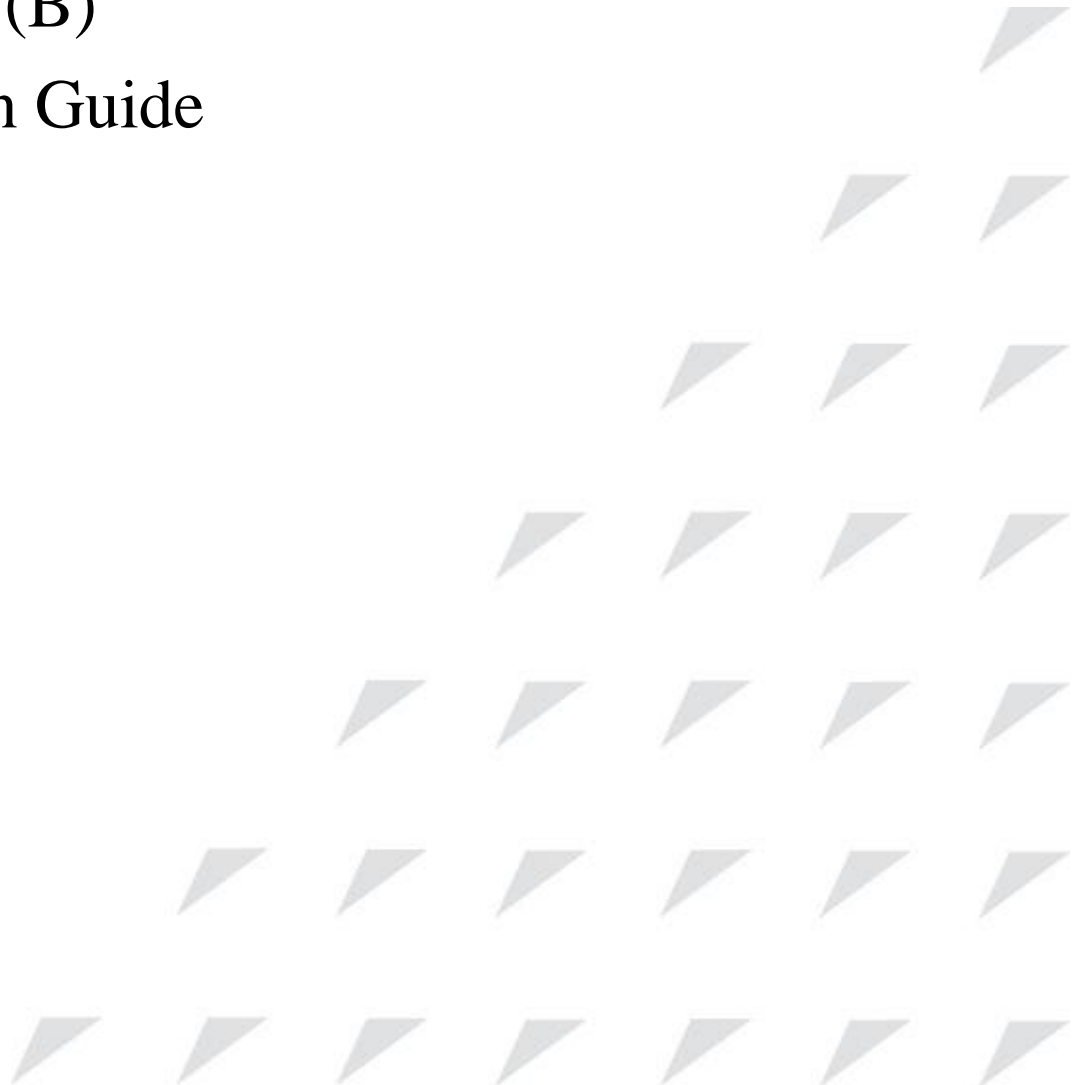


[www.raisecom.com](http://www.raisecom.com)

**ISCOM5508 (B)**  
**Configuration Guide**  
**(Rel\_03)**



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](mailto: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 © 2017

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 supported features and related configurations of the ISCOM5508, including basic configuration, EPON service configuration, multicast service configuration, VoIP service configuration, CATV service configuration, TDMoP service configuration, MAC address table configuration, VLAN configuration, Spanning Tree configuration, routing configuration, DHCP configuration, QoS configuration, OAM configuration, system security configuration, link security configuration, and system management configuration. In addition, this document provides related configuration examples. The appendix lists terms, acronyms, and abbreviations involved in this document.

