping cos-aware aggregate</pre>	Show VLAN+CoS mapping rules.

10.7 Configuring virtual interface

10.7.1 Default configurations

Function	Default value
VLAN mode of virtual interface	Transparent
Native VLAN	VLAN 1

10.7.2 Configuring VLAN of virtual interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface epon-onu slot-id/port-id/onu-id example: Raisecom(config)#interface epon-onu 3/2/1	Enter EPON ONU virtual interface configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-if-epon-onu-*/*:*)#vlan mode { transparent trunk } example: Raisecom(config-epon-onu-3/2:1)#vlan mode trunk	Configure virtual interface VLAN mode. You can use the no vlan-mode command to restore default configurations. • transparent: transparent transmission mode • trunk: Trunk mode
4	Raisecom(config-if-epon-onu-*/*:*)#native vlan vlan-id example: Raisecom(config-epon-onu-3/2:1)#native vlan 2	Configure the Native VLAN of the virtual interface. You can use the no vlan native command to restore default configurations. • vlan vlan-id: VLAN ID, an integer, ranging from 1 to 4094

10.7.3 Configuring VLAN translation on virtual interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface epon-onu slot-id/port-id/onu-id example: Raisecom(config)#interface epon-onu 3/2/1	Enter EPON ONU virtual interface configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-if-epon-onu-*/*:*)#vlan-mapping { ingress egress } outer vlan-id translate outer vlan-id example: Raisecom(config-if-epon-onu-3/2:1)#vlan-mapping ingress outer 1 translate outer 2	Configure 1:1 VLAN translation on the virtual interface. You can use the no vlan-mapping { ingress egress } outer vlan-id translate command to delete the configuration. • inner vlan-id: translated inner VLAN ID, an integer, ranging from 1 to 4094
4	Raisecom(config-if-epon-onu-*/*:*)#vlan-mapping outer vlan-id aggregate outer vlan-id example: Raisecom(config-if-epon-onu-3/2:1)#vlan-mapping outer 1 aggregate outer 2	Configure N:1 VLAN translation on the virtual interface. You can use the no vlan-mapping { ingress egress } outer vlan-id translate command to delete the configuration.

Step	Command	Description
	<pre>Raisecom(config-if-epon-onu- */*:*)#vlan-mapping outer form vlan-id to vlan-id aggregate outer vlan-id [inner copy-form-outer] example: Raisecom(config-if-epon-onu- 3/2:1)#vlan-mapping outer form 1 to 2 aggregate outer 3 inner copy- form-outer</pre>	- inner vlan-id: translated inner VLAN ID, an integer, ranging from 1 to 4094 - copy-from-outer: copy the outer VLAN ID to the inner.

10.7.4 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show interface epon-onu slot-id/port- id/onu-list vlan</pre>	Show configurations of the virtual interface.
2	<pre>Raisecom#show interface epon-onu slot-id/port- id/vport-list vlan-mapping { ingress egress } translate</pre>	Show 1:1 VLAN translation rules on the virtual interface.
3	<pre>Raisecom#show interface epon-onu slot-id/port- id/vport-list vlan-mapping aggregate</pre>	Show N:1 VLAN translation rules on the virtual interface.

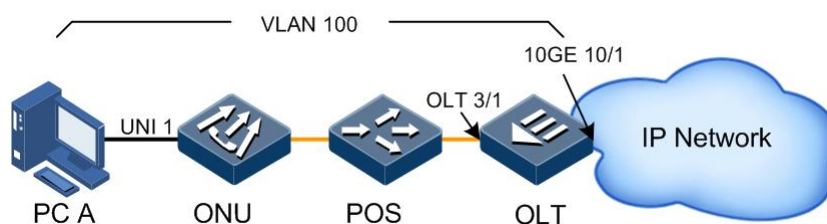
10.8 Configuration examples

10.8.1 Example for configuring VLAN

Networking requirements

As shown in Figure 10-3, the user connects the ONU through UNI 1 and the user VLAN is 100. The OLT connects the IP network through 10GE interface 10/1, and connects the ONU downstream through OLT PON interface 3/1. Under this network topology, activate the data service.

Figure 10-3 Configuring VLAN



Configuration steps

- Configure the OLT.

Step 1 Create a VLAN.

```
Raisecom#config  
Raisecom(config)#create vlan 100 active
```

Step 2 Configure the uplink 10GE interface VLAN.

```
Raisecom(config)#interface ten-gigabitethernet 10/1  
Raisecom(config-if-ten-gigabitethernet-10:1)#switchport mode trunk  
Raisecom(config-if-ten-gigabitethernet-10:1)#switchport trunk allowed  
vlan 100  
Raisecom(config-if-ten-gigabitethernet-10:1)#exit
```

Step 3 Configure PON interface VLAN.

```
Raisecom(config)#interface epon-olt 3/1  
Raisecom(config-if-epon-olt-3:1)#switchport mode trunk  
Raisecom(config-if-epon-olt-3:1)#switchport trunk allowed vlan 100  
Raisecom(config-if-epon-olt-3:1)#end
```

Step 4 Configure ONU auto-registration.

```
Raisecom#config  
Raisecom(config)#interface epon-olt 3/1  
Raisecom(config-if-epon-olt-3:1)#authorization mode none  
Raisecom(config-if-epon-olt-3:1)#exit
```

- Configure the ONU.

Step 5 Configure the user data VLAN.

```
Raisecom(config)#epon-onu uni ethernet 3/1/1/1  
Raisecom(config-epon-onu-ethernet-3/1/1:1)#vlan mode tagged  
Raisecom(config-epon-onu-ethernet-3/1/1:1)#native vlan 100  
Raisecom(config-epon-onu-ethernet-3/1/1:1)#end
```

Checking results

Show VLAN configurations of OLT 10GE interface 10/1 and PON interface respectively.

```
Raisecom#show interface ten-gigabitethernet 10/1 vlan
Port: 10/1
Administrative Mode: trunk
Operational Mode: trunk
Access Mode VLAN: 1
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 100
Operational Trunk Allowed VLANs: 1,100
Administrative Trunk Untagged VLANs: n/a
Operational Trunk Untagged VLANs: 1
Drop Untagged: No
```

```
Raisecom#show interface epon-olt 3/1 vlan
Port: 3/1
Administrative Mode: trunk
Operational Mode: trunk
Access Mode VLAN: 1
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 100
Operational Trunk Allowed VLANs: 1,100
Administrative Trunk Untagged VLANs: n/a
Operational Trunk Untagged VLANs: 1
Drop Untagged: No
```

Show the registered ONU.

```
Raisecom#show interface epon-onu creation-information
ONU ID   MAC Address   Mode   Creation Date   Device Type   State
Mng-mode
-----
3/1/1    000e.5e0a.7a0e   auto   2000-01-01,08:00 ISCOM5104(C)   active
oam
```

Show UNI VLAN configurations of the ONU.

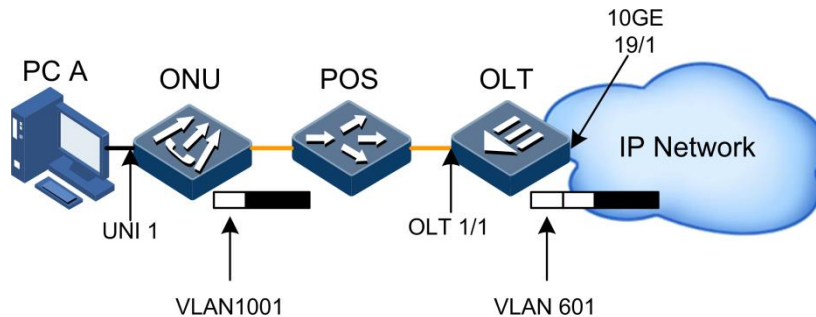
```
Raisecom#show epon-onu 3/1/1 uni ethernet 1 vlan
Port ID: 3/1/1/1
VLAN mode       : Tagged
Native VLAN     : 100(CoS 0)
Trans-rule list : n/a
Trunk allowed VLAN: n/a
Agg-rule list   : n/a
```

10.8.2 Example for configuring basic QinQ

Networking requirement

As shown in Figure 10-4, user PC A accesses the IP network through the OLT and ONU. The user belongs to VLAN 1001. The carrier transmits services through VLAN 601 and uses basic QinQ to meet this requirement.

Figure 10-4 Example for applying basic QinQ



Configuration steps

This step only involves basic QinQ configurations at PC A side of the user. That is, configure basic QinQ on the OLT.

- Configure the OLT.

Step 1 Create VLAN 601 and VLAN 1001 and activate them.

```
Raisecom#config  
Raisecom(config)#create vlan 601,1001 active
```

Step 2 Configure the VLAN of the 10GE 19/1 uplink port.

```
Raisecom(config)#interface ten-gigabitethernet 19/1  
Raisecom(config-if-ten-gigabitethernet-19:1)#switchport mode trunk  
Raisecom(config-if-ten-gigabitethernet-19:1)#switchport trunk allowed  
vlan 601  
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
```

Step 3 Configure the VLAN of (PON) OLT port 1/1.

```
Raisecom(config)#interface epon-olt 1/1  
Raisecom(config-if-epon-olt-1:1)#switchport mode access  
Raisecom(config-if-epon-olt-1:1)#switchport access vlan 601  
Raisecom(config-if-epon-olt-1:1)#vlan dot1q-tunnel  
Raisecom(config-if-epon-olt-1:1)#vlan tpid 8100
```

- Configure the ONU.

Step 4 Configure the UNI user VLAN.

```
Raisecom(config-if-epon-olt-1/1)#exit
Raisecom(config)#epon-onu uni ethernet 1/1/1/1
Raisecom(config-epon-onu-ethernet-1/1/1/1)#vlan mode tagged
Raisecom(config-epon-onu-ethernet-1/1/1/1)#native vlan 1001
Raisecom(config-epon-onu-ethernet-1/1/1/1)#end
```

Checking results

Show QinQ configurations of PON port OLT 1/1.

```
Raisecom#show interface epon-olt 1/1 vlan-mapping
          VLAN-mapping Drop Unmatched
Port ID      Cos-Aware  (Ingress|Egress) Dot1q-tunnel VLAN
Tpid
-----
-----
epon-olt1/1  No         (No | No)        Enable      0x8100
```

show VLAN configurations of UNI1.

```
Raisecom#show epon-onu 1/1/1 uni ethernet 1 vlan
Port ID: 1/1/1/1
  VLAN mode      : Tagged
  Native VLAN    : 1001(cos 0)
  Trans-rule list : n/a
  Trunk allowed VLAN: n/a
  Agg-rule list   : n/a
```

Show VLAN configurations of 10GE port 19/1.

```
Raisecom#show interface ten-gigabitethernet 19/1 vlan
Port: ten-gigabitethernet19/1
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 1
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 601
Operational Trunk Allowed VLANs: n/a
Administrative Trunk Untagged VLANs: n/a
Operational Trunk Untagged VLANs: n/a
Drop Untagged:No
```

Show VLAN configurations of PON port OLT 1/1.

```
Raisecom#show interface epon-olt 1/1 vlan
Port: epon-olt1/1
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 601
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: n/a
Administrative Trunk Untagged VLANs: 1
Operational Trunk Untagged VLANs: n/a
Drop Untagged:No
```

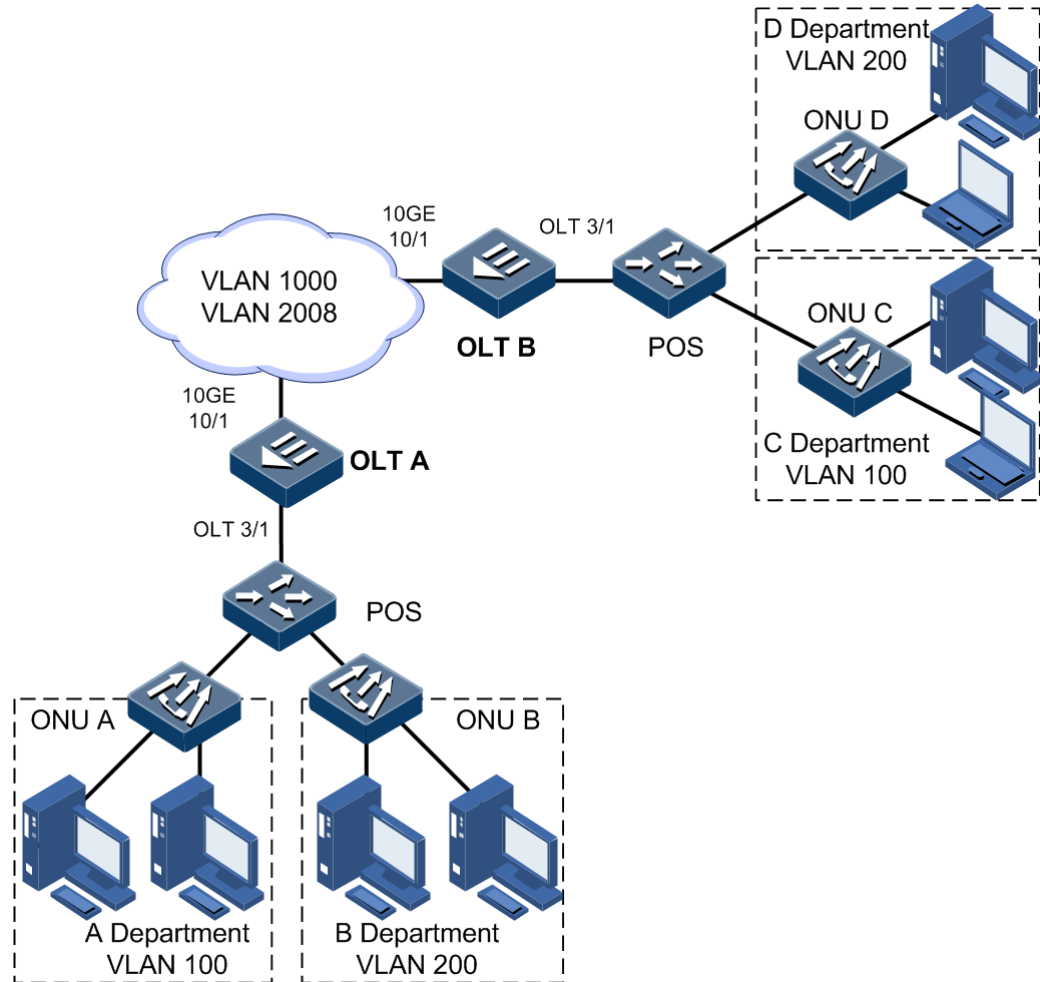
10.8.3 Example for configuring VLAN mapping

Networking requirements

As shown in Figure 10-5, OLT A connects Department A in VLAN 100 and Department B in VLAN 200 through OLT 3/1; OLT B connects Department C in VLAN 100 and Department D in VLAN 200 through OLT 3/1. In the carrier network, assign VLAN 1000 for Department A and Department C; and assign VLAN 2008 for Department B and Department D.

Configure 1:1 VLAN mapping on OLT A and OLT B to implement proper communication between the PC user or terminal user, and the server.

Figure 10-5 Configuring VLAN mapping



Configuration steps

Configurations on OLT A and OLT B are identical. Take OLT A for example.

Step 1 Create a VLAN and activate it.

```
Raisecom#config
Raisecom(config)#create vlan 100,200,1000,2008 active
```

Step 2 Configure uplink 10GE interface 10/1 to Trunk mode and allow VLAN 1000 and VLAN 2008 to pass.

```
Raisecom(config)#interface ten-gigabitethernet 10/1
Raisecom(config-if-ten-gigabitethernet-10:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-10:1)#switchport trunk allowed
vlan 1000,2008 confirm
Raisecom(config-if-ten-gigabitethernet-10:1)#exit
```

- Step 3 Configure the OLT interface 3/1 to Trunk mode and allow VLAN 100 and VLAN 200 to pass, and enable VLAN mapping.

```
Raisecom(config)#interface epon-olt 3/1
Raisecom(config-if-epon-olt-3:1)#switchport mode trunk
Raisecom(config-if-epon-olt-3:1)#switchport trunk allowed vlan 100,200
1000,2008 confirm
Raisecom(config-if-epon-olt-3:1)#vlan-mapping ingress outer 100 translate
outer 1000 inner copy-from-outer
Raisecom(config-if-epon-olt-3:1)#vlan-mapping ingress outer 200 translate
outer 2008 inner copy-from-outer
Raisecom(config-if-epon-olt-3:1)#switchport trunk untagged vlan 1000,2008
confirm
```

Checking results

Use the **show interface epon-olt slot-id/olt-id vlan-mapping { ingress | egress }** command to show 1:1 VLAN mapping configurations.

```
Raisecom#show interface epon-olt 3/1 vlan-mapping ingress
```

	Old	Old	New	New	IVLAN	
Port ID	OVID	IVID	OVID	IVID	Mapping	Action
epon-olt3/1	100	--	1000	--	copy-from-outer	
epon-olt3/1	200	--	2008	--	copy-from-outer	

11

Configuring routing

This chapter describes the routing feature and configure process of the device, and provides related configuration examples, including the following sections:

- Introduction
- Configuring ARP
- Configuring IPv6 basic functions
- Configuring route management
- Configuring static routes
- Configuring NDP
- Configuration examples

11.1 Introduction

11.1.1 ARP

In the TCP/IP network, each host is assigned with a 32-bit IP address, which is called a logical address. To transmit packets through physical links, the device must learn the physical address of the destination host. It means that the device should translate the IP address into a physical address.

In the Ethernet, a physical address is a 48-bit MAC address. The Address Resolution Protocol (ARP) can establish a mapping between IP addresses and MAC addresses, which can translate IP addresses into MAC addresses.

Entries in the ARP address table are classified into the following types:

- Static ARP entry: is used to perform static binding on an IP address and a MAC address. It is used to prevent ARP dynamic learning fraud.
 - Static ARP entries should be manually added and deleted.
 - Static ARP entries are not aged.
- Dynamic ARP entry: entries that are automatically established through ARP
 - Dynamic ARP entries are automatically generated by the device.
 - Dynamic ARP entries are aged when the aging time is exceeded, on conditions that dynamic ARP entries are not used.

The device support **learn-all** ARP entry dynamic learning mode. The device learns ARP request and response packets in this mode. For example, when Device A sends the ARP request packet to Device B, it writes the mapping between its IP address and its MAC address into the ARP request packet. Device B learns this mapping to its own ARP table after receiving the ARP request packet. Therefore, no ARP request is performed when Device B sends packets to Device A later.

11.1.2 IPv6

Overview

Internet Protocol Version 6 (IPv6) is the second-generation standard protocol of the network layer protocol. It is the next-generation IP protocol designed by the Internet Engineering Task Force (IETF) and is an upgraded version of IPv4.

The most obvious difference between IPv6 and IPv4 is that the length of the IP address is increased from 32 bits to 128 bits.

IPv6 address

IPv6 address representation:

The total length of an IPv6 address is 128 bits, and each address is divided into 8 groups, each group being represented by 4 hexadecimal numbers. Groups are separated from each other by a colon. For example: FB00:0000:230B:0000:0000:09B0:576A:130F.

In order to more conveniently represent the IPv6 address, you can have the following abbreviation shorthands:

- The leading "0" in each group can be omitted, so the above address can be written as FB00:0: 230B:0:0:9B0:576A:130F.
- When the address contains two or more consecutive groups of 0, you can use the double colon "::" instead, so the above address can be abbreviated as: FB00:0:230B::9B0:576A:130F.

An IPv6 address can be divided into the following two parts:

- Network prefix: the first n bits, equivalent to the network number in the IPv4 address
- Interface identifier: 128-n bits later, equivalent to the host number in the IPv4 address



Note

Only one double colon "::" can be used in an IPv6 address. Otherwise, when the device restores the address to 128 bits, the number of 0s represented by "::" cannot be determined.

11.1.3 Routing

Routing is used to select a route and forward packets to make devices in different network segments communicate. The routing is realized through routing protocols. Routing protocols, rules to maintain the routing table between devices, are used to discover routes, generate the routing table, and instruct packet forwarding.

Devices select a route through a routing table and then instruct packet forwarding through Forwarding Information Base (FIB). Each device saves a routing table and a FIB table at least.

The routing table saves routes discovered based on various routing protocols. According to route sources, routes in the routing table are grouped as below:

- Interface route or directly-connected route: routes discovered by link-layer protocols
- Static route: routes manually configured by the administrator
- Dynamic route: routes discovered by dynamic routing protocols

Each entry in a FIB indicates the physical interface or logical interface where packets of a network segment or a host should be forwarded to the next-hop device.

Default route

The default route is a special type of route. It takes effect when no other route can be matched in the routing table. In the routing table, the default route is designated as 0.0.0.0/0. If the destination IP address of a packet mismatches with any entry in the routing table, this packet will select the default route.

If no default route is configured for a device and the destination IP address of a packet is not in the routing table, the device will discard the packet and send an Internet Control Message Protocol (ICMP) packet to the sender, which indicates that the destination address or network is unreachable.

Static route

Static route refers to a type of route that is manually configured. The static route has the following advantages:

- Do not consume network bandwidth.
- Cannot be aged.
- Can accurately control the direction of data packets.

However, the static route has some disadvantages:

- Be configured manually.
- Increase workload of the administrator.

The static route is mainly applied to small- and medium-sized network.

Dynamic route

Dynamic route refers to a type of route that is automatically generated based on related dynamic routing protocols. Compared with the static route, it fits for larger network. In addition, the workload of the administrator is reduced. However, some network resources are consumed during generating and maintaining the dynamic routes.

Based on routing algorithms, dynamic routing protocols are grouped into:

- Distance-vector routing protocol, such as Routing Information Protocol (RIP)
- Link-state routing protocol, such as Open Shortest Path First (OSPF)

Route management

Routing is a behavior of passing a message through a network to a destination, and uses a routing table to forward it during the delivery process. Routing is required when devices

between different VLANs communicate, or devices in the same VLAN wish to communicate across different networks.

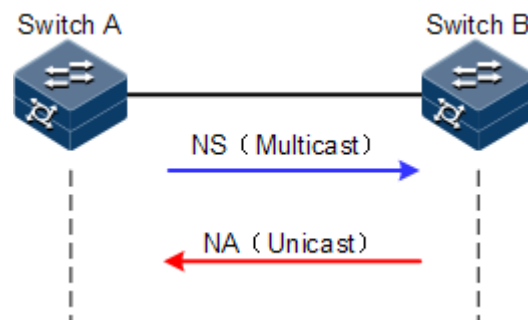
Route management uniformly manages routing tables, static routes, and various dynamic routing protocols through routing device identification.

11.1.4 NDP

Neighbor Discovery Protocol (NDP) is a neighbor discovery mechanism used on IPv6 devices in the same link. It is used to discover neighbors, obtain MAC addresses of neighbors, and maintain neighbor information.

NDP obtains data link layer addresses of neighbor devices in the same link, namely, MAC address, through the Neighbor Solicitation (NS) message and Neighbor Advertisement (NA) message.

Figure 11-1 Principles of NDP address resolution



As shown in Figure 11-1, take Switch A for example. Switch A obtains the data link layer address of Switch B as below:

- Step 2 Switch A sends a NS message in multicast mode. The source address of the NS message is the IPv6 address of Layer 3 interface on Switch A, and the destination address of the NS message is the multicast address of the requested node of the Switch B. The NS message even contains the data link layer address of Switch A.
- After receiving the NS message, Switch B judges whether the destination address of the NS message is the multicast address of the request node corresponding to the IPv6 address of Switch B. If yes, Switch B can obtain the data link layer address of Switch A, and sends a NA message which contains its data link layer address in unicast mode.
 - After receiving the NA message from Switch B, Switch A obtains the data link layer address of Switch B.

By sending ICMPv6 message, IPv6 NDP even has the following functions:

- Verify whether the neighbor is reachable.
- Detect duplicated addresses.
- Discover routers or prefix.
- Automatically configure addresses.
- Support redirection.

11.2 Configuring ARP

11.2.1 Preparing for configurations

Scenario

The mapping between IP addresses and MAC addresses is saved in the ARP address table.

In general, ARP address entries are maintained by devices dynamically. The device searches the mapping between IP addresses and MAC addresses automatically according to ARP. You need to configure the device manually only when adding static ARP address entries to prevent dynamic ARP learning spoofing.

Prerequisite

N/A

11.2.2 Default configurations

Default configurations of ARP on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Static ARP entries	N/A
Dynamic ARP learning mode	learn-all

11.2.3 Configuring static ARP entries



Caution

- The IP address of a static ARP entry must be in the same IP network segment with the VLAN interface.
- You need to add or delete static ARP entries manually.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# arp ip-address mac-address example: Raisecom(config)#arp 10.0.0.1 0050.8d4b.fd1e	Configure static ARP entries. You can use the no arp ip-address command to delete the entry. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • mac-address: MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456

11.2.4 Configuring dynamic ARP entries

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# arp aging-time <i>time</i> example: Raisecom(config)#arp aging-time 5000	Configure the aging time of dynamic ARP entries. • time: aging time of ARP entry, an integer, ranging from 60 to 2147483, in units of second

11.2.5 Checking configurations

No.	Command	Description
1	Raisecom# show arp	Show ARP address mapping entries.
2	Raisecom# show arp [<i>ip-address</i>]	Show ARP entries of a specified IP address.
3	Raisecom# show arp static	Show static ARP entries.
4	Raisecom# show arp summary	Show statistics of the ARP address table.

11.3 Configuring IPv6 basic functions

11.3.1 Preparing for configurations

Scenario

With the rapid development of the network, the IPv4 protocol slowly shows weaknesses, and the IPv6 protocol has more advantages than the IPv4 protocol. For example, IPv6 has a large number of address spaces, highly flexible message formats, and efficient route forwarding efficiency. IPv6 can not only solve the problem of network address resource limitation, but also solve the problem of limitations of device access to the Internet.

Prerequisite

N/A

11.3.2 Default configurations

Function	Default values
Layer 3 interface Ipv6	Disable
Stateless autoconfiguration address	Disable

11.3.3 Configuring IPv6 basic functions

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlanif <i>vlan-id</i> example: Raisecom(config)#interface vlanif 2	Enter VLAN interface configuration mode. • vlan-id : VLAN interface ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlanif-*)#ipv6 enable	Enable IPv6 on the Layer 3 interface. You can use the disable form of this command to disable the function.
4	Raisecom(config-vlanif-*)#ipv6 address <i>ipv6-address/prefix-length</i> [<i>eui-64</i>] example: Raisecom(config-vlanif-2)#ipv6 address 1030:0::48AA:1A2B/60	Configure the IPv6 address of the VLAN interface. • ipv6-address/prefix-length : IPv6 address with the mask length, such as A:B::C:D/M input • eui-64 : use eui-64 as the interface ID.
5	Raisecom(config-vlanif-*)#ipv6 address <i>ipv6-address</i> link-local example: Raisecom(config-vlanif-2)#ipv6 address fe80::3 link-local	(Optional) configure the IPv6 local link address of the VLAN interface. • ipv6-address : IPv6 address, in colon hexadecimal notation, such as fe80::3
6	Raisecom(config-vlanif-*)#ipv6 address <i>ipv6-address/prefix-length</i> anycast example: Raisecom(config-vlanif-2)#ipv6 address 1030:0::48AA:1A2B/60 anycast	(Optional) configure the IPv6 anycast address on the VLAN interface. • ipv6-address/prefix-length : IPv6 address with the mask length, such as A:B::C:D/M input
7	Raisecom(config-vlanif-*)#ipv6 address auto	(Optional) enable IPv6 address stateless autoconfiguration in VLAN interface mode.

11.3.4 Checking configurations

No.	Command	Description
1	Raisecom#show interface vlanif <i>vlan-id</i> ipv6 detail	Show IPv6 address configurations of the interface.

11.4 Configuring route management

11.4.1 Preparing for configurations

Scenario

It is used to uniformly manage routing tables.

Prerequisite

N/A

11.4.2 Configuring route management

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router id <i>ip-address</i> example: Raisecom(config)#router id 10.0.0.1	Configure the router ID. router-id: routing device ID, identifying a router device, in dotted decimal notation, ranging from 0.0.0.0 to 255.255.255.255

11.4.3 Checking routing table

No.	Command	Description
1	Raisecom# show ip route [detail]	Show route information.
2	Raisecom# show ip route <i>ip-address</i> [<i>ip-mask</i>] [longer-prefixes] [detail]	Show routes to a certain IP address.
3	Raisecom# show ip route <i>start-ip-address</i> <i>start-ip-mask end-ip-address end-ip-mask</i> [detail]	Show routes to a certain range of IP addresses.
4	Raisecom# show ip route protocol { static connected } [detail]	Show route information about a certain protocol.
5	Raisecom# show ip route summary	Show statistics on all routes.
6	Raisecom# show router id	Show the router ID.

11.5 Configuring static routes

11.5.1 Preparing for configurations

Scenario

Configure static routes for simple topology networks. You need to configure static routes manually to create an interconnected network.

Prerequisite

Configure the IP address of the VLAN interface correctly.

11.5.2 Configuring default gateway

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ip route 0.0.0.0 0.0.0.0 ip-address example: Raisecom(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.1	Configure the IP address of the default gateway. You can use the no router id command to delete the configuration. ip-address: IP address of the destination network, in dotted decimal notation, such as 10.0.0.0



Note

On the device, if the packet to be forwarded does not have a corresponding route, you can use the **ip route** command to configure the default gateway to forward the packet to the default gateway.

11.5.3 Configuring static routes

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ip routing	Enable routing. You can use the no ip routing command to disable this function.

Step	Command	Description
3	<pre>Raisecom(config)#ip route {ip-address mask ip-address/mask-length } nexthopip [distance value] [description description] [tag tag-id]</pre> example: <pre>Raisecom(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.1 distance 100 description route1 tag 1</pre>	Configure the static route. You can use the no ip route ip-address mask nexthopip command to delete the configuration. • ip-address: IP address of the destination network, in dotted decimal notation, such as 10.0.0.0 • mask: subnet mask, in dotted decimal notation, such as 255.0.0.0 • nexthopip: next-hop IP address, in dotted decimal notation, such as 10.0.0.0. The next-hop IP address cannot be the address of the IP interface. • distance distance: configure the administrative distance of the static route. The distance refers to the administrative distance, which is an integer ranging from 1 to 255. • description description: configure the description of static routes. The description is a character string. • tag tag-id: configure the ID of static route. The tag-id refers to the ID, which is an integer, ranging from 1 to 65535.
4	<pre>Raisecom(config)#ip route static distance value</pre> example: <pre>Raisecom(config)#ip route static distance 10</pre>	(Optional) configure the administrative distance of the static route. You can use the no ip route static distance command to restore default configurations. • value: administrative distance, an integer, ranging from 1 to 255

11.5.4 Configuring IPv6 static route

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip routing	Enable routing. You can use the no ip routing command to disable this function.
3	<pre>Raisecom(config)#ipv6 route-static { ipv6-address/prefix-length ipv6-address } nexthop-ipv6-address [distance distance-num] [description text] [tag tag-id]</pre> example: <pre>Raisecom(config)#ipv6 route-static 1:123::1:1/96 1:123::0:1 distance 100 description route1</pre>	Configure IPv6 static routes. You can use the no form of this command to delete this configuration. • ipv6-address/prefix-length: IPv6 route prefix. The IPv6 address has a mask, such as 1:123::0:1/96. • nexthop-ipv6-address: next-hop IPv6 address, such as 1:123::0:1 • distance distance-num: configure the administrative distance of the static route. The distance refers to distance, which is an integer ranging from 0 to 255. • description text: configure the description of the static route. The description refers to the description, which is a character string. • tag tag-id: configure the static route tag. The tag-id refers to the tag ID, which is an integer, ranging from 0 to 65535.

11.5.5 Checking configurations

No.	Command	Description
1	<code>Raisecom#show ip route [detail]</code>	Show detailed information about the route.
2	<code>Raisecom#show ip fib</code>	Show information about the IP FIB table.
3	<code>Raisecom#show ip route all detail</code>	Show information about all routes.
4	<code>Raisecom#show ip route all protocol { static connected } [detail]</code>	Show routing information about the specified routing protocol.
5	<code>Raisecom#show ip route ip-address [mask-address] [longer-prefixes] [detail]</code>	Show information about a route to a certain destination.
6	<code>Raisecom#show ip route ip-address1 mask-address1 ip-address2 mask-address2 [detail]</code>	Show information about the routes within two IP address ranges.
7	<code>Raisecom#show ip route summary</code>	Show IPv4 route statistics.
8	<code>Raisecom#show ipv6 route summary</code>	Show IPv6 route statistics.
9	<code>Raisecom#show ipv6 fib</code>	Show IPv6 FIB table entries.
10	<code>Raisecom#show ipv6 route { ipv6-address/prefix-length ipv6-address all static }</code>	Show the IPv6 routing table of the device.

11.6 Configuring NDP

11.6.1 Preparing for configurations

Scenario

IPv6 NDP not only implements IPv4 ARP, ICMP redirection, and ICMP device discovery, but also supports detecting whether the neighbor is reachable.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.
- Configure the IPv6 address of the Layer 3 interface.

11.6.2 Configuring static neighbor entries

To resolve the IPv6 address of a neighbor into the data link layer address, you can use the NS message and NA message, or manually configure static neighbor entries.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlanif <i>vlan-id</i> example: Raisecom(config)#interface vlanif 2	Enter VLAN interface configuration mode. • <i>vlan-id</i> : VLAN interface ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlanif-*)#ipv6 enable	Enable IPv6. You can use the disable form of this command to disable this function.
4	Raisecom(config-vlanif-*)#ipv6 neighbor <i>ipv6-address mac-address</i> example: Raisecom(config-vlanif-2)#ipv6 neighbor 2001::3 000E.5E12.3456	Configure static neighbor entries. • <i>ipv6-address</i> : IPv6 unicast address, in colon hexadecimal notation • <i>mac-address</i> : MAC address, in dotted hexadecimal notation. It should not be a multicast MAC address or an all-0 address.

11.6.3 Configuring times of sending NS messages for detecting duplicated addresses

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlanif <i>vlan-id</i> example: Raisecom(config)#interface vlanif 2	Enter VLAN interface configuration mode. • <i>vlan-id</i> : VLAN interface ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlanif-*)#ipv6 nd dad attempts <i>value</i> example: Raisecom(config-vlanif-2)#ipv6 nd dad attempts 5	Configure times of sending NS messages for detecting duplicated addresses. • <i>value</i> : times for sending NS, an integer, ranging from 0 to 600 where the value 0 means forbidding checking whether the address is occupied



Note

When the ISCOM6800 or ISCOM6860 obtain an IPv6 address, it uses the duplicated address detection function to determine whether the IPv6 address is already used by another device. After sending NS messages for a specified times and receiving no response, it determines that the IPv6 address is not duplicated and thus can be used.

11.6.4 Configuring maximum number of NDPs allowed to be learnt

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)# interface vlanif <i>vlan-id</i> example: Raisecom(config)#interface vlanif 2	Enter VLAN interface configuration mode. • <i>vlan-id</i> : VLAN interface ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlanif-*)# ipv6 neighbor max-learning-num <i>number</i> example: Raisecom(config-vlanif-2)#ipv6 neighbor max-learning-num 4	Configure the maximum number of NDPs allowed to be learnt. • <i>number</i> : the maximum number of NDPs, an integer, ranging from 1 to 4000

11.6.5 Configuring flag bit of stateful autoconfiguration

No.	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface vlanif <i>vlan-id</i>	Enter VLAN interface mode.
3	Raisecom(config-vlanif-*)# ipv6 nd autoconfig managed-address-flag	Configure the routable address flag bit of stateful automatic configuration.
4	Raisecom(config-vlanif-*)# ipv6 nd autoconfig other-flag	Configure other flag bits of stateful automatic configuration.

11.6.6 Configuring the reachable time of neighbors on an IPv6 interface

No.	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface vlanif <i>vlan-id</i> example: Raisecom(config)#interface vlanif 2	Enter VLAN interface configuration mode. • <i>vlan-id</i> : VLAN interface ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlanif-*)# ipv6 nd ns retrains-timer <i>time</i> example: Raisecom(config-vlanif-2)#ipv6 nd ns retrains-timer 2000	Configure the interval for probe retransmission of neighbor reachability on an IPv6 interface. • <i>time</i> : probe retransmission interval, an integer, ranging from 1000 to 429496729, in units of millisecond
4	Raisecom(config-vlanif-*)# ipv6 nd nud reachable-time <i>time</i> example: Raisecom(config-vlanif-2)#ipv6 nd nud reachable-time 2000	Configure the reachable state of the neighbor on the IPv6 interface. • <i>time</i> : probe retransmission interval, an integer, ranging from 1 to 3600000, in units of millisecond

11.6.7 Configuring RA messages

No.	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlanif <i>vlan-id</i> example: Raisecom(config)#interface vlanif 2	Enter VLAN interface configuration mode. vlan-id: VLAN interface ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlanif-*)#ipv6 nd ra repression	Enable RA advertisement repression.
4	Raisecom(config-vlanif-**)#ipv6 nd ra interval <i>min-interval max-interval</i> example: Raisecom(config-vlanif-2)#ipv6 nd ra interval 5 500	Configure the interval for advertising RA messages. - min-interval: minimum advertisement interval, an integer, ranging from 3 to 1350, in units of second - max-interval: maximum advertisement interval, an integer, ranging from 4 to 1800, in units of second
5	Raisecom(config-vlanif-*)#ipv6 nd ra advlinkmtu	Configure the advertisement MTU carried in the RA message.
6	Raisecom(config-vlanif-*)#ipv6 nd ra prefix <i>ipv6-prefix-address/prefix-length valid-lifetime preferred-lifetime [no-autoconfig] [off-link]</i> example: Raisecom(config-vlanif-1)#ipv6 nd ra prefix 1030:0::48AA:1A2B/60 180 20	Configure the prefix in the RA message. - ipv6-prefix-address/prefix-length: IPv6 address with the mask length, such as A:B::C:D/M input - valid-lifetime: valid life period, an integer, ranging from 0 to 4294967295, in units of second - preferred-lifetime: preferred lifetime. The address is in preferred status within the specified time. An integer, ranging from 0 to 4294967295, in units of second - no-autoconfig: the specified prefix cannot be used for automatic configuration. - off-link: the specified prefix is not is not directly reachable.
7	Raisecom(config-vlanif-*)#ipv6 nd ra router-lifetime <i>lifetime</i> example: Raisecom(config-vlanif-2)#ipv6 nd ra router-lifetime 1500	Configure the router lifetime in the RA message. time: lifetime, an integer, ranging from 4 to 9000, in units of second
8	Raisecom(config-vlanif-*)#ipv6 nd ra hop-limit <i>hop-limit</i> example: Raisecom(config-vlanif-2)#ipv6 nd ra hop-limit 2	Configure the hop limits in the RA message. hop-limit: hop limits, an integer, ranging from 0 to 255

11.6.8 Configuring router hops

Configure the hop limit of the routing device. It can be used to control the hop limit of the IPv6 unicast packets initially sent by the routing device. It can also be used as a parameter in the RA packet to help the host automatically configure the hop limit.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ipv6 nd hop-limit times example: Raisecom(config-vlanif-1)#ipv6 nd ra hop-limit 2	Configure the hops of the router. • times: hop limits, an integer, ranging from 0 to 255

11.6.9 Checking configurations

No.	Command	Description
1	Raisecom#show ipv6 neighbors [ipv6-address dynamic static vlan vlan-id]	Show the existing neighbor entries.
2	Raisecom#show ipv6 neighbors count { all dynamic static vlan vlan-id }	Show information about all neighbors.

11.6.10 Maintenance

No.	Command	Description
1	Raisecom(config)#clear ipv6 neighbors { all dynamic static vlan vlan-id } example: Raisecom(config)#clear ipv6 neighbors all	Clear neighbor entries on the device. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • static: static neighbors • dynamic: dynamic neighbors • all: all neighbors

11.7 Configuration examples

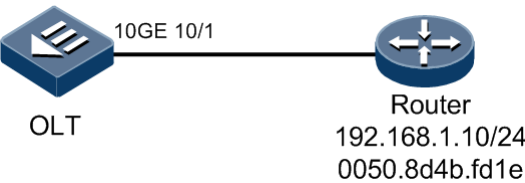
11.7.1 Example for configuring ARP

Networking requirements

As shown in Figure 11-2, the OLT device is connected to the host, and is connected to the upper-layer router through 10GE interface 10/1. The IP address of the router is 192.168.1.10, the mask is 255.255.255.0, and the MAC address is 0050.8d4b.fd1e.

You need to configure a corresponding static ARP entry on the OLT to enhance the communication security between the OLT and router.

Figure 11-2 ARP networking



Configuration steps

Add a static ARP entry.

```
Raisecom#config
Raisecom(config)#arp 192.168.1.10 0050.8d4b.fd1e
```

Checking results

Use the **show arp** command to show all entries in the ARP address table.

```
Raisecom#show arp

ARP mode: Learn all
IP Address      Mac Address      Interface      Type      Age(s)
-----
192.168.1.10    0050.8d4b.fd1e    ip1            static     3

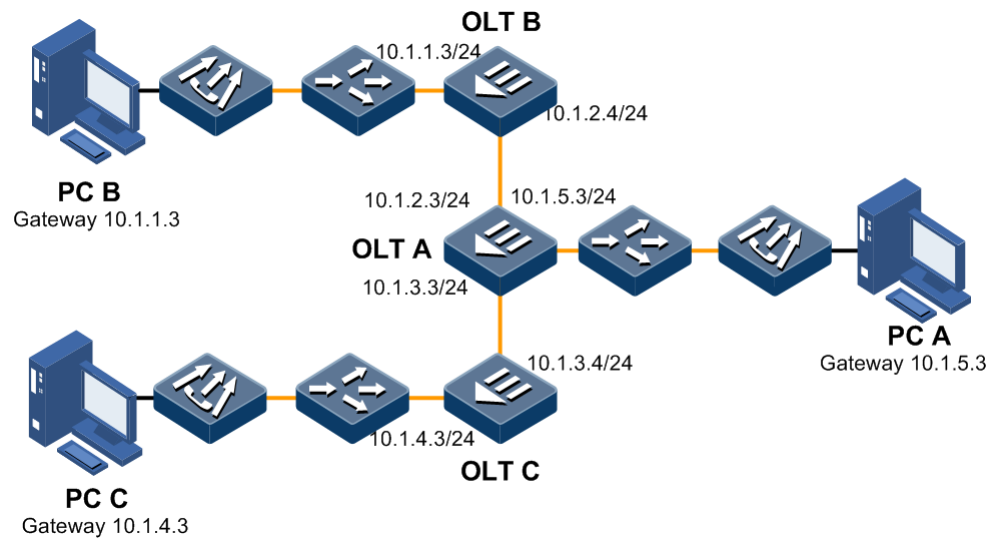
Total: 1
Static: 1
Dynamic:0
```

11.7.2 Example for configuring static routes

Networking requirements

Configure a static route so that any two PCs or OLTs in Figure 11-3 can ping each other. The IP addresses of the two interfaces of OLT B are 10.1.1.3/24 and 10.1.2.4/24; the IP addresses of the three interfaces of OLT A are 10.1.2.3/24, 10.1.5.3/24, and 10.1.3.3/24. The IP addresses of the two interfaces of OLT C are 10.1.3.4/24 and 10.1.4.3/24.

Figure 11-3 Configuring static routes



Configuration steps

Step 1 Configure the IP address of each device. The details are as below:

Step 2 Enable routing on OLT A and configure static routes.

```
Raisecom#config
Raisecom(config)#ip routing
Raisecom(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.4
Raisecom(config)#ip route 10.1.4.0 255.255.255.0 10.1.3.4
```

Step 3 Enable routing on OLT B and configure static routes.

```
Raisecom(config)#ip routing
Raisecom(config)#ip route 10.1.3.0 255.255.255.0 10.1.2.3
Raisecom(config)#ip route 10.1.4.0 255.255.255.0 10.1.2.3
Raisecom(config)#ip route 10.1.5.0 255.255.255.0 10.1.2.3
```

Step 4 Enable routing on OLT C and configure static routes.

```
Raisecom(config)#ip routing
Raisecom(config)#ip route 10.1.1.0 255.255.255.0 10.1.3.3
Raisecom(config)#ip route 10.1.2.0 255.255.255.0 10.1.3.3
Raisecom(config)#ip route 10.1.5.0 255.255.255.0 10.1.3.3
```

Step 5 Configure the default gateway of PC A to 10.1.5.3. Detailed configurations are as below.

Configure the default gateway of PC B to 10.1.1.3. Detailed configurations are as below.

Configure the default gateway of PC C to 10.1.4.3. Detailed configurations are as below.

Checking results

You can perform the following operations on any OLT to check whether all devices can communicate with each other.

```
Raisecom#ping 10.1.1.3
Sending 5, 72-byte ICMP Echos to 10.1.1.3 , timeout is 1 seconds:
!!!!
Success rate is 100 percent(5/5)
round-trip (ms)  min/avg/max = 0/0/0
```

12 Configuring DHCP

This chapter describes the DHCP feature and configuration process of the device, and provides related configuration examples, including the following sections:

- Introduction
- Configuring DHCP Snooping
- Configuring DHCP Relay
- Configuring DHCP Option 82
- Maintenance
- Configuration examples

12.1 Introduction

12.1.1 DHCP packet

Figure 12-1 shows the DHCP packet structure.

Figure 12-1 DHCP packet structure

0	7	15	23	31
op	htype	hlen	hops	
xid				
secs		flags		
ciaddr				
yiaddr				
siaddr				
giaddr				
chaddr				
sname				
file				
options				

Table 12-1 lists meanings of fields in the DHCP packet.

Table 12-1 Meanings of fields in the DHCP packet

Name	Length (B)	Description
op	1	Packet type • 1: request packet • 2: response packet
htype	1	Hardware address type of a DHCP client
hlen	1	Hardware address length of a DHCP client
hops	1	Number of DHCP relays that DHCP request packet pass The value is added by 1 every time the DHCP request packet passes through a DHCP relay.
xid	4	Transaction ID, a random number chosen by the DHCP client. It is used to identify an address request process.
secs	2	Time elapsed since the DHCP client initiates a DHCP request. At present, it is not used and is set to 0.
flags	2	The left first bit is a broadcast response identifier, which is used to identify the DHCP server sends response packets in the unicast/broadcast mode • 0: unicast • 1: broadcast Other bits are reserved.
ciaddr	4	IP address of the DHCP client, which is padded when the DHCP client is being bound, updated, or rebounded. In addition, this IP address can be used to respond the ARP request.
yiaddr	4	IP address of the DHCP client allocated by the DHCP server
siaddr	4	IP address of the DHCP server
giaddr	4	IP address of the first DHCP relay where the DHCP request packet
chaddr	16	Hardware address of the DHCP client
sname	64	Name of the DHCP server
file	128	Startup configuration file name and routing information about the DHCP client specified by the DHCP server
options	Variable	Optional variable fields, including the packet type, valid lease, IP address of the Domain Name System (DNS) server, and IP address of the Windows Internet Name Server (WINS).

12.1.2 DHCP Snooping

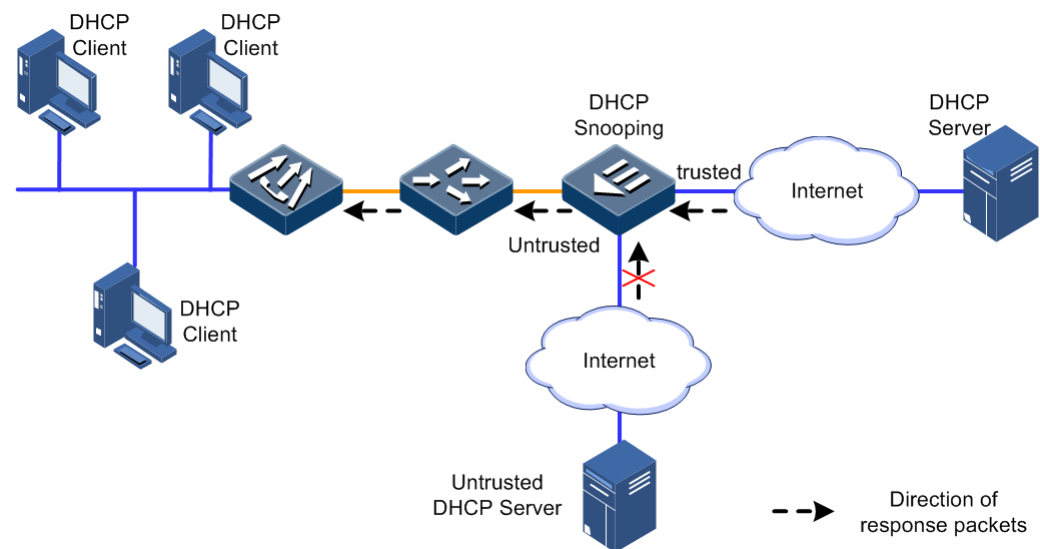
Overview of DHCP Snooping

The DHCP Snooping is a security feature of the DHCP, supporting the following functions:

- Ensure that DHCP clients obtain IP addresses from a legal DHCP server only.

When there is a private DHCP server in the network, DHCP clients may obtain incorrect IP addresses and related configurations, making network communication failed, as shown in Figure 12-2. To ensure that DHCP clients obtain IP addresses from a legal DHCP server, the DHCP Snooping mechanism allows configuring interfaces as trusted/untrusted interfaces. Trusted interfaces can forward received DHCP packets properly while untrusted interfaces will discard packets from DHCP servers.

Figure 12-2 DHCP Snooping networking



- Recoding the relationship between IP addresses and MAC addresses of DHCP clients

The DHCP Snooping records DHCP Snooping entries by listening requests and response packets received by trusted interfaces, including MAC addresses of DHCP clients, obtained IP addresses, interfaces connected to DHCP clients, and VLAN information of these interfaces. With this information, the DHCP Snooping can implement the following functions:

- Dynamic ARP Inspection (DAI): judge whether a user, who sends the ARP packet, is legal or not based on DHCP Snooping entries. It helps prevent illegal users' ARP attack.
- IP Source Guard: filter packets forwarded by an interface by dynamically obtaining DHCP Snooping entries. It helps prevent illegal packets from passing through the interface.

DHCP Snooping supporting Option

Option fields of a DHCP packet records the location information of DHCP clients. With these Option fields, the administrator can locate DHCP clients, and implement security and accounting control of DHCP clients.

If the device is enabled with DHCP Snooping supporting Option, it takes the following two actions when receiving a DHCP packet.

- When the device receives a DHCP request packet, it processes the packet based on whether Option fields are contained in the packet, configured processing policies, and padding modes, and then sends the processed packet to the DHCP server.
- When the device receives a DHCP response packet, if the packet contains an Option field, the device deletes this Option Field and forwards the DHCP request packet to DHCP clients. Otherwise, the device directly sends the DHCP request packet to DHCP clients.

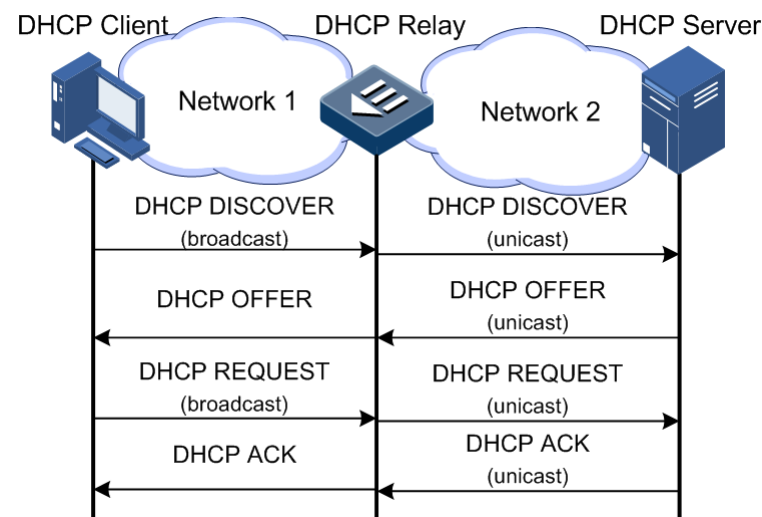
12.1.3 DHCP Relay

The initial DHCP asks DHCP clients and the DHCP server to be at the same network segment. For a network that contains multiple network segments, you must configure a DHCP server for each network segment, which consuming DHCP server resources.

The DHCP relay helps solve this problem. The DHCP relay provides relay services for DHCP clients and DHCP servers at different network segments. Therefore, DHCP clients at different network segments can share a DHCP server.

Figure 12-3 shows the working principle of DHCP Relay.

Figure 12-3 Working principle of DHCP Relay



As shown in Figure 12-3, a DHCP client sends a request packet to a DHCP server through the DHCP Relay. The DHCP Relay receives, processes, and forwards this packet to the DHCP server at a specified network segment. Based on information contained in the request packet, the DHCP server sends a packet back to the DHCP client through the DHCP Relay to finish dynamic configurations on the DHCP client.

12.1.4 DHCP Option 82

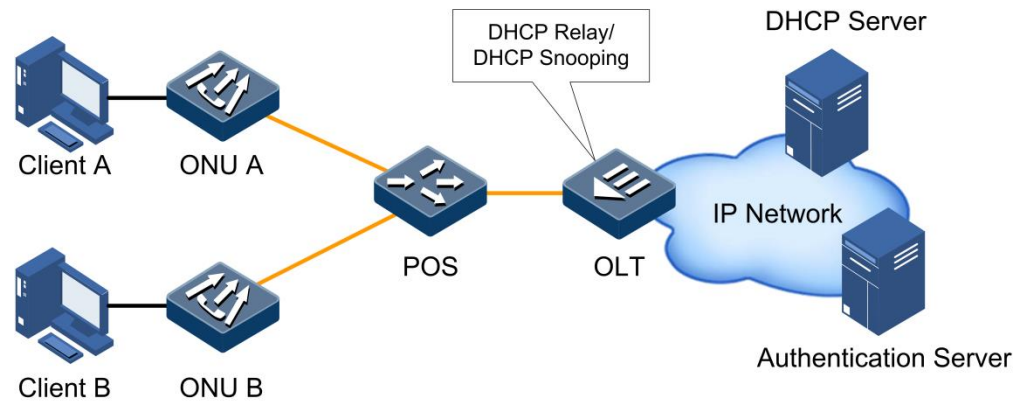
RFC 3046 defines Option 82 (DHCP Relay Agent Information Option), adding some options in the DHCP request packet. These options help the DHCP server locate users more accurately and adopt various address allocation policies for users.

The DHCP Option 82 contains 2 sub-options

- Remote ID (remote ID sub-option)

- Circuit ID (circuit ID sub-option)

Figure 12-4 Working principle of DHCP Option 82



As shown in Figure 12-4, the working process of DHCP Option 82 is as below.

- Step 2 Before a client is authenticated and gets a dynamic IP address, only authentication packets and DHCP packets can pass through the OLT enabled with DHCP Option 82.
- Step 3 The client sends an authentication request to the authentication server through the DHCP Relay/DHCP Snooping. The authentication server can manage the authority of the user.
- Step 4 After the authentication server authenticates the client's legality, it sends an authentication response packet to the client, informing the client's authority.
- Step 5 Based on the authority assigned by the authentication server, the client initiates an IP address request to the DHCP server. At the same time, the client adds its authority information to the DHCP Option 82 option fields.
- Step 6 The DHCP server, which supports DHCP Option 82 address allocation policy, allocates an IP address for the client based on the specified authority information carried in the DHCP Option 82 fields.

By combining the DHCP Option 82, authentication system, and the DHCP server that supports DHCP Option 82 address allocation policy together, you can use DHCP Option 82's Circuit ID and Remote ID sub-options to allocate different IP addresses to users. On one hand, this helps manage IP addresses more accurately. On the other hand, the device can perform policy routing based on the source IP address. Therefore, users with different IP addresses can have various routing rules and network access privileges.

12.2 Configuring DHCP Snooping

12.2.1 Preparing for configurations

Scenario

DHCP Snooping is a DHCP security feature, used to guarantee the DHCP client to get an IP address from the legal DHCP server and record the corresponding relationship between IP addresses and MAC addresses of the DHCP client.

The Option field of a DHCP packet records location information of the DHCP client. Administrators can locate the DHCP client through the Option field and control client security and accounting. The ISCOM6800 and ISCOM6860 configured with DHCP Snooping and Option can perform related operations according to the Option field.

Prerequisite

- DHCP Snooping and DHCP Relay are mutually exclusive. So you need to disable DHCP Relay before configuring DHCP Snooping.
- DHCP Snooping on the interface can take effect only after global DHCP Snooping is enabled. So you need to enable global DHCP Snooping before configuring DHCP Snooping on the interface.

12.2.2 Default configurations

Default configurations of DHCP Snooping on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Global DHCP Snooping	Disable
DHCP Snooping on interface	Enable
DHCP Snooping trust status on interface	Untrusted
DHCP Option 82	Unsupported

Default configurations of DHCP Snooping on the Raisecom ONU devices are as below.

Function	Default value
Global DHCP Snooping	Disabled
Interface DHCP Snooping	Disabled
Interface DHCP Snooping trusted status	Untrusted
DHCP Option 82	Disabled

12.2.3 Configuring global DHCP Snooping/DHCPv6 Snooping

Configuring global DHCP Snooping/DHCP Snooping on OLT

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#{ ip ipv6 } dhcp snooping example: Raisecom(config)#ip dhcp snooping	Enable global DHCP Snooping. You can use the no ip dhcp snooping command to disable this function. • ip: IP address • ipv6: IPv6 address

Configuring global DHCP Snooping on ONU

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id	Enter EPON ONU management configuration mode.
3	Raisecom(config-epon-onu-*//*:*)#ip dhcp snooping { enable disable }	Enable/Disable global DHCP Snooping on the ONU.

12.2.4 Configuring DHCP Snooping on interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#vlan id	Enter VLAN configuration mode.
3	Raisecom(config-vlan-*)#ip dhcp snooping	Enable VLAN DHCP Snooping. You can use the no ip dhcp snooping command to disable this function.

12.2.5 Configuring DHCP Snooping on interface (VLAN range mode)

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#vlan range list	Enter VLAN range configuration mode.
3	Raisecom(config-vlan-range-/*:*)#{ ip ipv6 } dhcp snooping	Enable VLAN DHCP Snooping. You can use the no { ip ipv6 } dhcp snooping command to disable this function.

12.2.6 Configuring DHCP Snooping trust on interface

Configuring DHCP Snooping trust on interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id example: Raisecom(config)#interface gigabitethernet 2/1</pre>	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: 1000 Mbit/s Ethernet interface configuration mode • ten-gigabitethernet: 10 Gbit/s Ethernet interface configuration mode
3	<pre>Raisecom(config-if-*:*:*)#{ ip ipv6 } dhcp snooping trust example: Raisecom(config-if-gigabitethernet- 2:1)#ip dhcp snooping trust</pre>	Enable DHCP Snooping trust on the interface. You can use the no ip dhcp snooping trust command to disable this function. • ip: IP address • ipv6: IPv6 address

Configuring DHCP Snooping trust on ONU interface

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</pre>	Enter EPON ONU UNI configuration mode.
3	<pre>Raisecom(config-epon-onu-ethernet- */*/*:*)#ip dhcp snooping trust { enable disable }</pre>	Enable/Disable DHCP Snooping trust on ONU interface.



Note

Generally, you need to make sure that the device connected interface at the DHCP server side is in trusted status, while the interface at the DHCP client side is in untrusted status

12.2.7 (Optional) configuring DHCP Snooping supporting Option 82

Configuring OLT DHCP Snooping Option 82

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#ip dhcp information option</pre>	Configure DHCP Snooping supporting Option 82. You can use the no ip dhcp information option command to disable this function.

Configuring DHCP Snooping DHCP Option 82 on ONU

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id	Enter EPON ONU management configuration mode.
3	Raisecom(config-epon-onu-*//*:*)#ip dhcp snooping information option82 user-defined { enable disable }	(Optional) enable/disable customizing the DHCP Option 82.



Note

If the device is enabled with DHCP Snooping without being configured with the DHCP Snooping supporting Option 82 function, the device will not process Option 82 fields in the packets. For packets without Option 82 fields, the device also does not perform insertion operation.

12.2.8 Checking configurations

No.	Command	Description
1	Raisecom#show ip dhcp snooping	Show DHCP Snooping configurations.
2	Raisecom#show ip dhcp snooping binding	Show information about the DHCP Snooping binding table.
3	Raisecom#show vlan id ip dhcp snooping	Show DHCP Snooping status of the VLAN.
4	Raisecom#show ip dhcp snooping statistics	Show DHCP Snooping statistics.
5	Raisecom#show ip dhcp snooping vlan Raisecom#show ipv6 dhcp snooping vlan	Show configurations of the DHCP Snooping VLAN.

Checking ONU configurations

No.	Command	Description
1	Raisecom#show epon-onu slot-id/olt-id/onu-id ip dhcp snooping	Show DHCP Snooping configurations.
2	Raisecom#show epon-onu slot-id/olt-id/onu-list ip dhcp snooping binding	Show information about the DHCP Snooping binding table.
3	Raisecom#show epon-onu slot-id/olt-id/onu-list uni ethernet [uni-id] ip dhcp snooping	Show DHCP Snooping configurations on the UNI.
4	Raisecom#show epon-onu slot-id/olt-id/onu-list uni ethernet [uni-id] ip dhcp snooping statistics	Show statistics of DHCP packets on the UNI.

12.2.9 Maintenance

No.	Command	Description
1	<code>Raisecom(config)#clear ip dhcp snooping binding</code>	Clear DHCP Snooping binding table.
2	<code>Raisecom(config)#clear ip dhcp snooping statistics</code>	Clear DHCP Snooping statistics.
3	<code>Raisecom(config)#clear ip dhcp relay binding</code>	Clear DHCP Relay binding table.
4	<code>Raisecom(config)#clear epon-onu slot-id/olt-id/onu-list uni ethernet [uni-id] ip dhcp relay statistics</code> example: <code>Raisecom(config)#clear epon-onu 3/1/1 uni ethernet 1 ip dhcp relay statistics</code>	Clear DHCP Relay statistics on the ONU UNI. - slot-id/olt-id/onu-list: ONU ID list. The slot-id refers to the slot ID, which is an integer; the olt-id refers to the PON interface ID, which is an integer; the onu-list refers to the OUN list of the PON interface, which is an integer. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". - uni-id: UNI ID, an integer
5	<code>Raisecom(config)#clear epon-onu slot-id/olt-id/onu-list uni ethernet [uni-id] ip dhcp snooping statistics</code> example: <code>Raisecom(config)#clear epon-onu 3/1/1 uni ethernet 1 ip dhcp snooping statistics</code>	Clear DHCP Snooping statistics on the ONU UNI. - slot-id/olt-id/onu-list: ONU ID list. The slot-id refers to the slot ID, which is an integer; the olt-id refers to the PON interface ID, which is an integer; the onu-list refers to the OUN list of the PON interface, which is an integer. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". - uni-id: UNI ID, an integer

12.3 Configuring DHCP Relay

12.3.1 Preparing for configurations

Scenario

When the DHCP client and DHCP server are in different network segments, you can use DHCP Relay to solve the problem. It can make the DHCP client and DHCP server in different network segments bear relay services, and relay DHCP protocol packets through network segments to the destination DHCP server, so that DHCP clients in different network segments can share the same DHCP server.

Prerequisite

- DHCP Snooping and DHCP Relay are mutually exclusive. So you need to disable DHCP Snooping before configuring DHCP Relay.

- DHCP Relay on the interface can take effect only after global DHCP Relay is enabled. So you need to enable global DHCP Relay before configuring DHCP Relay on the interface.

12.3.2 Default configurations

Default configurations of DHCP Relay on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Global DHCP Relay	Disable
DHCP Relay on interface	Enable
Destination IP address of interface enabled with DHCP Relay	N/A
Destination IP address of interface enabled with DHCP Relay on ONU	N/A
DHCP Relay trust status on interface	Untrusted
DHCP Option 82	Unsupported
Processing policy of request packets containing Option 82 field	Replace

12.3.3 Configuring global DHCP Relay

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip dhcp relay	Enable global DHCP Relay. You can use the no ip dhcp relay command to disable this function.

12.3.4 Configuring DHCP Relay on IP interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlanif id	Enter IP interface configuration mode.
3	Raisecom(config-vlanif-*)#ip dhcp relay	Configure DHCP Relay on the IP interface. You can use the no ip dhcp relay command to disable this function.

12.3.5 Configuring destination IP address of interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlanif <i>vlan-id</i> example: Raisecom(config)#interface vlanif 2	Enter VLAN interface configuration mode. • <i>vlan-id</i> : VLAN interface ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlanif-*)#ip dhcp relay	Enable DHCP Relay on the IP interface. You can use the no ip dhcp relay command to disable this function.
4	Raisecom(config)#ip dhcp relay interface vlanif { <i>all</i> <i>port-list</i> } target-ip <i>ip-address</i> example: Raisecom(config)#ip dhcp relay interface vlanif all target-ip 10.0.0.1	(Optional) configure the destination IP address of the VLAN interface. • <i>all</i> : all IP interfaces • <i>ip-list</i> : IP interface list, an integer, ranging from 0 to 31 • <i>ip-address</i> : VLAN destination IP address, in dotted decimal notation, such as 10.10.10.1



Note

- Each IP interface can be configured with up to 4 destination IP addresses.
- When the DHCP client connects the DHCP server through multiple DHCP relays, we recommend that the number of DHCP relays does not exceed 4.

12.3.6 Configuring destination IPv6 address on interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlanif <i>vlan-id</i> example: Raisecom(config)#interface vlanif 2	Enter VLAN interface configuration mode. <i>vlan-id</i> : VLAN interface ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlanif-*)#ipv6 dhcp relay	Configure DHCPv6 Relay on the IPv6 interface. You can use the no ipv6 dhcp relay command to disable this function.
4	Raisecom(config-vlanif-*)#ipv6 dhcp relay target-ip <i>ipv6-address</i> example: Raisecom(config-vlanif-2)#ipv6 dhcp relay target-ip 3001::1	(Optional) configure the destination IP address of the VLAN interface. • <i>ipv6-address</i> : IPv6 address, in colon hexadecimal notation, such as 3001::1

12.3.7 Configuring ONU DHCP Relay

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/1/1	Enter EPON ONU remote management mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*/*:*)#ip dhcp relay { enable disable }	Enable/Disable global DHCP Relay on the ONU.
4	Raisecom(config-epon-onu-*/*:*)#ip dhcp relay information option82 user-defined { enable disable }	Enable/Disable ONU DHCP Relay Option 82 to be/from being user-defined.
5	Raisecom(config-epon-onu-*/*:*)#ip dhcp relay ip-list ip-list target-ip ip-address example: Raisecom(config-epon-onu-3/1:1)#ip dhcp relay ip-if 1 target-ip 10.0.0.1	Configure the destination IP address of the ONU DHCP Relay IP interface. - ip-list: interface list, an integer, ranging from 0 to 14. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". - ip-address: IP address, in dotted decimal notation, such as 10.10.10.1
6	Raisecom(config-epon-onu-*/*:*)#exit Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id	Enter EPON ONU UNI configuration mode.
7	Raisecom(config-epon-onu-ethernet-*/*/*:*)#ip dhcp relay trust { enable disable }	Enable/Disable DHCP Relay trust on the ONU interface.
8	Raisecom(config-epon-onu-ethernet-*/*/*:*)#exit	Return back to ONU remote management configuration mode.

12.3.8 Configuring DHCP Relay trusted interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { gigaethernet ten-gigaethernet epon-olt ten-giga-epon-olt gpon-olt } slot-id/port-id	Enter physical interface configuration mode.
3	Raisecom(config-if-*/*:*)#ip dhcp relay information trusted	Configure a DHCP Relay trusted interface. You can use the no ip dhcp relay information trusted command to restore default configuration.



Note

Interface trust can take effect only when DHCP Relay supports DHCP Option 82.

12.3.9 Configuring DHCPv6 Relay on IP interface

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>vlanif id</i>	Enter IP interface configuration mode.
3	Raisecom(config-vlanif-*)# ipv6 dhcp relay	Configure DHCPv6 Relay on the IP interface. You can use the no ip dhcp relay command to disable this function.

12.3.10 (Optional) configuring policies for processing DHCP Relay request packets

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config-epon-onu-*/*:*)# exit Raisecom(config)# epon-onu uni ethernet <i>slot-id/olt-id/onu-id/uni-id</i> example: Raisecom(config)#epon-onu uni ethernet 3/2/1/1	Enter EPON ONU UNI configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • uni-id: ONU UNI ID
3	Raisecom(config-epon-onu-ethernet-*/*/*:*)# ip dhcp relay option82 policy { drop keep replace } example: Raisecom(config-epon-onu-ethernet-3/2/1:1)# ip dhcp relay option82 policy keep	Configure policies for processing DHCP Relay request packets. You can use the no ip dhcp relay option82 policy command to restore to default conditions. • drop: drop DHCP request packets with Option82. • keep: do not change DHCP request packets with Option82. • replace: replace Option 82 in the DHCP request packet.

12.3.11 Checking configurations

No.	Command	Description
1	Raisecom# show ip dhcp relay	Show DHCP Relay configurations.
2	Raisecom# show ip dhcp relay statistics	Show DHCP Relay statistics.

No.	Command	Description
3	Raisecom# show epon-onu slot-id/olt-id/onu-list ip dhcp relay	Show ONU DHCP Relay configurations.
4	Raisecom# show epon-onu slot-id/olt-id/onu-id uni ethernet [uni-id] ip dhcp relay	Show DHCP Relay configurations of the ONU UNI.
5	Raisecom# show epon-onu slot-id/olt-id/onu-list ip dhcp relay ip-if	Show configurations of the ONU DHCP Relay IP interface.
6	Raisecom# show epon-onu slot-id/olt-id/onu-id uni ethernet [uni-id] ip dhcp relay statistics	Show DHCP Relay statistics on the ONU UNI.
7	Raisecom# show interface vlanif id { ip ipv6 } dhcp relay	Show DHCP Relay status on the VLAN interface.
8	Raisecom# show ipv6 dhcp relay	Show configurations of DHCPv6 Relay.
9	Raisecom# show ipv6 dhcp relay statistics	Show statistics of DHCPv6 Relay.

12.4 Configuring DHCP Option 82

12.4.1 Preparing for configurations

Scenario

RFC 3046 defines DHCP Option 82 and adds some option information in the DHCP request packet to make the DHCP server determine user's location more accurately, and then take different address assignment strategies to different users.

Prerequisite

Enable DHCP Snooping or DHCP Relay.



Note

- Before configuring DHCP Option 82, you need to enable customized DHCP Option 82 firstly.
- To enable customized DHCP Option 82, see section 12.2.7 (Optional) configuring DHCP Snooping supporting Option 82.

12.4.2 Default configurations

Default configurations of DHCP Option 82 on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Global DHCP Option 82	Disable
Global DHCP Option attach-string	N/A

Function	Default value
Global remote-id	Switch-mac
Circuit-id of interface	N/A
Processing policy of DHCP packets containing Option 82 field	Transparent

Default configurations of DHCP Option 82 on the Raisecom ONU devices are as below.

Function	Default value
Global DHCP Option 82	Disable
Global DHCP Option attach-string	Null
Global remote-id mode	onumac
Interface circuit-id	Null

12.4.3 Enabling DHCP Option 82

Enabling DHCP Option82 on OLT

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip dhcp information option	Enable DHCP Option 82. You can use the no ip dhcp information option command to disable this function.

Enabling ONU Option82

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id	Enter EPON ONU management configuration mode.
3	Raisecom(config-epon-onu-*//*:*)#ip dhcp information option82 { enable disable }	Enable/Disable ONU Option82.

12.4.4 Configuring global DHCP Option attach-string

Configuring global DHCP Option attach-string on ONU

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/1/1	Enter EPON ONU remote management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*//*:*)#ip dhcp information option82 attach-string attach-string example: Raisecom(config-epon-onu-3/1:1)#ip dhcp information option82 attach-string raisecom	Configure the attach-string of Option 82 for the ONU. You can use the no ip dhcp information option82 attach-string command to restore default configurations. • attach-string: attach string, a string of 1 to 64 characters

12.4.5 Configuring global DHCP Option remote-id

Configuring global DHCP Option remote-id on OLT

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip dhcp information option remote-id { switch-mac client-mac switch-mac-string client-mac-string hostname string string } example: Raisecom(config)#ip dhcp information option remote-id switch-mac-string	Configure the remote ID of Option 82. You can use the no ip dhcp information option remote-id command to restore default configuration. • client-mac: the remote ID is the MAC address of the user, sent in binary form. • client-mac-string: the remote ID is the MAC address of the user, sent in form of a character string. • hostname: the remote ID is the host name, sent in form of a character string. • switch-mac: the remote ID is the MAC address of the device, sent in binary form. • switch-mac-string: the remote ID is the MAC address of the device, sent in form of a character string. • string string: the remote ID is the one customized by the user, which is a string of 1 to 64 characters.

Configuring global DHCP Option remote-id on ONU

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/1/1	Enter EPON ONU remote management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*//*:*)#ip dhcp information option82 remote-id string string example: Raisecom(config-epon-onu-3/1:1)#ip dhcp information option82 remote-id string raisecom	Configure the remote ID of Option 82. You can use the no ip dhcp information option82 remote-id string command to restore default configurations. • string: the remote ID is the MAC address of the device, which is sent in form of a character string. The string is user-defined remote ID, which is a string of 1 to 64 characters.
4	Raisecom(config-epon-onu-*//*:*)#ip dhcp information option82 remote-id mode { client-mac client-mac-string hostname onu-mac onu-mac-string user-defined string } example: Raisecom(config-epon-onu-3/1:1)#ip dhcp information option82 remote-id mode clientmac	Configure the filling mode of Option 82 remote ID. You can use the no ip dhcp information option82 remote-id mode command to restore default configurations. • onumac: the remote ID is the ONU MAC address, sent in binary form. • clientmac: the remote ID is the MAC address of the user host, sent in binary form. • onumac-string: the remote ID is the ONU MAC address, sent in form of a character string. • clientmac-string: the remote ID is the MAC address of the user host, sent in form of a character string. • hostname: the remote ID is the user host name, sent in form of a character string. • user-defined: the remote ID is user-defined. • string string: the remote ID is the MAC address of the device, sent in form of a character string. The string is the user-defined remote ID, ranging from 1 to 64 characters.

12.4.6 Configuring DHCP Option circuit-id on interface

Configuring DHCP Option circuit-id on OLT interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id</pre> example: <pre>Raisecom(config)#interface gigabitethernet 2/1</pre>	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode
3	<pre>Raisecom(config-if-*:*:*)#ip dhcp information option circuit-id string</pre> example: <pre>Raisecom(config-if-gigabitethernet-1:1)#ip dhcp information option circuit-id 1</pre>	Configure the CID sub-option of Option 82 on the interface. You can use the no ip dhcp informaion option circuit-id command to restore default configuration. • circuit-id: circuit ID, a character string, ranging from 1 to 63

Configuring DHCP Option circuit-id on interface

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</pre> example: <pre>Raisecom(config)#epon-onu uni ethernet 3/2/1/1</pre>	Enter EPON ONU UNI configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • uni-id: ONU UNI ID
3	<pre>Raisecom(config-epon-onu-ethernet-*/*/*:*)#ip dhcp information option82 circuit-id string</pre> example: <pre>Raisecom(config-epon-onu-ethernet-3/1/1:1)#ip dhcp information option82 circuit-id 1</pre>	Configure the circuit ID of Option 82 on the ONU UNI. You can use the no ip dhcp informaion option82 circuit-id command to restore default conditions. • circuit-id: circuit ID, a string of 1 to 64 characters

12.4.7 Configuring processing policy of Option 82 packet

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id</pre> example: <pre>Raisecom(config)#interface gigabitethernet 2/1</pre>	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode
3	<pre>Raisecom(config-if-*:*:*)#ip dhcp information option overwrite-policy { drop transparent }</pre> example: <pre>Raisecom(config-if-gigabitethernet-2:1)#ip dhcp information option overwrite-policy drop</pre>	Configure the processing policy to the DHCP request packet containing Option 82 on the interface. You can use the no ip dhcp information option overwrite-policy command to restore default configuration. • drop: drop DHCP Option82 request packets. • transparent: keep the DHCP Option82 request packets unchanged.
4	<pre>Raisecom(config-if-*:*:*)#ip dhcp information option overwrite-policy circuit-id replace { length len }</pre> example: <pre>Raisecom(config-if-gigabitethernet-2:1)#ip dhcp information option overwrite-policy replace length 20</pre>	Configure the processing policy to the circuit ID of the DHCP request packet containing Option 82. You can use the no ip dhcp information option overwrite-policy command to restore default conditions. • length len: replace the length of the DHCP Option82 request packet. The length is an integer ranging from 1 to 64.

12.4.8 Checking configurations

Checking OLT configurations

No.	Command	Description
1	<pre>Raisecom#show ip dhcp information option</pre>	Show DHCP Option configurations.

Checking ONU configurations

No.	Command	Description
1	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id ip dhcp information option82</pre>	Show configurations of DHCP Option82.
2	<pre>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id ip dhcp information option82</pre>	Show configurations of UNI DHCP Option82.

12.5 Maintenance

No.	Command	Description
1	Raisecom(config)#clear epon-onu slot-id/olt-id/onu-id uni ethernet uni-id ip dhcp snooping statistics example: Raisecom(config)#clear epon-onu 3/1/1 uni ethernet 1 ip dhcp snooping statistics	Clear DHCP Snooping statistics on the ONU UNI. - slot-id/olt-id/onu-list: ONU ID list. The slot-id refers to the slot ID, which is an integer; the olt-id refers to the PON interface ID, which is an integer; the onu-list refers to the OUN list of the PON interface, which is an integer. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". - uni-id: UNI ID, an integer
2	Raisecom(config)#clear epon-onu slot-id/olt-id/onu-id uni ethernet [uni] ip dhcp relay statistics example: Raisecom(config)#clear epon-onu 3/1/1 uni ethernet 1 ip dhcp relay statistics	Clear DHCP Relay statistics on the ONU interface. - slot-id/olt-id/onu-list: ONU ID list. The slot-id refers to the slot ID, which is an integer; the olt-id refers to the PON interface ID, which is an integer; the onu-list refers to the OUN list of the PON interface, which is an integer. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". - uni-id: UNI ID, an integer
3	Raisecom(config)#clear ip dhcp relay statistics	Clear DHCP Relay statistics.
4	Raisecom(config)#clear ip dhcp snooping binding	Clear the DHCP Snooping binding table.
5	Raisecom(config)#clear ip dhcp snooping statistics	Clear DHCP Snooping statistics.

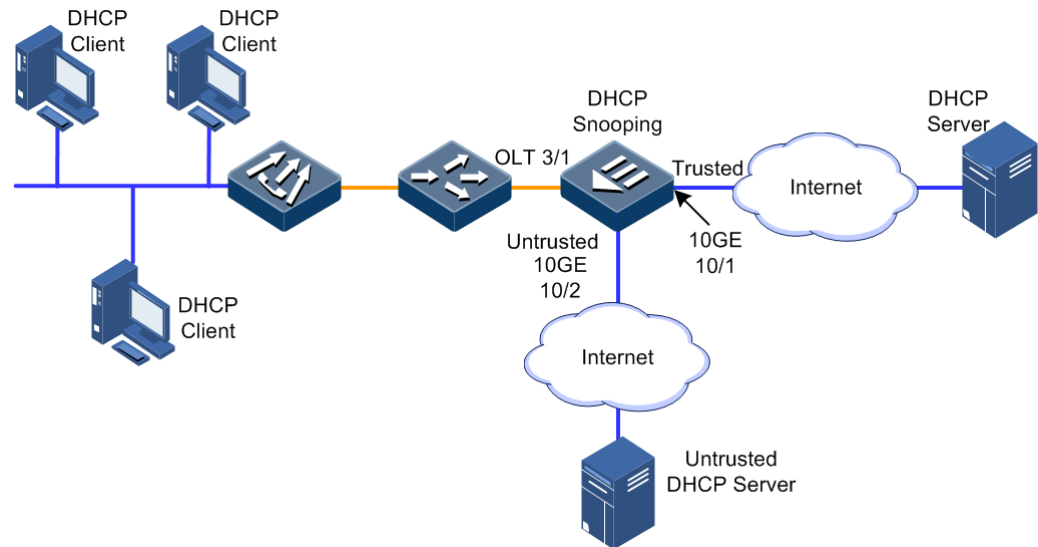
12.6 Configuration examples

12.6.1 Example for configuring DHCP Snooping

Networking requirements

As shown in Figure 12-5, the OLT, which works as a DHCP Snooping device, needs to ensure that the DHCP client can obtain IP addresses from a legal DHCP server. In addition, the OLT supports DHCP Option 82 to manage the DHCP client. Configure the filling information of the Circuit ID sub-option on interface OLT 3/1 as raisecom, and filling information of the Remote ID sub-option as user 01.

Figure 12-5 DHCP Snooping networking



Configuration steps

Step 1 Configure global DHCP Snooping.

```
Raisecom#config  
Raisecom(config)#ip dhcp snooping  
Raisecom(config)#vlan 1  
Raisecom(config-vlan-1)#ip dhcp snooping  
Raisecom(config-vlan-1)#exit
```

Step 2 Configure the trusted interface.

```
Raisecom(config)#interface ten-gigaethernet 10/1  
Raisecom(config-if-ten-gigaethernet-10:1)#ip dhcp snooping trust  
Raisecom(config-if-ten-gigaethernet-10:1)#exit
```

Step 3 Configure supporting DHCP Option82 and configure the Option 82 field.

```
Raisecom(config)#ip dhcp information option  
Raisecom(config)#ip dhcp information option remote-id string user01  
Raisecom(config)#interface epon-olt 3/1  
Raisecom(config-if-epon-olt-3:1)#ip dhcp information option circuit-id  
raisecom
```

Checking results

Use the **show ip dhcp information option** command to show DHCP client configurations.

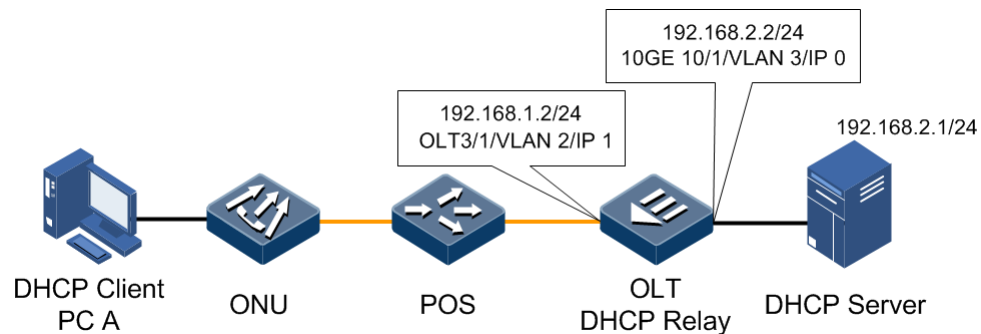
```
Raisecom#show ip dhcp information option
DHCP Option Config Information
Option 82: Enabled
Remote-ID Mode: string
Remote-ID String: user01
Port          Op82Policy    CircuitId
-----
Ten-gigabitethernet10/1  replace    --
epon-olt3/1          replace    raisecom
```

12.6.2 Example for configuring DHCP Relay

Networking requirements

As shown in Figure 12-6, the OLT, which works as a DHCP Relay device, needs to ensure that the DHCP client can obtain IP addresses through network segments. In addition, the OLT supports DHCP Option 82 to manage the DHCP client.

Figure 12-6 DHCP Relay networking



Configuration steps

Step 1 Configure global DHCP Relay.

```
Raisecom#config
Raisecom(config)#ip dhcp relay
Raisecom(config)#interface vlanif 2
Raisecom(config-vlanif-2)#ip dhcp relay
Raisecom(config-vlanif-1)#exit
Raisecom(config)#interface vlanif 3
Raisecom(config-vlanif-3)#ip dhcp relay
```

Step 2 Configure the destination IP address of IP interface 1.

```
Raisecom(config)#ip dhcp relay interface vlanif 2 target-ip 192.168.2.1
```

Step 3 Configure the device to support Option82.


```
Raisecom(config)#ip dhcp information option
```

Step 4 Configure 10GE interface 10/1 as the DHCP Relay trusted interface.

```
Raisecom(config)#interface ten-gigabitethernet 10/1
Raisecom(config-if-ten-gigabitethernet-10:1)#ip dhcp relay information
trusted
```

Checking results

Use the **show ip dhcp relay** command to show DHCP Relay configurations.

```
Raisecom#show ip dhcp relay
IP Interface  Enabled Status  Target IP Address
-----
0           Enabled  192.168.2.1
1           Enabled  --
2           Enabled  --
3           Enabled  --
4           Enabled  --
5           Enabled  --
6           Enabled  --
7           Enabled  --
8           Enabled  --
9           Enabled  --
10          Enabled  --
11          Enabled  --
12          Enabled  --
13          Enabled  --
14          Enabled  --
```

13 Configuring QoS (Applicable to the XEP8 (B) card)

This chapter describes the QoS feature and configuration process of the ISCOM6800 and ISCOM6860, and provides related configuration examples, including the following sections:

- Introduction
- Configuring traffic classification
- Configuring traffic monitoring
- Configuring traffic shaping
- Configuring congestion avoidance
- Configuring congestion management
- Configuring traffic policy
- Configuration examples

13.1 Introduction

Generally, Internet (IPv4), which bases on the store-and-forward mechanism, only provides "best-effort" service for users. When the network is overloaded or congested, this service mechanism cannot ensure that packets be transmitted timely and completely.

With the ever-growing of network application, users bring different service quality requirements on network application. Then network should distribute and schedule resources for different network applications according to users' demands.

Quality of Service (QoS) can ensure real-time and integrated service when the network is overloaded or congested and guarantee that the whole network runs efficiently.

13.1.1 Priority trust

Priority trust refers to that a packet adopts its own priority as the classification standard to perform follow-up QoS management on the packet. In general, the bigger the value is, the higher the priority is.

The ISCOM6800 and ISCOM6860 support port-based priority trust. The priorities are divided into priority based on Differentiated Services Code Point (DSCP) of IPv4 packets, priority

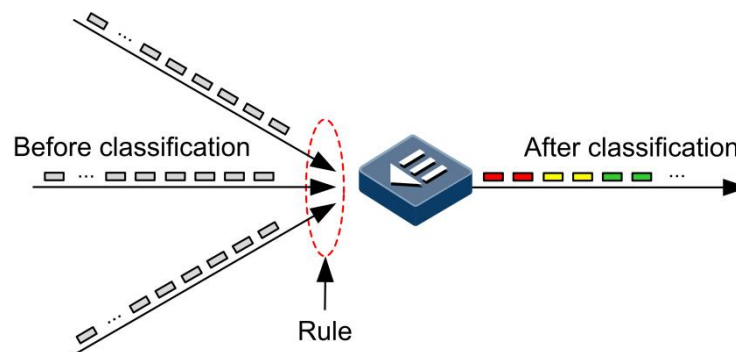
based on Class of Service (CoS) of VLAN packets, and priority based on Traffic Class (TC) of IPv6 packets.

13.1.2 Traffic classification

Traffic classification is a process that recognizes specified packets according to some certain rules. Packets matching different rules will be implemented with different QoS policies. Traffic classification is the prerequisite and basis for providing services differently.

The ISCOM6800 and ISCOM6860 support traffic classification based on Type of Service (ToS) priority and DSCP priority of IPv4 packets, TC of IPv6 packets, Access Control List (ACL) rules, and VLAN IDs. Figure 13-1 shows the traffic classification process.

Figure 13-1 Traffic classification process



ToS priority and DSCP priority

Figure 13-2 shows the IP packet header structure. An 8-bit ToS field is contained in this packet. The RFC1349 defines the first 3 bits of the ToS field representing the ToS priority, ranging from 0 to 7. In the RFC2474, the ToS field is re-defined. The first 6 bits (0–5 bits) represent the priority of IP packets, which is called DSCP priority, ranging from 0 to 63, where the last 2 bits (6 and 7 bits) are reserved bits. Figure 13-3 shows structures of ToS and DSCP priority packets.

Figure 13-2 IP packet header structure

4	8	16	32
Version	IHL	ToS	Total Length
Identification		Flags	Fragment Offset
Time-to-Live	Protocol	Header Checksum	
Source Address			
Destination Address			

Figure 13-3 Structures of ToS priority and DSCP priority packets

Bits:	0	1	2	3	4	5	6	7
RFC1349:	Precedence		Type of Service				0	
RFC2474:	DSCP						Unused	

CoS priority

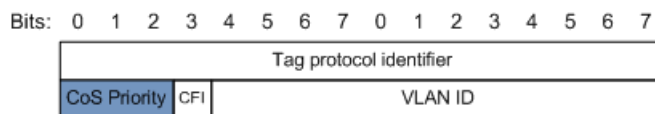
IEEE802.1Q-based VLAN packets are a modification of Ethernet packets. A 4-bit 802.1Q header is added between the source MAC address and protocol type, as shown in Figure 13-4. The 802.1Q header consists of a 2-bit Tag Protocol Identifier (TPID, valuing 0x8100) filed and a 2-bit Tag Control Information (TCI) field.

Figure 13-4 VLAN packet structure



The first 3 bits of TCI field represent the CoS priority, which ranges from 0 to 7, as shown in Figure 13-5. The bigger the number is, the higher the CoS priority is. CoS priority is used for ensuring service quality in Layer 2 network.

Figure 13-5 CoS priority packet structure



FL priority and TC priority

The IPv6 protocol supports FL priority-based and TC priority-based data traffic classification.

An IPv6 data packet contains a 40-byte basic header and an extension header with a fixed length. The TC field and FL field in the basic header of an IPv6 packet are related to QoS.

- TC field: an 8-bit field, like ToS of the TPv4 packet header, is used to identify service types of packets.
- FL field: a 20-bit field, used to identify packets from of same service flow. In addition, it can be used to re-classify packets of the same flow. Together with source and destination addresses, FL is uniquely identifying a service flow. All packets from the same service flow share the same FL. Therefore, the system can adopt identical processing modes on these packets.

13.1.3 Traffic policy

After performing traffic classification on packets, you need to perform different operations on packets in different categories. A traffic policy is a QoS policy in which traffic classification is bound to traffic behaviors.

Rate limiting based on traffic policy

Rate limiting refers to limiting network traffics. Rate limiting is used to control the rate of traffic in the network and drop the traffic that exceeds the rate. Therefore, you can control the traffic rate within a reasonable range. In addition, network resources and Carrier's benefits are protected.

Redirection

Redirection refers to that a packet is not forwarded according to the mapping between the original destination address and the interface. Instead, the packet is redirected to a specified interface for forwarding, realizing policy routing.

Remarking

Re-marking refers to reconfiguring some priority fields of the packet, so that devices can re-classify packets based on their own standards. In addition, downstream nodes can provide differentiated QoS services depending on remarking information.

13.1.4 Priority mapping

Priority mapping refers to sending packets to different queues with different local priorities according to configured mapping between external priority and local priority. Therefore, packets in different queues can be scheduled on the egress interface.



Note

The local priority refers to an internal priority that is assigned to the packet. It is related to the queue number on the egress interface. The bigger the value is, the more quickly the packet is processed.

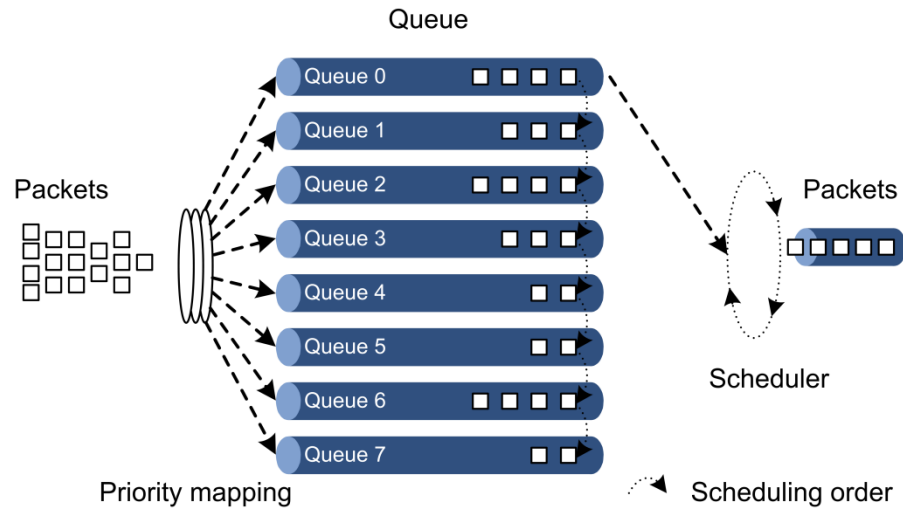
13.1.5 Congestion management

You need to perform the queue scheduling when delay-sensitive services need better QoS services than non-delay sensitive services and when the network is congested once in a while.

Queue scheduling adopts different scheduling algorithms to send packets in a queue. Scheduling algorithms supported by the ISCOM6800 and ISCOM6860 include Strict Priority (SP), Weight Round Robin (WRR), Deficit Round Robin (DRR), and SP+WRR. All scheduling algorithms are designed for addressing specified traffic problems. And they have different effects on bandwidth distribution, delay, and jitter.

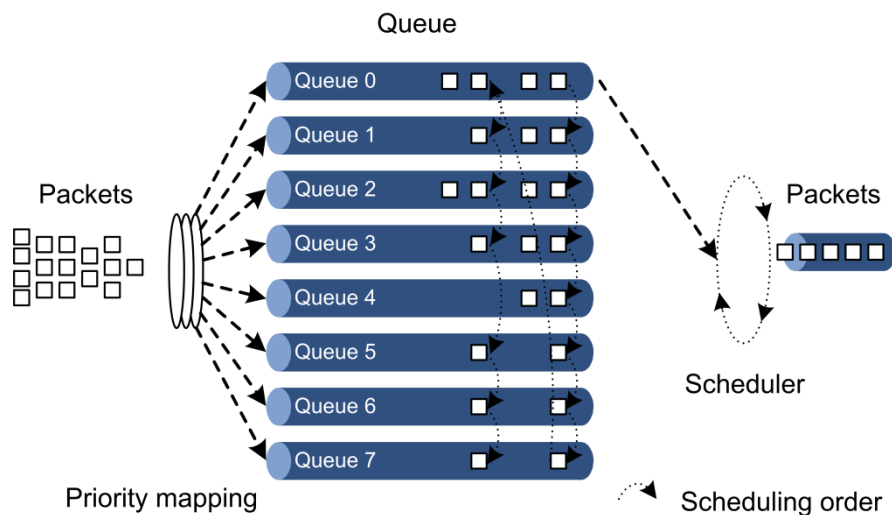
- SP: the device strictly schedules packets in a descending order of priority. Packets with lower priority cannot be scheduled until packets with higher priority are scheduled, as shown in Figure 13-6.

Figure 13-6 SP scheduling



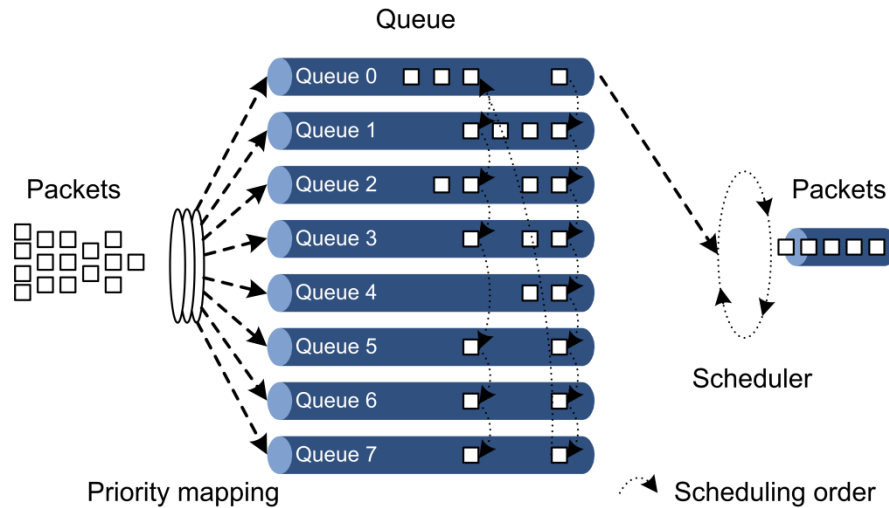
- WRR: on the basis of scheduling packets in a polling manner according to the priority, the device schedules packets according to the weight of the queue, as shown in Figure 13-7.

Figure 13-7 WRR scheduling



- DRR: on the basis of scheduling packets in a polling manner according to the priority, the device schedules packets according to the weight of the queue. In addition, during the scheduling, if one queue has redundant bandwidth, the device will temporarily assign this bandwidth to another queue. During next scheduling, the assigned schedule will return equal bandwidth to the original queue, as shown in Figure 13-8.