This document helps you master basic principles and configurations of the ISCOM5508, as well as networking with the ISCOM5508.

## Versions

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

Product name	Hardware version	Software version
ISCOM5508	B.00 or later	V2.6 or later

## Related manuals

The following table lists manuals and their contents related to the ISCOM5508.





Name	Description
<i>ISCOM5508 (B) Hardware Description</i>	This guide mainly introduces the hardware structure and cards, including product overview, components, fiber and cables, pluggable module, lookup table of LEDs, and lookup table of weight and power consumption.

Name	Description
<i>ISCOM5508 (B) Configuration Guide</i>	This guide mainly introduces supported services of the ISCOM5508 from aspects of service introduction, default configurations, configuration methods, and configuration examples, including basic configuration, EPON service configuration, multicast service configuration, VoIP service configuration, CATV service configuration, TDMoP service configuration, MAC address table configuration, VLAN configuration, Spanning Tree configuration, routing configuration, DHCP configuration, QoS configuration, OAM configuration, system security configuration, link security configuration, and system management configuration.

## Conventions

### Symbol conventions

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

Symbol	Description
 <b>Warning</b>	Indicate a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
 <b>Caution</b>	Indicate a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
 <b>Note</b>	Provide additional information to emphasize or supplement important points of the main text.
 <b>Tip</b>	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.
<b>Boldface</b>	Names of files, directories, folders, and users are in <b>boldface</b> . For example, log in as user <b>root</b> .
<i>Italic</i>	Book titles are in <i>italics</i> .

Convention	Description
<b>Lucida Console</b>	Terminal display is in <b>Lucida Console</b> .

## 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
<b>Boldface</b>	The keywords of a command line are in <b>boldface</b> .
<i>Italic</i>	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.
[ 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 03 (2017-02-04)

Third commercial release

- Added configurations of MAC address flapping.
- Added configurations of VLAN ACL.
- Added configurations of dynamic ARP entries.
- Added configurations of Key-chain.
- Added configurations of attack defense.
- Added VLAN-based DHCP Snooping and DHCP relay.
- Added IP Source Guard and DAI.

## Issue 02 (2015-12-08)

Second commercial release

- Fixed known bugs.
- Added partner template.
- Added PSE template.
- Added voice template.
- Adapted to software V2.41 and added BCMP.

## Issue 01 (2013-10-18)

Initial commercial release

# Contents

<b>1 Basic configurations .....</b>	<b>1</b>
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 Command history .....	9
1.1.7 Acquiring help.....	10
1.2 Accessing device .....	12
1.2.1 Accessing device through Console interface.....	12
1.2.2 Accessing device through Telnet .....	13
1.2.3 Accessing device through SSHv2 .....	14
1.2.4 Checking configurations .....	16
1.3 Managing users .....	16
1.3.1 Default configurations.....	16
1.3.2 Creating/Deleting users.....	17
1.3.3 Managing user privileges .....	17
1.3.4 Refining user privileges .....	17
1.3.5 Checking configurations .....	19
1.4 Managing cards .....	19
1.4.1 Default configurations.....	19
1.4.2 Creating cards .....	19
1.4.3 Rebooting cards .....	20
1.4.4 Managing fan .....	20
1.4.5 Checking configurations .....	21
1.5 Managing interfaces .....	21
1.5.1 Default configurations.....	21
1.5.2 Enabling/Disabling interfaces .....	22
1.5.3 Configuring basic properties of interfaces .....	23
1.5.4 Configuring interface statistics .....	24
1.5.5 Configuring flow control on interfaces .....	24