Figure 13-8 DRR scheduling



- **SP+WRR:** a scheduling mode combining the SP scheduling and the WRR scheduling together. In this mode, queues on a port are divided into 2 groups. You can specify the some queues to perform SP scheduling and others to perform WRR scheduling.

13.2 Configuring traffic classification

13.2.1 Preparing for configurations

Scenario

Traffic classification refers to identifying certain packets according to specified rules and performing different QoS policies on packets matched with different rules. Traffic classification is the premise and basis for differentiated services.

Traffic classification refers to indexing the mapping table according to the priority (such as DSCP priority) of the packet and mapping the packet priority to the local priority for traffic monitoring, congestion avoidance, and congestion management. Traffic classification is mainly used in the core nodes on the network and trusts priority information carried by the packet.

Prerequisite

N/A

13.2.2 Default configurations

Priority trust

Default configurations of priority trust are as below.

Function	Default value
Priority trust type on OLT	CoS

Function	Default value
Default priority of OLT interface	0

Priority mapping

Mapping among the CoS priority, local priority, and queue on the ISCOM6800 and ISCOM6860 is as below.

CoS priority	0	1	2	3	4	5	6	7
Local priority	0	1	2	3	4	5	6	7
Queue	0	1	2	3	4	5	6	7

Mapping among the DSCP priority, local priority, and queue on the ISCOM6800 and ISCOM6860 is as below.

DSCP priority	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
Local priority	0	1	2	3	4	5	6	7
Queue	0	1	2	3	4	5	6	7

13.2.3 Configuring priority trust

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { epon-olt ten-giga-epon- olt gpon-olt gigabitethernet ten- gigabitethernet } slot- id/port-id example: Raisecom(config)#interface gigabitethernet 2/1	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode

Step	Command	Description
3	<code>Raisecom(config-if-*:*:*)#mls qos trust dscp</code>	Configure trusting the DSCP field. You can use the no mls qos trust command to restore default configuration.  Note - For IPv4 packets, this command refers to trusting the DSCP field. For IPv6 packets, this command refers to trusting the Traffic Class field. - By default, interfaces on the device trust the CoS priority. Therefore, when you need to configure trusting the CoS priority, use the no form of this command to restore default configuration.
4	<code>Raisecom(config-if-*:*:*)#mls qos priority value</code> example: <code>Raisecom(config-if-gigabitethernet-1:1)#mls qos priority 1</code>	Configure the default priority of the interface. You can use the no mls qos priority command to restore default configuration.  Note For packets without the 802.1p field, use the default priority. value: interface default priority, an integer, ranging from 0 to 7

13.2.4 Configuring priority mapping

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mls qos mapping cos cos-value to localpriority local-priority</code> example: <code>Raisecom(config)#mls qos mapping cos 5 to localpriority 3</code>	(Optional) configure mapping between the CoS priority and local priority. You can use the no mls qos mapping cos command to restore default configuration. - cos-value: CoS value, an integer, ranging from 0 to 7 - local-priority: internal priority, an integer, ranging from 0 to 7
3	<code>Raisecom(config)#mls qos mapping dscp dscp-value to localpriority local-priority</code> example: <code>Raisecom(config)#mls qos mapping dscp 5 to localpriority 3</code>	(Optional) configure mapping between the DSCP priority and local priority. You can use the no mls qos mapping dscp command to restore default configuration. - dscp-value: DSCP value, an integer, ranging from 0 to 63 - local-priority: internal priority, an integer, ranging from 0 to 7

Step	Command	Description
4	<pre>Raisecom(config)#mls qos mapping localpriority local-priority to queue queue-id</pre> example: <pre>Raisecom(config)#mls qos mapping localpriority 5 to queue 3</pre>	(Optional) configure mapping between the local priority and queue. You can use the no mls qos mapping localpriority command to restore default configuration. - local-priority: internal priority, an integer, ranging from 0 to 7 - queue-id: queue ID, an integer, ranging from 0 to 7

13.2.5 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show interface { gigabitethernet ten-gigabitethernet epon-olt ten- giga-epon-olt gpon-olt } slot-id/port-id mls qos</pre>	Show QoS configurations on the interface, including interface trust mode, queue scheduling mode, and default CoS value.
2	<pre>Raisecom#show mls qos mapping cos</pre>	Show mapping between the CoS priority and local priority.
3	<pre>Raisecom#show mls qos mapping dscp</pre>	Show mapping between the DSCP priority and local priority.
4	<pre>Raisecom#show mls qos mapping local- priority</pre>	Show mapping between the local priority and queue.

13.3 Configuring traffic monitoring

13.3.1 Preparing for configurations

Scenario

Traffic monitoring is mainly used on the ingress interface of traffic, aiming to limit the input traffic.

To control the traffic, a mechanism is needed to measure the traffic of the device. The token bucket is the most widely used for measuring traffic at present.

The token bucket is a container to store tokens with a preset capacity. Tokens are arranged to the token bucket at a configured rate. When the bucket is full, excessive tokens will overflow. The token bucket is divided into single-token bucket and dual-token bucket by the quantity of the bucket. For the dual-token bucket, it is divided into single-rate and dual-rate by the input rate.

Prerequisite

N/A

13.3.2 Default configurations

N/A

13.3.3 Configuring rate limiting

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mls qos { aggregate-policer single-policer } policer-id cir cir cbs cbs [red { drop recolor { red green } set-cos value set-dscp value }] [green { drop recolor { red green } set-cos value set-dscp value }]	Create rate limiting rules and specify the action taken when the rate exceeds the threshold (single-token bucket monitoring).
3	Raisecom(config)#mls qos { aggregate-policer single-policer } policer-id cir cir cbs cbs [pir pir] pbs pbs [red { drop recolor { red green yellow } set-cos value set-dscp value }] [green { drop recolor { red green yellow } set-cos value set-dscp value }] [yellow { drop recolor { red green yellow } set-cos value set-dscp value }] [color-aware]	Create rate limiting rules and specify the action taken when the rate exceeds the threshold (dual-token bucket monitoring).



Note

- When you configure the PIR parameter, the rate limiter works in dual-token bucket mode. Otherwise, it works in single-token bucket mode.
- Rate limiting in the ingress direction is not supported.

13.3.4 Checking configurations

No.	Command	Description
1	Raisecom#show mls qos policer [policer-id]	Show configurations of the rate limiter.

13.4 Configuring traffic shaping

13.4.1 Preparing for configurations

Scenario

Traffic shaping aims to eliminate the burst traffic and smooth output traffic. Traffic shaping is usually used on the egress interface.

Similar to traffic monitoring, traffic shaping also adopts the token bucket to measure traffic while it will not drop packets. It either sends the packet or does not send the packet. Whether a packet is dropped or not depends on the drop policy for congestion avoidance when the packet is scheduled to a queue.

Prerequisite

N/A

13.4.2 Default configurations

Queue	CIR (kbit/s)	CBS (kbit/s)	Gts-buffer (Byte)
0	0	0	1000
1	0	0	1000
2	0	0	1000
3	0	0	1000
4	0	0	1000
5	0	0	1000
6	0	0	1000
7	0	0	1000

13.4.3 Configuring traffic shaping

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { gigabitethernet ten-gigabitethernet epon-olt ten-giga-epon-olt gpon-olt } slot-id/port-id	Enter physical interface configuration mode.
3	Raisecom(config-if-*:*:*)#mls qos shaping [queue queue-id] cir cir cbs cbs [gts-buffer size]	Configure traffic shaping.

13.4.4 Checking configurations

No.	Command	Description
1	Raisecom#show interface { gigabitethernet ten-gigabitethernet epon-olt ten-giga-epon-olt gpon-olt } slot-id/port-id mls qos queue shaping	Show configurations of traffic shaping.

13.5 Configuring congestion avoidance

13.5.1 Preparing for configurations

Scenario

Queue scheduling can only ease network congestion to some degree. When the congestion is continuous, the queue buffer will be used up and packet loss cannot be avoided. The simplest and most intuitive policy is tail drop.

However, if a number of TCP packets are dropped, this will cause TCP timeout, thus initiating the TCP slow start and congestion avoidance mechanism. Then, the Tx end of TCP decreases the Tx frequency of packets. When packets of multiple TCP connections are dropped, multiple TCP connections may enter slow start and congestion avoidance mode at the same time, which is called TCP global synchronization. In this case, multiple TCP connections decrease the Tx frequency of packets, thus lowering the bandwidth utilization rate of links.

To avoid TCP global synchronization and increase bandwidth utilization rate, Weighted Random Early Detection (WRED) drop policy is adopted.

Prerequisite

N/A

13.5.2 Default configurations

N/A

13.5.3 Configuring WRED scheduling

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { gigabitethernet ten-gigabitethernet epon-olt ten-giga-epon-olt gpon-olt } slot-id/port-id	Enter physical interface configuration mode.
3	Raisecom(config-if-**-*)#mls qos wred [queue queue-id] [red green yellow] low-limit value high-limit value drop-probability value	Configure WRED scheduling parameters.

13.5.4 Checking configurations

No.	Command	Description
1	Raisecom#show interface { gigabitethernet ten-gigabitethernet epon-olt ten-giga-epon-olt gpon-olt } slot-id/port-id mls qos queue wred	Show WRED configurations.

13.6 Configuring congestion management

13.6.1 Preparing for configurations

Scenario

Congestion management refers to allocating and controlling bandwidth when the network is congested. Congestion management adopts the queue technology to cache packets according to traffic classification, and then send packets to corresponding queues according to queue scheduling algorithms, thus providing differentiated services when the network is congested.

Prerequisite

N/A

13.6.2 Default configurations

Scheduling mode

Default configurations of the queue scheduling mode are as below.

Function	Default value
OLT queue scheduling mode	SP

Queue weight

Default weights of WDRR and WRR queues on the ISCOM6800 and ISCOM6860 are as below.

Queue	0	1	2	3	4	5	6	7
WDRR weight	1	1	1	1	1	1	1	1
WRR weight	1	1	1	1	1	1	1	1

13.6.3 Configuring SP scheduling

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id example: Raisecom(config)#interface gigabitethernet 2/1</pre>	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode
3	<pre>Raisecom(config-if-*:*:*)#mls qos queue scheduler sp</pre>	Configure the queue scheduling mode to SP. You can use the no mls qos queue scheduler command to restore default configuration.

13.6.4 Configuring WRR scheduling

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id example: Raisecom(config)#interface gigabitethernet 2/1</pre>	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode
3	<pre>Raisecom(config-if-*:*:*)#mls qos queue scheduler wrr</pre>	Configure the queue scheduling mode to WRR. You can use the no mls qos queue scheduler command to restore default configuration.
4	<pre>Raisecom(config-if-*:*:*)#mls qos queue wrr value0 value1 value2 value3 value4 value5 value6 value7 example: Raisecom(config-if-gigabitethernet- :2:1)#mls qos queue wrr 1 2 4 8 1 1 1 1</pre>	Configure the weight of each queue in WRR scheduling mode. • value 0 to 7: weight, an integer, ranging from 0 to 27

13.6.5 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show interface { gigabitethernet ten-gigabitethernet epon-olt ten-giga- epon-olt gpon-olt } slot-id/port-id mls qos</pre>	Show QoS configurations on the interface, including interface trust mode, queue scheduling mode, and default CoS value.

No.	Command	Description
2	<code>Raisecom#show interface { gigabitethernet ten-gigabitethernet epon-olt ten-giga-epon-olt gpon-olt } slot-id/port-id mls qos queue</code>	Show configurations of queue weights.

13.7 Configuring traffic policy

13.7.1 Preparing for configurations

Scenario

After traffic classification, you need to perform different operations on packets of different types.

Prerequisite

N/A

13.7.2 Default configurations

N/A

13.7.3 Configuring OLT traffic policy

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#{ ip-access-list list-number ipv6-access-list list-number 12-access-list list-number hybrid-access-list list-number user-access-list list-number }</code>	Create an ACL and enter ACL configuration mode.
3	<code>Raisecom(config-*-acl-*)#rule rule-id</code>	Create an ACL sub-rule and enter ACL sub-rule configuration mode.
4	<code>Raisecom(config-*-acl-*-*rule-*)#set { ip dscp value ip precedence value cos cos vlan vlan-id }</code>	Mark the data traffic.

13.8 Configuration examples

13.8.1 Example for configuring queue scheduling

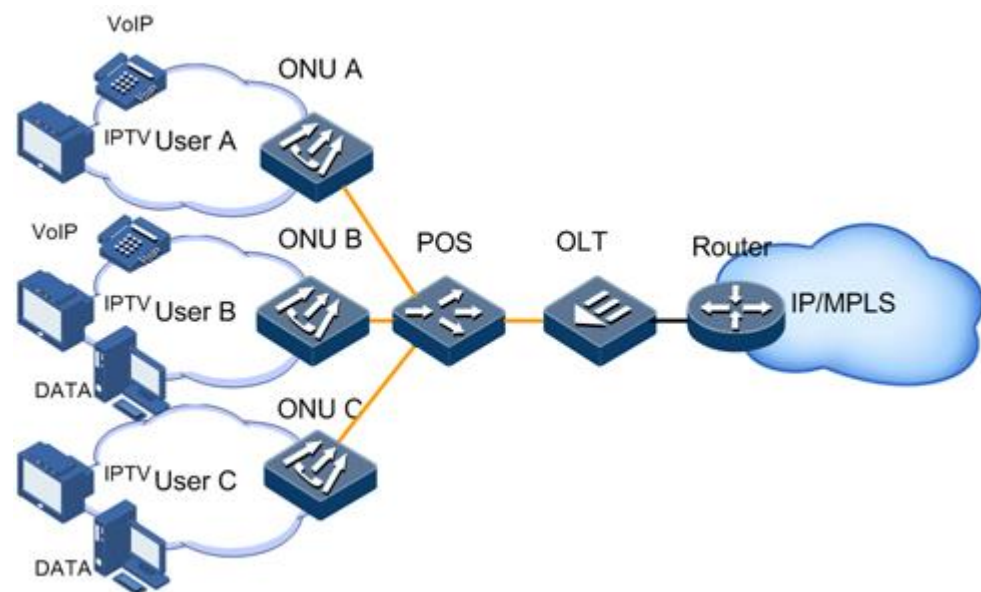
Networking requirements

As shown in Figure 13-9, User A provides voice and video services; User B provides voice, video, and data services; and User C provides video and data services.

CoS priority of voice services is 5; CoS priority of video services is 4; and CoS priority of data services is 2. Local priority of the above services is 6, 5, and 2 respectively.

- For voice services, perform SP scheduling to make the traffic transmitted preferentially.
- For video services, perform WRR scheduling and the weight is 15.
- For data services, perform WRR scheduling and the weight is 10. In addition, configure the drop threshold to 15 to avoid network congestion caused by too heavy burst traffic.

Figure 13-9 Configuring queue scheduling



Configuration steps

Step 1 Configure interface priority trust.

```
Raisecom#config
Raisecom(config)#interface epon-olt 1/1
Raisecom(config-if-1:1)#no mls qos trust dscp
```

Step 2 Configure mapping between the CoS priority and local priority.

```
Raisecom(config-if-1:1)#exit
```

```
Raisecom(config)#mls qos mapping cos 5 to localpriority 6
Raisecom(config)#mls qos mapping cos 4 to localpriority 5
Raisecom(config)#mls qos mapping cos 2 to localpriority 2
```

Step 3 Configure SP+WRR scheduling.

```
Raisecom(config)#interface pon-olt 1/1
Raisecom(config-if-pon-olt-1:1)#mls qos queue scheduler wrr
Raisecom(config-if-pon-olt-1:1)#mls qos queue wrr 1 1 10 1 1 15 0 0
```

Checking results

Use the **show mls qos mapping** command to show mapping configurations for specified priorities.

```
Raisecom#show mls qos mapping cos
```

```
CoS-LocalPriority Mapping:
```

```
CoS: 0 1 2 3 4 5 6 7
```

```
-----
LocalPriority: 0 1 2 3 5 6 6 7
```

14 Configuring system security

This chapter describes the system security feature and configuration process of the ISCOM6800 and ISCOM6860, and provides related configuration examples, including the following sections:

- Introduction
- Configuring ACL
- Configuring RADIUS
- Configuring TACACS+
- Configuring storm control
- Configuring interface isolation
- Configuring attack prevention
- Configuring anti-DoS attacks
- Maintenance
- Configuration examples

14.1 Introduction

14.1.1 ACL

Access Control List (ACL) is a set of ordered rules, which can control the device to receive or discard some data packets, thus preventing illegal packets from impacting network performance.

ACL is composed of **permit** | **deny** sentences. The rules are described by the source/destination MAC address, source/destination IP address, and interface ID of data packets. The device judges whether to receive or discard packets according to these rules.

14.1.2 RADIUS

Remote Authentication Dial In User Service (RADIUS) is a standard communication protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for remote users.

RADIUS works in client/server mode. Network devices are clients of the RADIUS server. RADIUS server is responsible for receiving users' connection requests, authenticating users, and replying configurations required by all clients to provide services for users. This mode can control users accessing devices and network to improve network security.

Clients and the RADIUS server communicate with each other through the shared key. The shared key is not transmitted through the network. In addition, any user password needs to be encapsulated when it is transmitted through clients and RADIUS. This helps prevent getting the user password by sniffing unsecure network.

RADIUS accounting is designed for RADIUS authenticated users. When a user logs in to the device, the device sends an accounting packet to the RADIUS accounting server to begin accounting. During login, the device sends accounting update packets to the RADIUS accounting server. When the user exits from the device, no accounting packet is sent to the RADIUS accounting server. These packets contain the login time. With these packets, the RADIUS accounting server can record the access time and operation of each user.

14.1.3 TACACS+

Terminal Access Controller Access Control System (TACACS+) is a network access authentication protocol similar to RADIUS. Compared with RADIUS, TACACS+ has the following features:

- Use the TCP port, providing higher transmission reliability. RADIUS uses a UDP port.
- Encapsulate the whole standard TACACS+ packet except for the TACACS+ header. Compared with RADIUS which encapsulates the user password only, TACACS+ provides higher security.
- Separate TACACS+ authentication from TACACS+ authorization and TACACS+ accounting, providing a more flexible deployment mode.

Therefore, compared with RADIUS, TACACS+ is more secure and reliable. However, as an open protocol, RADIUS is more widely used.

14.1.4 Storm control

In most scenarios of the Layer 2 network, unicast traffic is much heavier than broadcast traffic. If the rate for broadcast traffic is not limited, much bandwidth will be occupied when a broadcast storm is generated. Therefore, network performance is reduced and forwarding of normal unicast packets is seriously affected. Moreover, communication between devices may be interrupted.

Configuring storm control on Layer 2 devices can prevent broadcast storm when broadcast packets increase sharply on the network. Therefore, it ensures that unicast packets can be properly forwarded.

14.1.5 Interface isolation

Interface isolation adopts the isolation group method to implement data isolation among multiple interfaces on the device, thus enhancing network access security.

The ISCOM6800 and ISCOM6860 devices support the following three types of port isolation:

- OLT physical port isolation: include isolation between different ports on the same interface card and isolation between different ports on different interface cards.
- Port isolation in an OLT VLAN: one VLAN can have multiple isolation groups. The ports in the isolation group cannot communicate with each other. The ports between

different isolation groups can communicate with each other. A port that is not added to an isolation group in a VLAN can communicate with any port in the VLAN.

- ONU UNI isolation

14.2 Configuring ACL

14.2.1 Preparing for configurations

Scenario

ACL can help the network device recognize and filter specified data packets. Only after the device recognizes the specified packets, it can permit/deny the access of packets according to the configured policy.

ACL can be divided into the following types.

- IP ACL: classification rules are formulated according to the source or destination address, TCP or UDP port ID, and other data packet attributes carried by the IP header.
- IPv6 ACL: classification rules are formulated according to the source or destination address, TCP or UDP port ID, and other data packet attributes carried by the IPv6 header.
- Layer 2 ACL: classification rules are formulated according to the source MAC address, the destination MAC address, Layer 2 protocol type, and other Layer 2 information carried by the Layer 2 frame header.
- Hybrid ACL: classification rules are formulated according to the IP header and Layer 2 frame header. This type of ACL mixes characteristics of IP ACL and Layer 2 ACL.
- IPv6 hybrid ACL: classification rules are formulated according to the IPv6 header and Layer 2 frame header. This type of ACL mixes characteristics of IPv6 ACL and Layer 2 ACL.
- User ACL: formulate classification rules from the user's perspective.

The ACL application mode can be divided into the following three types according to actual scenarios:

- Based on the whole device
- Based on uplink and downlink of the interface
- Based on traffic from the ingress interface to egress interface

Prerequisite

N/A

14.2.2 Default configurations

N/A

14.2.3 Configuring IP ACL

Configuring IPv4 ACL

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ip-access-list <i>list-number</i> example: Raisecom(config)#ip-access-list 1001	Create an IPv4 ACL and enter IPv4 ACL configuration mode. You can use the no ip-access-list { all list-number } command to delete the ACL. • acl-number: ACL ID, an integer, ranging from 1001 to 2000
3	Raisecom(config-ip-acl-*)# description <i>desc-string</i> example: Raisecom(config-ip-acl-1010)#description raisecom	(Optional) configure descriptions of the IPv4 ACL. • desc-string: description, a string of 1 to 16 characters
4	Raisecom(config-ip-acl-*)# rule <i>rule-number</i> example: Raisecom(config-12-acl-1)#rule 2	Configure the ID of IPv4 ACL sub-rules and enter sub-rule configuration mode. • rule rule-id: Layer 2 sub-rule ID, an integer, ranging from 1 to 256
5	Raisecom(config-ip-acl-*--rule-*)# access-type { permit deny } example: Raisecom(config-ip-acl-1010-rule-100)#access-type deny	Configure the access type of the IPv4 ACL sub-rule. • deny: deny access when the conditions match. • permit: permit access when the conditions match.
6	Raisecom(config-ip-acl-*--rule-*)# match ip destination-address <i>ip-address</i> [<i>mask</i>] example: Raisecom(config-ip-acl-1010-rule-100)#match ip destination-address 10.0.0.1	Configure the destination IP address of the IPv4 ACL sub-rule. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • ip-mask: IP address mask, in dotted decimal notation, such as 255.0.0.0
7	Raisecom(config-ip-acl-*--rule-*)# match ip source-address <i>ip-address</i> [<i>mask</i>] example: Raisecom(config-ip-acl-1010-rule-100)#match ip source-address 10.0.0.1	Configure the source IP address of the IPv4 ACL sub-rule. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • ip-mask: IP address mask, in dotted decimal notation, such as 255.0.0.0

Step	Command	Description
8	<pre>Raisecom(config-ip-acl-*-rule-*)#match ip precedence { pri routine priority immediate flash flash-override critical internet network }</pre> example: <pre>Raisecom(config-ip-acl-1010-rule-100)#match ip precedence routine</pre>	Configure matching the IPv4 ACL sub-rule with the source IP precedence. • precedence-value: priority, an integer, ranging from 0 to 7 • routine priority immediate flash flash-override critical internet network: IP packet priority; routine: the priority is 0; priority: the priority is 1; immediate: the priority is 2; flash: the priority is 3; flash-override: the priority is 4; critical: the priority is 5; internet: the priority is 6; network: the priority is 7.
9	<pre>Raisecom(config-ip-acl-*-rule-*)#match ip tos { service-value normal min-monetary-cost min-delay max-reliability max-throughput }</pre> example: <pre>Raisecom(config-ip-acl-1010-rule-100)#match ip tos 10</pre>	Configure matching the IPv4 ACL sub-rule with the IP ToS. • tos-value: ToS value, an integer, ranging from 0 to 15 • normal min-monetary-cost min-delay max-reliability max-throughput: ToS type of IP packets; normal: normal TOS value (corresponding to ToS 0); min-monetary-cost: minimum cost TOS value (corresponding to ToS 1); max-reliability: maximum reliable TOS value (corresponding to ToS 2); max-throughput: maximum throughput TOS (corresponding to ToS 4).
10	<pre>Raisecom(config-ip-*-rule-*)#match ip dscp { diff-service-code af11 af12 af13 af21 af22 af23 af31 af32 af33 af41 af42 af43 cs1 cs2 cs3 cs4 cs5 cs6 cs7 ef default }</pre> example: <pre>Raisecom(config-ip-acl-1010-rule-100)#match ip dscp10</pre>	Configure matching the IPv4 ACL sub-rule with IP DSCP. • dscp-value: DSCP value, an integer, ranging from 0 to 63 • af11: AF11 dscp value (001010) • af12: AF12 dscp value (001100) • af13: AF13 dscp value (001110) • af21: AF21 dscp value (010010) • af22: AF22 dscp value (010100) • af23: AF23 dscp value (010110) • af31: AF31 dscp value (011010) • af32: AF32 dscp value (011100) • af33: AF33 dscp value (011110) • af41: AF41 dscp value (100010) • af42: AF42 dscp value (100100) • af43: AF43 dscp value (100110) • cs1: CS1 (priority 1) dscp value (001000) • cs2: CS2 (priority 2) dscp value (010000) • cs3: CS3 (priority 3) dscp value (011000) • cs4: CS4 (priority 4) dscp value (100000) • cs5: CS5 (priority 5) dscp value (101000) • cs6: CS6 (priority 6) dscp value (110000) The numbers in brackets are binary numbers, which can be converted to decimal numbers to correspond to DSCP values.

Step	Command	Description
11	<pre>Raisecom(config-ip-acl-* -rule-*)#match ip { fragments no- fragments } example: Raisecom(config-ip-acl-1010-rule- 100)#match ip fragments</pre>	Configure matching the IPv4 ACL sub-rule with the fragmented or non-fragmented packet. • fragments: if the IP packet is fragmented, the match succeeds. • no-fragments: if the IP packet is not fragmented, the match succeeds.
12	<pre>Raisecom(config-ip-* -rule-*)#match ip protocol { protocol-num ahp esp gre icmp igmp igmp igmp ipinip ospf pcp pim tcp udp } example: Raisecom(config-ip-acl-1010-rule- 100)#match ip protocol ahp</pre>	Configure matching the IPv4 ACL sub-rule with the IP upper protocol type. • protocol-id: protocol ID, an integer, ranging from 0 to 255 where 1 refers to ICMP, 17 refers to UDP, and 6 refers to TCP. • ahp esp gre icmp igmp igmp igmp ipinip ospf pcp pim tcp udp: upper-layer protocol type encapsulated by the IP packet, which also can be represented by the protocol ID

Step	Command	Description
13	<pre>Raisecom(config-ip-*--rule-*)#match ip tcp { destination-port source- port } { port-num bgp domain echo exec finger ftp ftp- data gopher hostname ident irc klogin kshell login lpd nntp pim-auto-rp pop2 pop3 smtp sunrpc syslog tacacs talk telnet time uucp whois www } example: Raisecom(config-ip-acl-1010-rule- 100)#match ip tcp destination-port bgp</pre>	Configure matching the IPv4 ACL sub-rule with the destination/source interface ID of the TCP packet. The packet type refers to the classical interface ID. • destination-port: UDP destination interface • source-port: UDP source interface • port-id: UDP interface ID, an integer, ranging from 0 to 65535 • bgp: border gateway protocol, the corresponding interface ID is 179. • domain: domain service protocol, the corresponding interface ID is 53. • echo: echo protocol, the corresponding interface ID is 7. • exec: Exec, the corresponding interface ID is 512. • finger: Finger, the corresponding interface ID is 79. • ftp: file transfer protocol, the corresponding interface ID is 21. • ftp-data: FTP data connection protocol, the corresponding interface ID is 20. • gopher: Gopher, the corresponding interface ID is 70. • hostname: NIC host name server, the corresponding interface ID is 101. • ident: identity protocol, the corresponding interface ID is 113. • irc: IRC, the corresponding interface ID is 194. • klogin: Kerberos login, the corresponding interface ID is 543. • kshellKerberos shell, the corresponding interface ID is 544. • loginLogin, the corresponding interface ID is 513. • lpd: printer service protocol, the corresponding interface ID is 515. • nntp: network news transfer protocol, the corresponding interface ID is 119. • pim-auto-rp: PIM Auto-RP, the corresponding interface ID is 496. • pop2: post office protocol v2, the corresponding interface ID is 109. • pop3: post office protocol v3, the corresponding interface ID is 110. • smtp: simple mail transfer protocol, the corresponding interface ID is 25. • sunrpcSun: remote process call, the corresponding interface ID is 111.
14	<pre>Raisecom(config-ip-*--rule-*)#match ip tcp { ack fin psh rst syn urg } example: Raisecom(config-ip-acl-1010-rule- 100)#match ip tcp ack</pre>	Configure matching the IPv4 ACL sub-rule with the TCP packet flag. • ack fin psh rst syn urg: type of SYN Flag in the TCP packet. If the type of the SYN Flag in the packet is the same as that defined by the rule, the match succeeds.

Step	Command	Description
15	<pre>Raisecom(config-ip-*rule-*)#match ip udp { destination-port source- port } { port-num biff bootpc bootps domain echo mobile-ip netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip snmp snmptrap sunrpc syslog tacacs talk tftp time who } example: Raisecom(config-ip-acl-1001-rule- 1)#match ip udp destination-port 69</pre>	Configure matching the IPv4 ACL sub-rule with the destination/source interface ID of the UDP packet. • destination-port: UDP destination interface • source-port: UDP source interface • port-id: UDP interface ID, an integer, ranging from 0 to 65535 • biff: Biff, the corresponding interface ID is 512 • bootpc: BOOTP Server, the corresponding interface ID is 68. • bootps: BOOTP server, the corresponding protocol interface ID is 67. • domain: domain service protocol, the corresponding interface ID is 53. • echo: echo protocol, the corresponding interface ID is 7. • mobile-ip: mobile IP registration, the corresponding interface ID is 434. • netbios-dgm: NetBios datagram service, the corresponding interface ID is 138. • netbios-ns: NetBios name service, the corresponding interface ID is 137. • netbios-ss: NetBios session service, the corresponding interface ID is 139. • ntp: network time protocol, the corresponding interface ID is 123. • pim-auto-rp: PIM Auto-RP, the corresponding interface ID is 496. • rip: routing information protocol, the corresponding interface ID is 520. • snmp: simple network management protocol, the corresponding interface ID is 161. • snmptrap: SNMP Traps, the corresponding interface ID is 162. • sunrpcun: remote process call, the corresponding interface ID is 111. • syslog: syslog, the corresponding interface ID is 514. • tacacsTAC: obtain control system. The corresponding interface ID is 49. • talkTalk, the corresponding interface ID is 517 • tftp: trivial file transfer protocol, the corresponding interface ID is 69. • timeTime, the corresponding interface ID is 37. • who: Who service, the corresponding interface ID is 513.

Configuring IPv6 ACL

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#ipv6-access-list <i>list-number</i> example: Raisecom(config)#ipv6-access-list 2001	Create an IPv6 ACL and enter IPv6 ACL configuration mode. You can use the no ipv6-access-list { all list-number } command to delete the ACL. acl-number: ACL ID, an integer, ranging from 2001 to 3000
3	Raisecom(config-ipv6-acl-*)#description <i>text</i> example: Raisecom(config-ip-acl-1010)#description raisecom	(Optional) configure descriptions of the IPv6 ACL. text: description, a string of 1 to 16 characters
4	Raisecom(config-ipv6-acl-*)#rule <i>rule-number</i> example: Raisecom(config-ipv6-acl-1)#rule 2	Configure the number of the IPv6 ACL sub-rule and enter sub-rule configuration mode. rule rule-id: Layer 2 sub-rule ID, an integer, ranging from 1 to 256
5	Raisecom(config-ipv6-acl-*-rule-*)#access-type { permit deny } example: Raisecom(config-ip-acl-1010-rule-100)#access-type deny	Configure the access type of the IPv6 ACL sub-rule. - deny: deny access when conditions match. - permit: allow access when conditions match.
6	Raisecom(config-ipv6-acl-*-rule-*)#match ip destination-address <i>ipv6-address/prefix-length</i> example: Raisecom(config-ipv6-acl-2001-rule-1)#match ip destination-address 3001::1/64	Configure the destination IP address of the IPv6 ACL sub-rule. destination-address ipv6-address/prefix: match the destination IPv6 address. The ipv6-address refers to the IPv6 address, which is in colon hexadecimal notation, such as 3001::1. The prefix refers to the IPv6 prefix, which is an integer ranging from 0 to 128.
7	Raisecom(config-ipv6-acl-*-rule-*)#match ip source-address <i>ipv6-address/prefix-length</i> example: Raisecom(config-ipv6-acl-2001-rule-1)#match ip source-address 3001::1/64	Configure the source IP address of the IPv6 ACL sub-rule. source-address ipv6-address/prefix: match the source IPv6 address. The ipv6-address refers to the IPv6 address, which is in colon hexadecimal notation, such as 3001::1. The prefix refers to the IPv6 prefix, which is an integer ranging from 0 to 128.
8	Raisecom(config-ipv6-acl-*-rule-*)#match ip traffic-class <i>user-level</i> example: Raisecom(config-ipv6-acl-2001-rule-1)#match ip traffic-class 100	Configure the IPv6 ACL sub-rule matching with the user level of the IPv6 packet. traffic-class user-level: match IPv6 Traffic-class. The user-level is an integer ranging from 0 to 255.
9	Raisecom(config-ipv6-acl-*-rule-*)#match ip protocol <i>ipv6-protocol-id</i> example: Raisecom(config-ipv6-acl-2001-rule-1)#match ip protocol 100	Configure the IPv6 ACL sub-rule matching with IP upper protocol type. protocol protocol-id: IPv6 is the type of the next packet header. The protocol-id is the protocol ID of the next packet, which is an integer ranging from 0 to 255.

Step	Command	Description
10	<pre>Raisecom(config-ipv6-acl-*--rule-*)#match ip tcp { destination-port source-port } { port-num bgp domain echo exec finger ftp ftp-data gopher hostname / ident irc klogin kshell login lpd nntp pim-auto-rp pop2 pop3 smtp sunrpc syslog tacacs talk telnet time uucp whois www }</pre> example: Raisecom(config-ipv6-acl-2001-rule-1)#match ip tcp destination-port 80	Configure matching the IPv6 ACL sub-rule with the destination/source interface ID of the TCP packet. • destination-port: TCP destination interface • source-port: TCP source interface • port-id: TCP interface ID, an integer, ranging from 0 to 65535 • bgp: boarder gateway protocol, the corresponding interface ID is 179. • domain: domain name service protocol, the corresponding interface ID is 53. • echo: echo protocol, the corresponding interface ID is 7. • exec: Exec, the corresponding interface ID is 512. • finger: Finger, the corresponding interface ID is 79. • ftp: file transfer protocol, the corresponding interface ID is 21 • ftp-data: FTP data connection protocol, the corresponding interface ID is 20. • gopher: Gopher, the corresponding interface ID is 70 • hostname: NIC host name server, the corresponding interface ID is 101. • ident: ID protocol, the corresponding interface ID is 113. • irc: IRC, the corresponding interface ID is 194. • klogin: Kerberos login, the corresponding interface ID is 543. • kshell: Kerberos shell, the corresponding interface ID is 544. • login: Login, the corresponding interface ID is 513. • lpd: printer service protocol, the corresponding interface ID is 515. • nntp: network news transfer protocol, the corresponding interface ID is 119. • pim-auto-rp: PIM Auto-RP, the corresponding interface ID is 496. • pop2: POP v2, the corresponding interface ID is 109 • pop3: POP v3, the corresponding interface ID is 110. • smtp: simple mail transfer protocol, the corresponding interface ID is 25. • sunrpcSun: remote process control, the corresponding interface ID is 111. • syslog: syslog, the corresponding interface ID is 514. • tacacsTAC: obtain control system, the corresponding interface ID is 49. • talkTalk: the corresponding interface ID is 517. • telnetTelnet: the corresponding interface ID is 23. • timeTime: the corresponding interface ID is 37.

Step	Command	Description
		• uucp: Unix-to-Unix copy program, the corresponding interface ID is 540. • whois: Nickname: the corresponding interface ID is 43. • www: global Internet, the corresponding interface ID is 80.
11	<pre>Raisecom(config-ipv6-acl-*--rule-*)#match ip tcp { ack fin psh rst syn urg }</pre> example: <pre>Raisecom(config-ipv6-acl-2001-rule-1)#match ip tcp ack</pre>	Configure matching the IPv6 ACL sub-rule with the TCP packet flag. • ack fin psh rst syn urg: type of SYN Flag in the TCP packet. If the type of the SYN Flag in the packet is the same as that defined by the rule, the match succeeds.
12	<pre>Raisecom(config-ipv6-acl-*--rule-*)#match ip flow-label label-value</pre> example: <pre>Raisecom(config-ipv6-acl-2001-rule-1)#match ip flow-label 100</pre>	Configure matching the IPv6 ACL sub-rule with the flow label of the IPv6 packet. • flow-label label-value: match IPv6 traffic tag. The flow-label is an integer ranging from 0 to 1048575.  Note The XEP8 (B) card does not support this function.
13	<pre>Raisecom(config-ipv6-acl-*--rule-*)#match ip udp { destination-port source-port } { port-num biff bootpc bootps domain echo mobile-ip netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip snmp snmptrap sunrpc syslog tacacs talk tftp time who }</pre> example: <pre>Raisecom(config-ipv6-acl-2001-rule-1)#match ip udp destination-port 69</pre>	Configure matching the IPv6 ACL sub-rule with the destination/source interface ID of the UDP packet. • destination-port: UDP destination interface • source-port: UDP source interface • port-id: UDP interface ID, an integer, ranging from 0 to 65535 • biff: Biff, the corresponding interface ID is 512 • bootpc: BOOTP Server, the corresponding interface ID is 68. • bootps: BOOTP server, the corresponding protocol interface ID is 67. • domain: domain service protocol, the corresponding interface ID is 53. • echo: echo protocol, the corresponding interface ID is 7. • mobile-ip: mobile IP registration, the corresponding interface ID is 434. • netbios-dgm: NetBios datagram service, the corresponding interface ID is 138. • netbios-ns: NetBios name service, the corresponding interface ID is 137. • netbios-ss: NetBios session service, the corresponding interface ID is 139. • ntp: network time protocol, the corresponding interface ID is 123. • pim-auto-rp: PIM Auto-RP, the corresponding interface ID is 496. • rip: routing information protocol, the corresponding interface ID is 520.

Step	Command	Description
		• snmp: simple network management protocol, the corresponding interface ID is 161. • snmptrap: SNMP Traps, the corresponding interface ID is 162. • sunrpcun: remote process call, the corresponding interface ID is 111. • syslog: syslog, the corresponding interface ID is 514. • tacacs: terminal access controller access-control system. The corresponding interface ID is 49. • talkTalk, the corresponding interface ID is 517 • tftp: trivial file transfer protocol, the corresponding interface ID is 69. • timeTime, the corresponding interface ID is 37. • who: Who service, the corresponding interface ID is 513.

14.2.4 Configuring Layer 2 ACL

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#l2-access-list <i>list-number</i> example: Raisecom(config)#l2-access-list 10	Create a Layer 2 ACL and enter Layer 2 ACL configuration mode. You can use the no l2-access-list <i>acl-number</i> command to delete the ACL. • acl-number: ACL ID, an integer, ranging from 1 to 1000
3	Raisecom(config-l2-acl- *)#description <i>text</i> example: Raisecom(config-ip-acl- 1010)#description <i>raisecom</i>	(Optional) configure descriptions of the Layer 2 ACL. • text: description, a string of 1 to 16 characters
4	Raisecom(config-l2-acl-*)#rule <i>rule-number</i> example: Raisecom(config-l2-acl-1)#rule 2	Configure the number of the Layer 2 ACL sub-rule and enter sub-rule configuration mode. • rule rule-id: Layer 2 subrule ID, an integer, ranging from 1 to 256
5	Raisecom(config-l2-acl-*rule- *)#access-type { permit deny } example: Raisecom(config-ip-acl-1010- rule-100)#access-type deny	Configure the access type of the Layer 2 ACL sub-rule. • deny: deny access when conditions match. • permit: allow access when conditions meet.
6	Raisecom(config-l2-acl-*rule- *)#match mac destination <i>mac</i> [<i>mac-mask</i>] example: Raisecom(config-l2-acl-1-rule- 1)#match mac destination 000e.5e01.0001 ffff.ffff.ffff	Configure the destination MAC address of the Layer 2 ACL sub-rule. • mac-address: MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456 • mask: MAC address mask, in dotted hexadecimal notation, such as FFFF.FFFF.FFFF

Step	Command	Description
7	<pre>Raisecom(config-l2-acl-* -rule-*)#match mac source mac [mac- mask]</pre> example: <pre>Raisecom(config-l2-acl-1-rule- 1)#match mac source 000e.5e01.0001 ffff.ffff.ffff</pre>	Configure the source MAC address of the Layer 2 ACL sub-rule. • mac-address: MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456 • mask: MAC address mask, in dotted hexadecimal notation, such as FFFF.FFFF.FFFF
8	<pre>Raisecom(config-l2-acl-* -rule-*)#match svlan svlan-id</pre> example: <pre>Raisecom(config-l2-acl-1-rule- 1)#match svlan 5</pre>	Configure matching the Layer 2 ACL sub-rule with the source SVLAN ID. • svlan-vlaue: external VLAN ID, an integer, ranging from 1 to 4094
9	<pre>Raisecom(config-l2-acl-* -rule-*)#match svlan-cos svlan-cos</pre> example: <pre>Raisecom(config-l2-acl-1-rule- 1)#match svlan-cos 5</pre>	Configure matching the Layer 2 ACL sub-rule with the SVLAN CoS. • svlan-cos: external VLAN CoS value, an integer, ranging from 0 to 7
10	<pre>Raisecom(config-l2-acl-* -rule-*)#match cvlan cvlan-id</pre> example: <pre>Raisecom(config-l2-acl-1-rule- 1)#match cvlan 2</pre>	Configure matching the Layer 2 ACL sub-rule with the source CVLAN ID. • cvlan-id: external VLAN ID, an integer, ranging from 1 to 4094
11	<pre>Raisecom(config-l2-acl-* -rule-*)#match cvlan-cos cvlan-cos</pre> example: <pre>Raisecom(config-l2-acl-1-rule- 1)#match cvlan-cos 5</pre>	Configure matching the Layer 2 ACL sub-rule with the CVLAN CoS. • cvlan-cos-vlaue: internal VLAN CoS value, an integer, ranging from 0 to 7  Note The configuration of ACL subrules matching CVLAN CoS is not supported in the ingress direction of the XEP(B) card.
12	<pre>Raisecom(config-l2-acl-* -rule-*)#match ethertype type mask</pre> example: <pre>Raisecom(config-l2-acl-1-rule- 1)# match ethertype type 255.255.255.0</pre>	Configure matching the Layer 2 ACL sub-rule with the frame type in the Layer 2 frame head. • type: type • mask: mask
13	<pre>Raisecom(config-l2-acl-* -rule-*)#match ethertype { arp eapol flowcontrol ip ipv6 loopback mpls mpls-mcast pppoe pppoe-disc x25 x75 }</pre> example: <pre>Raisecom(config-l2-acl-1-rule- 1)#match ethertype ipv6</pre>	Configure matching the Layer 2 ACL sub-rule with the protocol type in the Layer 2 frame head. • arp: address resolution protocol • eapol: EAPOL PAE/802.1x protocol • flowcontrol: 802.3x flow control • ip: IPv4 protocol • ipv6: IPv6 protocol • loopback: loopback protocol • mpls: MPLS unicast protocol • mpls-mcast: MPLS multicast protocol • pppoe: PPPoE session protocol • pppoe-disc: PPPoE discovery protocol • x25: X.25 protocol • x75: X.75 protocol

14.2.5 Configuring hybrid ACL

Configuring IPv4 hybrid ACL

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# hybrid-access-list <i>list-number</i> example: Raisecom(config)#hybrid-access-list 3001	Create a hybrid ACL and enter hybrid ACL configuration mode. You can use the no hybrid-access-list { all list-number } command to delete the ACL. • acl-number: ACL ID, an integer, ranging from 3001 to 4000
3	Raisecom(config-hybrid-acl-*)# description <i>text</i> example: Raisecom(config-ip-acl-1010)#description raisecom	(Optional) configure the description of hybrid ACL. • text: description, a string of 1 to 16 characters
4	Raisecom(config-hybrid-acl-*)# rule <i>rule-number</i> example: Raisecom(config-l2-acl-1)#rule 2	Configure the ID of the hybrid ACL sub-rule and enter sub-rule configuration mode. • rule-id: Layer 2 subrule ID, an integer, ranging from 1 to 256
5	Raisecom(config-hybrid-acl-*--rule-*)# access-type { permit deny } example: Raisecom(config-ip-acl-1010-rule-100)#access-type deny	Configure the access type of the hybrid ACL sub-rule. • deny: deny access when conditions match. • permit: allow access when conditions meet.
6	Raisecom(config-hybrid-acl-*--rule-*)# match mac destination <i>mac</i> [<i>mac-mask</i>] example: Raisecom(config-l2-acl-1-rule-1)#match mac destination 000e.5e01.0001 ffff.ffff.ffff	Configure the destination MAC address of the hybrid ACL sub-rule. • mac-address: MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456 • mask: MAC address mask, in dotted hexadecimal notation, such as FFFF.FFFF.FFFF
7	Raisecom(config-hybrid-acl-*--rule-*)# match mac source <i>mac</i> [<i>mac-mask</i>] example: Raisecom(config-l2-acl-1-rule-1)#match mac source 000e.5e01.0001 ffff.ffff.ffff	Configure the source MAC address of the hybrid ACL sub-rule. • mac-address: MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456 • mask: MAC address mask, in dotted hexadecimal notation, such as FFFF.FFFF.FFFF
8	Raisecom(config-hybrid-acl-*--rule-*)# match svlan <i>svlan-id</i> example: Raisecom(config-hybrid-acl-1-rule-1)#match svlan 5	Configure matching the hybrid ACL sub-rule with the source SVLAN ID. • svlan-vlaue: external VLAN ID, an integer, ranging from 1 to 4094
9	Raisecom(config-hybrid-acl-*--rule-*)# match svlan-cos <i>svlan-cos</i> example: Raisecom(config-hybrid-acl-1-rule-1)#match svlan-cos 5	Configure matching the hybrid ACL sub-rule with the SVLAN CoS. • svlan-cos-vlaue: external VLAN CoS value, an integer, ranging from 0 to 7

10	<pre>Raisecom(config-hybrid-acl-* -rule-*)#match cvlan cvlan-id</pre> example: <pre>Raisecom(config-hybrid-acl-1-rule-1) #match cvlan 5</pre>	Configure matching the hybrid ACL sub-rule with the source CVLAN ID. • cvlan-vlaue: external VLAN ID, an integer, ranging from 1 to 4094
11	<pre>Raisecom(config-hybrid-acl-* -rule-*)#match cvlan-cos cvlan-cos</pre> example: <pre>Raisecom(config-hybrid-acl-1-rule-1) #match cvlan-cos 5</pre>	Configure matching the hybrid ACL sub-rule with the CVLAN CoS. • cvlan-cos:internal VLAN CoS value, an integer, ranging from 0 to 7
12	<pre>Raisecom(config-hybrid-acl-* -rule-*)#match ethertype ethertype mask</pre> example: <pre>Raisecom(config-hybrid-acl-1-rule-1) #match ethertype ip 255.255.255.0</pre>	Configure matching the hybrid ACL sub-rule with the frame type in the hybrid frame head. • ethertype: type • mask: mask
13	<pre>Raisecom(config-hybrid-acl-* -rule-*)#match ethertype { arp eapol flowcontrol ip ipv6 loopback mpls mpls-mcast pppoe pppoedisc x25 x75 }</pre> example: <pre>Raisecom(config-hybrid-acl-1-rule-1) #match ethertype ipv6</pre>	Configure matching the hybrid ACL sub-rule with the protocol type in the hybrid frame head. • arp: address resolution protocol • eapol: EAPOL PAE/802.1x protocol • flowcontrol: 802.3x flow control protocol • ip: IPv4 protocol • ipv6: IPv6 protocol • loopback: loopback protocol • mpls: MPLS unicast protocol • mpls-mcast: MPLS multicast protocol • pppoe: PPPoE session protocol • pppoedisc: PPPoE discovery protocol • x25: X.25 protocol • x75: X.75 protocol
14	<pre>Raisecom(config-hybrid-acl-* -rule-*)#match ip destination-address ip- address [mask]</pre> example: <pre>Raisecom(config-hybrid-acl-1001- rule-1)#match ip destination- address 10.0.0.1</pre>	Configure the destination IP address of the hybrid ACL sub-rule. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • ip-mask: IP address mask, in dotted decimal notation, such as 255.0.0.0
15	<pre>Raisecom(config-hybrid-acl-* -rule-*)#match ip source-address ip- address [mask]</pre> example: <pre>Raisecom(config-hybrid-acl-1001- rule-1)#match ip source-address 10.0.0.1</pre>	Configure the source IP address of the hybrid ACL sub-rule. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • ip-mask: IP address mask, in dotted decimal notation, such as 255.0.0.0
16	<pre>Raisecom(config-hybrid-acl-* -rule-*)#match ip precedence { pri routine priority immediate flash flash-override critical internet network }</pre> example: <pre>Raisecom(config-hybrid-acl-1001- rule-1)#match ip precedence routine</pre>	Configure matching the hybrid ACL sub-rule with the source IP precedence. • precedence-value: priority, an integer, ranging from 0 to 7 • routine priority immediate flash flash-override critical internet network: IP packet priority; routine: the priority is 0; priority: the priority is 1; immediate: the priority is 2; flash: the priority is 3; flash-override: the priority is 4; critical: the priority is 5; internet: the priority is 6; network: the priority is 7.

17	<pre>Raisecom(config-hybrid-acl-* -rule-*)#match ip tos { <i>service-type</i> normal min-monetary-cost min- delay max-reliability max- throughput } example: Raisecom(config-hybrid-acl-1001- rule-1)#match ip tos normal</pre>	Configure matching the hybrid ACL sub-rule with the IP ToS. • tos-value: ToS, an integer, ranging from 0 to 15 • normal min-monetary-cost min-delay max-reliability max-throughput: ToS type of IP packet; normal: normal TOS (corresponding to ToS 0); min-monetary-cost: minimum cost TOS (corresponding to ToS 1); max-reliability: maximum reliable TOS (corresponding to ToS 2); max-throughput: maximum throughput TOS (corresponding to ToS 4).
18	<pre>Raisecom(config-hybrid-acl-* -rule-*)#match ip dscp { <i>diff-service- code</i> af11 af12 af13 af21 af22 af23 af31 af32 af33 af41 af42 af43 cs1 cs2 cs3 cs4 cs5 cs6 cs7 ef default } example: Raisecom(config-hybrid-acl-1001- rule-1)#match ip dscp af11</pre>	Configure hybrid ACL subrule to match IP DSCP. • dscp-value: DSCP, an integer, ranging from 0 to 63 • dscp: af11: AF11 dscp value (001010) • af12: AF12 dscp value (001100) • af13: AF13 dscp value (001110) • af21: AF21 dscp value (010010) • af22: AF22 dscp value (010100) • af23: AF23 dscp value (010110) • af31: AF31 dscp value (011010) • af32: AF32 dscp value (011100) • af33: AF33 dscp value (011110) • af41: AF41 dscp value (100010) • af42: AF42 dscp value (100100) • af43: AF43 dscp value (100110) • cs1: CS1 (priority 1) dscp value (001000) • cs2: CS2 (priority 2) dscp value (010000) • cs3: CS3 (priority 3) dscp value (011000) • cs4: CS4 (priority 4) dscp value (100000) • cs5: CS5 (priority 5) dscp value (101000) • cs6: CS6 (priority 6) dscp value (110000) • cs7: CS7 (priority 7) dscp value (111000) • ef: EF dscp value (101110) • default: default dscp (000000) • The numbers in the brackets are binary. After they are converted into decimal numbers, they will correspond to the DSCP values.
19	<pre>Raisecom(config-hybrid-acl-* -rule-*)#match ip { fragments no- fragments } example: Raisecom(config-hybrid-acl-1001- rule-1)#match ip fragments</pre>	Configure matching the hybrid ACL sub-rule with the fragmented or non-fragmented packet. • fragments: if the IP packet is fragmented, the match succeeds. • no-fragments: if the IP packet is not fragmented, the match succeeds.

20	<pre>Raisecom(config-hybrid-acl-<i>rule-*</i>)#match ip protocol { <i>protocol-num</i> ahp esp gre icmp igmp igrp ipinip ospf pcp pim tcp udp }</pre> example: Raisecom(config-hybrid-acl-1001- rule-1)#match ip protocol ahp	Configure matching the hybrid ACL sub-rule with the IP upper protocol type. • protocol-id: protocol ID, an integer, ranging from 0 to 255 • 1 refers to ICMP. • 17 refers to UDP. • 6 refers to TCP. • ahp esp gre icmp igmp igrp ipinip ospf pcp pim tcp udp: upper-layer protocol type encapsulated by the IP packet, which also can be represented by the protocol ID

21	<pre>Raisecom(config-hybrid-acl-<i>rule-*</i>)#match ip tcp { destination-port source-port } { <i>port-num</i> bgp domain echo exec finger ftp ftp-data gopher hostname / ident irc klogin kshell login lpd nntp pim-auto-rp pop2 pop3 smtp sunrpc syslog tacacs talk telnet time uucp whois www } example: Raisecom(config-hybrid-acl-1001- rule-1)#match ip tcp destination- port bgp</pre>	Configure matching the hybrid ACL sub-rule with the destination/source interface ID of the TCP packet. • destination-port: TCP destination interface • source-port: TCP source interface • port-id: TCP interface ID, an integer, ranging from 0 to 65535 • bgp: boarder gateway protocol, the corresponding interface ID is 179. • domain: domain name service protocol, the corresponding interface ID is 53. • echo: echo protocol, the corresponding interface ID is 7. • exec: Exec, the corresponding interface ID is 512. • finger: Finger, the corresponding interface ID is 79. • ftp: file transfer protocol, the corresponding interface ID is 21 • ftp-data: FTP data connection protocol, the corresponding interface ID is 20. • gopher: Gopher, the corresponding interface ID is 70 • hostname: NIC host name server, the corresponding interface ID is 101. • ident: ID protocol, the corresponding interface ID is 113. • irc: IRC, the corresponding interface ID is 194. • klogin: Kerberos login, the corresponding interface ID is 543. • kshell: Kerberos shell, the corresponding interface ID is 544. • loginLogin, the corresponding interface ID is 513 • lpd: printer service protocol, the corresponding interface ID is 515. • nntp: network news transfer protocol, the corresponding interface ID is 119. • pim-auto-rp: PIM Auto-RP, the corresponding interface ID is 496. • pop2: POP v2, the corresponding interface ID is 109 • pop3: POP v3, the corresponding interface ID is 110. • smtp: simple mail transfer protocol, the corresponding interface ID is 25. • sunrpcSun: remote process control, the corresponding interface ID is 111. • syslog: syslog, the corresponding interface ID is 514. • tacacsTAC: obtain control system. The corresponding interface ID is 49. • talkTalk, the corresponding interface ID is 517 • telnetTelnet, the corresponding interface ID is 23. • timeTime, the corresponding interface ID is 37. • uucpUnix-to-Unix copy program, the corresponding interface ID is 540. • whoisNickname, the corresponding interface ID is 43. • wwwworldwide internet, the corresponding interface ID is 80.

22	<pre>Raisecom(config-hybrid-acl-* -rule-*)#match ip tcp { ack fin psh rst syn urg } example: Raisecom(config-hybrid-acl-1001-rule-1)#match ip tcp ack</pre>	Configure matching the hybrid ACL sub-rule with the TCP packet flag. • ack fin psh rst syn urg: type of SYN Flag in the TCP packet. If the type of the SYN Flag in the packet is the same as that defined by the rule, the match succeeds.
23	<pre>Raisecom(config-hybrid-acl-* -rule-*)#match ip udp { destination-port source-port } { port-num biff bootpc bootps domain echo mobile-ip netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip snmp snmptrap sunrpc syslog tacacs talk tftp time who } example: Raisecom(config-ip-acl-1001-rule-1)#match ip udp destination-port 69</pre>	Configure the hybrid ACL subrule to match the destination/source interface ID of the UDP packet. • destination-port: UDP destination interface • source-port: UDP source interface • port-id: UDP interface ID, an integer, ranging from 0 to 65535 • biff: Biff, the corresponding interface ID is 512 • bootpc: BOOTP Server, the corresponding interface ID is 68. • bootps: BOOTP server, the corresponding protocol interface ID is 67. • domain: domain service protocol, the corresponding interface ID is 53. • echo: echo protocol, the corresponding interface ID is 7. • mobile-ip: mobile IP registration, the corresponding interface ID is 434. • netbios-dgm: NetBios datagram service, the corresponding interface ID is 138. • netbios-ns: NetBios name service, the corresponding interface ID is 137. • netbios-ss: NetBios session service, the corresponding interface ID is 139. • ntp: network time protocol, the corresponding interface ID is 123. • pim-auto-rp: PIM Auto-RP, the corresponding interface ID is 496. • rip: routing information protocol, the corresponding interface ID is 520. • snmp: simple network management protocol, the corresponding interface ID is 161. • snmptrap: SNMP Traps, the corresponding interface ID is 162. • sunrpcun: remote process call, the corresponding interface ID is 111. • syslog: syslog, the corresponding interface ID is 514. • tacacsTAC: obtain control system. The corresponding interface ID is 49. • talkTalk, the corresponding interface ID is 517 • tftp: trivial file transfer protocol, the corresponding interface ID is 69. • timeTime, the corresponding interface ID is 37. • who: Who service, the corresponding interface ID is 513.

Configuring IPv6 hybrid ACL

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ipv6-hybrid-access-list list-number example: Raisecom(config)#ipv6-hybrid-access-list 4001	Create an IPv6 hybrid ACL and enter hybrid ACL configuration mode. You can use the no ipv6-hybrid-access-list { all list-number } command to delete the ACL. • acl-number: ACL ID, an integer, ranging from 4001 to 5000
3	Raisecom(config-ipv6-hybrid-acl-*)#description text example: Raisecom(config-ip-acl-1010)#description raisecom	(Optional) configure the description of IPv6 hybrid ACL. • text: description, a string of 1 to 16 characters
4	Raisecom(config-ipv6-hybrid-acl-*)#rule rule-number example: Raisecom(config-ipv6-hybrid-acl-1)#rule 2	Configure the ID of the IPv6 hybrid ACL sub-rule and enter sub-rule configuration mode. • rule-id: Layer 2 subrule ID, an integer, ranging from 1 to 256
5	Raisecom(config-ipv6-hybrid-acl-* rule-*)#access-type { permit deny } example: Raisecom(config-ipv6-hybrid-acl-1-rule-2)#access-type deny	Configure the access type of the IPv6 hybrid ACL sub-rule. • deny: deny access when conditions match. • permit: allow access when conditions meet.
6	Raisecom(config-ipv6-hybrid-acl-* rule-*)#match mac destination mac [mac-mask] example: Raisecom(config-ipv6-hybrid-acl-1-rule-2)#match mac destination 000e.5e01.0001 FFFF.FFFF.FFFF	Configure the destination MAC address of the IPv6 hybrid ACL sub-rule. • mac-address: MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456 • mask: MAC address mask, in dotted hexadecimal notation, such as FFFF.FFFF.FFFF
7	Raisecom(config-ipv6-hybrid-acl-* rule-*)#match mac source mac [mac-mask] example: Raisecom(config-ipv6-hybrid-acl-1-rule-2)#match mac source 000e.5e01.0001 FFFF.FFFF.FFFF	Configure the source MAC address of the IPv6 hybrid ACL sub-rule.
8	Raisecom(config-ipv6-hybrid-acl-* rule-*)#match svlan svlan-id example: Raisecom(config-ipv6-hybrid-acl-1-rule-2)#match svlan 1	Match the IPv6 hybrid ACL sub-rule with the source SVLAN ID. • svlan-vlaue: external VLAN CoS value, an integer, ranging from 1 to 4094

Step	Command	Description
9	<pre>Raisecom(config-ipv6-hybrid-acl-**-rule-*)#match svlan-cos <i>svlan-cos</i></pre> example: <pre>Raisecom(config-ipv6-hybrid-acl-1-rule-2)#match svlan-cos 2</pre>	Match the IPv6 hybrid ACL sub-rule with the source SVLAN CoS. svlan-cos: external VLAN CoS value, an integer, ranging from 0 to 7
10	<pre>Raisecom(config-ipv6-hybrid-acl-**-rule-*)#match cvlan <i>cvlan-id</i></pre> example: <pre>Raisecom(config-ipv6-hybrid-acl-1-rule-2)#match cvlan 1</pre>	Configure matching the IPv6 hybrid ACL sub-rule with the source CVLAN ID. cvlan-vlaue: external VLAN ID, an integer, ranging from 1 to 4094
11	<pre>Raisecom(config-ipv6-hybrid-acl-**-rule-*)#match cvlan-cos <i>cvlan-cos</i></pre> example: <pre>Raisecom(config-ipv6-hybrid-acl-1-rule-2)#match cvlan-cos 2</pre>	Configure matching the IPv6 hybrid ACL sub-rule with the CVLAN CoS. cvlan-cos-vlaue: internal VLAN CoS, an integer, ranging from 0 to 7
12	<pre>Raisecom(config-ipv6-hybrid-acl-**-rule-*)#match ethertype <i>frame-type frame-type-mask</i></pre> example: <pre>Raisecom(config-ipv6-hybrid-acl-1-rule-2)#match ethertype match ethertype ipv6</pre>	Configure matching the IPv6 hybrid ACL sub-rule with the frame type in the L2 frame head. - frame-type: Ethernet frame type, hexadecimal numbers (0x0600-0xFFFF) - frame-type-mask: Ethernet frame type mask, hexadecimal numbers
13	<pre>Raisecom(config-ipv6-hybrid-acl-**-rule-*)#match ethertype { arp eapol flowcontrol ip ipv6 loopback mpls mpls-mcast pppeoe pppoe-disc x25 x75 }</pre> example: <pre>Raisecom(config-ipv6-hybrid-acl-1-rule-2)#match ethertype arp</pre>	Configure matching the IPv6 hybrid ACL sub-rule with the protocol type in the L2 frame head. - arp: address resolution protocol - eapol: EAPOL PAE/802.1x protocol - flowcontrol: 802.3x flow control protocol - ip: IPv4 protocol - ipv6: IPv6 protocol - loopback: loopback protocol - mpls: MPLS unicast protocol - mpls-mcast: MPLS multicast protocol - pppeoe: PPPoE session protocol - pppoe-disc: PPPoE discovery protocol - x25: X.25 protocol - x75: X.75 protocol
14	<pre>Raisecom(config-ipv6-hybrid-acl-**-rule-*)#match ip destination-address <i>ip-address [mask]</i></pre> example: <pre>Raisecom(config-ipv6-hybrid-acl-1-rule-2)#match ip destination-address 10.10.10.1</pre>	Configure the destination IP address of the IPv6 hybrid ACL sub-rule. - ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 - ip-mask: IP address mask, in dotted decimal notation, such as 255.0.0.0

Step	Command	Description
15	<pre>Raisecom(config-ipv6-hybrid-acl-*--rule-*)#match ip source-address ip-address [mask]</pre> example: <pre>Raisecom(config-ipv6-hybrid-acl-1-rule-2)#match ip source-address 10.10.10.1</pre>	Configure the source IP address of the IPv6 hybrid ACL sub-rule. - ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 - ip-mask: IP address mask, in dotted decimal notation, such as 255.0.0.0
16	<pre>Raisecom(config-ipv6-hybrid-acl-*--rule-*)#match ip traffic-class user-level</pre> example: <pre>Raisecom(config-ipv6-hybrid-acl-1-rule-2)#match ip traffic-class 100</pre>	Configure matching the IPv6 hybrid ACL sub-rule with the user level in the IPv6 packet. traffic-class user-level: match the IPv6 Traffic-class. The user-level is an integer ranging from 0 to 255.  Note This function is not supported by the XEP8 (B) card.
17	<pre>Raisecom(config-ipv6-hybrid-acl-*--rule-*)#match ip protocol protocol-id</pre> example: <pre>Raisecom(config-ipv6-hybrid-acl-1-rule-2)#match ip protocol 100</pre>	Configure matching the IPv6 hybrid ACL sub-rule with the IP upper protocol type. protocol protocol-id: IPv6 next packet head type. The protocol-id is the protocol ID of the next packet, which is an integer ranging from 0 to 255.

Step	Command	Description
18	<pre>Raisecom(config-ipv6-hybrid-acl-* -rule-*)#match ip tcp { destination-port source-port } { port-num bgp domain echo exec finger ftp ftp-data gopher hostname ident irc klogin kshell login lpd nntp pim-auto-rp pop2 pop3 smtp sunrpc syslog tacacs talk telnet time uucp whois www } example: Raisecom(config-ipv6-hybrid-acl-1-rule- 2)#match ip tcp destination-port bgp</pre>	Configure matching IPv6 hybrid ACL subrule with the source/destination interface ID of the TCP packet. The packet type represents the classic interface ID. • destination-address: destination IP address of the IP packet. If the destination IP address of the packet is the same as that defined by the rule, the match will succeed. • source-address: source IP address of the IP packet • port-id: TCP interface ID, an integer, ranging from 0 to 65535 • bgp: border gateway protocol, the corresponding interface ID is 179. • domain: domain service protocol, the corresponding interface ID is 53. • echo: echo protocol, the corresponding interface ID is 7. • exec: Exec, the corresponding interface ID is 512. • finger: Finger, the corresponding interface ID is 79. • ftp: file transfer protocol, the corresponding interface ID is 21. • ftp-data: FTP data connection protocol, the corresponding interface ID is 20. • gopher: Gopher, the corresponding interface ID is 70. • hostname: NIC host name server, the corresponding interface ID is 101. • ident: identity protocol, the corresponding interface ID is 113. • irc: IRC, the corresponding interface ID is 194. • kloginKerber

Step	Command	Description
19	<pre>Raisecom(config-ipv6-hybrid-acl-*-rule-*)#match ip udp { destination-port source-port } { port-num biff bootpc bootps domain echo mobile-ip netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip snmp snmptrap sunrpc syslog tacacs talk tftp time who }</pre> example: <pre>Raisecom(config-ipv6-hybrid-acl-1-rule-2)# match ip udp destination-port biff</pre>	Configure matching the IPv6 hybrid ACL subrule with the destination/source interface ID of the UDP packet. • destination-port: UDP destination interface • source-port: UDP source interface • port-id: UDP interface ID, an integer, ranging from 0 to 65535 • biff: Biff, the corresponding interface ID is 512 • bootpc: BOOTP client, the corresponding interface ID is 68 • bootps: BOOTP server, the corresponding interface ID is 67 • domain: domain service protocol, the corresponding interface ID is 53. • echo: echo protocol, the corresponding interface ID is 7. • mobile-ip: mobile IP registration, the corresponding interface ID is 434. • netbios-dgm: NetBios datagram, the corresponding interface ID is 138. • netbios-ns: NetBios name service, the corresponding interface ID is 137. • netbios-ss: NetBios session service, the corresponding interface ID is 139. • ntp: network time protocol, the corresponding interface ID is 123 • pim-auto-rp: PIM Auto-RP, the corresponding interface ID is 496. • rip: routing information protocol, the corresponding interface ID is 520. • snmp: simple network management protocol, the corresponding interface ID is 161. • snmptrap: SNMP Traps, the corresponding interface ID is 162. • sunrpcun: remote process call, the corresponding interface ID is 111. • syslog: syslog, the corresponding interface ID is 514. • tacacs: terminal access controller access-control system. The corresponding interface ID is 49. • talkTalk, the corresponding interface ID is 517 • tftp: trivial file transfer protocol, the corresponding interface ID is 69. • timeTime, the corresponding interface ID is 37. • who: Who service, the corresponding interface ID is 513.

14.2.6 Configuring user ACL

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#user-access-list profile field field-id layer { 12 13 14 } offset offset-value example: Raisecom(config)#user-access-list profile field 2 layer 12 offset 3	Configure customized ACL match objects. • field-id: match field ID, an integer, ranging from 1 to 8 • 12: match from Layer 2 header. • 13: match from Layer 3 header. • 14: match from Layer 4 header. • offset-value: offset value, an integer, ranging from 0 to 123  Note The XEP8 (B) card supports up to 3 fields . The maximum offset is 63.
3	Raisecom(config)#user-access-list acl-number example: Raisecom(config)#user-access-list 1010	Create a customized ACL and enter user ACL configuration mode. You can use the no user-access-list { all list-number } command to delete the ACL. • user-access-list acl-number: enter user-defined ACL subrule mode. The acl-number refers to the list ID, which is an integer ranging from 8001 to 9000.
4	Raisecom(config-user-acl-*)#description text example: Raisecom(config-user-acl-1010)#description raisecom	(Optional) configure descriptions of the user ACL. You can use the no description command to delete the description. • text: description, a string of 1 to 16 characters
5	Raisecom(config-user-acl-*)#rule rule-number example: Raisecom(config-user-acl-1)#rule 2	Configure the number of the user ACL sub-rule and enter sub-rule configuration mode. • rule rule-id: Layer 2 subrule ID, an integer, ranging from 1 to 256
6	Raisecom(config-user-acl-*-rule-*)#access-type { permit deny } example: Raisecom(config-user-acl-1010-rule-2)#access-type deny	Configure the access type of the user ACL sub-rule. • deny: deny access when conditions match. • permit: allow access when conditions meet.
7	Raisecom(config-user-acl-*-rule-*)#match field field-id content mask example: Raisecom(config-user-acl-1010-rule-2)#match field 1 abc	Configure the content of the ACL match field. • field-id: area ID, an integer, ranging from 1 to 8 • content: area contents, a character string • mask: area mask
8	Raisecom(config-user-acl-*-rule-*)#match tag-type { double-tag s-tagged untagged } example: Raisecom(config-user-acl-1010-rule-2)#match tag-type double-tagged	Configure matching the user ACL with packets of different Tag types. • double-tagged: double tag • single-tagged: single tag • untagged: untagged



Note

The XEP8 (B) card only supports Layer 2 ACL matching rules in the egress direction.

14.2.7 Applying ACL to device



Note

The ACL can be valid on the device only when an ACL is added to the filter. Multiple ACL matching rules can be added to the filter to form multiple filtering rules. When a filter is configured, the order in which ACL matching rules are added determines the priority of these rules. The earlier the rule is added, the higher the priority is. If there are conflicts in the matching calculation, the rule with the highest priority should prevail. When configuring commands, be careful when arranging the priorities of those rules in order to properly filter the packets.

Applying ACL based on whole device

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#filter { l2-access-list ip-access-list ipv6-access-list hybrid-access-list ipv6-hybrid-access-list user-access-list } acl-id [statistics]</code> example: <code>Raisecom(config)#filter ip-access-list 1010</code>	Configure applying filtering rules based on the whole device. If you have configured the statistics parameter, the system takes statistics according to the filtering rules. Note This function is not supported by the XEP8 (B) card. You can use the no filter acl-id command to delete the application relationship of the filtering rules. • l2-access-list acl-number: filter by Layer 2 ACL. • acl-number: ACL ID, an integer, ranging from 1 to 1000 • ip-access-list acl-number: filter by IPv4 ACL. • acl-number: ACL ID, an integer, ranging from 1001 to 2000 • ipv6-access-list acl-number: filter by IPv6 ACL. • acl-number: ACL ID, an integer, ranging from 2001 to 3000 • hybrid-access-list acl-number: filter by hybrid ACL. • acl-number: ACL ID, an integer, ranging from 3001 to 4000 • ipv6-hybrid-access-list: enter IPv6 hybrid ACL subrule mode. • list: ACL ID, an integer, ranging from 4001 to 5000 • user-access-list acl-number: filter by user-defined ACL. • acl-number: ACL ID, an integer, ranging from 8001 to 9000

Applying ACL based on uplink and downlink of interface

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	<pre> Raisecom(config)#filter { l2-access-list ip-access-list ipv6-access-list hybrid-access-list ipv6-hybrid-access- list user-access-list } <i>acl-id</i> { ingress egress } interface { epon- olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } <i>slot-id/port-list</i> [statistics] Raisecom(config)#filter user-access-list <i>acl-number</i> ingress interface { epon-olt <i>slot-id/port-list</i> epon-onu <i>slot-</i> <i>id/olt-id/onu-id</i> epon-onu <i>slot-id/olt-</i> <i>id/onu-id</i> gpon-olt <i>slot-id/port-list</i> gigabitethernet <i>slot-id/port-id</i> ten- gigabitethernet <i>slot-id/port-id</i> ten- giga-epon-olt <i>slot-id/port-id</i> port- channel <i>group-id</i> } [statistics] example: Raisecom(config)#filter ip-access-list 1010 interface gigabitethernet 3/1 </pre>	Configure applying ACL filtering rules to the downlink and uplink of the interface. If you have configured the statistics parameter, the system takes statistics according to the filtering rules.  Note The XEP8 (B) card only supports Layer 2 ACL in the egress direction. • l2-access-list acl-number: filter by Layer 2 ACL. The acl-number refers to the ACL ID, which is an integer ranging from 1 to 1000. • ip-access-list acl-number: filter by IPv4 ACL. The acl-number refers to ACL ID, which is an integer ranging from 1001 to 2000. • ipv6-access-list acl-number: filter by IPv6 ACL. The acl-number refers to ACL ID, which is an integer ranging from 2001 to 3000. • hybrid-access-list acl-number: filter by hybrid ACL. The acl-number refers to the ACL ID, which is an integer ranging from 3001 to 4000. • ipv6-hybrid-access-list list: enter IPv6 hybrid ACL subrule mode. The list refers to the list ID, which is an integer ranging from 4001 to 5000. • user-access-list acl-number: filter by user-defined ACL. The acl-number refers to the ACL ID, which is an integer ranging from 8001 to 9000. • epon-olt slot-id/port-id: EPON interface ID • gpon-olt slot-id/port-id: GPON interface ID • gigabitethernet slot-id/port-id: GE interface ID • ten-gigabitethernet slot-id/ port-id: 10GE interface ID • port-channel: filter packets in the receiving direction of the aggregation interface. • group-id: aggregation group ID, an integer

Applying ACL based on traffic from ingress interface to egress interface

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#filter { l2-access-list ip-access-list ipv6-access-list hybrid- access-list ipv6-hybrid-access-list } acl- id from interface { epon-olt ten-giga- epon-olt gpon-olt gigabitethernet ten- gigabitethernet } slot-id/port-list to interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten- gigabitethernet } slot-id/port-list [statistics]</pre> example: Raisecom(config)#filter ip-access-list 1010 from interface gigabitethernet 3/1 to interface gigabitethernet 3/10	Configure applying ACL filtering rules based on traffic from the ingress interface to egress interface. If you have configured the statistics parameter, the system takes statistics according to the filtering rules.  Note When you use this command, the ingress and egress interfaces should be on the same card. The XEP8 (B) card only supports Layer 2 ACL in the egress direction. • l2-access-list acl-number: filter by Layer 2 ACL. The acl-number refers to the ACL ID, which is an integer ranging from 1 to 1000. • ip-access-list acl-number: filter by IPv4 ACL. The acl-number refers to ACL ID, which is an integer ranging from 1001 to 2000. • ipv6-access-list acl-number: filter by IPv6 ACL. The acl-number refers to ACL ID, which is an integer ranging from 2001 to 3000. • hybrid-access-list acl-number: filter by hybrid ACL. The acl-number refers to ACL ID, which is an integer ranging from 3001 to 4000. • ipv6-hybrid-access-list list: enter IPv6 hybrid ACL subrule mode. The list refers to the list ID, which is an integer ranging from 4001 to 5000. • user-access-list acl-number: filter by user-defined ACL. The acl-number refers to the ACL ID, which is an integer ranging from 8001 to 9000. • epon-olt slot-id/port-id: EPON interface ID • gpon-olt slot-id/port-id: GPON interface ID • gigabitethernet slot-id/port-id: GE interface ID • ten-gigabitethernet slot-id/ port-id: 10GE interface ID • port-channel: filter packets in the receiving direction of the aggregation interface. • group-id: aggregation group ID, an integer

14.2.8 Checking configurations

Checking OLT configurations

No.	Command	Description
1	Raisecom# show ip-access-list [<i>list-number</i>]	Show IPv4 ACL configurations.
2	Raisecom# show ipv6-access-list [<i>list-number</i>]	Show IPv6 ACL configurations.
3	Raisecom# show l2-access-list [<i>list-number</i>]	Show Layer 2 ACL configurations.
4	Raisecom# show hybrid-access-list [<i>list-number</i>]	Show hybrid ACL configurations.
5	Raisecom# show ipv6-hybrid-access-list [<i>list-number</i>]	Show IPv6 hybrid ACL configurations.
6	Raisecom# show user-access-list [<i>list-number</i>]	Show user ACL configurations.
7	Raisecom# show user-access-list profile	Show the customized ACL match field.
8	Raisecom# show interface vlanif ip-access-list	Show ACL configurations of the VLAN interface.
9	Raisecom# show filter [<i>filter-number</i>] statistics	Show filter statistics.
10	Raisecom# show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id filter	Show filters already configured on the ONU interface.

14.3 Configuring RADIUS

14.3.1 Preparing for configurations

Scenario

You can deploy the RADIUS server on the network to perform authentication and accounting to control users from accessing the device and network. The device can be used as an agent of the RADIUS server, which authorizes users to access according to feedback from the RADIUS server.

Prerequisite

N/A

14.3.2 Default configurations

Default configurations of RADIUS on the ISCOM5508 are as below.

Function	Default value
RADIUS accounting	Disable
IP address and UDP interface ID of RADIUS authentication server	• IP address: 0.0.0.0 • UDP interface ID: 1812
IP address and UDP interface ID of RADIUS accounting server	• IP address: 0.0.0.0 • UDP interface ID: 1813
Shared key used to communicate with the RADIUS accounting server	N/A
Processing policy upon accounting failure	online
Time to send accounting update packets	0

14.3.3 Configuring RADIUS authentication

Step	Command	Description
1	Raisecom#radius [backup] <i>ip-address</i> [auth-port <i>port-id</i>] example: Raisecom#radius 10.0.0.1 auth-port 1000	Specify the IPv4 address and interface ID of the RADIUS authentication server. You can use the backup parameter to specify the backup RADIUS authentication server. • backup: configure the IP address of RADIUS backup authentication server. If you do not select this parameter, it configures the IP address of the active authentication server of RADIUS authentication server. • ip-address: IPv4 address, in dotted decimal notation, such as 10.10.10.1 • port-id: authentication interface ID, an integer, ranging from 1 to 65535
	Raisecom#radius [backup] <i>ipv6-address</i> [scopeid <i>string</i>] [auth-port <i>port-id</i>] example: Raisecom#radius 3001::1 auth-port 1000	Specify the IPv6 address and interface ID of the RADIUS authentication server. You can use the backup parameter to specify the backup RADIUS authentication server. • backup: configure the IP address of the backup RADIUS authentication server. If you do not select this parameter, it configures the IP address of the active RADIUS authentication server. • ipv6-address: IPv6 address, in colon hexadecimal notation, such as 3001::1 • port-id: authentication interface ID, an integer, ranging from 1 to 65535
2	Raisecom#radius-key <i>word</i> example: Raisecom#radius-key raisecom	Configure the shared key of RADIUS authentication. • word: secret key, a string of 1 to 200 characters

Step	Command	Description
3	<pre>Raisecom#user login { radius-user radius-local } server-no-response</pre> example: <pre>Raisecom#user login radius-user server-no-response</pre>	Configure the user login mode to RADIUS authentication. • radius-user: use RADIUS authentication. • tacacs-local: use TACACS+ authentication when local authentication and TACACS+ authentication co-exist.

14.3.4 Configuring RADIUS accounting

Step	Command	Description
1	<pre>Raisecom#aaa accounting login enable</pre>	Enable RADIUS accounting. You can use the aaa accounting login disable command to disable this function.
2	<pre>Raisecom#radius [backup] accounting-server ip-address [acct-port port-id]</pre> example: <pre>Raisecom#radius accounting-server 10.0.0.1 acct-port 1000</pre>	Specify the IPv4 address and UDP interface ID of the RADIUS accounting server. You can use the backup parameter to specify the backup RADIUS accounting server. • backup: configure the IP address of the backup RADIUS accounting server. If you do not select this parameter, it configures the IP address of the active RADIUS accounting server. • ip-address: IPv4 address, in dotted decimal notation, such as 10.10.10.1 • port-id: accounting interface ID, an integer, ranging from 1 to 65535
	<pre>Raisecom#radius [backup] accounting-server ipv6-address [scopeid string] [acct-port port-id]</pre> example: <pre>Raisecom#radius accounting-server 3001::1 acct-port 1000</pre>	Specify the IPv6 address and UDP interface ID of the RADIUS accounting server. You can use the backup parameter to specify the backup RADIUS accounting server. • backup: configure the IP address of the backup RADIUS accounting server. If you do not select this parameter, it configures the IP address of the active RADIUS accounting server. • ipv6-address IPv6 address, in colon hexadecimal notation, such as 3001::1 • port-id: accounting interface ID, an integer, ranging from 1 to 65535
3	<pre>Raisecom#radius accounting-server key string</pre> example: <pre>Raisecom#radius accounting-server key raisecom</pre>	Configure the shared key used to communicate with the RADIUS accounting server. The shared key should be consistent with that configured on the RADIUS accounting server; otherwise, accounting fails. • string: secret key, a string of 1 to 200 characters

Step	Command	Description
4	<pre>Raisecom#aaa accounting fail { online offline } example: Raisecom#aaa accounting fail offline</pre>	Configure the processing policy upon accounting failure. • online: permit login after authentication failure. • offline: deny login after authentication failure.
5	<pre>Raisecom#aaa accounting update period example: Raisecom#aaa accounting update 10</pre>	Configure the period to send accounting update packets. If it is configured to 0, accounting update packets will not be sent.  Note Through accounting the start packet, update packet, and end packet, the RADIUS accounting server records the access time and operations of each user. • period: sending period, an integer, ranging from 0 to 300, in units of minute

14.3.5 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show radius-server</pre>	Show RADIUS server configurations.
2	<pre>Raisecom#show aaa accounting</pre>	Show RADIUS accounting server running conditions.

14.4 Configuring TACACS+

14.4.1 Preparing for configurations

Scenario

You can deploy the TACACS+ server on the network to perform authentication and accounting to control users from accessing the device and network. TACACS+ is safer and more reliable than RADIUS. The device can be used as an agent of the TACACS+ server, which authorizes users to access according to feedback from the TACACS+ server.

Prerequisite

N/A

14.4.2 Default configurations

By default, the ISCOM6800 and ISCOM6860 are not configured with TACACS+ authentication server address and shared key. Both the user login mode and the enable login mode are local-user.

Function	Default value
IP address of TACACS+ authentication server	0.0.0.0
IP address of TACACS+ accounting server	0.0.0.0
Shared key	N/A
User login mode	local-user
Enable login mode	local-user

14.4.3 Configuring TACACS+

Step	Command	Description
1	Raisecom#tacacs-server [backup] <i>ip-address</i> example: Raisecom#tacacs-server backup 10.0.0.1	Specify the IPv4 address of the TACACS+ authentication server. You can use the backup parameter to specify the backup TACACS+ authentication server. • backup: configure the IP address of backup TACACS+ authentication server. If you do not select this parameter, it configures the IP address of the primary TACACS+ authentication server. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1
	Raisecom#tacacs-server [backup] <i>ipv6-address</i> [scopeid string] example: Raisecom#tacacs-server backup 3001::1	(Optional) specify the IPv6 address of the TACACS+ authentication server. You can use the backup parameter to specify the backup TACACS+ authentication server. • backup: configure the IP address of backup TACACS+ authentication server. If you do not select this parameter, it configures the IP address of the primary TACACS+ authentication server. • ipv6-address: IPv6 address, in colon hexadecimal notation, such as 3001:1

Step	Command	Description
2	Raisecom#tacacs-server key <i>string</i> example: Raisecom#tacacs-server key raisecom	Configure the shared key of TACACS+ authentication. • string: secret key, a string of 1 to 200 characters
3	Raisecom# enable login tacacs-local [server-no-response]	(Optional) configure login mode in privileged mode.

14.4.4 Configuring TACACS+ accounting

Step	Command	Description
1	Raisecom#tacacs [backup] accounting-server <i>ip-address</i> example: Raisecom#tacacs accounting-server 10.0.0.1	Specify the IPv4 address of the TACACS+ accounting server. You can use the backup parameter to specify the backup TACACS+ accounting server. • backup: configure the IP address of backup TACACS+ accounting server. If you do not select this parameter, it configures the IP address of the primary TACACS+ accounting server. • ip-address: IPv4 address, in dotted decimal notation, such as 10.10.10.1
	Raisecom#tacacs [backup] accounting-server <i>ipv6-address</i> [scopeid <i>string</i>] example: Raisecom#tacacs accounting-server 3001::1	(Optional) specify the IPv6 address of the TACACS+ accounting server. You can use the backup parameter to specify the backup TACACS+ accounting server. • backup: configure the IP address of backup TACACS+ accounting server. If you do not select this parameter, it configures the IP address of the primary TACACS+ accounting server. • ipv6-address: IPv6 address, in colon hexadecimal notation, such as 3001:1

14.4.5 Checking configurations

No.	Command	Description
1	Raisecom# show tacacs-server	Show TACACS+ server configurations.

14.5 Configuring storm control

14.5.1 Preparing for configurations

Scenario

Configuring storm control on Layer 2 devices can prevent broadcast storm occurring when broadcast packets increase sharply on the network. Therefore, it makes sure that unicast packets can be properly forwarded.

The following forms of traffic may cause broadcast traffic, so you need to limit the bandwidth for them on Layer 2 devices.

- DLF traffic: the unicast traffic whose destination MAC address is not in the MAC address table, which is broadcasted by Layer 2 devices.
- Unknown multicast traffic: the multicast traffic whose destination MAC address is not in the MAC address table, which is broadcasted by Layer 2 devices.
- Broadcast traffic: the traffic whose destination MAC address is a broadcast MAC address, which is broadcasted by Layer 2 devices.

Prerequisite

Connect the interface, configure its physical parameters, and make it Up at the physical layer.

14.5.2 Default configurations

Default configurations of storm control on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Broadcast storm control	Enable
Multicast group storm control	Disable
DLF storm control	Disable
Rate threshold	1024 kbit/s (the 10 Gbit/s interface is 4096 kbit/s)
Burst length	512 Kbytes (the 10 Gbit/s interface is 1024 kB)

Default configurations of storm control on Raisecom ONU devices are as below.

Function	Default value
Storm control over broadcast packets	Enable
Storm control over multicast group packets	Enable
DLF storm control	Disable
Rate threshold	1000 kbit/s

Function	Default value
Burst length threshold	4B
Packet rate threshold	1000pps

14.5.3 Configuring storm control

Configuring storm control on OLT

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id example: Raisecom(config)#interface gigabitethernet 2/1	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode
3	Raisecom(config-if-**-*)#storm-control { all broadcast dlf multicast } example: Raisecom(config-if-gigabitethernet-2:1)#storm-control dlf	Enable storm control over broadcast, multicast, and DLF traffic. • all: broadcast packets, DLF packets, and multicast packets • broadcast: broadcast packets • dlf: DLF packets, • multicast: multicast packets
4	Raisecom(config-if-**-*)#storm-control bps value burst example: Raisecom(config-if-gigabitethernet-3/1:1)#storm-control bps 2048 1024	(Optional) configure the rate limit of storm control. • value: rate, an integer, ranging from 64 to 1048576, in units of kbit/s • burst: burst size, an integer, ranging from 4 to 16384, in units of Byte

Configuring storm control on ONU

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)# epon-onu <i>slot-id/olt-id/onu-id</i> example: Raisecom(config)#epon-onu 2/1/1	Enter EPON ONU remote management configuration mode. - slot-id: slot ID - olt-id: PON interface ID - onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*//*:*)# storm-control { broadcast dlf multicast all } { enable disable } example: Raisecom(config-epon-onu-2/1:1)#storm-control dlf enable	Enable/Disable storm control over broadcast traffic, multicast traffic, and DLF traffic. - all: broadcast packets, DLF packets, and multicast packets - broadcast: broadcast packets - dlf: DLF packets, - multicast: multicast packets
4	Raisecom(config-epon-onu-*//*:*)# storm-control bps <i>rate</i> [<i>burst</i>] example: Raisecom(config-if-gigabitethernet-3/1:1)#storm-control bps 2048 1024	(Optional) configure the rate and burst length threshold of storm control. - rate: rate, an integer, ranging from 64 to 1048576, in units of kbit/s - burst: burst size, an integer, ranging from 4 to 16384, in units of Byte
5	Raisecom(config-epon-onu-*//*:*)# storm-control pps <i>rate</i> example: Raisecom(config-epon-onu-3/1:1)#storm-control pps 2000	(Optional) configure the packet rate threshold of storm control. rate: packet rate, an integer, ranging from 1000 to 1000000, in units of pps

Checking configurations

No.	Command	Description
1	Raisecom# show epon-onu <i>slot-id/olt-id/onu-id</i> storm-control	Show configurations of ONU storm control.

14.6 Configuring interface isolation

14.6.1 Preparing for configurations

Scenario

Interface isolation implements data isolation among multiple interfaces on the device by adopting isolation groups. You can isolate different physical interfaces or interfaces in the same VLAN by creating isolation groups to enhance safety of network access.

Prerequisite

N/A

14.6.2 Default configurations

Default configurations of interface isolation on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Ethernet interface isolation	Disable
EPON interface isolation	Enable

Default configurations of interface isolation on the Raisecom ONU device.

Function	Default value
UNI isolation	Enable

14.6.3 Configuring OLT interface isolation

Configuring interface isolation

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id example: Raisecom(config)#interface gigabitethernet 2/1	Enter physical interface configuration mode. • epon-olt: enter EPON interface configuration mode. • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: 1000 Mbit/s Ethernet interface configuration mode • ten-gigabitethernet: 10 Gbit/s Ethernet interface configuration mode
3	Raisecom(config-if-*:*:*)#isolate-group { group-id default } example: Raisecom(config-gigabitethernet-2:1)#isolate-group 2	Create the isolation group for physical interfaces. If a specified isolation group exists, add interfaces to the group. You can use the no isolate-group group-id command to delete the isolation group or interfaces from the specified isolation group. • group-id: isolation group, an integer, ranging from 2 to 128

Configuring VLAN isolation

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id example: Raisecom(config)#interface gigabitethernet 2/1	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: 1000 Mbit/s Ethernet interface configuration mode • ten-gigabitethernet: 10 Gbit/s Ethernet interface configuration mode
3	Raisecom(config-if-*:*:*)#vlan vlan-id isolate-group group-id example: Raisecom(config-gigabitethernet-2:1)#vlan 1 isolate-group 1	Create a VLAN isolation group. If a specified isolation group exists, add interfaces to the group. You can use the no vlan vlan-id isolate-group group-id command to delete the isolation group or interfaces from the specified isolation group. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • group-id: isolation group, an integer, ranging from 1 to 8

14.6.4 Configuring ONU interface isolation

Configuring ONU UNI isolation

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id	Enter EPON ONU UNI configuration mode.
3	Raisecom(config-epon-onu-ethernet-*/*:*)#switchport isolation { enable disable }	Enable/Disable UNI isolation.

14.6.5 Checking configurations

No.	Command	Description
1	Raisecom#show isolate-group [group-id]	Show configurations of physical interface isolation.
2	Raisecom#show vlan-isolate-group vlan vlan-id [group-id]	Show configurations of the VLAN isolation group.

No.	Command	Description
3	Raisecom# show epon-onu slot-id/olt-id/onu-id uni ethernet isolation	Show ONU UNI isolation.

14.7 Configuring attack prevention

14.7.1 Preparing for configurations

Scenario

To avoid packet attacks, you can configure attack prevention to filter extra packets.

Prerequisite

N/A

14.7.2 Default configurations

N/A

14.7.3 Configuring attack prevention

No.	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# attack-defense land	(Optional) prevent LAND attacks.
3	Raisecom(config)# attack-defense large-icmp [size size] example: Raisecom(config)# attack-defense large-icmp size 300	(Optional) prevent oversized ICMP packet attacks. • size size: the maximum length of ICMP frame, an integer, ranging from 256 to 2048, in units of Byte
4	Raisecom(config)# attack-defense smurf	(Optional) prevent SMURF attacks.
5	Raisecom(config)# attack-defense urpf	(Optional) prevent URPF attacks.

14.7.4 Checking configurations

No.	Command	Description
1	Raisecom# show attack-defense	Show configurations of attack prevention.

14.8 Configuring anti-DoS attacks

14.8.1 Preparing for configurations

Scenario

To prevent DoS attack packets, you can configure this command to filter different protocols.

Prerequisite

N/A

14.8.2 Default configurations

N/A

14.8.3 Configuring anti-DoS attacks

No.	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#anti-dos { ack arp dhcp dns icmp igmp syn udp }	Configure the type of anti-DoS attack protocol.
3	Raisecom(config)#anti-dos aging-time <i>time</i>	Configure the aging time of anti-DoS attack.
4	Raisecom(config)#anti-dos rate-limit <i>rate</i>	Limit the rate of DoS attack packets.

14.8.4 Checking configurations

No.	Command	Description
1	Raisecom#show anti-dos black-list	Show configurations of anti-DoS attacks.

14.9 Maintenance

No.	Command	Description
1	<pre>aisecom(config)#clear filter <i>filter-number</i> [rule <i>rule-list</i>] statistics Raisecom(config)#clear filter <i>filter-list</i> statistics example: Raisecom(config)#clear filter 1 statistics</pre>	Clear ACL filter statistics. • filter-number: filter ID, an integer, ranging from 1 to 1024 • filter-list: filter list ID, an integer, ranging from 1 to 1024. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • rule rule-list: L2 sub-rule mode ID, an integer, ranging from 1 to 256. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
2	<pre>Raisecom(config)#clear tacacs statistics</pre>	Clear TACACS+ statistical data.

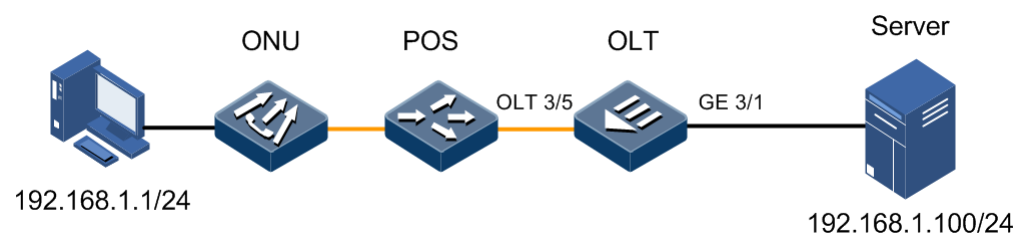
14.10 Configuration examples

14.10.1 Example for configuring ACL

Networking requirements

As shown in Figure 14-1, to control users' access to the server, you can configure ACL forbidding 192.168.1.1 to access the server 192.168.1.100.

Figure 14-1 ACL networking



Configuration steps

Step 1 Configure IP ACL.

```

Raisecom#config
Raisecom(config)#ip-access-list 1001
Raisecom(config-ip-acl-1001)#rule 1
Raisecom(config-ip-acl-1001-rule-1)#access-type deny
Raisecom(config-ip-acl-1001-rule-1)#match ip destination-address
192.168.1.100 255.255.255.0
```

```
Raisecom(config-ip-acl-1001-rule-1)#match ip source-address 192.168.1.1
255.255.255.0
Raisecom(config-ip-acl-1001-rule-1)#exit
Raisecom(config-ip-acl-1001)#rule 2
Raisecom(config-ip-acl-1001-rule-2)#access-type permit
Raisecom(config-ip-acl-1001-rule-2)#match ip destination-address 0.0.0.0
255.255.255.255
Raisecom(config-ip-acl-1001-rule-2)#match ip source-address 0.0.0.0
255.255.255.255
Raisecom(config-ip-acl-1001-rule-2)#exit
Raisecom(config-ip-acl-1001)#exit
```

Step 2 Apply ACL on the interface OLT 1/1.

```
Raisecom(config)#filter ip-access-list 1001 ingress interface epon-olt
3/1
```

Checking results

Use the **show ip-access-list** to show IP ACL configurations.

```
Raisecom#show ip-access-list 1001
description ACL-1001
rule 1
  match ip source-address 255.255.255.0 255.255.255.0
  match ip destination-address 255.255.255.0 255.255.255.0
  access-type deny

rule 2
  match ip source-address 255.255.255.255
  match ip destination-address 255.255.255.255
  access-type permit
```

Use the **show filter** command to show filter configurations.