1.5.6 Configuring IP interface.....	25
1.5.7 Configuring out-of-band network management interface .....	25
1.5.8 Cutting interface services.....	25
1.5.9 Checking configurations .....	26
1.6 Managing time .....	27
1.6.1 Default configurations.....	27
1.6.2 Configuring time and time zone.....	28
1.6.3 Configuring DST .....	28
1.6.4 Configuring NTP .....	29
1.6.5 Configuring SNTP .....	30
1.6.6 Checking configurations .....	30
1.7 Upgrade and backup.....	30
1.7.1 Introduction.....	30
1.7.2 Configuring server .....	31
1.7.3 Upgrading OLT system files .....	31
1.7.4 Backing up OLT system files .....	32
1.7.5 Upgrading ONU system files .....	32
1.7.6 Managing ONU configuration files .....	33
1.7.7 Configuring auto-save.....	33
1.7.8 Configuring ONU auto-upgrade .....	33
1.7.9 Configuring ONU performance template.....	34
1.7.10 Checking configurations .....	34
1.8 Task scheduling .....	35
1.8.1 Introduction.....	35
1.8.2 Default configurations.....	35
1.8.3 Configuring task scheduling .....	35
1.8.4 Checking configurations .....	35
1.9 Maintenance .....	35
1.10 Configuration examples .....	36
1.10.1 Example for configuring out-of-band network management .....	36
1.10.2 Example for configuring in-band network management.....	36
1.10.3 Example for upgrading OLT through TFTP.....	37
1.10.4 Example for configuring ONU auo-upgrade.....	39
1.10.5 Example for refining user privileges .....	40
<b>2 Configuring EPON services .....</b>	<b>41</b>
2.1 Overview of EPON .....	41
2.1.1 Structure of EPON system .....	41
2.1.2 EPON principle .....	42
2.1.3 Splitting ratio .....	44
2.1.4 ONU authentication .....	44
2.1.5 ONU management .....	45



2.1.6 Data encryption .....	46
2.1.7 DBA .....	46
2.1.8 Layer 2 isolation .....	47
2.1.9 FEC .....	47
2.1.10 Maximum RTT .....	47
2.2 Quick configuration of EPON services .....	48
2.2.1 Example for configuring EPON Ethernet data service .....	48
2.2.2 Example for configuring PON+LAN typical networking (data service+network management) .....	50
2.3 Registration and deregistration .....	53
2.3.1 Default configurations .....	53
2.3.2 Configuring ONU registration .....	54
2.3.3 Configuring ONU deregistration .....	55
2.3.4 Checking configurations .....	55
2.4 Configuring ONU IP address pool .....	56
2.4.1 Default configuration .....	56
2.4.2 Creating address pool .....	56
2.4.3 Binding PON interface .....	56
2.4.4 Checking configurations .....	57
2.5 Configuring ONU SNMP template .....	57
2.5.1 Default configuration .....	57
2.5.2 Creating template and configuring it .....	57
2.5.3 Checking configurations .....	57
2.6 Configuring ONU template .....	58
2.6.1 Default configuration .....	58
2.6.2 Creating template and configuring it .....	58
2.6.3 Binding template .....	58
2.6.4 Checking configurations .....	59
2.7 Configuring ONU line template .....	59
2.7.1 Default configuration .....	59
2.7.2 Creating template and configuring it .....	59
2.7.3 Binding profile .....	60
2.7.4 Checking configurations .....	60
2.8 Configuring ONU service profile .....	60
2.8.1 Default configuration .....	60
2.8.2 Creating profile and configuring it .....	60
2.8.3 Binding profile .....	63
2.8.4 Checking configurations .....	63
2.9 Configuring partner profile .....	64
2.9.1 Default configurations .....	64
2.9.2 Creating profile .....	64
2.9.3 Configuring profile .....	64
2.9.4 Checking configurations .....	65