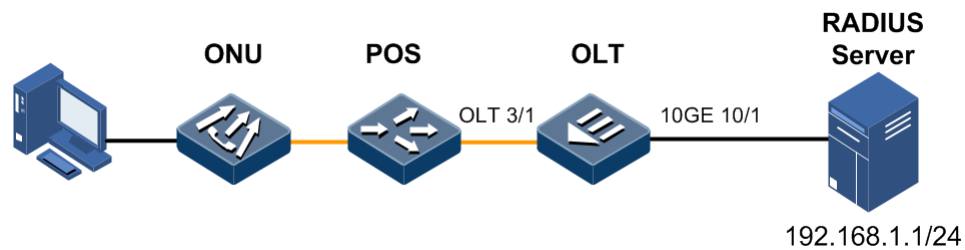
```
Raisecom#show filter
Filter ID : 1001
ACL ID   : 1
Hardware  : Yes
Egress Port : epon-olt 3/1
Ingress Port : epon-olt 3/1
Statistics : Disable
```

14.10.2 Example for configuring RADIUS

Networking requirements

As shown in Figure 13-2, to control user access to the device, you need to configure RADIUS authentication and accounting on the OLT to authenticate users logging in to the OLT and record their operations. The interval for sending update packets is 2 minutes, and the user is offline when the accounting fails.

Figure 14-2 RADIUS application networking



Configuration steps

Step 1 Authenticate login users through RADIUS.

```
Raisecom#radius 192.168.1.1
Raisecom#radius-key raisecom
Raisecom#user login radius-user
```

Step 2 Configure RADIUS accounting for login users.

```
Raisecom#aaa accounting login enable
Raisecom#radius accounting-server 192.168.1.1
Raisecom#radius accounting-server key raisecom
Raisecom#aaa accounting fail offline
Raisecom#aaa accounting update 120
```

Checking results

Use the **show radius-server** command to check whether RADIUS configurations are correct.

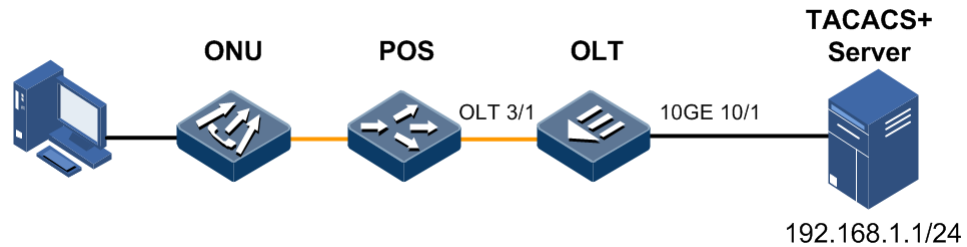
```
Raisecom#show radius-server
Authentication server IP:      192.168.1.1 port:1812
Backup authentication server IP: 0.0.0.0 port:1812
Authentication server key:    raisecom
Accounting server IP:         192.168.1.1 port:1813
Backup accounting server IP:   0.0.0.0 port:1813
Accounting server key:        raisecom
```

14.10.3 Example for configuring TACACS+

Networking requirements

As shown in Figure 13-3, to control user access to the device, you need to deploy the TACACS+ authentication feature on the OLT to authenticate users logging in to the OLT.

Figure 14-3 TACACS+ application networking



Configuration steps

Step 1 Configure TACACS+ authentication for login users.

```
Raisecom#tacacs-server 192.168.1.1
Raisecom#tacacs-server key raisecom
Raisecom#user login tacacs-user
```

Checking results

Use the **show tacacs-server** command to check whether TACACS+ configurations are correct.

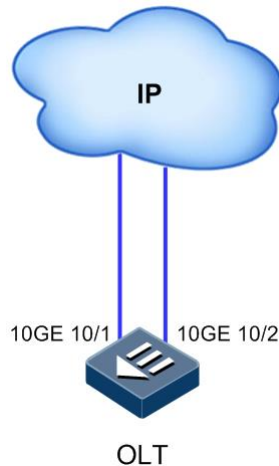
```
Raisecom#show tacacs-server
Server Address:      192.168.1.1
Backup server Address: 0.0.0.0
Sever Shared Key:    raisecom
Total Packet Sent:   0
Total Packet Recv:   0
Num of Error Packets: 0
Accounting server Address: 0.0.0.0
Backup Accounting server Address: 0.0.0.0
```

14.10.4 Example for configuring storm control

Networking requirements

As shown in Figure 14-4, to limit effects on the OLT by broadcast storm, you need to deploy storm control on the OLT to limit broadcast and unknown unicast packets. The threshold is 2000 kbit/s and the burst size value is 1024 Kbytes.

Figure 14-4 Storm control networking



Configuration steps

Configure storm control on the OLT.

```

Raisecom#config
Raisecom(config)#interface ten-gigabitethernet 10/1
Raisecom(config-if-ten-gigabitethernet-10:1)#storm-control broadcast
Raisecom(config-if-ten-gigabitethernet-10:1)#storm-control dlf
Raisecom(config-if-ten-gigabitethernet-10:1)#storm-control bps 2000 burst
1024
Raisecom(config-if-ten-gigabitethernet-10:1)#exit
Raisecom(config)#interface ten-gigabitethernet 10/2
Raisecom(config-if-ten-gigabitethernet-10:2)#storm-control broadcast
Raisecom(config-if-ten-gigabitethernet-10:2)#storm-control dlf
Raisecom(config-if-ten-gigabitethernet-10:2)#storm-control bps 2000 burst
1024
  
```

Checking results

Use the **show storm-control** to show storm control configurations.

```

Raisecom#show storm-control
  
```

Port	Broadcast	Multicast	DLF_Unicast	Threshold
gigabitethernet10/1	enable	disable	enable	2000Kb/s Burst 1024 KB
gigabitethernet10/2	enable	disable	enable	2000Kb/s Burst 1024 KB

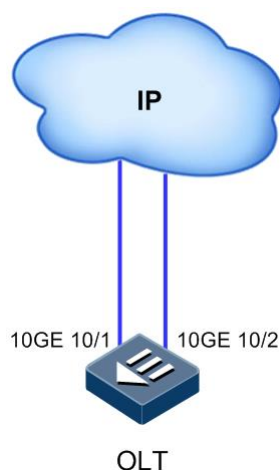
14.10.5 Example for configuring anti-DoS attacks

Networking requirements

As shown in Figure 14-5, to prevent the device from DoS attacks of the ARP type, you need to configure anti-DoS attack on the OLT. The configuration requirements are as below:

- Configure the protocol type of anti-DOS attacks as ARP.
- Configure the aging time of anti-DOS attacks to 20s.
- Configure the rate of DoS attack packets to 100pps.

Figure 14-5 Anti-DoS attack networking



Configuration steps

Step 1 Configure the protocol type of anti-DoS attack to ARP.

```
Raisecom#config  
Raisecom(config)#anti-dos arp
```

Step 2 Configure the aging time of anti-DoS attacks to 20s.

```
Raisecom(config)#anti-dos aging-time 20
```

Step 3 Configure the rate of DoS attack packets to 100pps.

```
Raisecom(config)#anti-dos rate-limit 100  
Raisecom(config)#exit
```

Checking results

Use the **show anti-dos black-list** command to show configurations of anti-DoS attacks.

```
Raisecom#show anti-dos black-list
```

```
Anti-DOS : SYN : Disable  
Anti-DOS : ACK : Disable  
Anti-DOS : ICMP : Disable  
Anti-DOS : UDP : Disable  
Anti-DOS : DNS : Disable  
Anti-DOS : ARP : Enable  
Anti-DOS : IGMP : Disable  
Anti-DOS : DHCP : Disable  
Anti-DOS limit rate : 100 (pps)  
Anti-DOS aging time : 20 (s)
```

Black-list:

MAC address	VLAN	Port	Protocol Type

15

Configuring link security

This chapter describes the link security feature and configuration process of the ISCOM6800 and ISCOM6860, and provides related configuration examples, including the following sections:

- Introduction
- Configuring link aggregation
- Configuring EPON OLT backbone fiber protection (TypeB)
- Configuring cross-OLT EPON port dual-homed protection (Type B)
- Configuring port backup
- Maintenance
- Configuration examples

15.1 Introduction

15.1.1 Link aggregation

With link aggregation, multiple physical Ethernet interfaces are combined to form a logical Link Aggregation Group (LAG). Multiple physical links in one LAG are taken as a logical link. Link aggregation helps share loads among members in a LAG. Link aggregation can not only implement load balancing among member interfaces but also improve link reliability and bandwidth.

Manual link aggregation

Manual link aggregation refers to a process that multiple physical interfaces are aggregated to a logical interface. Links under a logical interface share loads. In this mode, the status of link aggregation interfaces is not easy to be observed.

LACP

Link Aggregation Control Protocol (LACP) is a protocol based on IEEE802.3ad. With LACP, the device communicates with the peer through the Link Aggregation Control Protocol Data Unit (LACPDU). After LACP is enabled on an interface, the interface sends a LACPDU to inform the peer of its system LACP priority, system MAC address, interface LACP priority, interface ID, and operation key.

After receiving the LACPDU, the peer compares its information with that received by other interfaces to choose an interface that can be set to selected status. Therefore, both ends reach a consensus on the interface status (selected). The operation key is a configuration combination automatically generated based on configurations of the interface, such as the rate, duplex mode, and Up/Down status. In a LAG, interfaces in the selected status share the identical operation key.

15.1.2 EPON port link protection

The ISCOM6820-EP (A) supports Type B, Type C, and Type D PON port protection and cross-OLT PON port dual-homed Type B protection. The main protection forms are as below:

- OLT backbone fiber protection (Type B): redundancy of backbone fiber and OLT PON port.
- PON full protection (Type C): OLT dual PON ports, ONU dual PON ports, redundancy of backbone fiber, optical splitter and distribution fiber.
- PON full protection (Type D): OLT dual PON ports, ONU dual PON ports, redundancy of backbone fiber, optical splitter and distribution fiber.
- Cross-OLT PON port dual-homed Type B protection: it is an extension of standard Type B protection. Support redundancy of backbone fiber, OLT' PON port, and uplink port.

OLT backbone fiber protection (Type B)

OLT backbone fiber protection (Type B) refers to the redundancy protection of backbone fiber and OLT PON port. The two PON ports of the OLT use independent PON MAC chips and optical modules for protection.

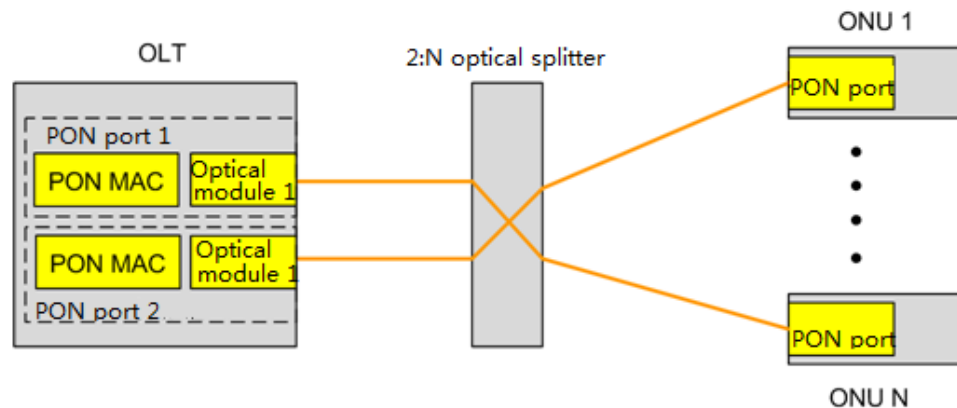
Type B protection is suitable for the protection of PON ports in the same PON port and the same OLT. The requirements are as below:

- OLT: the standby OLT PON port is in cold backup state. The OLT detects the link status and the PON port status, and the switching is completed by the OLT. The OLT should ensure that the service information of the primary PON port can be backed up to the backup PON port synchronously, so that the backup PON port can maintain the ONU's service attributes unchanged during the protection process.
- Optical splitter: use a 2:N optical splitter.

ONU: no special requirements.

Figure 15-1 shows the principle of OLT backbone fiber protection (Type B).

Figure 15-1 Principle of OLT backbone fiber protection (Type B)



PON full protection (Type C)

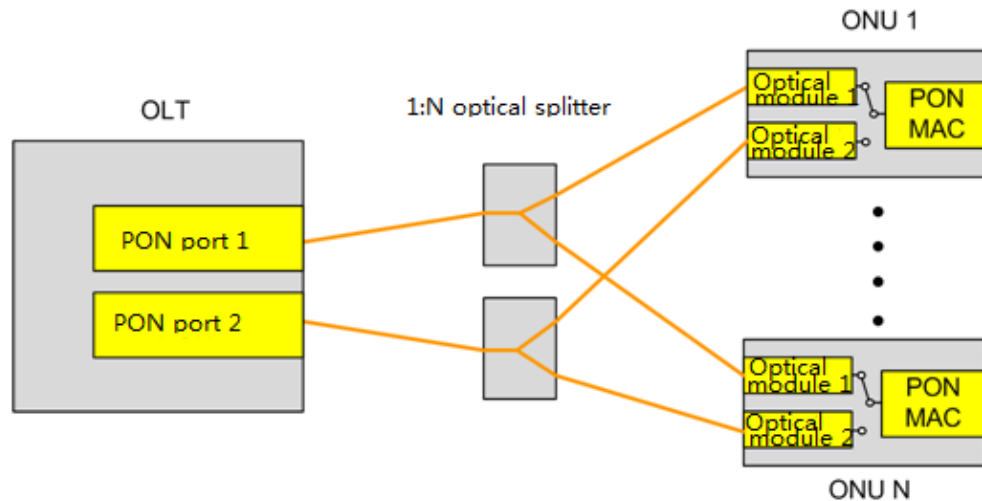
PON full protection (Type C) refers to OLT dual PON ports, ONU dual optical modules, dual backbone fibers, dual optical splitters and dual distribution fibers.

PON full protection (Type C) is suitable for the scenarios of the same PON MAC address (two optical modules share one MAC address) on the same PON port, different PON MAC addresses (each optical module has one MAC address) on the same PON port, and PON ports on the same OLT. The requirements are as below:

- OLT: the active and standby OLT PON ports are in hot backup working state. The ONU and OLT both detect the link status, and decide whether to switch services according to the link status. The OLT should ensure that the service information of the primary PON port can be backed up to the backup PON port synchronously, so that the backup PON port can maintain the ONU's service attributes unchanged during the protection process.
- Optical splitter: use two 1:N optical splitters.
- ONU: the ONU uses one PON MAC address and different optical modules. The spare optical module is in cold backup state. Both the OLT and the ONU detect the link status and decide whether to switch services according to the link status.

Figure 15-2 shows the principle of Type C full protection.

Figure 15-2 Principle of Type C full protection



PON full protection (Type D)

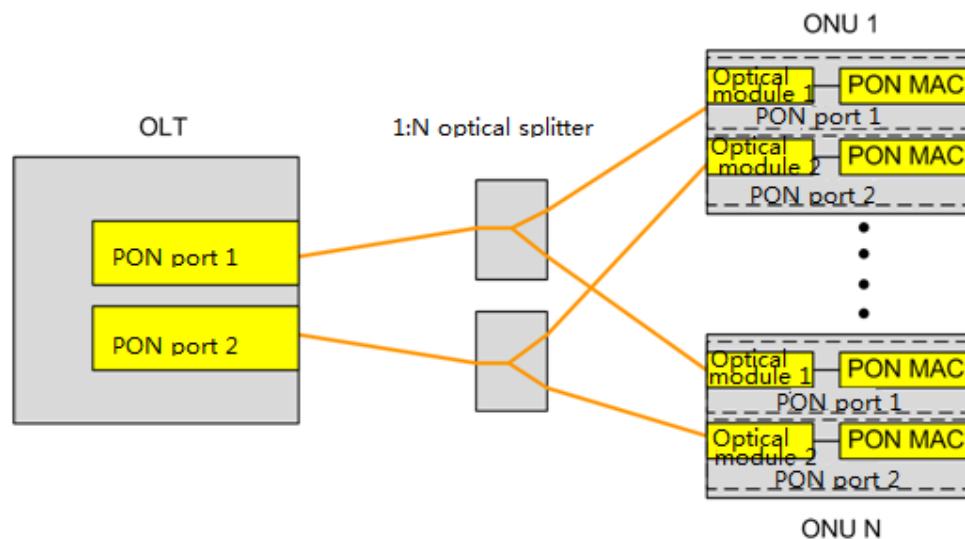
PON full protection (Type D) refers to OLT dual PON ports, ONU dual PON ports, dual backbone fibers, dual optical splitters and dual distribution fibers.

PON full protection (Type D) is suitable for the scenarios of the same PON MAC address (two optical modules share one MAC address) on the same PON port, different PON MAC addresses (each optical module has one MAC address) on the same PON port, and PON ports on the same OLT. The requirements are as below:

- OLT: the active and standby OLT PON ports are in hot backup working state. The ONU and OLT detect the link status and port status bidirectionally and complete service switching respectively. The OLT should ensure that the service information of the primary PON port can be backed up to the backup PON port synchronously, so that the backup PON port can maintain the ONU's service attributes unchanged during the protection process.
- Optical splitter: use two 1:N optical splitters.
- ONU: each optical module of the ONU corresponds to a different PON MAC. The ONU should be able to ensure that the service information of the primary PON port can be backed up to the backup PON port simultaneously, so that the backup PON port can maintain the ONU's service attributes unchanged during the protection process.

Figure 15-3 shows principle of PON full protection (Type D).

Figure 15-3 Principle of PON full protection (Type D)



Cross-OLT PON port dual-homed protection (Type B)

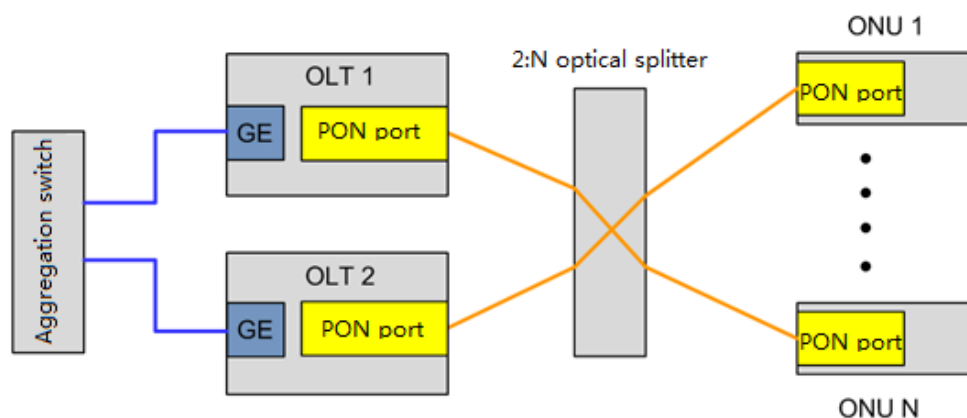
Cross-OLT PON port dual-homed protection (Type B) is an extension based on the standard Type B protection, providing redundancy protection for the backbone fiber, OLT, PON port and uplink port.

Cross-OLT PON port dual-homed protection (Type B) is suitable for protection between PON ports on different OLTs. The requirements are as below:

- OLT: the standby OLT optical module is in cold backup state. The OLT will detect the link status and PON port status and complete switching.
- Optical splitter: use a 2:N optical splitter.
- ONU: no special requirements.

Figure 15-4 shows principle of cross-OLT PON port dual-homed protection (Type B).

Figure 15-4 Principle of cross-OLT PON port dual-homed protection (Type B)



15.1.3 Interface backup

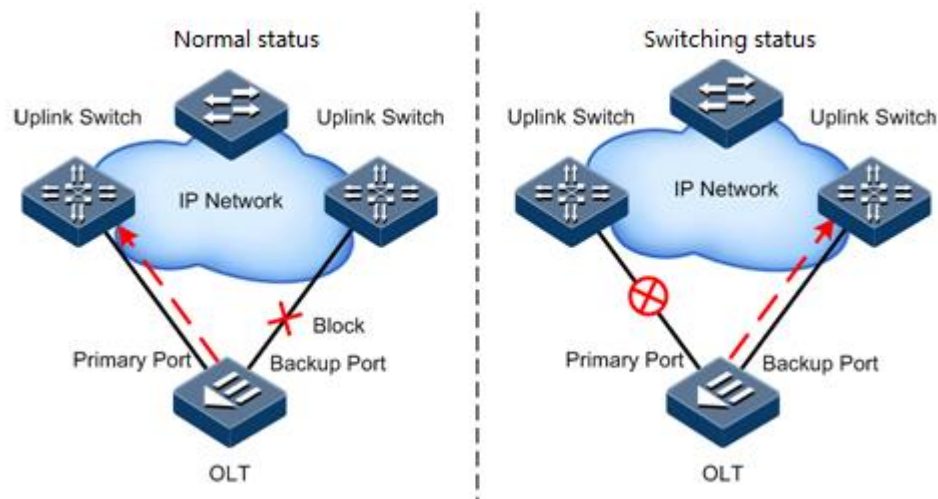
Interface backup is another solution for STP. You can manually configure interface backup when STP is disabled to achieve basic link redundancy.

Interface backup relies on an interface backup group. An interface backup group consists of a pair of interfaces, including a primary interface and a backup interface. Its function is realized as below:

- When the device is in the normal forwarding state, all services will be forwarded from the primary interface.
- When the link of the primary interface fails, the device automatically switches services to the backup interface for forwarding.

Figure 15-5 shows the principle of interface backup.

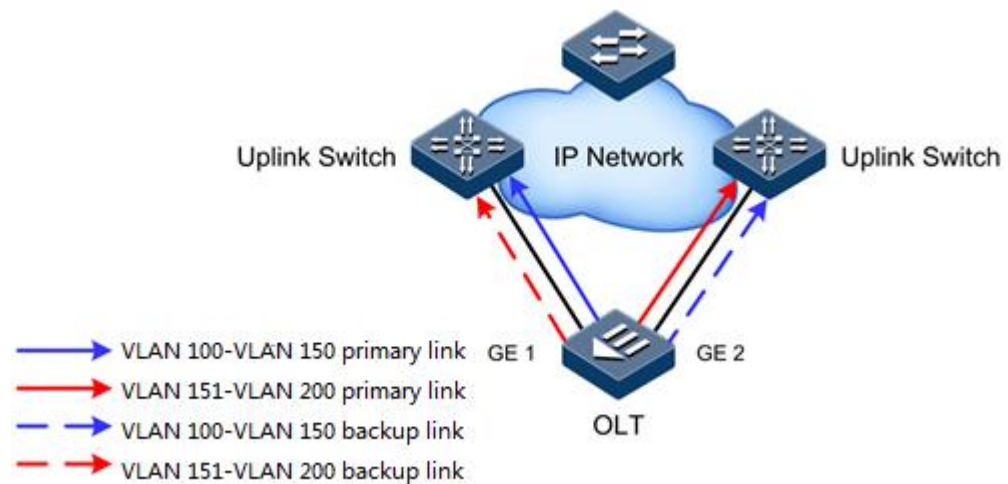
Figure 15-5 Principle of interface backup



VLAN-based interface backup

Interface backup can be applied to a VLAN, and two interfaces can simultaneously forward services in different VLANs. As shown in Figure 15-6, VLAN-based interface backup is implemented by creating a VLAN and adding interfaces to the VLAN.

Figure 15-6 VLAN-based interface backup



In different VLANs, the forwarding status of interfaces is as below:

Under normal circumstances, configure the OLT to VLAN 100–VLAN 150. GE1 is the primary interface and GE2 is the backup interface. In VLAN 151–VLAN 200, GE2 is the primary interface and GE1 is the backup interface. Then GE1 forwards traffic in VLAN 1–VLAN 100, and GE2 forwards traffic in VLAN 101–VLAN 200.

- When a link fault occurs on GE 1, GE 2 is responsible for forwarding traffic to VLAN 100–VLAN 150.
- After GE 1 is restored to normal state for a period of time (recovery delay), GE 1 forwards traffic in VLAN 100–VLAN 150, and GE 2 forwards traffic in VLAN 151–VLAN 200.

With this approach, VLAN-based interface can be used for load balancing. At the same time, this application does not depend on the configuration of the uplink device, which is convenient for the user to operate.

15.2 Configuring link aggregation

Scenario

When you need to provide higher bandwidth and more reliable services for a link between two devices, you can configure link aggregation.

With link aggregation, multiple physical Ethernet interfaces are added to a LAG and are aggregated to a logical link. Link aggregation helps sharing uplink and downlink traffic among members in the LAG. Therefore, it helps get higher bandwidth and helps members in one LAG back up data for each other, thus improving the reliability of the connection.

Prerequisite

Configure physical parameters of the interface and make it Up at the physical layer.

15.2.2 Default configurations

Default configurations of link aggregation on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Link aggregation	Enable
LACP link aggregation	Enable
LAG	N/A
Load balancing mode	sxordmac
LACP system priority	32768

15.2.3 Configuring manual link aggregation

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface port-channel port-channel-number example: Raisecom(config)#interface port-channel 2	Enter LAG configuration mode.
3	Raisecom(config-port-channel-*)#port- channel mode manual	Configure manual link aggregation.
4	Raisecom(config-port-channel-*)#port- channel loading-sharing mode { dip sip dmac smac sxordip sxordmac } example: Raisecom(config-port-channel-2)#port- channel loading-sharing mode sip	Configure the load balancing mode of the LAG. • dip: choose the forwarding interface based on destination IP address. • dmac: choose the forwarding interface based on destination MAC address. • sip: choose the forwarding interface based on source IP address. • smac: choose the forwarding interface based on source MAC address. • sxordip: choose the forwarding interface based on the logical XOR results of the source and destination IP addresses. • sxordmac: choose the forwarding interface based on the logical XOR results of the source and destination MAC addresses.

Step	Command	Description
5	<pre>Raisecom(config-port-channel-*)#interface { gigabitethernet ten-gigabitethernet } slot-id/port-list example: Raisecom(config-port-channel-2)#interface gigabitethernet 2/1</pre>	Add interfaces to the LAG in batch. You can use the no interface gigabitethernet slot-id/port-list command to delete the interface from the LAG. • gigabitethernet: 1000 Mbit/s Ethernet interface • ten-gigabitethernet: 10 Gbit/s Ethernet interface • slot-id/port-list: distributed interface ID. The slot-id refers to the slot ID, which is an integer; the port-list refers to the interface ID, which is an integer. It supports specific values, such as "3/1,2,3"; it also supports a range, such as "3/1-3".
	<pre>Raisecom(config-port-channel-*)#exit Raisecom(config)#interface { gigabitethernet ten-gigabitethernet } slot-id/port-id Raisecom(config-if-*-*:*)#port-channel group-id example: Raisecom(config-if-gigabitethernet-3/1)#port-channel 1</pre>	Add an interface to the LAG. You can use the no port-channel group-id command to delete the interface from the LAG. • group-id: link aggregation group ID, an integer, ranging from 1 to 32



Note

In the same LAG, member interfaces that share loads must be identically configured to avoid improper forwarding of packets. These configurations include QinQ, VLAN, interface properties, and MAC address learning.

- QinQ: QinQ enabling/disabling status on the interface, added outer VLAN tag, and policies for adding outer VLAN Tags for different inner VLAN IDs.
- VLAN: the allowed VLAN, default VLAN ID, link type (Trunk, Hybrid or Access) of the interface, subnet VLAN configurations, protocol VLAN configurations, and whether VLAN packets carrying Tag.
- Interface properties: whether added to the isolation group or not, interface rate, duplex mode, and link Up/Down status.
- MAC address learning: whether enabled with the MAC address learning, whether configured with the MAC address limit on the interface, and whether continuing the forwarding mechanism when the MAC address table is full.

15.2.4 Configuring static LACP link aggregation

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#lACP system- priority system-priority</pre> example: <pre>Raisecom(config)#lACP system- priority 1</pre>	(Optional) configure the LACP system priority.  Note The higher priority end is the active end. LACP chooses active and backup interfaces according to the active end configurations. The smaller the number is, the higher the priority is. By default, the LACP system priority is 32768. The device with a smaller MAC address will be chosen as the active end if the LACP system priority is identical. You can use the no lACP system-priority command to restore default configuration. • system-priority: configure system LACP priority which is an integer ranging from 0 to 65535. The smaller the value is, the higher the priority is.
3	<pre>Raisecom(config)#interface port- channel port-channel-number</pre> example: <pre>Raisecom(config)#interface port- channel 2</pre>	Enter LAG configuration mode.
4	<pre>Raisecom(config-port-channel- *)#port-channel mode lACP-static</pre>	Configure the static LACP LAG.
5	<pre>Raisecom(config-port-channel- *)#port-channel loading-sharing mode { dip sip dmac smac sxordip sxordmac }</pre> example: <pre>Raisecom(config-port-channel- 1)#port-channel loading-sharing mode sip</pre>	Configure the load balancing mode of the LAG. • dip: choose the forwarding interface based on destination IP address. • dmac: choose the forwarding interface based on destination MAC address. • sip: choose the forwarding interface based on source IP address. • smac: choose the forwarding interface based on source MAC address. • sxordip: choose the forwarding interface based on the logical XOR results of the source and destination IP addresses. • sxordmac: choose the forwarding interface based on the logical XOR results of the source and destination MAC addresses.
6	<pre>Raisecom(config-port-channel- *)#interface { gigabitEthernet ten-gigabitEthernet } slot- id/port-list</pre> example: <pre>Raisecom(config-port-channel- 2)#interface gigabitEthernet 2/1</pre>	Add interfaces to the LAG in batch. You can use the no interface gigabitEthernet slot-id/port-list command to delete the interface from the LAG. • gigabitEthernet: 1000 Mbit/s Ethernet interface • ten-gigabitEthernet: 10 Gbit/s Ethernet interface • slot-id/port-list: distributed interface ID. The slot-id refers to the slot ID, which is an integer; the port-list refers to the interface ID, which is an integer. It supports specific values, such as "3/1,2,3"; it also supports a range, such as "3/1-3".

Step	Command	Description
	<pre> Raisecom(config-port-channel- *)#exit Raisecom(config)#interface { gigabitethernet ten- gigabitethernet } slot-id/port-id Raisecom(config-if-*-*:*)#port- channel group-id example: Raisecom(config-if- gigabitethernet-3/1)#port-channel 1 </pre>	Add an interface to the LAG. You can use the no port-channel group-id command to delete the interface from the LAG. group-id: link aggregation group ID, an integer, ranging from 1 to 32



Note

- Interfaces in a static LACP LAG can be in active or standby status. Both active and standby interfaces can receive/send LACP packets, but standby interfaces cannot forward client packets.
- The system selects a default interface based on the following conditions in order: whether its neighbour is discovered, maximum interface rate, highest interface LACP priority (the smaller the value is, the higher the priority is), and smallest interface ID. The default interface is in active status. Interfaces, which have the same rate, peer device, and operation key with the default interface, are also in active status. Other interfaces are in standby status.

15.2.5 Configuring dynamic LACP

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre> Raisecom(config)#interface { gigabitethernet ten- gigabitethernet } slot-id/port-id example: Raisecom(config)#interface gigabitethernet 3/1 </pre>	Enter physical interface configuration mode. - gigabitethernet: 1000 Mbit/s Ethernet interface configuration mode - ten-gigabitethernet: 10 Gbit/s Ethernet interface configuration mode - slot-id: slot ID - port-id: interface ID
3	Raisecom(config-if-*-*:*)#lACP dynamic	Enable dynamic LACP on the physical interface.
4	<pre> Raisecom(config-if-*-*:*)#lACP timeout { fast slow } example: Raisecom(config-if-gigabitethernet- 1:1)#lACP timeout slow </pre>	Configure the LACP timeout mode on the interface. - fast: fast mode - slow: slow mode
5	<pre> Raisecom(config-if-*-*:*)#lACP mode { active passive } example: Raisecom(config-if-gigabitethernet- 1:1)#lACP mode active </pre>	Configure the LACP mode on the interface. - active: LACP active aggregation mode - passive: LACP passive aggregation mode

Step	Command	Description
6	Raisecom(config-if-**-*:*)#lACP port-priority value example: Raisecom(config-if-gigabitethernet-1:1)#lacpport-priority 1000	Configure the LACP priority on the interface. port-priority: interface LACP priority, an integer, ranging from 0 to 65535. The smaller the value is, the higher the priority is, and the more likely the interface becomes the active interface.

15.2.6 Checking configurations

No.	Command	Description
1	Raisecom#show interface port-channel [group-id]	Show configurations of the link aggregation group.
2	Raisecom#show lACP system	Show system LACP configurations.
3	Raisecom#show lACP neighbor	Show information about neighbor LACP, including tags, interface priority, device ID, Age, operation key, interface ID, and interface state machine.
4	Raisecom#show lACP internal	Show configurations of local LACP interface.
5	Raisecom#show lACP statistics	Show interface LACP statistics, including the total number of received/sent LACP packets, Marker packets, and Marker Response packets, and the number of error packets.

15.3 Configuring EPON OLT backbone fiber protection (TypeB)

15.3.1 Preparing for configurations

Scenario

OLT backbone fiber protection (Type B) is suitable for the following scenarios:

- Protection between PON ports on the same PON card of the OLT.
- OLT cross-PON card PON port protection.

Prerequisite

When configuring Type B protection, ensure that there is no created ONU on the backup PON port.

15.3.2 Default configurations

N/A

15.3.3 Configuring OLT backbone fiber protection (Type B)



Caution

- You must enable isolation among member PON ports in the OLT backbone fiber protection (Type B) to ensure normal service switching.
- Member PON ports in the OLT backbone fiber protection (Type B) group cannot be closed.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#protect-group group-id primary slot-id/olt-id secondary slot-id/olt-id type backbone-pon-protect	Create an OLT backbone fiber protection group. You can use the no protect-group group-id command to delete the protection group.
3	Raisecom(config)#protect-group group-id { enable disable }	Enable/Disable the protection group.
4	Raisecom(config)#sync-data protect-group { group-id all }	Synchronize the configuration data of the primary PON port and the primary ONU link to the secondary PON port and the secondary ONU link. Note When the configuration of the main PON port changes, you need to execute a synchronization command to synchronize the configuration of the PON primary port to the secondary PON port.
5	Raisecom(config)#protect-group group-id auto-recover-time time	(Optional) configure the time for the service to be automatically switched to the primary link. You can use the no protect-group group-id auto-recover-time command to restore to the default condition.
6	Raisecom(config)#protect-group group-id force-switch	(Optional) configure forced switch.
7	Raisecom(config)#protect-group group-id lock { primary secondary null }	(Optional) lock the working link of the protection group.

15.3.4 Configuring ONU backbone fiber protection (Type B)

To ensure that the ONU will not cause service interruption due to de-registration when the backbone fiber switch of the OLT occurs, you need to configure Holdover on the ONU to prevent the ONU deregistration.

Configure the equipment that needs OLT backbone fiber protection (Type B).

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id	Enter EPON ONU remote management configuration mode.
3	Raisecom(config-epon-onu-*/*:*)#protect-group holdover time time	Configure the ONU Holdover time. You can use the no protect-group holdover time command to restore to the default condition.  Note We recommend configuring the Holdover time larger than 200ms.
4	Raisecom(config-epon-onu-*/*:*)#protect-group holdover { activated time time deactivated }	Enable/Disable Holdover.

15.3.5 Checking configurations

Step	Command	Description
1	Raisecom#show protect-group group-id	Show configurations and running status of the protection group.
2	Raisecom#show epon-onu slot-id/olt-id/onu-list holdover	Show time configurations of the ONU Holdover.

15.4 Configuring cross-OLT EPON port dual-homed protection (Type B)

15.4.1 Preparing for configurations

Scenario

Cross-OLT PON port dual-homed protection (Type B) is suitable for protection between PON ports on different OLTs.

Prerequisite

Prerequisites for configuring cross-OLT PON port dual-homed protection (Type B):

- The active and standby member ports should be open.
- Normal Layer 3 communication can be carried out between two OLTs.

- There should be no created ONU on the backup link.

15.4.2 Default configurations

N/A

15.4.3 Configuring cross-OLT PON port dual-homed protection (Type B)



Caution

Ensure that the configuration parameters (enable/disable, recovery time, and lock status) and alarm status of the protection groups on the two OLTs are consistent. Otherwise, do not perform protection switching on the two OLTs.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#protect-group group-id primary slot-id/olt-id secondary slot-id/olt-id type backbone-pon-protect-extend local-port-role { primary secondary } peer-device-description string peer-device-ip-address ip-address	Configure the cross-OLT PON port protection group. You can use the no protect-group group-id command to delete the protection group.
3	Raisecom(config)#protect-group group-id { enable disable }	Enable/Disable the protection group.
4	Raisecom(config)#protect-group group-id auto-recover-time time	(Optional) configure the time for the service to be automatically switched back to the primary link. You can use the no protect-group group-id auto-recover-time command to restore to the default condition.
5	Raisecom(config)#protect-group group-id force-switch	(Optional) configure the forced switch.
6	Raisecom(config)#protect-group group-id lock { primary secondary null }	(Optional) lock the working link of the protection group.



Note

The configuration of the active and standby OLTs cannot be automatically synchronized. You need to manually synchronize the configuration data of each member port and all ONUs on the two OLTs.

15.4.4 Configuring ONU PON protection

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)# epon-onu slot-id/olt-id/onu-id	Enter EPON ONU remote management configuration mode.
3	Raisecom(config)# protect-group auto-recover-time time	(Optional) configure the time of the service to be automatically switched back to the main link. You can use the no protect-group auto-recover-time command to restore to the default condition.
4	Raisecom(config)# protect-group force-switch	(Optional) forcibly switch the working link of the protection group.
5	Raisecom(config)# protect-group lock { primary secondary }	(Optional) lock the working link of the protection group.
6	Raisecom(config)# protect-group primary port-number	(Optional) configure the primary link interface ID of the ONU PON protection group. You can use the no protect-group primary command to restore to the default condition.

15.4.5 Checking configurations

No.	Command	Description
1	Raisecom(config)# show protect-group [<i>group-id</i>]	Show configurations and running status of the protection group.
2	Raisecom(config)# show epon-onu slot-id/olt-id/onu-list holdover	Show ONU Holdover configurations.
3	Raisecom(config)# show epon-onu { primary secondary swithed } protect-group	Show configurations and status of ONU protection groups under different working links.
4	Raisecom(config)# show epon-onu slot-id/olt-id/onu-list protect-group	Show configurations and status of the ONU protection group.

15.5 Configuring port backup

15.5.1 Preparing for configurations

You can manually configure port backup to implement basic link redundancy.

15.5.2 Default configurations

Default configurations of interface backup on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Interface backup group	N/A
Interface recovery	Enable
Interface recovery delay	15s
Interface backup group VLAN	1 to 4094

15.5.3 Creating interface backup group

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#create port-backup group <i>group-id</i>	Create an interface backup group. You can use the no create backup-port group <i>group-id</i> command to delete the configuration.
3	Raisecom(config)#port-backup group <i>group-id</i> { enable disable }	Enable/disable the interface backup group.  Note The following two reasons may lead to failure in enabling interface backup group: • The interface backup group does not exist. • The primary/backup interface is not configured in the interface backup group.

15.5.4 Configuring interface backup group

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#port-backup group <i>group-id</i> vlanlist <i>vlan-list</i>	Configure interface backup group VLAN. You can use the no port-backup group <i>group-id</i> vlanlist command to restore default configurations.
3	Raisecom(config)#interface { gigabitethernet ten-gigabitethernet } <i>slot-id/port-id</i>	Enter physical interface configuration mode.
4	Raisecom(config-if-<i>slot-id</i>:<i>port-id</i>)#port-backup group <i>group-id</i> { primary-port backup-port }	Configure the primary interface and backup interface. You can use the no port-backup group <i>group-id</i> { primary-port backup-port } command to delete the configuration.
5	Raisecom(config-if-<i>slot-id</i>:<i>port-id</i>)#port-backup group <i>group-id</i> restore-mode { enable disable }	Enable/Disable interface recovery.

Step	Command	Description
6	Raisecom(config-if-*-*:*)#port-backup group group-id restore-delay time	Configure interface recovery delay. You can use the no port-backup group group-id restore-delay command to restore default configurations.

15.5.5 Configuring force switch

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#port-backup group group-id force-switch	Configure force switch on the interface backup group.  Note - When force switch is configured on the interface backup group, the system configures the primary interface to blocked status and the backup interface to forwarding status without considering the current status of the primary/backup interface. - When force switch is disabled on the interface backup group, the system configures the primary interface to forwarding status and the backup interface to blocked status without considering the current status of the primary/backup interface.

15.5.6 Checking configurations

No.	Command	Description
1	Raisecom#show port-backup group [group-id]	Show interface backup configurations.

15.6 Maintenance

No.	Command	Description
1	Raisecom(config)#clear ethernet ring ring-id statistics	Clear statistics on the protection ring.

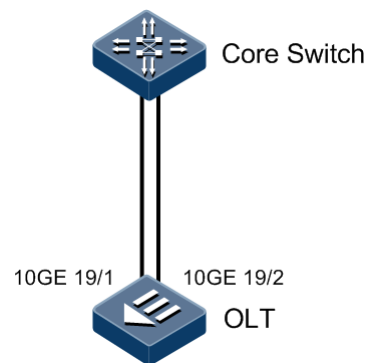
15.7 Configuration examples

15.7.1 Example for configuring manual link aggregation

Networking requirements

As shown in Figure 15-7, to improve link reliability between the OLT and uplink aggregation switch, you can configure manual link aggregation on the OLT. Add 10GE 19/1 and 10GE 19/2 to the LAG to form a single logical interface. The LAG performs load balancing according to the source MAC address.

Figure 15-7 Manual link aggregation networking



Configuration steps

Step 1 Create a manual LAG and the group ID is 1.

```
Raisecom#config  
Raisecom(config)#interface port-channel 1  
Raisecom(config-port-channel-1)#port-channel mode manual
```

Step 2 Configure the load sharing mode for link aggregation.

```
Raisecom(config-port-channel-1)#port-channel loading-sharing mode smac  
Raisecom(config-port-channel-1)#exit
```

Step 3 Add interfaces to the LAG.

```
Raisecom(config)#interface ten-gigabitethernet 19/1  
Raisecom(config-if-ten-gigabitethernet-10:1)#port-channel 1  
Raisecom(config-if-ten-gigabitethernet-10:1)#exit  
Raisecom(config)#interface ten-gigabitethernet 19/2  
Raisecom(config-if-ten-gigabitethernet-10:2)#port-channel 1  
Raisecom(config-if-ten-gigabitethernet-10:2)#exit
```

Checking results

Use the **show port-channel** command to show global configurations of manual link aggregation.

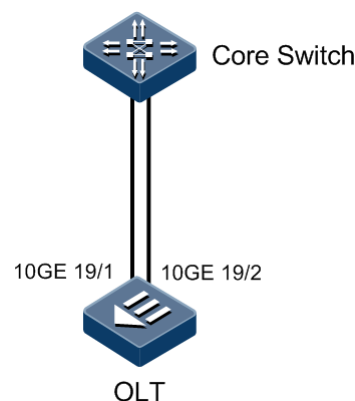
```
Raisecom#show port-channel 1
Port-channel ID : 1
Mode           : Manual
Load-sharing Mode : smac
Member ports    : ten-gigabitethernet 19/1,2
Efficient ports :
```

15.7.2 Example for configuring static LACP link aggregation

Networking requirements

As shown in Figure 15-8, to improve link reliability between the OLT and uplink aggregation switch, you can configure static LACP link aggregation on the OLT. Add 10GE 19/1 and 10GE 19/2 to the LAG. 10GE 19/1 works as the primary link, and 10GE 19/2 works as the backup link.

Figure 15-8 Static LACP link aggregation networking



Configuration steps

Step 1 Create a static LACP LAG.

```
Raisecom#config
Raisecom(config)#interface port-channel 1
Raisecom(config-port-channel-1)#port-channel mode lacp-static
Raisecom(config-port-channel-1)#exit
```

Step 2 Add interfaces to the LAG.

```
Raisecom(config)#interface ten-gigabitethernet 19/1
Raisecom(config-if-ten-gigabitethernet-19:1)#port-channel 1
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
Raisecom(config)#interface ten-gigabitethernet 19/2
Raisecom(config-if-ten-gigabitethernet-19:2)#port-channel 1
Raisecom(config-if-ten-gigabitethernet-19:2)#exit
```

- Step 3 Configure the priority of 10GE interface 19/1 to make the 10GE 19/1 as the primary link and 10GE 19/2 as the backup link.

```
Raisecom(config)#interface ten-gigabitethernet 19/1
Raisecom(config-if-ten-gigaethgigabitethernet-19:1)#lACP port-priority
10000
Raisecom(config-if-ten-gigaethgigabitethernet-19:1)#exit
```

Checking results

Use the **show port-channel** command on the OLT to show static LACP link aggregation global configurations.

```
Raisecom#show interface port-channel
Port-channel ID : 1
Mode           : LACP-static
Load-sharing Mode : smac
Member ports   : ten-gigabitethernet 19/1,2
Efficient ports :
```

Use the **show lACP internal** command on the OLT to show configurations of the local system, such as LACP interface status, flag, interface priority, management key, operation key, and status of interface state machine.

```
Raisecom#show lACP internal
Flags:
  S - Device is requesting Slow LACPDUS
  F - Device is requesting Fast LACPDUS
  A - Device is in Active mode
  P - Device is in Passive mode
```

```
Port State Flags Port-Pri Admin-key Oper-key Port-State
```

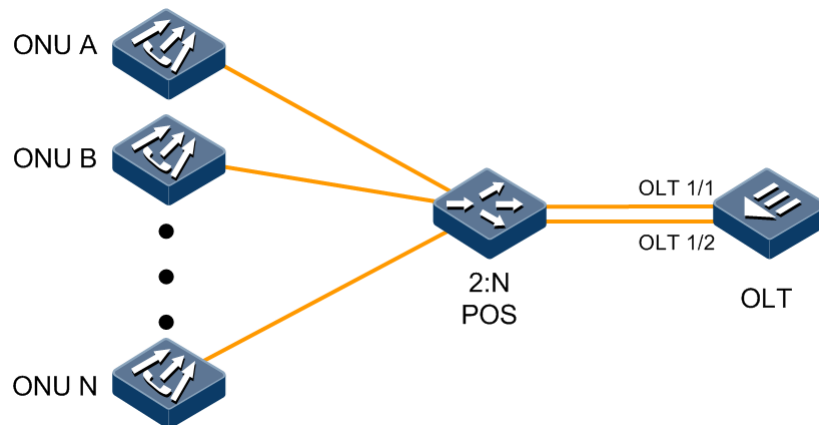
```
-----
1/1 up   FA 10000 0x1 0x1 0x4d
1/2 down FA 32768 0x1 0x1 0x4d
```

15.7.3 Example for configuring OLT backbone fiber protection (TypeB)

Networking requirements

As shown in Figure 15-9, to improve the reliability of the link between the OLT and the ONU, you need to configure OLT backbone fiber protection (Type B) on the OLT. Add OLT 1/1 and OLT 1/2 to the protection group, where OLT 1/1 is the primary link and OLT 1/2 is the backup link. Configure the switchover recovery time to 10 minutes, and the Holdover time of ONU 1/1/1 to 1000 milliseconds.

Figure 15-9 OLT backbone fiber protection (Type B)



Configuration steps

Step 1 Create an OLT backbone fiber protection group.

```
Raisecom#config
Raisecom(config)#protect-group 1 primary 1/1 secondary 1/2 type backbone-pon-protect
```

Step 2 Synchronize the configuration data of the primary PON port and primary ONU link to the secondary PON port and secondary ONU link.

```
Raisecom(config)#sync-data protect-group 1
```

Step 3 Configure the recovery time.

```
Raisecom(config)#protect-group 1 auto-recover-time 10
```

Step 4 Enable the protection group.


```
Raisecom(config)#protect-group 1 enable
```

Step 5 Configure the ONU Holdover time.

```
Raisecom(config)#epon-onu 1/1/1
Raisecom(config-epon-onu-1/1:1)#protect-group holdover time 1000
Raisecom(config-epon-onu-1/1:1)#protect-group holdover activated time
1000
Raisecom(config-epon-onu-1/1:1)#end
```

Checking results

Use the **show protect-group** command to check the configurations and running status of the protection group on the OLT.

```
Raisecom(config)#show protect-group 1

Group type           : Backbone pon protection
Primary line         : 1/1
Primary line state   : Normal
Secondary line        : 1/2
Secondary line state  : LOS
Group admin status    : Enabled
Group lock status     : Unlocked
Group working status  : Normal
Auto-recovery time    : 10 min
Successful switching count: 0
Last switching result : Succeeded
```

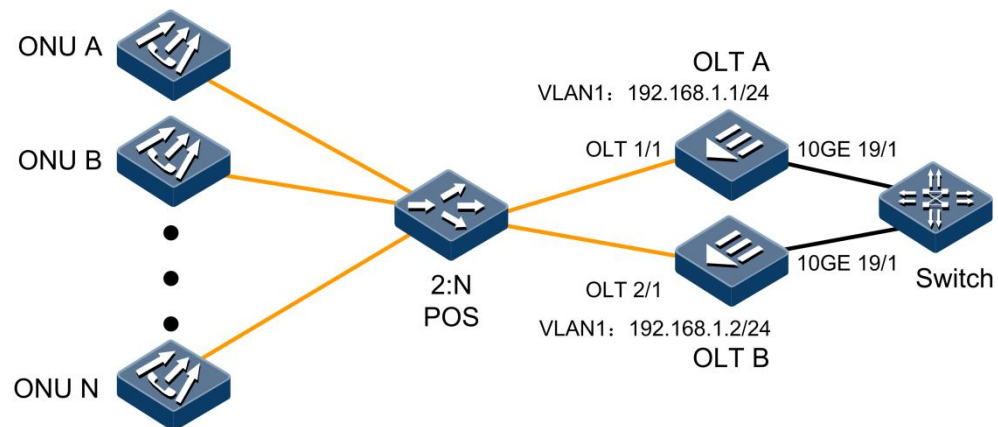
15.7.4 Configuring cross-OLT PON port dual-homed protection (Type B)

Networking requirements

As shown in Figure 15-10, to improve the reliability of the overall link, you need to configure cross-OLT PON port dual-homed protection by using two OLTs.

- OLT A is the primary device. The IP address of the VLAN interface is 192.168.1.1. The OLT 1/1 port is connected to the POS downstream. The 10GE 19/1 port is connected to the switch upstream.
- OLT B is the standby device. The IP address of the VLAN interface is 192.168.1.2. The OLT 2/1 port is connected to the POS downstream. The the 10GE 19/1 port is connected to the switch upstream.

Figure 15-10 Cross-OLT PON port dual-homed protection (Type B)



Configuration steps

- Configure OLT A.

Step 1 Configure the IP address of the VLAN interface.

```
Raisecom#config
Raisecom(config)#interface vlanif 1
Raisecom(config-vlanif-1)#ip address 192.168.1.1 255.255.255.0
Raisecom(config-vlanif-1)#end
```

Step 2 Configure the device description.

```
Raisecom#config
Raisecom(config)#device description ISCOM6800a
```

Step 3 Create the cross-OLT PON port dual-homed protection group.

```
Raisecom(config)#protect-group 1 primary 1/1 secondary 2/1 type backbone-
pon-protect-extend local-port-role primary peer-device-description
ISCOM6800b peer-divice-ip-address 192.168.1.2
```

Step 4 Enable the protection group.

```
Raisecom(config)#protect-group 1 enable
Raisecom(config)#end
```

- Configure OLT B.

Step 5 Configure the IP address of the device VLAN interface.

```
Raisecom#config
Raisecom(config)#interface vlanif 1
Raisecom(config-vlanif-1)#ip address 192.168.1.2 255.255.255.0
Raisecom(config-vlanif-1)#end
```

Step 6 Configure the device description.

```
Raisecom#config
Raisecom(config)#device description ISCOM6800b
```

Step 7 Create the cross-OLT PON port dual-homed protection group.

```
Raisecom#config
Raisecom(config)#protect-group 1 primary 1/1 secondary 2/1 type backbone-
pon-protect-extend local-port-role secondary peer-device-description
ISCOM6800a peer-dvices-ip-address 192.168.1.1
```

Step 8 Enable the protection group.

```
Raisecom(config)#protect-group 1 enable
Raisecom(config)#end
```

Checking results

Use the **show protect-group** command to check the configurations and running status of the OLT protection group on OLT A.

```
Raisecom#show protect-group 1
Group ID: 1
  Group type           : Backbone PON protection between OLTs
  Primary line         : 1/1
  Primary line state   : Normal
  Secondary line       : 2/1
  Secondary line state : LOS
  Group admin status   : Enabled
  Group lock status    : Unlocked
  Group working status : Normal
  Auto-recovery time   : 0 min
  Successful switching count: 1
  Last switching result : Succeeded
  Local port role      : primary-port
  Peer device description : ISCOM6800b
  Peer device IP address : 192.168.1.2
  Last alarm status    : Normal
```

Use the **show protect-group** command to check the configurations and running status of the OLT protection group on OLT B.

```
Raisecom#show protect-group 1
Group ID: 1
  Group type           : Backbone PON protection between OLTs
  Primary line         : 1/1
  Primary line state    : Normal
  Secondary line        : 2/1
  Secondary line state  : LOS
  Group admin status    : Enabled
  Group lock status     : Unlocked
  Group working status  : Normal
  Auto-recovery time    : 0 min
  Successful switching count: 1
  Last switching result : Succeeded
  Local port role       : secondary-port
  Peer device description : ISCOM6800b
  Peer device IP address : 192.168.1.1
  Last alarm status     : Normal
```

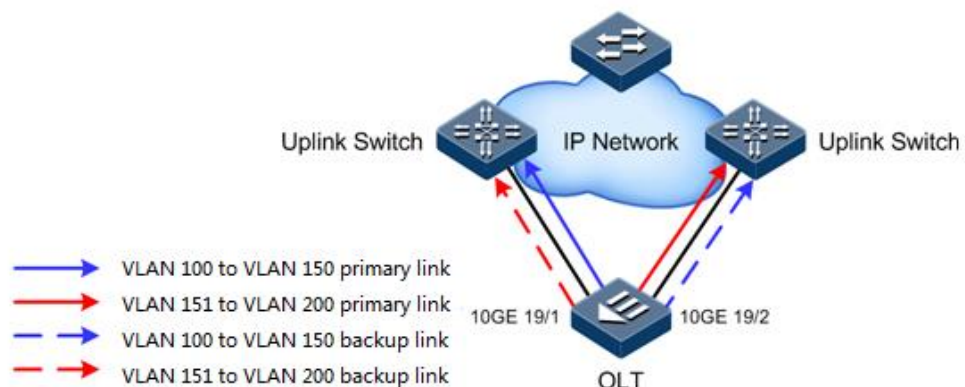
15.7.5 Example for configuring interface backup

Networking requirements

- 10GE interface 19/1 is the primary interface of VLAN 100 to VLAN 150, and 10GE interface 19/2 is the backup interface of VLAN 100–VLAN 150.
- 10GE interface 19/2 is the primary interface of VLAN 151–VLAN 200, and 10GE interface 19/1 is the backup interface of VLAN 151–VLAN 200.

As shown in Figure 15-11, to ensure the link security of the uplink interface on the OLT, configure interface backup on it to realize link protection and load balancing. The requirements are as below:

Figure 15-11 Interface backup networking



Configuration steps

Step 1 Create an interface backup group and configure the primary and backup interfaces.

```
Raisecom#config
Raisecom(config)#create port-backup group 1
Raisecom(config)#interface ten-gigabitethernet 19/1
Raisecom(config-if-ten-gigabitethernet-19:1)#port-backup group 1 primary-
port
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
Raisecom(config)#interface ten-gigabitethernet 19/2
Raisecom(config-if-ten-gigabitethernet-19:2)#port-backup group 1 backup-
port
Raisecom(config-if-ten-gigabitethernet-19:2)#exit
Raisecom(config)#create port-backup group 2
Raisecom(config)#interface gigabitethernet 19/1
Raisecom(config-if-ten-gigabitethernet-19:1)#port-backup group 2 backup-
port
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
Raisecom(config)#interface ten-gigabitethernet 19/2
Raisecom(config-if-ten-gigabitethernet-19:2)#port-backup group 2 primary-
port
Raisecom(config-if-ten-gigabitethernet-19:2)#exit
```

Step 2 Configure the VLAN list of the interface backup group.

```
Raisecom(config)#port-backup group 1 vlanlist 100-150
Raisecom(config)#port-backup group 2 vlanlist 151-200
```

Step 3 Enable the interface backup group.

```
Raisecom(config)#port-backup group 1 enable
Raisecom(config)#port-backup group 2 enable
```

Checking results

Use the **show port interface backup** command to show interface backup configurations.

```
Group Id: 1
Primary Port(State): ten-gigabitethernet19/1(Forwarding)
Backup Port(State) : ten-gigabitethernet19/2(Discarding)
Vlanlist           : 100-150
Restore delay      : 15
Restore mode       : enable
switch state       : no force
switch count       : 0
-----
```

```
Group Id: 2
Primary Port(State): ten-gigabitethernet19/2(Forwarding)
Backup Port(State) : ten-gigabitethernet19/1(Discarding)
Vlanlist           : 151-200
Restore delay      : 15
Restore mode       : enable
switch state       : no force
switch count       : 0
-----
```

16 Configuring system management

This chapter describes the basic principle and configuration process of the system management and maintenance feature of the ISCOM6800 and ISCOM6860, and provides related configuration examples, including the following sections:

- Introduction
- Configuring SNMP
- Configuring optical module DDM
- PPPoE Agent
- Watchdog
- Configuring system log
- Configuring port mirroring
- Configuring link detection
- Configuring PPPoE Agent
- Configuring system monitoring
- Illegal ONU alarms
- Configuring link monitoring
- Configuring alarm and event management
- Maintenance
- Configuration examples

16.1 Introduction

16.1.1 SNMP

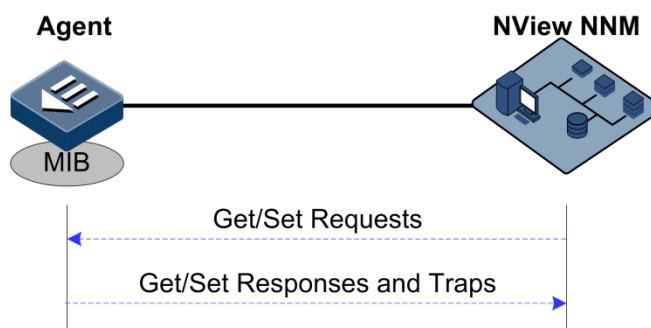
Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to solve problems in managing network devices connected to the Internet. Through SNMP, a network management system can manage all network devices that support SNMP, including monitoring network status, modifying configurations of a network device,

and receiving network alarms. SNMP is the most widely used network management protocol in TCP/IP networks.

Working mechanism

SNMP is divided into two parts: Agent and NMS. The Agent and NMS communicate by SNMP packets sent through UDP. The working mechanism of SNMP is shown in Figure 16-1.

Figure 16-1 Working mechanism of SNMP



Raisecom Nview NNM system can provide friendly Human Machine Interface (HMI) to facilitate network management. The below functions can be implemented through it:

- Send request packets to the managed device.
- Receive reply packets and Trap packets from the managed device, and show results.

Agent is a program stayed in the managed device, realizing the below functions:

- Receive/Reply request packets from Nview NNM system.
- Read/Write packets and generate response packets according to the packet types, and then return the results to Nview NNM system.
- Define triggering conditions according to protocol module. Enter/Exit system or restart device when conditions are satisfied. The response module sends Trap packets to Nview NNM system through agent to report current status of the device.



Note

Agent can be configured with several versions. Agent use different versions to communicate with different Nview NNM systems. However, SNMP version of the Nview NNM system must be consistent with the one on Agent when they are communicating. Otherwise, they cannot communicate properly.

Protocol versions

At present, SNMP has three versions: v1, v2c, and v3, described as below.

- SNMPv1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a password. The network management system can visit the agent only by specifying its community name correctly. If the community name carried in a SNMP message is not accepted by the device, the message will be dropped.
- Compatible with SNMPv1, SNMPv2c also uses community name authentication mechanism. SNMPv2c supports more operation types, data types, and error codes, and thus better identifying errors.

- SNMPv3 uses User-based Security Model (USM) authentication mechanism. You can configure whether USM authentication is enabled and whether encryption is enabled to provide higher security. USM authentication mechanism allows authenticated senders and prevents unauthenticated senders. Encryption is to encrypt messages transmitted between the network management system and agents, thus preventing interception.

MIB

Management Information Base (MIB) is the collection of all objects managed by NMS. It defines attributes for the managed objects:

- Name
- Access authority
- Data type

The device-related statistic contents can be reached by accessing data items. Each proxy has its own MIB. MIB can be taken as an interface between NMS and Agent, through which NMS can read/write every managed object in Agent to manage and monitor the device.

MIB stores information in a tree structure. Its root is on the top without a name. Nodes of the tree are the managed objects, which take a unique path starting from root (OID) for identification. SNMP packets can access network devices by checking the nodes in MIB tree directory.

The ISCOM6800 and ISCOM6860 devices support the standard MIB library and Raisecom customized MIB library.

16.1.2 Optical module DDM

Small Form-factor Pluggables (SFP) is an optical module in optical module transceivers. The SFP Digital Diagnostic Monitoring (DDM) provides a method for monitoring performance. By analyzing monitored data provided by the SFP module, the administrator can predict the lifetime of the SFP module, isolate system faults, and verify the compatibility of the SFP module.

The SFP module provides 5 performance parameters:

- Temperature of the transceiver
- Internal Power Feeding Voltage (PFV)
- Tx bias current
- Tx optical power
- Rx optical power

16.1.3 System log

The system log refers to that the device records the system information and debugging information in a log and sends the log to the specified destination. When the device fails to work, you can check and locate the fault easily.

The system information and debugging output will be sent to the system log to be processed. According to the configuration, the system will send the log to various destinations. The destinations that receive the system log are divided into:

- Console: send the log message to the local console through Console interface.
- Host: send the log message to the host.

- Monitor: send the log message to the monitor, such as Telnet terminal.
- Buffer: send the log message to the buffer of the device.

The system log is usually in the following format:

timestamp module-level- Message content

The following is an example of system log:

```
FEB-22-2005 14:27:33 CONFIG-7-CONFIG:USER "raisecom" Run "logging on"
FEB-22-2005 06:46:20 CONFIG-6-LINK_D:port 2 Link Down
FEB-22-2005 06:45:56 CONFIG-6-LINK_U:port 2 Link UP
```

The format of system log output to the host is as below:

timestamp module-level- Message content

The following figure is an example of system log sent to the host.

```
07-01-200811:31:28Local0.Debug20.0.0.6JAN 01 10:22:15 ISCOM6800 and
ISCOM6860: CONFIG-7-CONFIG:USER " raisecom " Run " logging on "
07-01-200811:27:41Local0.Debug20.0.0.6JAN 01 10:18:30 ISCOM6800 and
ISCOM6860: CONFIG-7-CONFIG:USER " raisecom " Run " ip address 20.0.0.6
255.0.0.0 1 "
```

The system log is divided into eight levels by severity, as listed in Table 16-1.

Table 16-1 Log levels

Severity	Level	Description
Emergencies	0	The system cannot be used.
Alerts	1	Immediate processing is required.
Critical	2	Serious status
Errors	3	Errored status
Warnings	4	Warning status
Notifications	5	Normal but important status
Informational	6	Informational event
Debugging	7	Debugging information



Note

The severity of output information can be configured manually. When you send information according to the configured severity, you can just send the information whose severity is less than or equal to that of the configured information. For example, when the information is configured with level 3 (or the severity is errors), the information whose level ranges from 0 to 3, that is, the severity ranging from emergencies to errors, can be sent.

Classification of alarms

There are 3 kinds of alarms according to properties of an alarm:

- Fault alarm: alarms generated because of hardware failure or anomaly of important functions, such as interface Down alarm
- Recovery alarm: alarms generated when device failure or abnormal function returns to normal, such as interface Up alarm;
- Event alarm: prompted alarms or alarms that are generated because the fault alarm and recovery alarm cannot be related, such as alarms generated because of failing to Ping.

Alarms are divided into 5 types according to functions:

- Communication alarm: alarms related to the processing of information transmission, including alarms generated because of communication failure between Network Elements (NEs), NEs and NMS, or NMS and NMS
- Service quality alarm: alarms caused by service quality degradation, including congestion, performance decline, high resource utilization rate, and the bandwidth reducing
- Processing error alarm: alarms caused by software or processing errors, including software errors, memory overflow, version mismatching, and abnormal program aborts
- Environmental alarm: alarms caused by equipment location-related problems, including the temperature, humidity, ventilation. and other abnormal working conditions
- Device alarm: alarms caused by failure of physical resources, including the power supply, fan, processor, clock, input/output interface, and other hardware.

Alarm output

There are 3 alarm output modes:

- Alarm buffer: alarms are recorded in tabular form, including the current alarm table and history alarm table.
 - Current alarm table: records alarms which are not cleared, acknowledged or restored.
 - History alarm table: consists of acknowledged and restored alarms, recording the cleared, auto-restored, or manually acknowledged alarms.
- Log: alarms are generated to system log when recorded in the alarm buffer, and stored in the alarm log buffer.
- Trap: alarms sent to the Nview NNM system when the Nview NNM system is configured

Alarms will be broadcasted according to various terminals configured on the ISCOM6800 and ISCOM6860, including CLI terminal and Nview NNM system.

Log output of alarms starts with the symbol "#", and the output format is:

#Index TimeStamp HostName ModuleName/Severity/name:Arise From Description

Table 16-2 lists alarm fields.

Table 16-2 Alarm fields

Field	Description
Index	Alarm index
TimeStamp	Time when an alarm is generated
ModuleName	Name of a module that generates an alarm
Severity	Alarm level
Name	Alarm name
Arise From Description	Descriptions about an alarm

Alarm levels

The alarm level is used to identify the severity degree of an alarm. The level is defined in Table 16-3.

Table 16-3 Alarm levels

Level	Description	Syslog
Critical (3)	This alarm has affected system services and requires immediate troubleshooting. Restore the device or source immediately if they are completely unavailable, even it is not during working time.	1 (Alert)
Major (4)	This alarm has affected the service quality and requires immediate troubleshooting. Restore the device or source service quality if they decline; or take measures immediately during working hours to restore all performances.	2 (Critical)
Minor (5)	This alarm has not influenced the existing service yet, which needs further observation and take measures at appropriate time so as to avoid more serious fault.	3 (Error)
Warning (6)	This alarm will not affect the current service, but maybe the potential error will affect the service, so it can be considered as needing to take measures.	4 (Warning)
Indeterminate (2)	Uncertain alarm level, usually the event alarm.	5 (Notice)
Cleared (1)	This alarm shows to clear one or more reported alarms.	5 (Notice)

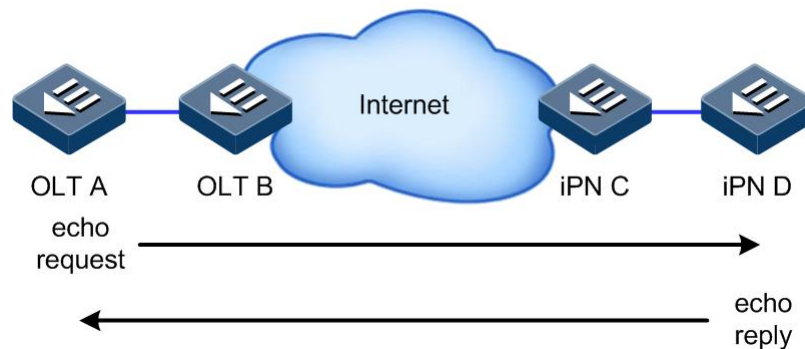
16.1.4 Ping

Ping derives from the sonar location operation, which is used to detect whether the network is normally connected.

Ping is achieved with ICMP echo packets. If an Echo Reply packet is sent back to the source address during a valid period after the Echo Request packet is sent to the destination address, it indicates that the route between source and destination address is reachable. If no Echo Reply packet is received during a valid period and timeout information is displayed on the sender, it indicates that the route between source and destination addresses is unreachable.

Figure 16-2 shows the working principle of Ping

Figure 16-2 Working principle of Ping



16.1.5 Traceroute

Just as Ping, Traceroute is a commonly-used maintenance method in network management. Traceroute is often used to test the network nodes of packets from sender to destination, detect whether the network connection is reachable, and analyze network fault.

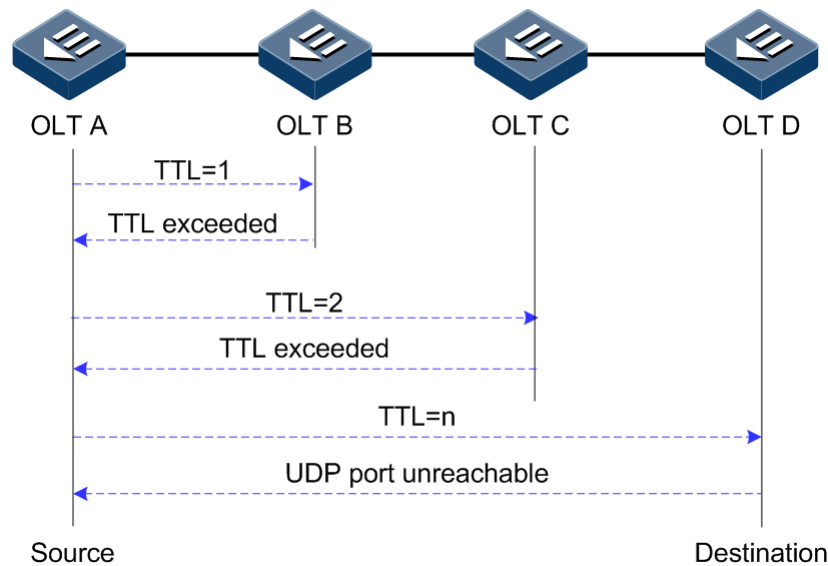
The following shows how Traceroute works:

- First, send a TTL=1 sniffer packet (where the UDP port ID of the packet is unavailable to any application programs in destination side).
- TTL deducts 1 when reaching the first hop. Because the TTL value is 0, in the first hop the device returns an ICMP timeout packet, indicating that this packet cannot be sent.
- The sending host adds 1 to TTL and resends this packet.
- Because the TTL value is reduced to 0 in the second hop, the device will return an ICMP timeout packet, indicating that this packet cannot be sent.

The above steps continue until the packet reaches the destination host which will not return ICMP timeout packets. Because the port ID of the destination host is not used, the destination host will send a port unreachable packet and finish the test. Thus, the sending host can record the source address of each ICMP TTL timeout packet and analyze the path to the destination according to the response packet.

Figure 16-3 shows the working principle of Traceroute.

Figure 16-3 Working principle of Traceroute



16.1.6 Alarm and event management

Alarm and event management refers to recording, configuring, and checking alarms and events. Through alarm and event management, you can maintain the device to ensure that it can work properly and efficiently.



Note

The difference between alarms and events is: alarms have two statuses, one is generation status and the other is elimination status; however, events only have the generation status.

Alarm and event management mainly include the following operations:

- Alarm delay: to prevent frequent occurrence of alarm report and alarm recovery report, you need to enable alarm delay. After alarm delay is enabled, alarms generated in the system are reported to the NMS after a delay rather than immediately. If the alarm recovers in the delay, it will not be reported to the NMS. The alarm is recorded in the history alarm table instead of the current alarm table. In the history alarm table, the alarm is identified as the alarm failing to be reported to the NMS due to alarm delay by the flag bit.
- Alarm filtering: you can perform alarm filtering on a specified alarm source or alarm ID. Alarms in filtering status are recorded in the current alarm table instead of being reported to the NMS. In the current alarm table, the alarm is identified as the alarm failing to be reported to the NMS due to alarm filtering by the flag bit. Alarm filtering will not stop until you disable it manually.
- Alarm masking: it is divided into general alarm masking and timed alarm masking.
 - General alarm masking: you perform general alarm masking on a specified alarm source or alarm ID, that is, NALM. The alarm in NALM status is not recorded in the current/history alarm table, and is not reported to the NMS. Alarm masking will not stop until you disable it manually.
 - Timed alarm masking: you perform timed alarm masking on a specified alarm source or alarm ID, that is, NALM-TI. The alarm in NALM-T1 status is not recorded in the

current/history alarm table, and is not reported to the NMS. Timed alarm masking will be disabled in a specified interval and it supports periodical alarm masking.

- Event masking: you perform event masking on a specified event source or event ID. The event in masking status is neither reported to the NMS nor recorded in the history event table. Event masking will not stop until you disable it manually.

16.1.7 PPPoE proxy

PPPoE proxy is used to process the Point to Point Protocol Over Ethernet (PPPoE) authentication packets, that is, to add more information about access devices to the PPPoE packet, so that the server can obtain sufficient information to identify users. PPPoE proxy can effectively prevent account sharing or account theft in the PPPoE authentication process, ensuring network security.

You can select the PPPoE dial-up mode to connect to the network. You can use this account to access the network through different interfaces of the device as long as you are successfully authenticated by the same authentication server. However, it is difficult for the server to distinguish the user based only on the authentication information including the username and password. After PPPoE agent is added, the authentication packet will carry information such as the device interface in addition to the user name and password. If the information such as the interface ID recognized by the authentication server is inconsistent with the configuration, the authentication fails. This prevents unauthorized users from stealing the accounts of other legitimate users.

The PPPoE protocol adopts the client/server mode, and the OLT acts as a relay agent. The user connects to the network through PPPoE authentication. If the server needs to locate the user, more user information is needed in the authentication packet.

Users need to go through two phases to access the network through PPPoE. The first phase is the discovery phase, namely, the authentication phase. The second phase is the session phase. PPPoE+ processes the packets in the discovery phase.

- The client accesses the network through PPPoE and then sends a broadcast PPPE Active Discovery Initiation (PADI) packet, which is used to find the authentication server.
- The authentication server that receives the PADI packet sends a unicast PPPoE Active Discovery Offer (PADO) packet to respond.
- If there are multiple authentication servers that send PADO packets, the client selects one of them and sends a unicast PADR (PPPoE Active Discovery Request) packet to request authentication.
- After receiving the PADR packet, if considering that the user is legitimate, the authentication server sends a unicast PPPoE Active Discovery Session-Confirmation (PADS) packet to respond to the PADR packet. At this point, the discovery phase is complete.
- The main function of the PPPoE proxy is to add user identification information to PADI and PADR packets. The server can determine whether the identifier information matches the user account and decide whether to allocate resources.

16.2 Configuring SNMP

16.2.1 Default configurations

Default configurations of SNMP on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value			
SNMP view	By default, system, internet, and iso			
SNMP community	By default, public and private			
	Index	CommunityName	ViewName	Permission
	1	public	internet	ro
	2	private	internet	rw
SNMP access group	By default, initialnone and initial			
SNMP user	By default, none, md5nopriv, and shanopriv			
Mapping between SNMP user and access group	Index	UserName	SecModel	GroupName
	0	none	usm	initialnone
	1	md5nopriv	usm	initial
	2	shanopriv	usm	initial
Identification and contact of administrators	support@Raisecom.com			
Device location	world china raisecom			
Trap status	enable			
IP address of SNMP target host	N/A			
Interval to send KeepAlive Trap from the device to the SNMP NMS	300s			

16.2.2 Configuring basic functions of SNMPv1/v2c

To protect itself and prevent its MIB from unauthorized access, the SNMP Agent proposes the concept of community. The management station in the same community must use the community name in all Agent operations; otherwise, the request will not be accepted.

The community name refers to using different SNMP strings to identify different SNMP groups. Different communities can have read-only or read-write access permission. Groups with read-only permission can only query the device information, while groups with read-write authority can configure the device in addition to querying the device information.

SNMPv1/v2c uses the community name authentication scheme. SNMP packets which are inconsistent with the community name will be discarded.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#snmp-server view view-name oid-tree [mask] { included excluded } example: Raisecom(config)#snmp-server view mib1 1.3.6.1.2.1 1.1.1.1.0.1 included</pre>	(Optional) create the SNMP view and configure the MIB variable range. • view-name: view name, a string of 1 to 32 characters • oid-tree: OID of the MIB subtree corresponding to the view • mask: subtree OID mask, with the value of 0 or 1. The maximum length is 16 characters, which means it supports a subtree of the depth of 128, such as 1.1.1.1.0.1. If a certain bit is 0, it indicates that this bit of the MIB variable in the view is not necessarily the same as the value of the bit of the subtree OID. For example, the MIB subtree of a view has an OID of 1.3.6.1.2.1 and a mask of 1.1.1.1.0.1. The first four and last bits of the MIB variable in this view must be the same as the subtree, namely, 1.3.6.1.x.1, and the fifth x can be any number from 0 to 9. That is, the MIB variable in the view is 1.3.6.1.0.1, 1.3.6.1.1.1 ... 1.3.6.1.9.1, totally 9, and if the parameter is not selected, the default mask is empty. • included: the MIB variable in the view is included in the subtree. • excluded: the MIB variable in the view is excluded in the subtree.
3	<pre>Raisecom(config)#snmp-server community com-name [view view- name] { ro rw } example: Raisecom(config)#snmp-server community guest view mib1 ro</pre>	Create the community name and configure the corresponding view and access privilege. • string: community name, a string of 1 to 32 characters • view view-name: MIB view that the community can access, view name, a string of 1 to 32 characters. If you do not select this parameter, the view that can be accessed is internet by default. • ro: the community's permission is read-only, only reading the data of the agent. • rw: the community's permissions are read and write, reading data of the agent or writing data into the agent.

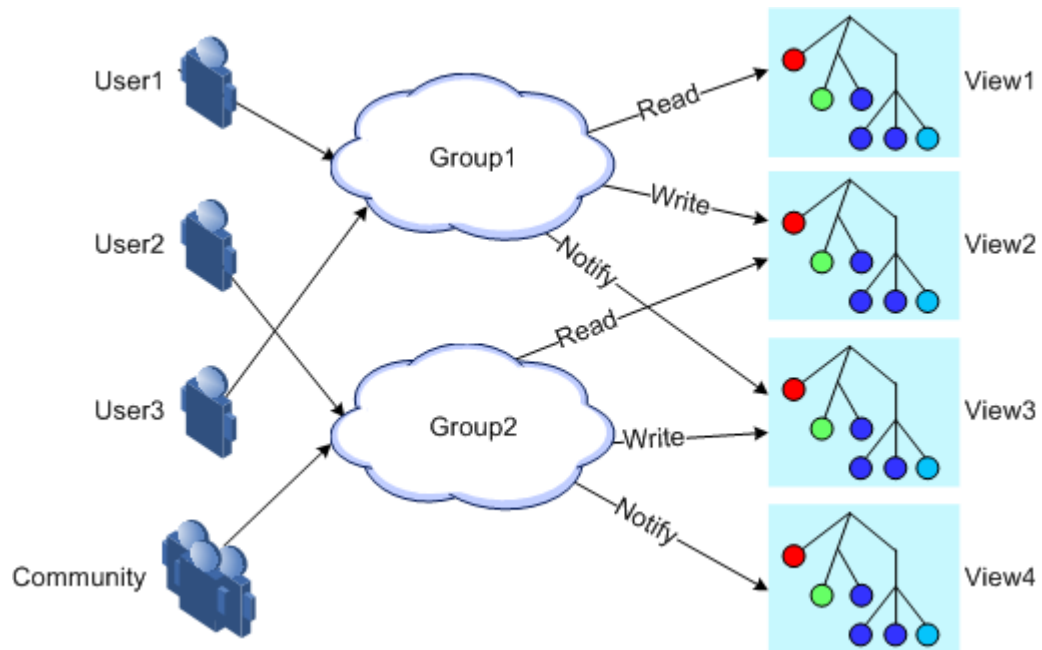
16.2.3 Configuring basic functions of SNMPv3

SNMPv3 adopts the USM user authentication mechanism. The USM comes up with the concept of access group: one or more users correspond to one access group; each access group sets the related read, write and announcement views; users in the access group have access permission in this view. User access group sending the Get and Set request must have permission corresponding to the request; otherwise the request will not be accepted.

As shown in Figure 16-4, the network management station uses SNMPv3 to access the ISCOM6800 and ISCOM6860 and the configuration is as below:

- Configure the user.
- Check which access group the user belongs to.
- Configure the view permission of the access group.
- Create a view.

Figure 16-4 Authentication mechanism of SNMPV3



Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#snmp-server view <i>view-name oid-tree [mask]</i> { included excluded } example: Raisecom(config)#snmp-server view mib1 1.3.6.1.2.1 1.1.1.1.0.1 included	Create the SNMP view and configure the MIB variable range. • view-name: view name, a string of 1 to 32 characters • oid-tree: OID of the MIB subtree corresponding to the view • mask: subtree OID mask, with the value of 0 or 1. The maximum length is 16 characters, which means it supports a subtree of the depth of 128, such as 1.1.1.1.0.1. If a certain bit is 0, it indicates that this bit of the MIB variable in the view is not necessarily the same as the value of the bit of the subtree OID. For example, the MIB subtree of a view has an OID of 1.3.6.1.2.1 and a mask of 1.1.1.1.0.1. The first four and last bits of the MIB variable in this view must be the same as the subtree, namely, 1.3.6.1.x.1, and the fifth x can be any number from 0 to 9. That is, the MIB variable in the view is 1.3.6.1.0.1, 1.3.6.1.1.1 ... 1.3.6.1.9.1, totally 9, and if the parameter is not selected, the default mask is empty. • included: the MIB variable in the view is included in the subtree. • excluded: the MIB variable in the view is excluded in the subtree.

Step	Command	Description
3	<pre>Raisecom(config)#snmp-server user username [remote engineid] authentication { md5 sha } authpassword</pre> example: <pre>Raisecom(config)#snmp-server user user1 authentication md5 raisecom</pre>	Create the user and configure the authentication mode. • user-name: SNMP group user name, a string of 1 to 32 characters • remote engine-id: specify the ID of the remote SNMP engine. • engine-id: SNMP engine ID to which the username can be contacted. • md5: configure the user authentication mode and use the MD5 hash function for authentication. • sha: configure the user authentication mode and use the SHA-1 hash function for authentication. • authpassword: key, which is combined with a hash function to generate a verification code to implement authentication.
4	<pre>Raisecom(config)#snmp-server user username [remote engineid] authkey { md5 sha } authkey</pre> example: <pre>Raisecom(config)#snmp-server user user1 authkey md5 raisecom</pre>	Create the user and configure information about the authentication key. • user-name: SNMP group user name, a string of 1 to 32 characters • remote engine-id: specify the ID of the remote SNMP engine. • engine-id: SNMP engine ID to which the username can be contacted. • md5: configure the user authentication mode and use the MD5 hash function for authentication. • sha: configure the user authentication mode and use the SHA-1 hash function for authentication. • authkey: key, which is combined with a hash function to generate a verification code to implement authentication.
5	<pre>Raisecom(config)#snmp-server user username [remote engineid]</pre> example: <pre>Raisecom(config)#snmp-server user user1</pre>	Create the user and configure the remote SNMP engine ID. • user-name: SNMP group user name, a string of 1 to 32 characters • remote engine-id: specify the ID of the remote SNMP engine. • engine-id: SNMP engine ID to which the username can be contacted.

Step	Command	Description
6	<pre>Raisecom(config)#snmp-server access group-name [read view- name] [write view-name] [notify view-name] [context context-name { exact prefix }] usm { noauthnopriv authnopriv } example: Raisecom(config)#snmp-server access guestgroup read mib2 usm authnopriv</pre>	Create and configure the SNMPv3 access group. • group-name: SNMP group name, a string of 1 to 32 characters • read: users in the SNMP group can only read the contents of the agent. • write: users in the SNMP group can write data to the Agent. • notify: users in the SNMP group can use Notification. • view-name: view name, a string of 1 to 32 characters • context string: specify the context name. • string: context name or prefix, a string of 1 to 32 characters • exact: exactly match the context name. • prefix: match the first few characters of the context name. • usm: use the SNMP v3 security model. • noauthnopriv: do not authenticate SNMP packets nor encrypt them. It is applied to the SNMP v3 security model. • authnopriv: authenticate SNMP packets but does not encrypt them. It is applied to the SNMP v3 security model.
7	<pre>Raisecom(config)#snmp-server group group-name user username { v1sm v2csm usm } example: Raisecom(config)#snmp-server group raisecom v1sm</pre>	Configure mapping between the user and access group. • group-name: SNMP group name, a string of 1 to 32 characters • v1sm: use the SNMP v1 security model. SNMP has three security models; v1 has the lowest security level; v2c is second; and v3 has the highest security level. • v2csm: use the SNMP v2c security model.

16.2.4 Configuring other information about SNMP

Configure other information of SNMP, including:

- Identification and contact of administrators
- Physical location of the ISCOM6800 and ISCOM6860

SNMPv1, v2c, and v3 are in support of the above configurations.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#snmp-server contact <i>contact</i> example: Raisecom(config)#snmp-server contact service@raisecom.com	(Optional) configure identification and contact of administrators.  Note For example, use the E-mail as the identification and contact of administrators. • contact: NMS contact mode, a character string, such as E-mail
3	Raisecom(config)#snmp-server location <i>location</i> example: Raisecom(config)#snmp-server location raisecom	(Optional) specify the physical location of the device. • location: geographical location, a character string, such as raisecom_beijing_china, without spaces

16.2.5 Configuring Trap



Note

Except for the destination host configuration, Trap configurations of SNMPv1, v2c, and v3 are identical.

Trap refers the unrequested information sent by the device to the NMS, which is used to report some critical events.

To configure the Trap feature, you need to complete the following tasks:

- Configure basic functions of SNMP. If using SNMPv1 and v2c, configure the community name; if using SNMPv3, configure the user name and SNMP view.
- Configure the routing protocol, and ensure that the route between the device and NMS is reachable.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#snmp-server host ip- address version { 1 2c } name [udpport port-id]</pre> example: <pre>Raisecom(config)#snmp-server host 10.0.0.1 version 3 raisecom udpport 1</pre>	(Optional) configure the IPv4 Trap/Notification target host based on SNMPv1/v2. - ip-address: IPv4 address of the target host, in dotted decimal notation, such as 10.10.10.1. 1 2c 3 refers to the SNMP version used. 1 refers to SNMP v1 ; 2c refers to SNMP v2c. 3 refers to SNMP v3; community-string: community name, a string; SNMP v1 and SNMP v2c use the community for authentication. If the community of the NMS is inconsistent with the community configured on the agent, the trap cannot be received. - udpport port-id: UDP interface ID of the destination host receiving trap information. If the parameter is not selected, the default interface ID is 162. The port-id refers to the interface ID, which is an integer, ranging from 1 to 65535.
3	<pre>Raisecom(config)#snmp-server host ip- address version 3 { noauthnopriv authnopriv } name [udpport value]</pre> example: <pre>Raisecom(config)#snmp-server host 10.0.0.1 version 3 authnopriv raisecom</pre>	(Optional) configure the IPv4 Trap/Notification target host based on SNMPv3. - ip-address: IPv4 address of the target host, in dotted decimal notation, such as 10.10.10.1 1 2c 3 refers to the SNMP version used. 1 refers to SNMP v1 ; 2c refers to SNMP v2c. 3 refers to SNMP v3. - community-string: community name, a string; SNMP v1 and SNMP v2c use the community for authentication. If the community of the NMS is inconsistent with the community configured on the agent, the trap cannot be received. - udpport port-id: UDP interface ID of the target host receiving trap information. If the parameter is not selected, the default interface ID is 162. The port-id refers to the interface ID, which is an integer, ranging from 1 to 65535. - authnopriv: authenticate SNMP packets but does not encrypt them. - noauthnopriv: neither authenticate nor encrypt SNMP packets.

Step	Command	Description
4	<pre>Raisecom(config)#snmp-server host ipv6 ipv6-address [scopeid string] version { 1 2c } name [udpport value]</pre> example: <pre>Raisecom(config)#snmp-server host 3001::1 version 3 raisecom udpport 1</pre>	(Optional) configure the IPv6 Trap/Notification target host based on SNMPv1/v2. • ip-address: IPv4 address of the destination host, in dotted decimal notation, such as 10.10.10.1 • ipv6-address: IPv6 address of the target host, in colon hexadecimal notation, such as 3001::1. • 1 2c 3 refers to the SNMP version used. 1 refers to SNMP v1; 2c refers to SNMP v2c. 3 refers to SNMP v3. • community-string: community name, a string; SNMP v1 and SNMP v2c use the community for authentication. If the community of the NMS is inconsistent with the community configured on the agent, the trap cannot be received. • udpport port-id: UDP interface ID of the target host receiving trap information. If the parameter is not selected, the default interface ID is 162. • port-id: the port-id refers to the interface ID, which is an integer, ranging from 1 to 65535.
5	<pre>Raisecom(config)#snmp-server host ipv6 ipv6-address [scopeid string] version 3 { noauthnopriv authnopriv } name [udpport value]</pre> example: <pre>Raisecom(config)#snmp-server host 3001::1 version 3 authnopriv raisecom</pre>	(Optional) configure the IPv6 Trap/Notification target host based on SNMPv3. • ipv6-address: IPv6 address of the target host, in hexadecimal format, such as 3001::1 • udpport port-id: UDP interface ID of the target host receiving trap information. If the parameter is not selected, the default interface ID is 162. The port-id refers to the interface ID, which is an integer, ranging from 1 to 65535. • authnopriv: authenticate SNMP packets but does not encrypt them. • noauthnopriv: neither authenticate nor encrypt SNMP packets. • user-name: user name in the SNMP group, a character string. SNMP v3 uses the user name for authentication. If the community of the NMS is inconsistent with the community configured on the agent, the trap cannot be received.
6	<pre>Raisecom(config)#snmp-server enable traps</pre>	Enable the OLT to send Trap. You can use the no snmp-server enable traps command to disable this function.

Step	Command	Description
7	<pre>Raisecom(config)#snmp-server keepalive-trap { enable disable pause }</pre> example: <pre>Raisecom(config)#snmp-server keepalive-trap enable</pre>	Enable/Disable/Pause the OLT to send KeepAlive Trap. • enable: enable the device to send keepalive trap packets periodically. • disable: disable the device from sending keepalive trap packets periodically. • pause: pause the function of sending keepalive trap packets periodically.
8	<pre>Raisecom(config)#snmp-server keepalive-trap interval period</pre> example: <pre>Raisecom(config)#snmp-server keepalive-trap interval 600</pre>	Configure the interval to send KeepAlive Trap from the device to the SNMP NMS. You can use the no snmp-server keepalive-trap interval command to restore default configuration. • period: interval for sending Keepalive Trap packets, an integer, ranging from 120 to 28800, in units of second

16.2.6 Checking configurations

No.	Command	Description
1	<code>Raisecom#show snmp access</code>	Show privilege information about all access groups.
2	<code>Raisecom#show snmp community</code>	Show configurations of the SNMP community.
3	<code>Raisecom#show snmp config</code>	Show SNMP basic configurations.
4	<code>Raisecom#show snmp group</code>	Show mapping between the SNMP user and access group.
5	<code>Raisecom#show snmp host</code>	Show information about the SNMP target host.
6	<code>Raisecom#show snmp statistics</code>	Show SNMP statistics.
7	<code>Raisecom#show snmp user</code>	Show SNMP user information.
8	<code>Raisecom#show snmp view</code>	Show SNMP view information.

16.3 Configuring optical module DDM

16.3.1 Default configurations

Default configurations of optical module DDM on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Global optical module DDM	Enable (read-only)
Global optical module DDM alarm Trap	Enable (read-only)

Function	Default value
Optical module DDM on the interface	Disable
Optical module DDM alarm Trap	Disable

16.3.2 Configuring optical module DDM

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port/id	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#transceiver ddm { enable disable }	Enable/Disable optical module DDM.
4	Raisecom(config-if-*-*:*)#snmp trap transceiver { enable disable }	(Optional) enable/disable optical module DDM alarm Trap.

16.3.3 Configuring optical module DDM

Configuring OLT optical module DDM

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config-epon-onu-*/*:*)#interface { epon-olt ten-giga-epon-olt gpon-olt } slot-id/olt-id example: Raisecom(config)#interface epon-olt 2/1	Enter PON interface configuration mode. • epon-olt: EPON interface configuration mode • gpon-olt: GPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • slot-id: slot ID • port-id: PON interface ID
3	Raisecom(config-if-*-*olt-*/*)#transceiver rx-onu-power onu onu-id monitor { enable disable } example: Raisecom(config-if-epon-olt-3/1)#transceiver rx- onu-power onu 2 monitor enable	Enable/Disable optical module DDM. • onu-id: ONU ID under the PON interface

Step	Command	Description
4	<pre>Raisecom(config-if-*olt- /*) #transceiver rx-onu-power onu onu-id { high-threshold low- threshold } threshold-value example: Raisecom(config-if-epon-olt- 3/1) #transceiver rx-onu-power onu onu-id high-threshold 5000</pre>	Configure the threshold of ONU uplink optical power received at the OLT side. • onu-id: ONU ID under the PON interface • high-threshold threshold-value: high threshold, an integer, ranging from -4000 to 816 • low-threshold threshold-value: low threshold, an integer, ranging from -4000 to 816

Configuring ONU optical module alarm

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config) #epon-onu slot-id/olt- id/onu-id example: Raisecom(config) #epon-onu 3/2/1</pre>	Enter EPON ONU remote management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	<pre>Raisecom(config-epon-onu-*//*:*) #snmp trap transceiver { voltage bias temp tx-power rx-power } { high- alarm high-warning low-warning low-alarm } { enable disable } example: Raisecom(config-epon-onu-3/2:1) #snmp trap transceiver bias high-alarm enable</pre>	Configure ONU optical module alarms. • bias: bias current • rx-power: Rx power • temp: temperature • tx-power: luminous power • voltage: voltage • high-alarm: high alarm • high-warning: high warning • low-alarm: low alarm • low-warning: low warning • disable: disable SNMP Trap optical module. • enable: enable SNMP Trap optical module.

16.3.4 Checking configurations

No.	Command	Description
1	Raisecom#show transceiver	Show the global and interface status of the OLT optical module measurement and diagnosis.
2	<pre>Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt } slot- id/olt-id transceiver rx-onu-power [violation]</pre>	Show information about the uplink average optical power of the ONU received by the optical module under the OLT PON interface.
3	<pre>Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id ddm [detail]</pre>	Show the current performance, alarm status, and alarm threshold of the OLT optical module.

No.	Command	Description
4	Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id ddm history [15m 24h]	Show history performance parameters of the OLT optical module.
5	Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id ddm information	Show the status of the OLT optical module.
6	Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id ddm threshold-violation	Show the time from the last violation of the OLT optical module to the present and corresponding violation value.
7	Raisecom#show epon-onu slot-id/olt-id/onu-list transceiver information	Show information about the ONU optical module.
8	Raisecom#show epon-onu slot-id/olt-id/onu-list transceiver detail	Show parameters of the ONU optical module.
9	Raisecom#show epon-onu slot-id/olt-id/onu-list snmp trap transceiver	Show configurations of ONU optical module parameter alarms.
10	Raisecom#show gpon-onu slot-id/olt-id/onu-list transceiver	Show information about the eGPON ONU optical module.
11	Raisecom#show gpon-onu slot-id/olt-id/onu-id transceiver	Show information about the GPON ONU optical module.

16.4 PPPoE Agent

16.4.1 Default configurations

Function	Default values
PPPoE Agent global functions	Disabled
PPPoE Agent interface functions	Disabled
Trusted interface	N/A
Packet processing strategy	transparent
Overwriting start position	0
Overwriting length	24

Configuring PPPoE Agent

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id example: Raisecom(config)#interface gigabitethernet 1/3	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode
3	Raisecom(config-if-*/*/:*)#pppoeagent trust	(Optional) configure the interface as a PPPoE Agent trusted interface. You can use the no pppoeagent trust command to restore default configurations.  Note When a device receives a PPPoE packet (such as PADI packet), it only forwards the packet to the trusted port. Therefore, you should configure the port connected to the legal PPPoE server as a trusted port.
4	Raisecom(config-if-*/*/:*)#pppoeagent circuit-id circuit-id example: Raisecom(config-if-epon-olt-1:3)#pppoeagent circuit-id pppoe-0-8-1-1	(Optional) configure Circuit ID of the interface. You can use the no pppoeagent circuit-id command to restore default configurations. • string: customized character string, a string of 1 to 127 characters
5	Raisecom(config-if-*/*/:*)#pppoeagent overwrite-policy { transparent drop replace [offset offset length length] } example: Raisecom(config-if-gpon-olt-1:3)#pppoeagent overwrite-policy drop	(Optional) re-write the processing policy of PPPoE Agent packets. • replace: overwrite • transparent: transparent transmission • drop: drop

16.4.2 Enabling PPPoE Agent

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#pppoeagent { enable disable }	Enable/Disable global PPPoE Agent.
3	Raisecom(config)#interface { gigabitethernet ten-gigabitethernet epon-olt ten-giga-epon-olt gpon-olt } slot-id/port-id	Enter physical interface configuration mode.
4	Raisecom(config-if-*/:*)#pppoeagent { enable disable }	Enable/Disable PPPoE Agent on the interface.