2.10 Configuring PSE profile.....	65
2.10.1 Default configurations.....	65
2.10.2 Creating profile .....	65
2.10.3 Configuring profile .....	66
2.10.4 Checking configurations .....	66
2.11 Configuring voice profile .....	66
2.11.1 Default configurations.....	66
2.11.2 Creating profile .....	67
2.11.3 Configuring profile.....	67
2.11.4 Checking configurations .....	68
2.12 Configuring ONU QoS profile .....	68
2.12.1 Default configuration .....	68
2.12.2 Creating profile .....	68
2.12.3 Configuring parameters of ONU QoS template .....	68
2.13 Configuring DBA template .....	70
2.13.1 Default configuration .....	70
2.13.2 Creating template .....	70
2.13.3 Modifying template.....	71
2.13.4 Checking configurations .....	72
2.14 Configuring EPON interface.....	72
2.14.1 Default configuration .....	72
2.14.2 Configuring interface .....	72
2.14.3 Configuring data encryption .....	72
2.14.4 Configuring maximum RTT.....	73
2.14.5 Checking configurations .....	73
2.15 Configuring ONU.....	74
2.15.1 Default configurations.....	74
2.15.2 Basic configurations of ONU .....	76
2.15.3 Configuring ONU management .....	76
2.15.4 Configuring ONU management IP.....	78
2.15.5 Activating ONU .....	80
2.15.6 Rebinding ONU .....	80
2.15.7 Configuring ONU SNMP parameters .....	80
2.15.8 Configuring ONU UNI .....	81
2.15.9 Configuring ONU UNI alarm .....	82
2.15.10 Configuring ONU serial interface .....	87
2.15.11 Configuring data encryption.....	88
2.15.12 Configuring DBA.....	88
2.15.13 Configuring FEC.....	89
2.15.14 Configuring OAM remote loopback .....	90
2.15.15 Configuring DLF and BPDU forwarding.....	90
2.15.16 Configuring partner discovery .....	90

2.15.17 Configuring PPPoE agent .....	91
2.15.18 Configuring PoE .....	92
2.15.19 Checking configurations .....	94
2.16 Configuration examples .....	96
2.16.1 Example for configuring ONU auto-registration .....	96
2.16.2 Example for configuring ONU registration in MAC-based authentication mode .....	97
<b>3 Configuring multicast services.....</b>	<b>99</b>
3.1 Overview of multicast services .....	99
3.1.1 Multicast .....	99
3.1.2 IGMP Snooping .....	104
3.1.3 IGMP Proxy .....	104
3.1.4 MVR .....	105
3.1.5 Dynamic controllable multicast .....	106
3.2 Quick configuration of multicast services .....	106
3.2.1 Example for configuring IGMP Snooping .....	106
3.2.2 Example for configuring dynamic controllable multicast .....	109
3.3 Configuring static multicast .....	113
3.3.1 Preparing for configurations .....	113
3.3.2 Default configurations.....	113
3.3.3 Configuring static multicast .....	113
3.3.4 Configuring unknown multicat filter .....	113
3.3.5 Checking configurations .....	114
3.4 Configuring IGMP Snooping .....	114
3.4.1 Preparing for configurations .....	114
3.4.2 Default configurations.....	114
3.4.3 Configuring IGMP Snooping .....	115
3.4.4 (Optional) configuring aging time of multicast routing entries.....	116
3.4.5 (Optional) configuring immediate-leave .....	117
3.4.6 Checking configurations .....	118
3.5 Configuring IGMP Proxy.....	118
3.5.1 Preparing for configurations .....	118
3.5.2 Default configurations.....	119
3.5.3 Configuring IGMP Proxy.....	119
3.5.4 Checking configurations .....	120
3.6 Configuring MVR .....	121
3.6.1 Preparing for configurations .....	121
3.6.2 Default configurations.....	121
3.6.3 Configuring basic MVR.....	121
3.6.4 Checking configurations .....	121
3.7 Configuring multicast group limit.....	122
3.7.1 Preparing for configurations .....	122