Checking configurations

Step	Command	Description
1	Raisecom#show pppoeagent	Show configurations of PPPoE Agent.
2	Raisecom#show interface { gigabitethernet ten-gigabitethernet epon-olt ten-giga-epon-olt gpon-olt } slot-id/port-id pppoeagent statistics	Show PPPoE Agent statistics on the interface.

16.5 Watchdog

16.5.1 Default configurations

Funtion	Default value
Enable/Disable Watchdog	Enable

16.5.2 Configuring Watchdog

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#watchdog { enable disable }	Enable/Disable Watchdog.

16.5.3 Checking configurations

No.	Command	Description
1	Raisecom#show watchdog	Show Watchdog configurations.

16.6 Configuring system log

16.6.1 Default configurations

Default configurations of system log on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
System log	Enable
Output system log to the console	Enable (output level: notifications)
Log host	N/A
Output system log to the monitor	N/A
Log rate configurations	0, no limit
Timestamp configurations of system log	Absolute time

16.6.2 Configuring basic information about system log

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#logging on	Enable system log. You can use the no logging on command to disable this function.
3	Raisecom(config)#logging time-stamp { relative-start none } example: Raisecom(config)#logging time-stamp relative-start	Configure the type of timestamp. • none: no timestamp • relative-start: the timestamp refers to the relative time, which is a time period, namely, the time elapsed after system startup.
4	Raisecom(config)#logging rate rate example: Raisecom(config)#logging rate 100	Configure the Tx rate of system log. • log-num: logs processed per second, an integer, ranging from 1 to 10000

Step	Command	Description
5	<pre>Raisecom(config)#exit Raisecom#logging-file <i>module name</i> example: Raisecom#logging-file acl</pre>	Enable/Disable file recording of the module. • module-name: file name of the module: acl alarm all anti-dos arp arpproxy attack-defense autosave capture card clock config ctc-stack cu dai dba dbms ddm device dhcp dot3epon dot3oam driver environ ering-config erps evbroker file filter gpon-onu-remote gpon-protect gpononu-file ha if image-update ipsg lacp lbd license linkstatetrack llid mac-config mcast mirror mstp ndp ndsnooping ntp omcc omccpacket onu-file onu-register onu-remote-mng onu-template ping pktrtx pon-config-load pon-monitor pon-port-monitor pon-profile pon-protect pon-sys pon-transceiver pon-trap portbackup portisolate pppoeagent qinq radius ratelimit relay ressynch rpc sal scrn serial-service service-port snmp sntp ssh stelnet stg stormcontrol sys-mon tacacsplus telnet traceroute trunk uplink-protect uplinkprotect vlan
6	<pre>Raisecom#config Raisecom(config)#logging file severity { <i>severity-level</i> alerts critical emergencies errors informational notifications warnings } example: Raisecom(config)#logging file severity 6</pre>	Configure the file log level of the module. • severity-level: log severity ID, an integer, ranging from 0 to 6, representing level 1 to level 6 • emergencies: level 0, the most serious. The system can not be used. You need to restart the device. • alerts: level 1, very serious. You need to take immediate action. • critical: level 2, serious. You need to take measures or analyze the reasons. • errors: level 3, error. It will not affect services, but you need to pay attention. • warnings: level 4, warning. It may cause service failure. You need to pay attention. • notifications: level 5, normal, key operational information when the device is running normally • informational: level 6, notification event, general operation information when the device is running normally

16.6.3 Configuring output direction of system log

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#logging history	(Optional) record system log in the buffer.

Step	Command	Description
	Raisecom(config)#logging console severity { <i>severity-level</i> alerts critical debugging emergencies errors informational notifications warnings } example: Raisecom(config)#logging console severity errors	(Optional) output system log to the Console interface and configure parameter information. • log-level: severity level of the log, an integer, ranging from 0 to 6, representing level 0–level 6 respectively • emergencies: level 0, most serious, the system can not be used, and the device need restarting. • alerts: level 1, very serious, requiring immediate action • critical: level 2, serious, need to take measures or analyze the reasons. • errors: level 3, error, it will not affect services but need to pay attention. • warnings: level 4, warning, may cause service failure and need to pay attention. • notifications: level 5, normal, key operational information when the device is running normally • informational: level 6, notification event, general operation information when the device is running normally • debugging: level 7, debugging information, general operational information when the device is running normally, can be ignored
	Raisecom(config)#logging host <i>host-id</i> { ip ipv6 } address <i>ip-address</i> facility { local0 local1 local2 local3 local4 local5 local6 local7 } severity [<i>log-level</i> alerts critical debugging emergencies errors informational notifications warnings] example: Raisecom(config)#logging host 1 ip address 10.0.0.1 facility local0 severity 1	(Optional) output system log to the log host. • ip-address: IP address of log host, in dotted decimal notation, such as 10.10.10.1 • host-id: log host ID, an integer, ranging from 1 to 10 • local0 local1 local2 local3 local4 local5 local6 local7 : log host ID • log-level: severity level of the log, an integer, ranging from 0 to 6, representing level 0–level 6 respectively • emergencies: level 0, most serious, the system can not be used, and the device need restarting. • alerts: level 1, very serious, requiring immediate action • critical: level 2, serious, need to take measures or analyze the reasons. • errors: level 3, error, it will not affect services but need to pay attention. • warnings: level 4, warning, may cause service failure and need to pay attention. • notifications: level 5, normal, key operational information when the device is running normally • informational: level 6, notification event, general operation information when the device is running normally

Step	Command	Description
	<pre>Raisecom(config)#logging monitor severity { severity-level alerts critical debugging emergencies errors informational notifications warnings } example: Raisecom(config)#logging monitor warnings</pre>	(Optional) output system log to the monitor terminal and configure the alarm level. - log-level: severity level of the log, an integer, ranging from 0 to 7, representing level 0–level 7 respectively - emergencies: level 0, most serious, the system can not be used, and the device need restarting. - alerts: level 1, very serious, requiring immediate action - critical: level 2, serious, need to take measures or analyze the reasons. - errors: level 3, error, it will not affect services but need to pay attention. - warnings: level 4, warning, may cause service failure and need to pay attention. - notifications: level 5, normal, key operational information when the device is running normally - informational: level 6, notification event, general operation information when the device is running normally - debugging: level 7, debugging information, general operational information when the device is running normally, can be ignored
3	<pre>Raisecom(config)#logging command- host { ip address ip-address ipv6 address ipv6-address } example: Raisecom(config)#logging command- host ip address 10.0.0.1</pre>	(Optional) configure the CLI operation log host. - ip address ip-address: IPv4 address, in dotted decimal notation, such as 10.10.10.1 - ipv6 ipv6-address: IPv6 address, in colon hexadecimal notation, such as 3001::1

16.6.4 Checking configurations

No.	Command	Description
1	<code>Raisecom#show logging</code>	Show system log configurations.
2	<code>Raisecom#show logging host</code>	Show information about the system log host.
3	<code>Raisecom#show logging history</code>	Show information about system log buffer.
4	<code>Raisecom#show logging statistics</code>	Show statistics of system log.
5	<code>Raisecom#show logging command-host</code>	Show information about CLI operation log host.
6	<code>Raisecom#show logging file</code>	Show information about logs recorded to the file.
7	<code>Raisecom#show logging-file module</code>	Show the logging file module.

16.7 Configuring port mirroring

16.7.1 Default configurations

N/A

16.7.2 Configuring port mirroring on OLT

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mirror { enable disable }	Enable/disable global port mirroring.
3	Raisecom(config)#interface { epon-olt ten-giga-epon-olt gpon-olt gigabitethernet ten-gigabitethernet } slot-id/port-id example: Raisecom(config)#interface gigabitethernet 1/3	Enter physical interface configuration mode. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE Ethernet interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode
4	Raisecom(config-if-*/*)#mirror monitor-port uni-id example: Raisecom(config-epon-onu-3/1:1)#mirror monitor-port 5	(Optional) configure the monitor port (a port cannot be the monitor port and the mirroring port at the same time). You can use the no mirror monitor-port command to delete the monitor port.  Note The EPON interface can be configured as the mirroring source port only instead of the monitor port. The Ethernet interface can be configured as the monitor port or mirroring source port. • uni-id: UNI, an integer, ranging from 1 to 24
5	Raisecom(config-if-*/*)#mirror source-port { both egress ingress } example: Raisecom(config-epon-onu-3/1:1)#mirror source-port-list both	(Optional) configure the mirroring source port. You can use no mirror source-port command to delete the port. • both: monitor the mirroring port in both ingress and egress directions. • egress: monitor the mirroring port in the egress direction. • ingress: monitor the mirroring port in the ingress direction.

16.7.3 Configuring ONU port mirroring

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#epon-onu slot-id/olt-id/onu-id example: Raisecom(config)#epon-onu 3/2/1	Enter EPON ONU remote management configuration mode. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface
3	Raisecom(config-epon-onu-*//*:*)#mirror { enable disable }	Enable/Disable port mirroring.
4	Raisecom(config-epon-onu-*//*:*)#mirror monitor-port uni-id example: Raisecom(config-epon-onu-3/1:1)#mirror monitor-port 5	Configure the monitor interface (a port cannot be the monitor port and the mirroring port at the same time).. You can use the no mirror monitor-port command to delete the port. • uni-id: UNI ID, an integer, ranging from 1 to 24
5	Raisecom(config-epon-onu-*//*:*)#mirror source-port-list { both egress ingress } uni-list [uplink] example: Raisecom(config-epon-onu-3/1:1)# mirror source-port-list both 1	Configure the source interface and monitoring mode. You can use the no mirror source-port-list { both egress ingress } command to restore default configurations. • both: monitor the mirroring port in both ingress and egress directions. • egress: monitor the mirroring port in the egress direction. • ingress: monitor the mirroring port in the ingress direction. • uni-id: the UNI interface acts as a mirroring port. The ID is an integer ranging from 1 to 24. • uplink: the ONU uplink interface acts as a mirroring port.

16.7.4 Checking configurations

No.	Command	Description
1	Raisecom#show mirror	Show configurations of port mirroring on the OLT.
2	Raisecom#show epon-onu slot-id/olt-id/onu-id mirror	Show configurations of ONU mirroring.

16.8 Configuring link detection

16.8.1 Ping

Step	Command	Description
1	<pre>Raisecom#ping ip-address [count num] [size size] [waittime period] [source ip-address] example: Raisecom#ping 10.0.0.1</pre>	Test whether the IPv4 remote host is reachable. • ip-address: IPv4 address of the destination device, in dotted decimal notation, such as 10.10.10.1 • count num: specify the number of probe packets to be sent to exit the PING program. num: an integer, ranging from 1 to 65535 • size size: specify the size of the probe IPv4 packet. The size is an integer ranging from 0 to 65507, in units of Byte. • Waittime period: specify the time that the PING program waits for a response. If there is no response after the time elapsed, the destination is considered unreachable. Period is an integer ranging from 1 to 60, in units of second. • source ip-address: IPv4 address of the source device, in dotted decimal notation, such as 10.10.10.1
2	<pre>Raisecom#ping6 ipv6-address [count num] [size size] [waittime timeout] example: Raisecom#ping 3001::1</pre>	Test whether the IPv6 remote host is reachable. • ip-address: IPv6 address of the destination device, in dotted decimal notation, such as 10.10.10.1 • count num: specify the number of probe packets to be sent to exit the PING program. num: an integer, ranging from 1 to 65535 • size size: specify the size of the probe IPv6 packet. The size is an integer ranging from 0 to 65507, in units of Byte. • Waittime period: specify the time that the PING program waits for a response. If there is no response after the time elapsed, the destination is considered unreachable. Period is an integer ranging from 1 to 60, in units of second. • source ip-address: IPv6 address of the source device, in dotted decimal notation, such as 10.10.10.1



Note

You cannot execute other operations on the device in the process of Ping. You can execute other operations after pressing **Ctrl+C** to interrupt Ping or the Ping process finishes.

16.8.2 Traceroute



Note

Configure the IP address and default gateway for the device before using the Traceroute function.

Step	Command	Description
1	Raisecom#traceroute <i>ip-address</i> [firstttl <i>first-ttl</i>] [maxttl <i>max-ttl</i>] [port <i>port-number</i>] [waittime <i>period</i>] [count <i>times</i>] example: Raisecom#traceroute 10.0.0.1	Test the IPv4 network connectivity using the traceroute command and show the packet-traversed network nodes. • ip-address: IP address of the destination host or network, in dotted decimal notation, such as 10.10.10.1 • firstttl <i>first-ttl</i>: initial TTL, the first-ttl is an integer ranging from 1 to 255. • maxttl <i>max-ttl</i>: maximum TTL, the max-ttl is an integer ranging from 1 to 255. When the number of hops of the probe packet exceeds the value, the destination is considered unreachable. • port <i>port-number</i>: destination interface ID of UDP packets, the port-number is an integer ranging from 1 to 65535. • waittime <i>period</i>: specify the timeout period for the Traceroute program to wait for a probe response. The period is an integer ranging from 1 to 60, in units of second. If the destination response has not been received until the timeout elapsed, the destination is considered unreachable. • count <i>times</i>: number of probe packets sent in the same hop, the times is an integer ranging from 1 to 10.

Step	Command	Description
2	<pre>Raisecom#tracertoute ipv6 ipv6-address [firstttl first-ttl] [maxttl max-ttl] [port slot-id/port-id] [waittime period] [count count] example: Raisecom#tracertoute 3001::1</pre>	Test the IPv6 network connectivity using the tracertoute command and show the packet-traversed network nodes. • ipv6 ipv6-address: IPv6 address of the destination host, in colon hexadecimal notation, such as 3001::1 • firstttl first-ttl: initial TTL, the first-ttl is an integer ranging from 1 to 255. • maxttl max-ttl: maximum TTL, the max-ttl is an integer ranging from 1 to 255. When the number of hops of the probe packet exceeds the value, the destination is considered unreachable. • port port-number: destination interface ID of UDP packets, the port-number is an integer ranging from 1 to 65535. • waittime period: specify the timeout period for the Tracertoute program to wait for a probe response. The period is an integer ranging from 1 to 60, in units of second. If the destination response has not been received until the timeout elapsed, the destination is considered unreachable. • count times: number of probe packets sent in the same hop, the times is an integer ranging from 1 to 10.

16.9 Configuring PPPoE Agent

16.9.1 Default configurations

Function	Default value
PPPoE agent global function	Disable
PPPoE agent interface function	Disable
Trust interface	N/A
Packet processing policy	Transparent transmission
Overwrite start location	0
Overwrite length	24

16.9.2 Configuring PPPoE Agent

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { gigabitethernet ten-gigabitethernet gpon-olt } slot-id/port-id example: Raisecom(config)#interface gigabitethernet 3/1	Enter physical interface configuration mode. • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode • slot-id: slot ID • port-id: interface ID
3	Raisecom(config-if-*/*/:*)#pppoeagent trust	(Optional) configure the interface as the trusted interface of PPPoE agent. You can use the no pppoeagent trust command to restore default configurations.  Note When a device receives a PPPoE packet (such as PADI packet), it only forwards the packet to the trusted interface. Therefore, you should configure the interface connected to the legal PPPoE server as a trusted interface.
4	Raisecom(config-if-*/*/:*)#pppoeagent circuit-id string example: Raisecom(config-if-epon-olt-1:1)#pppoeagent circuit-id ppoe-0-8-1-1	(Optional) configure interface Circuit ID. You can use the no pppoeagent circuit-id command to restore default configurations. • string: interface customized value string, a string of 1 to 127 characters
5	Raisecom(config-if-*/*/:*)#pppoeagent overwrite-policy { transparent drop replace } example: Raisecom(config-if-gpon-olt-1:3)#pppoeagent overwrite-policy drop	(Optional) configure the processing policy of PPPoE packets. • replace: overwrite • transparent: transparent transmission • drop: drop
6	raisecom(config-if-*/*/:*)#pppoeagent overwrite-policy replace offset value length value example: Raisecom(config-if-gpon-olt-2:1)#pppoeagent overwrite-policy drop	(Optional) configure partial overwriting policy for PPPoE packets. • offset value: overwrite start location, an integer, ranging from 0 to 64 • length value: overwrite length, an integer, ranging from 0 to 128

16.9.3 Enabling PPPoE proxy

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#pppoeagent { enable disable }	Enable/Disable global PPPoE Agent.
3	Raisecom(config)#interface { epon-olt slot-id/port-id epon-onu slot-id/olt-id/onu-id gigabitethernet slot-id/port-id ten-gigabitethernet slot-id/port-id serial slot-id/port-id }y	Enter interface configuration mode.
4	Raisecom(config-if-*/*/:*)#pppoeagent { enable disable }	Enable/Disable PPPoE Agent on an interface.

16.9.4 Checking configurations

Step	Command	Description
1	Raisecom#show interface { epon-olt slot-id/port-id epon-onu slot-id/olt-id/onu-id gigabitethernet slot-id/port-id ten-gigabitethernet slot-id/port-id serial slot-id/port-id } pppoeagent	Show configurations of PPPoE Agent.

16.10 Configuring system monitoring

16.10.1 Default configurations

Default configurations of system monitoring on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Temperature monitoring	Enable
Power monitoring	Enable
Fan monitoring	Enable
CPU utilization threshold Trap	Disable
CPU alarm rising threshold	80
CPU alarm falling threshold	30
Available memory utilization threshold Trap	Disable

Function	Default value
Memory monitoring alarm threshold	1

16.10.2 Configuring temperature monitoring

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#shelf temperature-threshold <i>threshold-value</i> example: Raisecom(config)#shelf temperature-threshold 70	Configure the temperature alarm threshold. When the temperature of the device exceeds the threshold, an alarm will be reported. threshold: temperature alarm threshold, an integer, ranging from 45 to 90
3	Raisecom(config)#temperature high-alarm threshold <i>threshold</i> [<i>slot slot-id</i>] example: Raisecom(config)#temperature high-alarm threshold 100 slot 1	Configure the temperature alarm threshold of the device card. - threshold: temperature alarm threshold, an integer, ranging from 30 to 150 - slot slot-id: slot ID, an integer
4	Raisecom(config)#power off high temperature	Enable over-temperature management of the device card.
5	Raisecom(config)#power off temperature recover threshold <i>threshold</i> [<i>slot slot-id</i>] example: Raisecom(config)#power off temperature recover threshold 50	Configure the temperature recovery threshold of the device card. - threshold: temperature recovery threshold, an integer, ranging from 30 to 150 - slot slot-id: slot ID, an integer
6	Raisecom(config)#power off temperature threshold <i>threshold</i> [<i>slot slot-id</i>] example: Raisecom(config)#power off temperature threshold 100	Configure the over-temperature management threshold of the device card. - threshold: temperature recovery threshold, an integer, ranging from 30 to 150 - slot slot-id: slot ID, an integer

16.10.3 Configuring CPU monitoring

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#cpu threshold-trap [slot slot-list] example: Raisecom(config)#cpu threshold-trap slot 19	Enable/Disable CPU utilization rate threshold Trap. Slot1 and Slot 2 do not support configuring system monitoring alarm parameters. • slot slot-list: slot list, an integer, ranging from 3 to 4. It supports specific values, such as "3,2"; it also supports a range, such as "3-4".
3	Raisecom(config)#cpu rising-threshold threshold example: Raisecom(config)#cpu rising-threshold 80	Configure the CPU alarm rising threshold. • rising-threshold threshold: alarm rising threshold. The threshold is an integer ranging from 1 to 99, representing 1% to 99%.
4	Raisecom(config)#cpu falling-threshold threshold example: Raisecom(config)#cpu falling-threshold 20	Configure CPU alarm falling threshold. • falling-threshold threshold: alarm falling threshold. The threshold is an integer ranging from 1 to 99, representing 1% to 99%.
5	Raisecom(config)#cpu threshold-interval threshold example: Raisecom(config)#cpu threshold-interval 10	Configure the monitoring period of CPU utilization rate. • threshold-interval threshold: CPU sampling interval. The threshold is an integer ranging from 5 to 36000.

16.10.4 Configuring memory monitoring

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#memory avail-trap [slot slot-list] example: Raisecom(config)#memory avail-trap slot 3	Configure the enabled/disabled status of idle memory utilization rate Traps. • slot-list: interface list, an integer, ranging from 1 to 4

Step	Command	Description
3	<pre>Raisecom(config)#memory avail-threshold threshold [slot slot-list]</pre> example: <pre>Raisecom(config)#memory avail-threshold 10 slot 3</pre>	Configure the threshold of memory monitoring alarm. • threshold: memory over-low alarm threshold, an integer, ranging from 1 to 50 • slot-list: interface list, a character string

16.10.5 Checking configurations

No.	Command	Description
1	Raisecom#show fan	Show the fan status and configurations.
2	Raisecom#show power	Show power card information, including power card type, related threshold configurations, input and output voltage, related alarm status, and power card version.
3	Raisecom#show device	Show information about the device, including temperature, temperature alarm threshold, power, and fan.
4	Raisecom#show card-power [slot slot-id]	Check the voltage information about cards in all slots (excluding voltage cards and fan slots), including voltage status, voltage, and so on.
5	Raisecom#show card-temperature [slot slot-id]	Show temperature information about cards in call slots. It will not display information about the slots where cards are not in position.
6	Raisecom#show cpu-utilization [[alarm] slot slot-id]	Show CPU dynamic utilization rate of the card in the specified slot.
7	Raisecom#show process sorted { normal-priority process-name }	Show status of each task.
8	Raisecom#show process cpu [sorted { 1min / 10min / 5sec / invoked }]	Show running status of each task.
9	Raisecom#show process taskname	Show detailed running status of a specified task.
10	Raisecom#show process dead	Show information about dead tasks.
11	Raisecom#show memory [slot slot-list]	Check the memory usage of the card in the specified slot. This command is only available for rack-mounted devices.
12	Raisecom#show abnormal-reboot [slot slot-list]	Display abnormal startup information.
13	Raisecom#show abnormal-reboot last [slot slot-list]	View the status of the last abnormal start task.

No.	Command	Description
14	Raisecom#show abnormal-reboot last wait-info [slot slot-list]	Display wait messages of the last abnormal start task.
15	Raisecom#show epon-onu slot-id/olt-id/onu-list cpu-utilization	Show ONU CPU utilization.
16	Raisecom#show epon-onu slot-id/olt-id/onu-list memory	Show ONU memory.

16.11 Illegal ONU alarms

16.11.1 Default configurations

Function	Default value
Illegal ONU alarm allows the configuration of the number of entries to be reported and the recovery time when the alarm is received again after silence.	Illegal ONU alarms allow no limit on the number of entries that can be reported. By default, it will not be recovered when only the number of entries is configured but the recovery time is not configured.
Interval for reporting illegal ONU alarms	60s

16.11.2 Configuring illegal ONU alarm reporting

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#trap illegal-onu limit numbers [times]	(Optional) configure the number of allowed entries for illegal ONU alarms and the recovery time when the alarm is received again after silence. You can use the no trap illegal-onu limit command to restore to the default condition.  Note The first parameter is the number of traps for illegal ONU alarms that are allowed to be reported. When this value is exceeded, the alarm is silent and no more alarm will be reported. When the ONU is powered off and restarted, if the interval for receiving the alarm again exceeds the configured recovery time, it will directly report the alarm. At this time, you need to limit the interval again, otherwise it will continue to remain silent.

Step	Command	Description
3	<code>Raisecom(config)#trap illegal-onu interval time slot { all slot-list }</code>	(Optional) configure the interval for reporting illegal ONU alarms. You can use the no trap illegal-onu interval slot { all slot-list } command to restore to the default condition.

16.11.3 Checking configurations

Step	Command	Description
1	<code>Raisecom#show trap illegal-onu limit</code>	Show the number of allowed illegal alarm reports and the recovery time.
2	<code>Raisecom#show trap illegal-onu interval slot { all slot-list }</code>	Show the reporting interval of illegal ONU alarm reporting.

16.12 Configuring link monitoring

Link monitoring refers to monitoring links between the OLT and ONU. The ISCOM6800 and ISCOM6860 support the following alarm events for link monitoring.

Alarm event	Description
ONU registration event	This event is generated when some ONU is registered successfully.
ONU deregistration event	This event is generated when some ONU is deregistered. Common reasons to cause this event are as below: • The ONU is reset. • The backbone fiber or branch fiber connected to the ONU fails. • Severely errored code is generated.
ONU illegal registration event	This event is generated when an unauthorized ONU tries to apply for registration. This event is caused because the OLT interface is in non-auto-authentication mode and the ONU is not installed.
Upstream/Downstream BER TCA	This event is generated when the upstream/downstream BER on the logical link exceeds 10^{-9} . Generally, this alarm is caused by poor-quality optical signals.
Upstream/Downstream FER TCA	This event is generated when the upstream/downstream FER on the logical link exceeds 10^{-9} . Generally, this alarm is caused by weak optical signals.

16.12.1 Default configurations

Default configurations of link monitoring on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Illegal ONU registration alarm	Enable
ONU registration failure alarm	Enable
Upstream/Downstream FER TCA	Disable
LLID mismatch TCA	Disable
Threshold of LLID mismatch TCA	5000 frame/s
Key update failure alarm	Disable
Upstream/Downstream BER TCA	Disable

16.12.2 Configuring link monitoring

OLT alarm configurations are controlled by the alarm switch, which independently takes effect on each OLT interface. Each alarm switch is composed of a general switch and a group of specific switches. Some severe alarms are reported to the NMS fixedly and cannot be disabled.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface { gigabitethernet ten-gigabitethernet gpon-olt } slot-id/port-id example: Raisecom(config)#interface gigabitethernet 3/1	Enter interface configuration mode. • gpon-olt : GPON interface configuration mode • gigabitethernet : GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode • slot-id: slot ID • port-id: interface ID
3	Raisecom(config-if-*-olt-*:*)#snmp trap { enable disable }	(Optional) enable/disable alarm reporting.
4	Raisecom(config-if-*-olt-*:*)#snmp trap encryption-key-update-failure { enable disable }	(Optional) enable/disable key update failure alarm.
5	Raisecom(config-if-*-olt-*:*)#snmp trap ber-threshold-crossing downstream { enable disable }	(Optional) enable/disable downlink BER TCA.
6	Raisecom(config-if-*-olt-*:*)#snmp trap ber-threshold-crossing upstream { enable disable }	(Optional) enable/disable uplink BER TCA.
7	Raisecom(config-if-*-olt-*:*)#snmp trap fer-threshold-crossing downstream { enable disable }	(Optional) enable/disable downlink FER TCA.

Step	Command	Description
8	Raisecom(config-if-*olt-*:*)#snmp trap fer-threshold-crossing upstream { enable disable }	(Optional) enable/disable uplink FER TCA.
9	Raisecom(config-if-*olt-*:*)#snmp trap llid-mismatch-threshold-crossing { enable disable }	(Optional) enable/disable LLID mismatch TCA.
10	Raisecom(config-if-*olt-*:*)#snmp trap llid-mismatch-threshold-crossing threshold <i>rate</i> example: Raisecom(config-if-epon-olt-1:1)#snmp trap llid-mismatch-threshold-crossing threshold 6000	(Optional) configure the threshold of LLID mismatch TCA. • rate: alarm threshold, an integer, ranging from 1 to 20 000 000, in units of frame/second
11	Raisecom(config-if-*olt-*:*)#snmp trap onu-registration-unauthorized { enable disable }	(Optional) enable/disable illegal ONU registration alarm.
12	Raisecom(config-if-*olt-*:*)#snmp trap onu-registration-failure { enable disable }	(Optional) enable/disable ONU registration failure alarm.
13	Raisecom(config-if-*olt-*:*)#snmp trap onu-laser-always-on { enable disable }	(Optional) enable/disable ONU laser-always-on alarm.
14	Raisecom(config-if-*olt-*:*)#snmp trap onu-laser-always-on threshold <i>power</i> example: Raisecom(config-if-epon-olt-1:1)# snmp trap onu-laser-always-on threshold 20	(Optional) configure the threshold of ONU laser-always-on alarm. • power: optical power threshold, an integer, ranging from 1 to 32, in units of dB
15	Raisecom(config-if-*olt-*:*)#snmp trap errored-frame { enable disable }	(Optional) enable/disable DOT3OAM errored-frame alarms.
16	Raisecom(config-if-*olt-*:*)#snmp trap errored-frame threshold <i>value</i> example: Raisecom(config-if-epon-olt-1:1)#snmp trap errored-frame threshold 456 789	(Optional) configure the threshold of DOT3OAM errored-frame-period alarm. • value: number of detection threshold frames of DOT3OAM errored-frame alarms, an integer, ranging from 1 to 2000000000
17	Raisecom(config-if-*olt-*:*)#snmp trap errored-frame-period { enable disable }	(Optional) enable/disable DOT3OAM errored-frame-seconds-summary alarm.
18	Raisecom(config-if-*olt-*:*)#snmp trap errored-frame-period threshold <i>value</i> example: Raisecom(config-if-epon-olt-1:1)#snmp trap errored-frame-period threshold 3500	(Optional) configure the detection threshold of DOT3OAM errored-frame-period alarms. • value: detection threshold of DOT3OAM errored-frame-period alarms, an integer, ranging from 1 to 2000000000
19	Raisecom(config-if-*olt-*:*)#snmp trap errored-frame-seconds-summary { enable disable }	(Optional) enable/disable DOT3OAM errored-frame-seconds-summary alarms.
20	Raisecom(config-if-*olt-*:*)#snmp trap errored-symbol-period { enable disable }	(Optional) enable/disable DOT3OAM errored-symbol-period alarms.

Step	Command	Description
21	<code>Raisecom(config-if-*olt-*.*)#snmp trap port-ber { enable disable }</code>	(Optional) enable/disable BER alarms on the OLT interface.

16.12.3 Checking configurations

No.	Command	Description
1	<code>Raisecom#show interface { epon-olt ten-giga-epon-olt gpon-olt } slot-id/olt-list snmp trap</code>	Show alarm management configurations on the OLT.
2	<code>Raisecom#show interface epon-onu slot-id/olt-id/onu-id snmp trap transceiver</code>	Show alarm management configurations on the ONU.

16.13 Configuring alarm and event management

16.13.1 Default configurations

Default configurations of alarm and event management on the ISCOM6800 and ISCOM6860 are as below.

Function	Default value
Alarm Trap	Enable
Event Trap	Enable
Alarm delay	Disable
Alarm delay interval	10s
Timed alarm masking interval	3600s

16.13.2 Configuring alarm management

The alarm management feature on the ISCOM6800 and ISCOM6860 includes alarm reporting, alarm masking, and alarm delay.

Configuring alarm reporting

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.

Step	Command	Description
2	<code>Raisecom(config)#alarm traps { enable disable }</code>	Enable/Disable alarm reporting.
3	<code>Raisecom(config)#alarm active-table delete listname sn</code> example: <code>Raisecom(config)#alarm active-table delete notice 5</code>	(Optional) delete alarms in the current alarm table according to the serial number. The deleted alarms are recorded in the historical alarm table. • listname: advertisement name, a character string • sn: alarm ID, an integer

Configuring alarm masking

Alarm masking supports masking alarms based on the alarm source or alarm ID. If an alarm is in masking status, the system will not monitor the alarm.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#alarm inhibit dev [alarm-id alarm-id]</code> example: <code>Raisecom(config)#alarm inhibit dev alarm-id 1</code>	Configure alarm masking on the alarm source of the whole device. If you do not configure the alarm-id alarm-id parameter, it is believed that the alarm ID is not specified and all alarms generated on the whole device are masked. • alarm-id alarm-id: alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer.
	<code>Raisecom(config)#alarm inhibit [range] slot slot-list [alarm-id alarm-id]</code> example: <code>Raisecom(config)#alarm inhibit range slot 1</code>	Configure alarm masking on the alarm source of the OLT slots. If you do not configure the alarm-id alarm-id parameter, it is believed that the alarm ID is not specified and all alarms generated in the OLT slots are masked. • slot-id: slot ID, an integer • alarm-id alarm-id: alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer.

Step	Command	Description
	Raisecom(config)#alarm inhibit [range] interface { gigabitethernet ten-gigabitethernet epon-olt ten-giga-epon-olt gpon-olt } slot- id/port-id [alarm-id alarm-id] example: Raisecom(config)#alarm inhibit interface gigabitethernet 3/1	Configure alarm masking on the alarm source of the OLT interfaces. If you do not configure the alarm-id alarm-id parameter, it is believed that the alarm ID is not specified and all alarms generated on the OLT interfaces are masked. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode • slot-id: slot ID • port-id: interface ID • alarm-id alarm-id: alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer.
	Raisecom(config)#alarm inhibit [range] interface epon-onu slot- id/olt-id/onu-id [alarm-id alarm- id] example: Raisecom(config)#alarm inhibit interface epon-onu 3/1/1	Configure alarm masking on the alarm source of the ONU. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • alarm-id alarm-id: alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer.
	Raisecom(config)#alarm inhibit interface epon-onu slot-id/olt- id/onu-id [range] uni uni-id [alarm-id alarm-id] example: Raisecom(config)#alarm inhibit interface epon-onu 3/1/1 range uni 3	Configure alarm masking with ONU UNI as the alarm source. If the alarm-id alarm-id is not configured, the alarm ID is not restricted. As long as the source is the ONU UNI ID, all alarms are masked. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • uni-id: ONU Ethernet interface ID • alarm-id alarm-id: alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer.
3	Raisecom(config)#alarm inhibit { dev slot port onu uni } alarm-id alarm-id example: Raisecom(config)#alarm inhibit dev alarm-id 3	Configure alarm masking based on alarm ID. • dev: the alarm source is the device. • slot: the alarm source is the slot. • olt: the alarm source is the device interface. • onu: the alarm source is the ONU connected downstream to the device. • uni: the alarm source is the Ethernet interface of the ONU. • alarm-id alarm-id: configure alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer.

Step	Command	Description
4	Raisecom(config)#alarm inhibit time dev [alarm-id <i>alarm-id</i>] [interval <i>interval</i>] [start <i>start-time</i> every time stop <i>end-time</i>] example: Raisecom(config)#alarm inhibit time dev alarm-id 2	Configure timed alarm masking on the alarm source of the whole device. If you do not configure the alarm-id <i>alarm-id</i> parameter, it is believed that the alarm ID is not specified and all alarms generated on the whole device are masked. • alarm-id <i>alarm-id</i>: configure alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer. • interval <i>interval</i>: configure the interval of alarm masking. The interval is an integer ranging from 3600 to 86400, in units of second. If this parameter is not selected, the default alarm masking interval 3600 seconds will be used. • start-time <i>start-time</i>: configure the start time of alarm masking. The format of start-time is: month-day-year hour:minute:second • every time: interval from the end of the alarm masking to the start of the next alarm masking, an integer, ranging from 3600 to 86400, in units of second • end-time <i>end-time</i>: configure the end time of alarm masking. The format of end-time is: month-day-year hour:minute:second.
	Raisecom(config)#alarm inhibit time [range] slot <i>slot-list</i> [alarm-id <i>alarm-id</i>] [interval <i>interval</i>] [start <i>start-time</i> every time stop <i>end-time</i>] example: Raisecom(config)#alarm inhibit time range slot 1	Configure timed alarm masking on the alarm source of the OLT slots. If you do not configure the alarm-id <i>alarm-id</i> parameter, it is believed that the alarm ID is not specified and all alarms generated in the OLT slots are masked. • slot: the alarm source is the slot. • alarm-id <i>alarm-id</i>: configure alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer. • interval <i>interval</i>: configure the interval of alarm masking. The interval is an integer ranging from 3600 to 86400, in units of second. If this parameter is not selected, the default alarm masking interval 3600 seconds will be used. • start-time <i>start-time</i>: configure the start time of alarm masking. The format of start-time is: month-day-year hour:minute:second • every time: interval from the end of the alarm masking to the start of the next alarm masking, an integer, ranging from 3600 to 86400, in units of second • end-time <i>end-time</i>: configure the end time of alarm masking. The format of end-time is: month-day-year hour:minute:second.

Step	Command	Description
	<pre>Raisecom(config)#alarm inhibit time [range] interface { gigabitethernet ten-gigabitethernet epon-olt ten-giga-epon-olt gpon-olt } slot- id/port-id [alarm-id alarm-id] [interval interval] [start start- time every time stop end-time]</pre> example: <pre>Raisecom(config)#alarm inhibit time interface gigabitethernet 3/1</pre>	Configure timed alarm masking on the alarm source of the OLT interfaces. If you do not configure the alarm-id <i>alarm-id</i> parameter, it is believed that the alarm ID is not specified and all alarms generated on the OLT interfaces are masked. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode • slot-id: slot ID • port-id: interface ID • alarm-id alarm-id: configure alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer. • interval interval: configure the interval of alarm masking. The interval is an integer ranging from 3600 to 86400, in units of second. If this parameter is not selected, the default alarm masking interval 3600 seconds will be used. • start-time start-time: configure the start time of alarm masking. The format of start-time is: month-day-year hour:minute:second • every time: interval from the end of the alarm masking to the start of the next alarm masking, an integer, ranging from 3600 to 86400, in units of second • end-time end-time: configure the end time of alarm masking. The format of end-time is: month-day-year hour:minute:second.

Step	Command	Description
	Raisecom(config)#alarm inhibit time [range] interface epon-onu slot- id/olt-id/onu-id [alarm-id alarm- id] [interval interval] [start start-time every time stop end-time] example: Raisecom(config)#alarm inhibit time interface epon-onu 3/1/1	Configure timing alarm masking with the alarm source being the ONU. If the alarm-id alarm-id parameter is not configured, it indicates that there is no limit on the alarm ID and all alarms with the ONU ID as the source will be masked. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • alarm-id alarm-id: configure alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer. • interval interval: configure the interval of alarm masking. The interval is an integer ranging from 3600 to 86400, in units of second. If this parameter is not selected, the default alarm masking interval 3600 seconds will be used. • start-time start-time: configure the start time of alarm masking. The format of start-time is: month-day-year hour:minute:second • every time: interval from the end of the alarm masking to the start of the next alarm masking, an integer, ranging from 3600 to 86400, in units of second • end-time end-time: configure the end time of alarm masking. The format of end-time is: month-day-year hour:minute:second.

Step	Command	Description
	<pre>Raisecom(config)#alarm inhibit time interface epon-onu slot-id/olt- id/onu-id [range] uni uni-id [alarm-id alarm-id] [interval interval] [start start-time every time stop end-time]</pre> example: <pre>Raisecom(config)#alarm inhibit time interface epon-onu 3/1/1 uni 1</pre>	Configure timed alarm masking with the alarm source of ONU UNI. If the alarm-id <i>alarm-id</i> is not configured, the alarm ID is not restricted. As long as the source is the ONU UNI ID, all alarms are masked. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • uni-id: ONU Ethernet interface ID • alarm-id alarm-id: configure alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer. • interval interval: configure the interval of alarm masking. The interval is an integer ranging from 3600 to 86400, in units of second. If this parameter is not selected, the default alarm masking interval 3600 seconds will be used. • start-time start-time: configure the start time of alarm masking. The format of start-time is: month-day-year hour:minute:second • every time: interval from the end of the alarm masking to the start of the next alarm masking, an integer, ranging from 3600 to 86400, in units of second • end-time end-time: configure the end time of alarm masking. The format of end-time is: month-day-year hour:minute:second.

Step	Command	Description
5	<pre>Raisecom(config)#alarm inhibit time { dev slot port onu uni } alarm-id alarm-id [interval interval] [start start-time every time stop end-time]</pre> example: <pre>Raisecom(config)#alarm inhibit time dev alarm-id 1</pre>	Configure timed alarm masking based on alarm ID. • dev: the alarm source is the device. • slot: the alarm source is the slot. • olt: the alarm source is the device interface. • onu: the alarm source is the ONU connected downstream to the device. • uni: the alarm source is the Ethernet interface of the ONU. • alarm-id alarm-id: configure alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer. • interval interval: configure the interval of alarm masking. The interval is an integer ranging from 3600 to 86400, in units of second. If this parameter is not selected, the default alarm masking interval 3600 seconds will be used. • start-time start-time: configure the start time of alarm masking. The format of start-time is: month-day-year hour:minute:second • every time: interval from the end of the alarm masking to the start of the next alarm masking, an integer, ranging from 3600 to 86400, in units of second • end-time end-time: configure the end time of alarm masking. The format of end-time is: month-day-year hour:minute:second.
6	<pre>Raisecom(config)#alarm inhibit interval time</pre> example: <pre>Raisecom(config)#alarm inhibit interval 7200</pre>	(Optional) configure the interval of timed alarm masking. • second: default interval of alarm masking, an integer, ranging from 3600 to 86400, in units of second.

Configuring alarm filtering

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#alarm filter dev [alarm-id alarm-id]</pre> example: <pre>Raisecom(config)#alarm filter dev alarm-id 1</pre>	Configure alarm filtering on the alarm source of the whole device. If you do not configure the alarm-id alarm-id parameter, it is believed that the alarm ID is not specified and all alarms generated on the whole device are filtered. • alarm-id alarm-id: configure alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer.

Step	Command	Description
3	Raisecom(config)#alarm filter [range] slot <i>slot-list</i> [alarm-id <i>alarm-id</i>] example: Raisecom(config)#alarm filter slot 1	Configure alarm filtering on the alarm source of the OLT slots. If you do not configure the alarm-id <i>alarm-id</i> parameter, it is believed that the alarm ID is not specified and all alarms generated in the OLT slots are filtered. • slot: the alarm source is the slot. • alarm-id alarm-id: configure alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer.
4	Raisecom(config)#alarm filter [range] interface { gigabitethernet ten-gigabitethernet epon-olt ten-giga-epon-olt gpon-olt } <i>slot-id/port-id</i> [alarm-id <i>alarm-id</i>] example: Raisecom(config)#alarm filter interface gigabitethernet 3/1	Configure alarm filtering on the alarm source of the OLT interfaces. If you do not configure the alarm-id <i>alarm-id</i> parameter, it is believed that the alarm ID is not specified and all alarms generated on the OLT interfaces are filtered. • alarm-id alarm-id: configure alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode • slot-id: slot ID • port-id: interface ID
5	Raisecom(config)#alarm filter [range] interface epon-onu <i>slot-id/olt-id/onu-id</i> [alarm-id <i>alarm-id</i>] example:	Configure alarm filtering with the alarm source being the ONU interface. If the alarm-id <i>alarm-id</i> parameter is not configured, it indicates that there is no limit on the alarm ID and all alarms with the ONU ID as the source will be masked. • alarm-id alarm-id: configure alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface

Step	Command	Description
6	<pre>Raisecom(config)#alarm filter interface epon-onu slot-id/olt- id/onu-id [range] uni uni-id [alarm-id alarm-id] example:</pre>	Configure alarm filtering with the alarm source of ONU UNI. If the alarm-id <i>alarm-id</i> parameter is not configured, it indicates that there is no limit on the alarm ID and all alarms with the ONU ID as the source will be masked. • alarm-id alarm-id: configure alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • uni-id: ONU Ethernet interface ID
7	<pre>Raisecom(config)#alarm filter { dev slot port onu uni } alarm-id alarm-id example: Raisecom(config)#alarm filter dev alarm-id 1</pre>	Configure alarm filtering based on the alarm ID. • alarm-id alarm-id: configure alarm filtering based on alarm type. The alarm-id refers to the alarm type, which is an integer. • dev: the alarm source is the device. • slot: the alarm source is the slot. • olt: the alarm source is the device interface. • onu: the alarm source is the ONU connected downstream to the device. • uni: the alarm source is the Ethernet interface of the ONU.

16.13.3 Configuring event management

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#event traps enable	Enable event Traps.
3	<pre>Raisecom(config)#event inhibit dev [event-id event-id] example: Raisecom(config)#event inhibit dev</pre>	Configure event masking on the event source of the whole device. If you do not configure the event-id <i>event-id</i> parameter, it is believed that the event ID is not specified and all events generated on the whole device are masked. • event-id event-id: configure alarm filtering based on alarm type. The event-id refers to the alarm type, which is an integer.

Step	Command	Description
4	<pre>Raisecom(config)#event inhibit [range] slot slot-list [event-id event-id] example: Raisecom(config)#event inhibit range slot 1</pre>	Configure event masking on the event source of the OLT slots. If you do not configure the event-id event-id parameter, it is believed that the event ID is not specified and all events generated in the OLT slots will be masked. • slot-list: slot ID list • event-id event-id: configure alarm filtering based on alarm type. The event-id refers to the alarm type, which is an integer.
5	<pre>Raisecom(config)#event inhibit [range] interface { gigabitethernet ten- gigabitethernet epon-olt ten- giga-epon-olt gpon-olt } slot- id/port-id [event-id event-id] example: Raisecom(config)#event inhibit interface gigabitethernet 3/1</pre>	Configure event masking on the event source of the OLT interfaces. If you do not configure the event-id event-id parameter, it is believed that the event ID is not specified and all events generated on the OLT interfaces are masked. • event-id event-id: configure alarm filtering based on alarm type. The event-id refers to the alarm type, which is an integer. • epon-olt: EPON interface configuration mode • ten-giga-epon-olt: 10G EPON interface configuration mode • gpon-olt: GPON interface configuration mode • gigabitethernet: GE interface configuration mode • ten-gigabitethernet: 10GE interface configuration mode • slot-id: slot ID • port-id: interface ID
6	<pre>Raisecom(config)#event inhibit [range] interface epon-onu slot- id/olt-id/onu-id [event-id event-id] example: Raisecom(config)#event inhibit range interface epon-onu 3/1/1</pre>	Configure alarm masking with the alarm source being the ONU interface. If the event-id event-id parameter is not configured, it indicates that there is no limit on the alarm ID and all alarms with the ONU ID as the source will be masked. • event-id event-id: configure alarm filtering based on alarm type. The event-id refers to the alarm type, which is an integer. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface

Step	Command	Description
7	<pre>Raisecom(config)#event inhibit interface epon-onu slot-id/olt-id/onu-id [range] uni uni-id [event-id event-id] example: Raisecom(config)#event inhibit interface epon-onu 3/1/1 range uni 1</pre>	Configure event masking with the event source of ONU UNI. If the event-id event-id parameter is not configured, it indicates that there is no limit on the alarm ID and all alarms with the ONU ID as the source will be masked. • event-id event-id: configure alarm filtering based on alarm type. The event-id refers to the alarm type, which is an integer. • slot-id: slot ID • olt-id: PON interface ID • onu-id: ONU ID under the PON interface • uni-id: ONU Ethernet interface ID
8	<pre>Raisecom(config)#event inhibit { dev slot port onu uni } event-id event-id example: Raisecom(config)#event inhibit slot event-id 2</pre>	Configure event masking based on event ID. • event-id event-id: configure alarm filtering based on alarm type. The event-id refers to the alarm type, which is an integer. • dev: the alarm source is the device. • slot: the alarm source is the slot. • olt: the alarm source is the device interface. • onu: the alarm source is the ONU connected downstream to the device. • uni: the alarm source is the Ethernet interface of the ONU.

16.13.4 Checking configurations

No.	Command	Description
1	Raisecom#show alarm inhibit	Show alarm masking configurations.
2	Raisecom#show alarm filter	Show alarm filtering configurations.
3	Raisecom#show alarm active-table slot slot-id [detail]	Show the alarm table in the current slot according to the alarm source, alarm type, or alarm generation time.
4	Raisecom#show alarm active-table interface { gpon-olt slot-id/olt-id gpon-onu slot-id/olt-id/onu-id } [detail]	Show GPON current alarm lists.
5	Raisecom#show alarm clear-table interface { gpon-olt slot-id/olt-id gpon-onu slot-id/olt-id/onu-id }	Show current CPON alarm clearing lists of the system.
6	Raisecom#show alarm alarm-id alarm-id	Show alarm details.

No.	Command	Description
7	Raisecom#show event inhibit	Show event masking configurations of alarm management.
8	Raisecom#show event history-table [slot slot-id onu slot-id/olt-id/onu-id port slot-id/port-id dev event-id event-id start_time start-time end_time end-time] [detail]	Show history event table, which can be checked based on event source, event type, and event occurrence time.
9	Raisecom#show event event-id event-id	Show details of the alarm event.