3.7.2 Default configurations.....	122
3.7.3 Configuring multicast group limit on ONU .....	122
3.7.4 Checking configurations .....	122
3.8 Configuring dynamic controllable multicast .....	123
3.8.1 Preparing for configurations .....	123
3.8.2 Default configurations.....	123
3.8.3 Configuring global function.....	123
3.8.4 Configuring user management .....	124
3.8.5 Configuring channel management .....	124
3.8.6 Configuring preview rules .....	124
3.8.7 Configuring CDR.....	125
3.8.8 Checking configurations .....	126
3.9 Configuring MLD Snooping .....	126
3.9.1 Preparing for configurations .....	126
3.9.2 Default configurations.....	127
3.9.3 Configuring MLD Snooping.....	127
3.9.4 Checking configurations .....	127
3.10 Configuring MLD Proxy.....	128
3.10.1 Preparing for configurations .....	128
3.10.2 Default configurations.....	128
3.10.3 Configuring MLD Proxy.....	128
3.10.4 Checking configurations .....	129
3.11 Configuring multicast VLAN.....	130
3.11.1 Preparing for configurations.....	130
3.11.2 Default configurations.....	130
3.11.3 Configuring multicast VLAN.....	130
3.11.4 Checking configurations .....	131
3.12 Maintenance .....	132
<b>4 Configuring VoIP services .....</b>	<b>133</b>
4.1 Overview of VoIP services .....	133
4.1.1 VoIP.....	133
4.1.2 SIP.....	134
4.1.3 H.248.....	135
4.2 Quick configuration of VoIP services.....	137
4.2.1 Example for configuring SIP voice service (Proxy call) .....	137
4.2.2 Example for configuring SIP voice service (Direct call) .....	141
4.2.3 Example for configuring H.248 voice service.....	145
4.3 Configuring VoIP .....	149
4.3.1 Preparing for configurations .....	149
4.3.2 Default configurations.....	149
4.3.3 Configuring VoIP protocol type .....	150

4.3.4 Configuring network parameters of signalling traffic .....	150
4.3.5 Configuring network parameters of media traffic .....	152
4.3.6 Checking configurations .....	153
4.4 Configuring POTS interface.....	154
4.4.1 Preparing for configurations .....	154
4.4.2 Default configurations.....	154
4.4.3 Configuring interface properties .....	154
4.4.4 Configuring phone number .....	155
4.4.5 Configuring other functions .....	155
4.4.6 Checking configurations .....	156
4.5 Configuring SIP .....	157
4.5.1 Preparing for configurations .....	157
4.5.2 Default configurations.....	157
4.5.3 Configuring basic functions of SIP .....	158
4.5.4 Configuring SIP Proxy/Register server .....	159
4.5.5 Configuring SIP heartbeat .....	160
4.5.6 Configuring SIP user authentication .....	160
4.5.7 Configuring CID .....	161
4.5.8 Configuring call waiting .....	161
4.5.9 Configuring three-way calling .....	161
4.5.10 Configuring Modem transparent transmission .....	162
4.5.11 Configuring polarity reversal service .....	162
4.5.12 Configuring hotline service.....	163
4.5.13 Configuring mapping rule of SIP phone numbers.....	163
4.5.14 Configuring user deregistration and re-registration .....	165
4.5.15 Checking configurations .....	165
4.6 Configuring H.248 .....	166
4.6.1 Preparing for configurations .....	166
4.6.2 Default configurations.....	166
4.6.3 Configuring basic functions of H.248.....	167
4.6.4 Configuring H.248 authentication.....	168
4.6.5 Configuring MG.....	168
4.6.6 Configuring MGC .....	170
4.6.7 Configuring TID .....	170
4.6.8 Configuring MG heartbeat .....	172
4.6.9 Configuring H.248 digitmap .....	173
4.6.10 Checking configurations .....	173
4.7 Configuring second dialing .....	174
4.7.1 Preparing for configurations .....	174
4.7.2 Default configurations.....	175
4.7.3 Configuring second dialing .....	175
4.7.4 Checking configurations .....	175

4.8 Configuring fax .....	175
4.8.1 Preparing for configurations .....	175
4.8.2 Default configurations.....	176
4.8.3 Configuring fax .....	176
4.8.4 Checking configurations .....	177
4.9 Configuring call process tone.....	177
4.9.1 Preparing for configurations .....	177
4.9.2 Default configurations.....	177
4.9.3 Configuring call process tone.....	178
4.9.4 Checking configurations .....	178
4.10 Configuring call emulation test .....	179
4.10.1 Preparing for configurations .....	179
4.10.2 Default configurations.....	179
4.10.3 Configuring call emulation test.....	179
4.10.4 Checking configurations .....	180
4.11 Maintenance .....	180
<b>5 Configuring CATV services.....</b>	<b>181</b>
5.1 Overview of CATV services.....	181
5.2 Quick configuration of CATV services .....	182
5.2.1 Networking requirements.....	182
5.2.2 Configuration steps .....	183
5.2.3 Checking results.....	183
5.3 Preparing for configurations.....	183
5.4 Configuring CATV services .....	184
5.5 Checking configurations .....	184
<b>6 Configuring TDMoP services.....</b>	<b>185</b>
6.1 Overview of TDMoP services .....	185
6.1.1 TDMoP service encapsulation modes .....	186
6.1.2 TDMoP clock synchronization principles .....	189
6.1.3 Overview of Bundle .....	190
6.2 Quick configuration of TDMoP services.....	191
6.2.1 Networking requirements.....	191
6.2.2 Configuration steps .....	194
6.2.3 Checking results.....	198
6.3 Default configurations.....	200
6.4 Configuring global parameters of TDMoP.....	200
6.5 Configuring TDMoP interface mode.....	201
6.6 Configuring TDMoP system clock.....	202
6.7 Configuring Bundle.....	202
6.7.1 Creating and enabling Bundle.....	202
6.7.2 Configuring parameters of Bundle .....	202

6.7.3 Configuring parameters of E1/T1 interface .....	203
6.7.4 Configuring related information of PSN .....	203
6.7.5 Configuring packet load time and Jitter Buffer .....	204
6.8 Checking configurations .....	205
6.9 Maintenance .....	205
<b>7 Configuring MAC address .....</b>	<b>206</b>
7.1 Overview of MAC address table .....	206
7.2 Configuring dynamic MAC address.....	208
7.2.1 Preparing for configurations .....	208
7.2.2 Default configurations.....	208
7.2.3 Configuring MAC address learning .....	209
7.2.4 (Optional) configuring aging time of MAC address .....	209
7.2.5 (Optional) configuring MAC address limit .....	210
7.2.6 Checking configurations .....	211
7.3 Configuring static MAC address .....	212
7.3.1 Preparing for configurations .....	212
7.3.2 Default configurations.....	212
7.3.3 Configuring static unicast MAC address .....	212
7.3.4 Configuring static multicast MAC address .....	213
7.3.5 Configuring MAC address flapping.....	214
7.3.6 Checking configurations .....	214
7.4 Maintenance and search .....	215
7.4.1 Preparing for configurations .....	215
7.4.2 Default configurations.....	215
7.4.3 Clearing MAC address.....	215
7.4.4 Searching MAC address.....	216
7.4.5 Tracing MAC address .....	216
7.4.6 Checking configurations .....	216
7.5 Configuration examples .....	217
7.5.1 Example for configuring dynamic MAC address.....	217
7.5.2 Example for configuring static MAC address .....	220
<b>8 Configuring VLAN .....</b>	<b>222</b>
8.1 Overview of VLAN.....	222
8.1.1 VLAN .....	222
8.1.2 QinQ.....	226
8.1.3 VLAN translation.....	227
8.2 Configuring VLAN .....	227
8.2.1 Preparing for configurations .....	227
8.2.2 Default configurations.....	228
8.2.3 