16.14 Maintenance

No.	Command	Description
1	Raisecom(config)#clear logging history	Clear logging records in the log buffer.

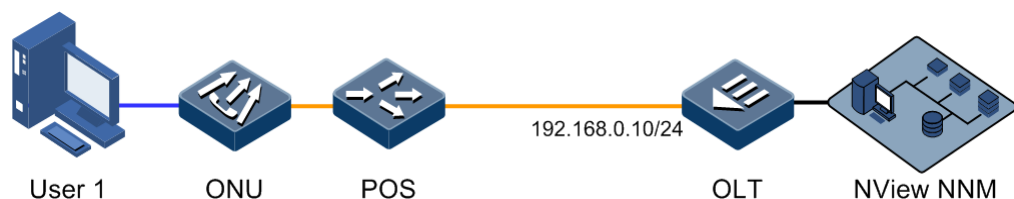
16.15 Configuration examples

16.15.1 Example for configuring SNMP

Networking requirements

As shown in Figure 16-5, the IP address of the OLT is 192.168.0.10. User 1 adopts the md5 authentication algorithm (the authentication password is raisecom) to access mib2 view with all MIB variables under 1.3.6.1.2.1. Create the access group of the guestgroup with the security mode of USM, the security level as authentication without encryption, and the readable view name is mib2. Complete mapping from User 1 with the security level of USM to the guestgroup, and show the results.

Figure 16-5 SNMPv3 networking



Configuration steps

Step 1 Configure the IP address.

```
Raisecom(config)#interface vlanif 10
Raisecom(config-vlanif-10)#ip address 192.168.0.10 10
Raisecom(config-vlanif-10)#exit
```

Step 2 Configure the view and its OID tree range.

```
Raisecom(config)#snmp-server view mib2 1.3.6.1.2.1 1.1.1.1.0.1 included
```

Step 3 Configure the SNMP user.

```
Raisecom(config)#snmp-server user guestuser1 authentication md5 raisecom
```

Step 4 Configure the SNMP access group.

```
Raisecom(config)#snmp-server access guestgroup read mib2 usm authnopriv
```

Step 5 Configure users belonging to a specified access group.

```
Raisecom(config)#snmp-server group guestgroup user user1 usm
```

Checking results

Show names and attributes of all access groups.

```
Raisecom#show snmp access
Index      :0
Group      :initial
Security Model :usm
Security Level :authnopriv
Context Prefix :--
Context Match :exact
Read View    :internet
Write View    :internet
Notify View   :internet

Index      :1
```

```

Group      :guestgroup
Security Model :usm
Security Level :authnopriv
Context Prefix :--
Context Match :exact
Read View   :mib2
Write View   :--
Notify View  :internet

Index      :2
Group      :initialnone
Security Model :usm
Security Level :noauthnopriv
Context Prefix :--
Context Match :exact
Read View   :system
Write View   :--
Notify View  :internet

```

Show mapping between all access groups and their names.

Raisecom#**show snmp group**

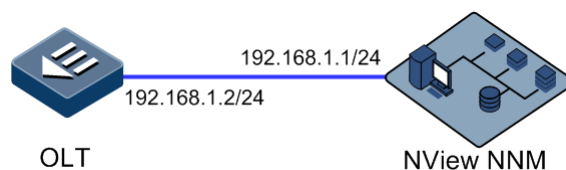
Index	UserName	SecModel	GroupName
0	none	usm	initialnone
1	user1	usm	guestgroup
2	md5nopriv	usm	initial
3	shanopriv	usm	initial

16.15.2 Example for configuring KeepAlive Trap

Networking requirements

The IP address of the OLT is 192.168.1.2, the target host address of the SNMP v2c Trap is 192.168.1.1, the read and write community name is public, and the SNMP version is v2c. Configure the interval for the OLT to send KeepAlive Trap to the SNMP network management station to 120s, and enable KeepAlive Trap.

Figure 16-6 KeepAlive networking



Configuration steps

Step 1 Configure the management IP address of the OLT.

```
Raisecom#config
Raisecom(config)#interface vlanif 1
Raisecom(config-vlanif-1)#ip address 192.168.1.2 255.255.255.0
Raisecom(config-vlanif-1)#exit
```

Step 2 Configure the Trap destination host IP address of SNMP.

```
Raisecom(config)#snmp-server host 192.168.1.1 version 2c public
```

Step 3 Configure KeepAlive Trap.

```
Raisecom(config)#snmp-server keepalive-trap enable
Raisecom(config)#snmp-server keepalive-trap interval 120
```

Checking results

Use the **show keepalive** command to check KeepAlive basic configurations.

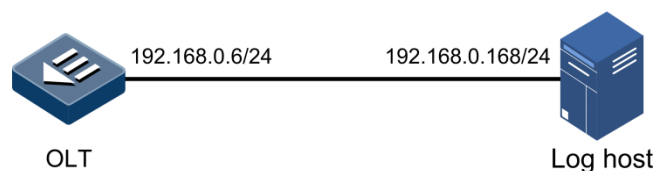
```
Raisecom#show keepalive
Keepalive Admin State:Enable
Keepalive trap interval:120s
Keepalive trap count:1
```

16.15.3 Example for outputting system log to host

Networking requirements

As shown in Figure 16-7, to output log information to the log host for the convenience of users to check it at any time, configure the system log function.

Figure 16-7 Outputting system log to host



Configuration steps

Step 1 Configure the IP address of the OLT.

```
Raisecom#config
```

```
Raisecom(config)#interface vlanif 1
Raisecom(config-vlanif-1)#ip address 192.168.0.6 255.255.255.0 1
Raisecom(config-vlanif-1)#exit
```

Step 2 Configure outputting system log to the log host.

```
Raisecom(config)#logging on
Raisecom(config)#logging time-stamp relative-start
Raisecom(config)#logging rate 10
Raisecom(config)#logging host 1 ip address 192.168.0.168 facility local0
severity warnings
```

Checking results

Use the **show logging** command to show system log configurations.

```
Raisecom#show logging
Syslog logging : Enable
Rate-limited : 10 messages per second
Logging time-stamp : Relative time-stamp
Console logging : Enable
Console severity : Notifications
Monitor logging : Disable
Monitor severity : Informational
History logging : Enable
History severity : Debugging
File logging : Disable
File severity : Informational
```

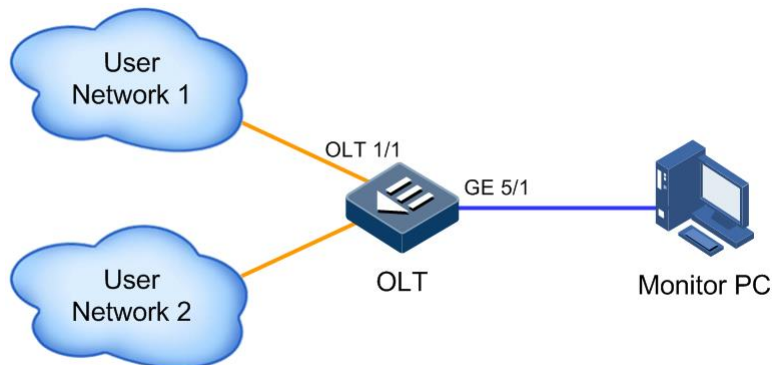
16.15.4 Example for configuring OLT port mirroring

Networking requirements

The network administrator hopes to monitor the packets of the OLT and the user network 1 through the data monitoring equipment, so as to capture the packet flow when a fault or abnormality occurs, to analyze and find the root cause of the problem and solve it in time.

Among them, the user network 1 is connected to the OLT through the port OLT 1/1, and the data monitoring equipment is connected to the port GE 5/1 of the OLT. The network administrator needs to capture all the upstream and downstream data of the OLT 1/1.

Figure 16-8 OLT local port mirroring



Configuration steps

Step 1 Enable OLT local port mirroring.

```
Raisecom#config  
Raisecom(config)#mirror enable
```

Step 2 Configure the mirroring source port.

```
Raisecom(config)#interface epon-olt 1/1  
Raisecom(config-if-epon-olt-1:1)#mirror source-port both  
Raisecom(config-if-epon-olt-1:1)#exit
```

Step 3 Configure the monitoring port.

```
Raisecom(config)#interface gigabitethernet 5/1  
Raisecom(config-if-gigabitethernet-5:1)#mirror monitor-port
```

Checking results

Use the **show mirror** command to check system log configurations.

```
Raisecom#show mirror  
Mirror: Enable  
Local monitor port: gigabitethernet5/1  
Source Port ID          Direction  
-----  
epon-olt1/1             both
```

17

Ring network protection

This chapter describes basic principles and configuration procedures for ring network protection, including the following section:

- G.8032 overview
- Configuring G.8032
- Configuration examples

17.1 G.8032 overview

G.8032 Ethernet Ring Protection Switching (ERPS) is an APS protocol based on the ITU-T G.8032 recommendation. It is a link-layer protocol specially used in Ethernet rings. Generally, ERPS can avoid broadcast storm caused by data loopback in Ethernet rings. When a link/device on the Ethernet ring fails, traffic can be quickly switched to the backup link to ensure restoring services quickly.

G.8032 uses the control VLAN on the ring network to transmit ring network control information. Meanwhile, combining with the topology feature of the ring network, it discovers network fault quickly and enables the backup link to restore service fast.

17.2 Configuring G.8032

17.2.1 Preparing for configurations

Scenario

With development of Ethernet to telecom-grade network, voice and video multicast services bring higher requirements on Ethernet redundant protection and fault-recovery time. The fault-recovery time of current STP system is in second level that cannot meet requirements.

By defining different roles for nodes on a ring, G.8032 can block a loopback to avoid broadcast storm in normal condition. Therefore, the traffic can be quickly switched to the protection line when working lines or nodes on the ring fail. This helps eliminate the loop, perform protection switching, and automatically recover from faults. In addition, the switching time is shorter than 50ms.

The ISCOM600 and ISCOM6860 support the single ring, intersecting ring, and tangent ring.

G.8032 provides a mode for detecting faults based on physical interface status. The ISCOM600 and ISCOM6860 learn link fault quickly and switches services immediately, so this mode is suitable for detecting the fault between neighboring devices.

Prerequisite

- Connect the interface.
- Configure its physical parameters to make it Up.
- Create VLANs.
- Add interfaces to VLANs.

17.2.2 Default configurations of G.8032

Function	Default value
Protocol VLAN	1
Protection ring mode	Revertive
Ring WTR timer	6min
Ring protocol version	2
Guard timer	500ms
Ring Hold-off timer	0ms
Trap	Disable
Tributary ring virtual channel mode in intersecting node	With
Ring Propagate switch in crossing node	Disable

17.2.3 Creating G.8032 ring



Caution

- Only one device on the protection ring can be configured to the Ring Protection Link (RPL) Owner and one device is configured to the RPL neighbor. Other devices are configured to ring forwarding nodes.
- The tangent ring consists of 2 independent single rings. Configurations on the tangent ring are identical to the ones on the common single ring. The intersecting ring consists of a primary ring and a tributary ring. Configurations on the primary ring are identical to the ones on the common single ring. For detailed configurations of the tributary ring, see section 17.2.5 (Optional) creating G.8032 tributary ring.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#ethernet ring- protection ring-id east interface { interface-type interface-number port-channel port-channel-number } west interface { interface-type interface-number port-channel port- channel-number } [node-type rpl-owner rpl { east west }] [not- revertive] [protocol-vlan vlan-id] [block-vlanlist vlan-list] example: Raisecom(config)#ethernet ring- protection 1 east interface ten- gigabitethernet 1/1/1 west interface ten-gigabitethernet 1/1/2 node-type rpl-owner rpl east</pre>	Create a ring and configure the node to RPL Owner.  Note The eastbound interface and westbound interface cannot be the same one. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • east: eastbound interface • west: westbound interface • gigabitethernet slot-id/port-id: GE interface ID. The slot-id refers to the slot ID, which is an integer. The port-id refers to the PON interface ID, which is an integer. • ten-gigabitethernet slot-id/port-id: 10GE interface ID. The slot-id refers to the slot ID, which is an integer. The port-id refers to the PON interface ID, which is an integer. • port-channel port-channel-number: aggregation group ID, an integer, ranging from 1 to 32 • rpl-owner: the node type is RPL Owner, located at one end of RPS. It is in interface blocking state when the link is normal. When a fault occurs, it will transition to active state automatically. • not-revertive: the protection ring transitions to non-revertive mode. When the link is recovering from fault, the traffic will be switched from the protection link to the working link if the device is in revertive mode; the traffic will not be switched if the device is in non-revertive mode; if the parameter is not configured, the device is in revertive mode by default. • protocol-vlan: protocol VLAN, used for transmitting ERPS packets. The vlan-id refers to the VLAN ID, which is an integer, ranging from 1 to 4094. • block-vlanlist: blocked VLAN list • vlan-list: VLAN ID list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

Step	Command	Description
	<pre> Raisecom(config)#ethernet ring- protection <i>ring-id</i> east interface { <i>interface-type interface-number</i> port-channel <i>port-channel-number</i> } west interface { <i>interface-type</i> <i>interface-number</i> port-channel <i>port- channel-number</i> } node-type rpl- neighbour rpl { east west } [not- revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-list</i>] example: Raisecom(config)#ethernet ring- protection 1 east interface ten- gigabitethernet 1/1/1 west interface ten-gigabitethernet 1/1/2 node-type rpl-neighbour rpl east </pre>	Create a ring and configure the node to RPL Neighbour. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • east: eastbound interface • west: westbound interface • gigabitethernet slot-id/port-id: GE interface ID. The slot-id refers to the slot ID, which is an integer. The port-id refers to the PON interface ID, which is an integer. • ten-gigabitethernet slot-id/port-id: 10GE interface ID. The slot-id refers to the slot ID, which is an integer. The port-id refers to the PON interface ID, which is an integer. • port-channel port-channel-number: aggregation group ID, an integer, ranging from 1 to 32 • rpl-owner: the node type is RPL Owner, located at one end of RPS. It is in interface blocking state when the link is normal. When a fault occurs, it will transition to active state automatically. • not-revertive: the protection ring transitions to non-revertive mode. When the link is recovering from fault, the traffic will be switched from the protection link to the working link if the device is in revertive mode; the traffic will not be switched if the device is in non-revertive mode; if the parameter is not configured, the device is in revertive mode by default. • protocol-vlan: protocol VLAN, used for transmitting ERPS packets. The vlan-id refers to the VLAN ID, which is an integer, ranging from 1 to 4094. • block-vlanlist: blocked VLAN list • vlan-list: VLAN ID list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

Step	Command	Description
	<pre>Raisecom(config)#ethernet ring- protection ring-id east interface { interface-type interface-number port-channel port-channel-number } west interface { interface-type interface-number port-channel port- channel-number } [not-revertive] [protocol-vlan vlan-id] [block- vlanlist vlan-list] example: Raisecom(config)#ethernet ring- protection 1 east interface ten- gigabitethernet 1/1/1 west interface ten-gigabitethernet 1/1/2 node-type rpl east</pre>	Create a ring and configure the node to a transit node. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • east: eastbound interface • west: westbound interface • gigabitethernet slot-id/port-id: GE interface ID. The slot-id refers to the slot ID, which is an integer. The port-id refers to the PON interface ID, which is an integer. • ten-gigabitethernet slot-id/port-id: 10GE interface ID. The slot-id refers to the slot ID, which is an integer. The port-id refers to the PON interface ID, which is an integer. • port-channel port-channel-number: aggregation group ID, an integer, ranging from 1 to 32 • not-revertive: the protection ring transitions to non-revertive mode. When the link is recovering from fault, the traffic will be switched from the protection link to the working link if the device is in revertive mode; the traffic will not be switched if the device is in non-revertive mode; if the parameter is not configured, the device is in revertive mode by default. • protocol-vlan: protocol VLAN, used for transmitting ERPS packets. The vlan-id refers to the VLAN ID, which is an integer, ranging from 1 to 4094. • block-vlanlist: blocked VLAN list • vlan-list: VLAN ID list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
3	<pre>Raisecom(config)#ethernet ring- protection ring-id name string example: Raisecom(config)#ethernet ring- protection 1 name Raisecom</pre>	(Optional) configure a name for the protection ring. Up to 32 bytes are available. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • string: protection ring name, a string of 1 to 32 characters

Step	Command	Description
4	Raisecom(config)#ethernet ring-protection ring-id version { 1 2 } example: Raisecom(config)#ethernet ring-protection 1 version 2	(Optional) configure the protocol version. The protocol version of all nodes on a protection ring should be identical. In protocol version 1, protection rings are distinguished based on the protocol VLAN. Therefore, you need to configure different protocol VLANs for protection rings. We recommend configuring different protocol VLANs for protection rings even if protocol version 2 is used. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • 1: protocol version1 • 2: protocol version2
5	Raisecom(config)#ethernet ring-protection ring-id guard-time guard-time example: Raisecom(config)#ethernet ring-protection 1 guard-time 1000	(Optional) after the ring Guard timer is configured, the failed node does not process APS packets during a period. In a bigger ring network, if the failed node recovers from a fault immediately, it may receive the fault notification sent by the neighbor node on the protection ring. Therefore, the node is in Down status again. You can configure the ring Guard timer to solve this problem. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • guard-time: value of the guard timer, an integer, ranging from 20 to 2000, in units of millisecond
6	Raisecom(config)#ethernet ring-protection ring-id wtr-time wtr-time example: Raisecom(config)#ethernet ring-protection 1 wtr-time 10	(Optional) configure the ring WTR timer. In revertive mode, when the working line recovers from a fault, traffic is not switched to the working line unless the WTR timer times out. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • wtr-time: value of the WTR timer, an integer, ranging from 1 to 12, in units of second
7	Raisecom(config)# ethernet ring-protection ring-id wtb-time wtb-time example: Raisecom(config)#ethernet ring-protection 1 wtb-time 10	(Optional) configure the WTB timer. You can use the no form of this command to restore default conditions. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • wtr-time: value of the WTR timer, an integer, ranging from 1 to 12, in units of second

Step	Command	Description
8	Raisecom(config)#ethernet ring-protection ring-id holdoff-time holdoff-time example: Raisecom(config)#ethernet ring-protection 1 holdoff-time 1	(Optional) configure the ring Hold-off timer. After the Hold-off timer is configured, when the working line fails, the system will delay processing the fault. It means that traffic is delayed to be switched to the protection line. This helps prevent frequent switching caused by working line vibration.  Note If the ring Hold-off timer value is too great, it may influence 50ms switching performance. Therefore, we recommend configuring the ring Hold-off timer value to 0. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • holdoff-time: value of the Holdoff timer, an integer, ranging from 0 to 100, in units of 100ms

17.2.4 Enabling Trap

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ethernet ring-protection trap { enable disable }	Enable G.8032 Trap.

17.2.5 (Optional) creating G.8032 tributary ring



Caution

- Only the intersecting ring consists of a primary ring and a tributary ring.
- Configurations of the primary ring are identical to those of the single/tangent ring. For details, see section 17.2.3 Creating G.8032 ring.
- For the intersecting ring, configure its primary ring and then the tributary ring. Otherwise, the tributary ring will fail to find the interface of the primary ring, thus failing to establish the virtual channel of the tributary ring.
- The ID of the tributary ring must be greater than that of the primary ring.
- Configurations of non-intersecting nodes of the intersecting ring are identical to those of the single/tangent ring. For details, see section 17.2.3 Creating G.8032 ring.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#ethernet ring- protection ring-id { east west } interface { interface-type interface- number port-channel port-channel- number } node-type rpl-owner [not- revertive] [protocol-vlan vlan-id] [block-vlanlist vlan-list] example: Raisecom(config)#ethernet port-channel 1 east interface ten-gigabitethernet 19/1 node-type rpl-owner</pre>	Create a tributary ring on the intersecting node and configure the intersecting node as the RPL Owner. If not-revertive is configured, the protection ring transitions to non-revertive mode. When the link is recovering from fault, the traffic will be switched from the protection link to the working link if the device is in revertive mode; the traffic will not be switched if the device is in non-revertive mode. The protection ring is in revertive mode by default.  Note The link between two intersecting nodes of the intersecting ring belongs to the primary ring. Therefore, when configuring a tributary ring on the intersecting node, you can only configure one of the eastbound interface or westbound interface. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • east: eastbound interface • west: westbound interface • gigabitethernet slot-id/port-id: GE port ID. The slot-id refers to the slot ID, which is an integer. The port-id refers to the PON interface ID, which is an integer. • ten-gigabitethernet slot-id/port-id: 10GE port ID. The slot-id refers to the slot ID, which is an integer. The port-id refers to the PON interface ID, which is an integer. • port-channel port-channel-number: aggregation group ID, an integer, ranging from 1 to 32 • not-revertive: the protection ring transitions to non-revertive mode. When the link is recovering from fault, the traffic will be switched from the protection link to the working link if the device is in revertive mode; the traffic will not be switched if the device is in non-revertive mode; if the parameter is not configured, the device is in revertive mode by default. • protocol-vlan: protocol VLAN, used for transmitting ERPS packets. The vlan-id refers to the VLAN ID, which is an integer, ranging from 1 to 4094. • block-vlanlist: blocked VLAN list • vlan-list: VLAN ID list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

Step	Command	Description
	<pre>Raisecom(config)#ethernet ring- protection ring-id { east west } interface { interface-type interface- number port-channel port-channel- number } node-type rpl-neighbour [not-revertive] [protocol-vlan vlan-id] [block-vlanlist vlan-list] example: Raisecom(config)#ethernet ring- protection 1 east interface port- channel 1 node-type rpl-neighbour</pre>	Create a tributary ring on the intersecting node and configure the node as the RPL Neighbour. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • east: eastbound interface • west: westbound interface • gigabitethernet slot-id/port-id: GE interface ID. The slot-id refers to the slot ID, which is an integer. The port-id refers to the PON interface ID, which is an integer. • ten-gigabitethernet slot-id/port-id: 10GE interface ID. The slot-id refers to the slot ID, which is an integer. The port-id refers to the PON interface ID, which is an integer. • port-channel port-channel-number: aggregation group ID, an integer, ranging from 1 to 32 • not-revertive: the protection ring transitions to non-revertive mode. When the link is recovering from fault, the traffic will be switched from the protection link to the working link if the device is in revertive mode; the traffic will not be switched if the device is in non-revertive mode; if the parameter is not configured, the device is in revertive mode by default. • protocol-vlan: protocol VLAN, used for transmitting ERPS packets. The vlan-id refers to the VLAN ID, which is an integer, ranging from 1 to 4094. • block-vlanlist: blocked VLAN list • vlan-list: VLAN ID list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

Step	Command	Description
	<pre>Raisecom(config)#ethernet ring- protection ring-id { east west } interface { interface-type interface- number port-channel port-channel- number } [not-revertive] [protocol- vlan vlan-id] [block-vlanlist vlan- list]</pre> example: Raisecom(config)#ethernet ring- protection 1 west interface port- channel 2	Create a tributary ring on the intersecting node and configure the node as the ring forwarding node. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • east: eastbound interface • west: westbound interface • gigabitethernet slot-id/port-id: GE interface ID. The slot-id refers to the slot ID, which is an integer. The port-id refers to the PON interface ID, which is an integer. • ten-gigabitethernet slot-id/port-id: 10GE interface ID. The slot-id refers to the slot ID, which is an integer. The port-id refers to the PON interface ID, which is an integer. • port-channel port-channel-number: aggregation group ID, an integer, ranging from 1 to 32 • not-revertive: the protection ring transitions to non-revertive mode. When the link is recovering from fault, the traffic will be switched from the protection link to the working link if the device is in revertive mode; the traffic will not be switched if the device is in non-revertive mode; if the parameter is not configured, the device is in revertive mode by default. • protocol-vlan: protocol VLAN, used for transmitting ERPS packets. The vlan-id refers to the VLAN ID, which is an integer, ranging from 1 to 4094. • block-vlanlist: blocked VLAN list • vlan-list: VLAN ID list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

Step	Command	Description
3	Raisecom(config)#ethernet ring-protection <i>ring-id</i> raps-vc { with without } example: Raisecom(config)#ethernet ring-protection 1 raps-vc without	(Optional) configure the tributary ring virtual channel mode on the intersecting node. Because the link between the intersecting nodes belongs to the primary ring, the transmission mode of the protocol packets in the tributary ring is different from that of the primary ring, and can be divided into the with and without modes: • With: the primary ring provides a path for the tributary ring APS packets. The tributary ring intersecting node receives the tributary ring APS packets and sends them to the primary ring. The primary ring completes the communication between the tributary ring intersecting nodes. • Without: the tributary ring APS packets on the intersecting node are terminated and will not be transmitted to the primary ring. This mode requires that the tributary ring cannot block the tributary ring protocol VLAN (to ensure that tributary ring packets can pass through the Owner). By default, the virtual channel of the tributary ring adopts the with mode. Transmission modes on 2 intersecting nodes must be identical. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • with: adopt with mode. • without: adopt without mode.
4	Raisecom(config)#ethernet ring-protection <i>ring-id</i> propagate enable example: Raisecom(config)#ethernet ring-protection 1 propagate enable	Enable the ring Propagate switch on the intersecting node. Because data of the tributary ring needs to be transmitted through the primary ring, there is a MAC address table of the tributary ring on the primary ring. When the tributary ring fails, it needs to use the Propagate switch to inform the primary ring of refreshing the MAC address table to avoid traffic loss. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255

17.2.6 (Optional) configuring G.8032 switching control

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#ethernet ring- protection <i>ring-id</i> force-switch { east west }</pre> example: <pre>Raisecom(config)#ethernet ring- protection 1 force-switch east</pre>	Switch the traffic on the protection ring to the west/east interface forcibly. FS can be configured on multiple interfaces of multiple ring nodes. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • east: block the eastbound interface and forcibly switch traffic to the westbound interface. • west: block the westbound interface and forcibly switch traffic to the eastbound interface.
3	<pre>Raisecom(config)#ethernet ring- protection <i>ring-id</i> manual-switch { east west }</pre> example: <pre>Raisecom(config)#ethernet ring- protection 1 manual-switch west</pre>	Switch the traffic on the protection ring to the west/east interface manually. Its priority is lower than the one of FS and APS. MS can be configured on one interface of a ring node. • ring-id: Ethernet ring ID, an integer, ranging from 1 to 255 • east: block the eastbound interface and forcibly switch traffic to the westbound interface. • west: block the westbound interface and forcibly switch traffic to the eastbound interface.



Note

By default, traffic is automatically switched to the protection line when the working line fails. Therefore, you need to configure ERPS control in some special cases.

17.2.7 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show ethernet ring-protection [<i>ring-id</i>]</pre>	Show configurations of the G.8032 ring.
2	<pre>Raisecom#show ethernet ring-protection [<i>ring-id</i>]status</pre>	Show G.8032 ring status.
3	<pre>Raisecom#show ethernet ring-protection [<i>ring-id</i>] statistics</pre>	Show G.8032 ring statistics.

17.2.8 Maintenance

Command	Description
Raisecom(config)#clear ethernet ring-protection ring-id statistics example: Raisecom(config)#clear ethernet ring-protection 1 statistics	Clear statistics about the protection ring. ring-id: Ethernet ring ID, an integer, ranging from 1 to 255
Raisecom(config)#clear ethernet ring-protection ring-id command example: Raisecom(config)#clear ethernet ring-protection 1 command	Clear ring switching control commands. ring-id: Ethernet ring ID, an integer, ranging from 1 to 255

17.3 Configuration examples

17.3.1 Example for configuring single-ring G.8032 protection

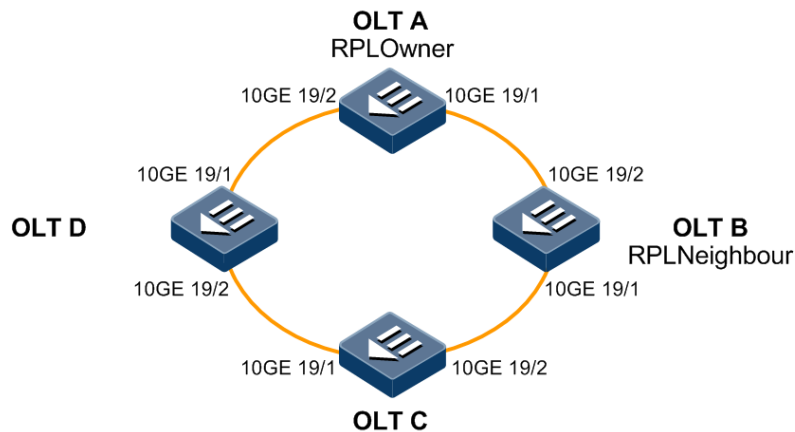
Networking requirements

As shown in Figure 17-1, to improve the reliability of the Ethernet, you can use OLT A, OLT B, OLT C, and OLT D to form a G.8032 single ring.

OLT A acts as the RPL Owner. OLT B acts as an RPL Neighbour. The RPL link between OLT A and OLT B is blocked.

The protocol VLAN is 1 by default. The blocked VLAN ranges from 1 to 4094.

Figure 17-1 Single ring G.8032 networking



Configuration steps

Step 1 Add interfaces to VLAN 1 to VLAN 4094.

Configure OLT A.

```
Raisecom#config
Raisecom(config)#interface ten-gigabitethernet 19/1
Raisecom(config-if-ten-gigabitethernet-19:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
Raisecom(config)#interface ten-gigabitethernet 19/2
Raisecom(config-if-ten-gigabitethernet-19:2)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:2)#exit
```

Configure OLT B.

```
Raisecom#config
Raisecom(config)#interface ten-gigabitethernet 19/1
Raisecom(config-if-ten-gigabitethernet-19:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
Raisecom(config)#interface ten-gigabitethernet 19/2
Raisecom(config-if-ten-gigabitethernet-19:2)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:2)#exit
```

Configure OLT C.

```
Raisecom#config
Raisecom(config)#interface ten-gigabitethernet 19/1
Raisecom(config-if-ten-gigabitethernet-19:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
Raisecom(config)#interface ten-gigabitethernet 19/2
Raisecom(config-if-ten-gigabitethernet-19:2)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:2)#exit
```

Configure OLT D.

```
Raisecom#config
Raisecom(config)#interface ten-gigabitethernet 19/1
Raisecom(config-if-ten-gigabitethernet-19:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
Raisecom(config)#interface ten-gigabitethernet 19/2
Raisecom(config-if-ten-gigabitethernet-19:2)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:2)#exit
```

Step 2 Create an ERPS protection ring.

Configure OLT A.

```
Raisecom(config)#ethernet ring-protection 1 east ten-gigabitethernet 19/1
west ten-gigabitethernet 19/2 node-type rpl-owner rpl east
```

Configure OLT B.

```
Raisecom(config)#ethernet ring-protection 1 east ten-gigabitethernet 19/1
west ten-gigabitethernet 19/2 node-type rpl-neighbour rpl west
```

Configure OLT C.

```
Raisecom(config)#ethernet ring-protection 1 east ten-gigabitethernet 19/1
west ten-gigabitethernet 19/2
```

Configure OLT D.

```
Raisecom(config)#ethernet ring-protection 1 east ten-gigabitethernet 19/1
west ten-gigabitethernet 19/2
```

Checking results

On the device, use the **show ethernet ring-protection status** command to check whether the G.8032 protection ring is effective.

Take OLT A as an example. The RPL link is blocked to prevent loops. After the WTR timer expires, the loop status is as below:

```
Raisecom#show ethernet ring-protection status
Id/Name          Bridge-State  Last Occur(ago)
SwitchTimes  East-State  west-State  Traffic-vlanlist
-----
1            Idle      0 days, 0: 0: 50: 750  2
Block        forward  1-4094
```

Manually disconnect the link between OLT B and OLT C to simulate a failure, use the command again on OLT A to view the status of the G.8032 protection ring, and switch the RPL link to the forwarding state.

```
Raisecom#show ethernet ring-protection status
```


Id/Name	Bridge-State		Last Occur(ago)
	SwitchTimes	East-State West-State Traffic-vlanlist	
1		Protection	0 days, 0: 0: 55: 950 2
forward	forward	1-4094	

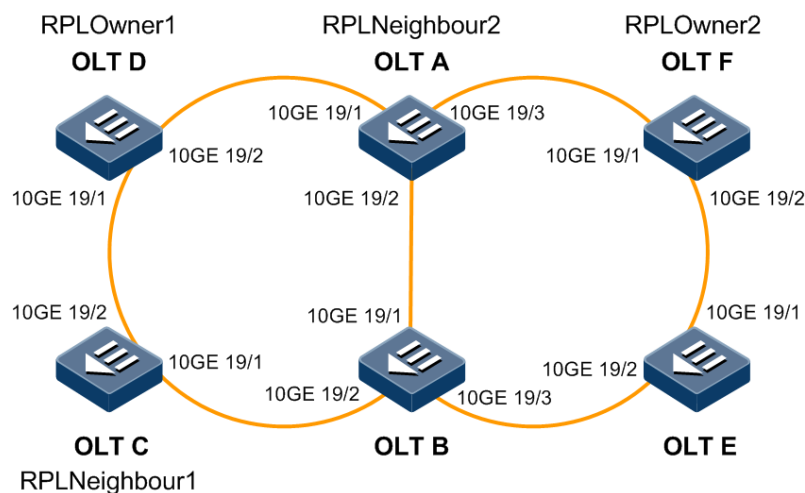
17.3.2 Example for configuring intersecting ring G.8032 protection

Networking requirements

As shown in Figure 17-2, to improve the reliability of the Ethernet network, you can use OLT A, OLT B, OLT C, OLT D, OLT E, and OLT F to form an ERPS intersecting ring.

- OLT A, OLT B, OLT C, and OLT D form the main ring. OLT D is the RPL Owner of the main ring. OLT C is the RPL Neighbour of the main ring. The blocking port is 10GE 19/1 of OLT D. The protocol VLAN is VLAN 1 by default.
- OLT A, OLT B, OLT E, and OLT F form the tributary ring. OLT F is the RPL Owner of the tributary ring. OLT A is the RPL Neighbour of the tributary ring. The blocking port is 10GE 19/1 of OLT F. The protocol VLAN is 4094. The virtual path mode of the tributary ring is the default with mode.
- The blocking VLAN of the main ring and tributary ring ranges from 1 to 4094 by default.

Figure 17-2 Intersecting ring G.8032 networking



Configuration steps

Step 1 Create VLAN 4094 and add interfaces to VLAN 1 to VLAN 4094.

Configure OLT A.

```

Raisecom#config
Raisecom(config)#create vlan 4094 active
Raisecom(config)#interface ten-gigabitethernet 19/1
Raisecom(config-if-ten-gigabitethernet-19:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:1)#exit

```

```
Raisecom(config)#interface ten-gigabitethernet 19/2
Raisecom(config-if-ten-gigabitethernet-19:2)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:2)#exit
Raisecom(config)#interface ten-gigabitethernet 19/3
Raisecom(config-if-ten-gigabitethernet-19:3)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:3)#exit
```

Configure OLT B.

```
Raisecom#config
Raisecom(config)#create vlan 4094 active
Raisecom(config)#interface ten-gigabitethernet 19/1
Raisecom(config-if-ten-gigabitethernet-19:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
Raisecom(config)#interface ten-gigabitethernet 19/2
Raisecom(config-if-ten-gigabitethernet-19:2)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:2)#exit
Raisecom(config)#interface ten-gigabitethernet 19/3
Raisecom(config-if-ten-gigabitethernet-19:3)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:3)#exit
```

Configure OLT C.

```
Raisecom#config
Raisecom(config)#create vlan 4094 active
Raisecom(config)#interface ten-gigabitethernet 19/1
Raisecom(config-if-ten-gigabitethernet-19:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
Raisecom(config)#interface ten-gigabitethernet 19/2
Raisecom(config-if-ten-gigabitethernet-19:2)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:2)#exit
```

Configure OLT D.

```
Raisecom#config
Raisecom(config)#create vlan 4094 active
Raisecom(config)#interface ten-gigabitethernet 19/1
Raisecom(config-if-ten-gigabitethernet-19:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
Raisecom(config)#interface ten-gigabitethernet 19/2
Raisecom(config-if-ten-gigabitethernet-19:2)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:2)#exit
```

Configure OLT E.

```
Raisecom#config
Raisecom(config)#create vlan 4094 active
Raisecom(config)#interface ten-gigabitethernet 19/1
Raisecom(config-if-ten-gigabitethernet-19:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
Raisecom(config)#interface ten-gigabitethernet 19/2
Raisecom(config-if-ten-gigabitethernet-19:2)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:2)#exit
```

Configure OLT F.

```
Raisecom#config
Raisecom(config)#create vlan 4094 active
Raisecom(config)#interface ten-gigabitethernet 19/1
Raisecom(config-if-ten-gigabitethernet-19:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:1)#exit
Raisecom(config)#interface ten-gigabitethernet 19/2
Raisecom(config-if-ten-gigabitethernet-19:2)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-19:2)#exit
```

Step 2 Create a G.8032 main ring.

Configure OLT A.

```
Raisecom(config)#ethernet ring-protection 1 east interface ten-
gigabitethernet 19/1 west interface ten-gigabitethernet 19/2
```

Configure OLT B.

```
Raisecom(config)#ethernet ring-protection 1 east interface ten-
gigabitethernet 19/1 west interface ten-gigabitethernet 19/2
```

Configure OLT C.

```
Raisecom(config)#ethernet ring-protection 1 east interface ten-
gigabitethernet 19/1 west interface ten-gigabitethernet 19/2 node-type
rpl-neighbour rpl west
```

Configure OLT D.

```
Raisecom(config)#ethernet ring-protection 1 east interface ten-
gigabitethernet 19/1 west interface ten-gigabitethernet 19/2 node-type
rpl-owner rpl east
```

Step 3 Configure a G.8032 tributary ring.

Configure OLT A.

```
Raisecom(config)#ethernet ring-protection 2 east interface ten-
gigabitethernet 19/3 node-type rpl-neighbour protocol-vlan 4094
Raisecom(config)#ethernet ring-protection 2 propagate enable
```

Configure OLT B.

```
Raisecom(config)#ethernet ring-protection 2 east interface ten-
gigabitethernet 19/3 protocol-vlan 4094
Raisecom(config)#ethernet ring-protection 2 propagate enable
```

Configure OLT E.

```
Raisecom(config)#ethernet ring-protection 2 east interface ten-
gigabitethernet 19/1 west interface ten-gigabitethernet 19/2 protocol-
vlan 4094
```

Configure OLT F.

```
Raisecom(config)#ethernet ring-protection 2 east interface ten-
gigabitethernet 19/1 west interface ten-gigabitethernet 19/2 node-type
rpl-owner rpl east protocol-vlan 4094
```

Checking results

Use the **show ethernet ring-protection status** command to check whether the G.8032 protection ring is effective.

Check OLT A, OLT D, and OLT F respectively and wait for the WTR to expire. The results are:

```
Raisecom#show ethernet ring-protection status
Id/Name          Bridge-State  Last Occur(ago)
SwitchTimes  East-State  west-State  Traffic-vlanlist
-----
1            forward    Idle        0 days, 0: 0: 50: 750    2
forward      forward    1-4094
-----
```

```
2                               Idle      0  days, 0: 0: 50: 750    2
forward      forward          1-4094
```

```
Raisecom#show ethernet ring-protection status
Id/Name                Bridge-State  Last Occur(ago)
SwitchTimes  East-State  West-State  Traffic-vlanlist
-----
1                               Idle      0  days, 0: 0: 50: 750    2
block      forward          1-4094
```

```
Raisecom#show ethernet ring-protection status
Id/Name                Bridge-State  Last Occur(ago)
SwitchTimes  East-State  West-State  Traffic-vlanlist
-----
2                               Idle      0  days, 0: 0: 50: 750    2
block      forward          1-4094
```

18 Appendix

This chapter includes the following sections:

- Terms
- Acronyms and abbreviations

18.1 Terms

A

Alarm	Alarm refers to a human-observable indication that draws attention to a failure (detected fault) usually giving an indication of the severity of the fault. It is reported when a fault is detected by a device or by the NMS during the process of polling devices. Each alarm corresponds to a recovery alarm. After a recovery alarm is received, the status of the corresponding alarm changes to cleared.

Alarm Filtering	The NView NNM system does not receive alarms that do not comply with filtering rules from a device.

Alarm masking	The device does not record alarms complying with the masking rules nor report the alarms to the NMS.

Alarm inhibition	The device only records and reports root alarms except correlative alarms when alarm inhibition is enabled.

C

Current alarm	The current alarm is defined according to the operation status of the alarm. All uncleared or unfiltered alarms are called as current alarms.

D

Dynamic ARP Inspection (DAI)	A security feature that can be used to verify the ARP data packets in the network. With DAI, the administrator can intercept, record, and discard ARP packets with invalid MAC address/IP address to prevent common ARP attacks.

Device Scan	The device scans network devices in the IP address range, and adds them automatically to the NMS.
Dynamic Host Configuration Protocol (DHCP)	A technology used for assigning IP address dynamically. It can automatically assign IP addresses for all clients in the network to reduce workload of the administrator. In addition, it can implement centralized management of IP addresses.

F

Forward Error Correction (FEC)	It is a method to increase the transmission distance by adding an Error Correcting Code (ECC). It supports longer transmission distance and larger splitting ratio.

H

H.248	It is a media gateway control protocol proposed by the 16th working group of ITU-T in 2000 based on the MGCP. H.248/MeGaCo protocol is the gateway control protocol used to connect the MGC and MG. It can be applied between the media gateway and softswitch, or softswitch and H.248/MeGaCo terminal. It is also an important protocol supported by the softswitch.

I

Internet Assigned Numbers Authority (IANA)	The organization operated under 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.
In-band Network Management	The NMS exchanges information with a device through service networks.

L

Link Aggregation	With link aggregation, multiple physical Ethernet interfaces are combined to form a logical aggregation group. Multiple physical links in one aggregation group are taken as a logical link. Link aggregation helps share traffic among member interfaces in an aggregation group. In addition to effectively improving the reliability on links between devices, link aggregation can help gain greater bandwidth without upgrading hardware.

N

Network Element (NE)	A network device to be managed by the NMS as a network element

NMS Monitor	It refers to auxiliary programs of the NMS, which can manage various service programs and monitor the operation status of the system.
Network Time Protocol (NTP)	A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed time server and clients. NTP is used to perform clock synchronization on all devices that have clocks in the network. Therefore, the devices can provide different applications based on a unified time. In addition, NTP can ensure a very high accuracy with an error of 10ms or so.

O

Open Shortest Path First (OSPF)	An internal gateway dynamic routing protocol, which is used to decide the route in an Autonomous System (AS)
Optical Distribution Network (ODN)	It refers to the optical transmission channel between the OLT and ONU.
Out-of-band network management	The mode in which the NMS and device communicate network management information through another network independent of the service network

P

Performance monitoring	The NMS collects and displays performance data of the device, such as traffic and packet loss rate.

Q

QinQ	802.1Q in 802.1Q (QinQ), also called Stacked VLAN or Double VLAN, is extended from 802.1Q and defined by IEEE 802.1ad recommendation. This VLAN feature allows the equipment to add a VLAN tag to a tagged packet. The implementation of QinQ is to add a public VLAN tag to a packet with a private VLAN tag, making the packet encapsulated with two layers of VLAN tags. The packet is forwarded over the ISP's backbone network based on the public VLAN tag and the private VLAN tag is transmitted as the data part of the packet. In this way, the QinQ feature enables the transmission of the private VLANs to the peer end transparently. There are two QinQ types: basic QinQ and selective QinQ.
Quality of Service (QoS)	A network security mechanism, used to solve problems of network delay and congestion. When the network is overloaded or congested, QoS can ensure that packets of important services are not delayed or discarded and the network runs high efficiently. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio.

R

Resource It refers to the managed objects in the NMS, including the device, chassis, card, and interface.

Remote Authentication Dial In User Service (RADIUS) RADIUS refers to a protocol used to authenticate and account users in the network. RADIUS works in client/server mode. The RADIUS server is responsible for receiving users' connection requests, authenticating users, and replying configurations required by all clients to provide services for users.

S

Symbol A schematic topology node, which helps clearly show the network structure while cannot be managed

Simple Network Management Protocol (SNMP) A network management protocol defined by Internet Engineering Task Force (IETF) used to manage devices in the Internet. SNMP can make the network management system to remotely manage all network devices that support SNMP, including monitoring network status, modifying network device configurations, and receiving network event alarms. At present, SNMP is the most widely-used network management protocol in the TCP/IP network.

SyncE A technology that adopts Ethernet link code stream to recover clocks, and provides high-precision frequency synchronization for the Ethernet similar to SDH clock synchronization. Different from the traditional network which just synchronizes data packets on the receiving node, the internal clock synchronization mechanism of the SyncE is real-time.

T

Topology Topology includes routes and devices, describing the interconnection relationship among network nodes. It also refers to the network structure in general sense, namely, the physical layout of connected devices.

Trap It refers to a way of sending alarms to the NMS. Alarms are reported to the system through SNMP packets.

Time Division Multiplexing (TDM) TDM is a method of transmitting multiple independent signals (digitalized data, voice, or video signals) over a common signal path by means of synchronized switches at each end of the transmission line so that each signal appears on the line only a fraction of time in an alternating pattern.

Time Division Multiple Access (TDMA)	TDMA is a channel access method for shared medium networks. It allows several users to share the same frequency channel by dividing the signal into different timeslots. The users transmit in rapid succession, one after the other, each using its own timeslot. This allows multiple base stations to share the same transmission medium while using only a part of its channel capacity. On the condition of fixed time and synchronization, the base station can receive signals of each mobile terminal from each timeslot without interference. Meantime, signals sent by the base station to the mobile terminals are transmitted through the specified timeslots in sequence. As long as each mobile terminal receives signals from the specified timeslot, corresponding signals will be identified from the multiplexed signals and received in sequence.
U	
User	A user using the NMS client, with available NMS features determined by a set of management domains of users and user groups, and operation rights
User group	A user group can provide the same management domain and operation right for group members.
V	
Virtual Local Area Network (VLAN)	VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segments logically rather than physically, thus implementing multiple virtual work groups which are based on Layer 2 isolation and do not affect each other.

18.2 Acronyms and abbreviations

3	
3GPP	The 3rd Generation Partnership Project
A	
ACL	Access Control List
AES	Advanced Encryption Standard
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
B	

BPDU	Bridge Protocol Data Unit
C	
CATV	Community Antenna Television
CDR	Calling Detail Records
CFI	Canonical Format Indicator
CoS	Class of Service
CPE	Customer Premises Equipment
CPU	Central Processing Unit
D	
DAI	Dynamic ARP Inspection
DBA	Dynamic Bandwidth Allocation
DHCP	Dynamic Host Configuration Protocol
DRR	Deficit Round Robin
DSCP	Differentiated Services Code Point
E	
EoC	Ethernet over Coaxial
EPON	Ethernet Passive Optical Network
ERPS	Ethernet Ring Protection Switching
F	
FEC	Forward Error Correction
FIB	Forwarding Information Base
FTP	File Transfer Protocol
G	
GE	Gigabit Ethernet
GPON	Gigabit-Capable PON
I	
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP Snooping	Internet Group Management Protocol Snooping
IGMP	Internet Group Management Protocol
IP	Internet Protocol
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector
L	
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LLID	Logical Link Identifier
M	
MAC	Medium Access Control
MD5	Message-Digest Algorithm 5
MIB	Management Information Base
MPCP	Multi-Point Control Protocol
MTU	Maximum Transferred Unit
MVR	Multicast VLAN Registration
N	
NAT	Network Address Translation
NMS	Network Management System
NNM	Network Node Management
NTP	Network Time Protocol
O	
OAM	Operation Administration and Management
ODN	Optical Distribution Network
OID	Object Identifier

OLT	Optical Line Terminal
ONU	Optical Network Unit
OSI	Open System Interconnect
OSPF	Open Shortest Path First
P	
PC	Personal Computer
PE	Provider Edge
PoE	Power Over Ethernet
PPPoE	Point-to-Point Protocol over Ethernet
Q	
QoS	Quality of Service
R	
RADIUS	Remote Authentication Dial In User Service
RF	Radio Frequency
RIP	Routing Information Protocol
S	
SFP	Small Form-factor Pluggables
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol)
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SSHv2	Secure Shell v2
STP	Spanning Tree Protocol
T	
TACACS+	Terminal Access Controller Access Control System

TC	Transparent Clock
TCI	Tag Control Information
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TFTP	Trivial File Transfer Protocol
ToS	Type of Service
TPID	Tag Protocol Identifier
U	
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
V	
VID	VLAN Identifier
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
W	
WRR	Weight Round Robin

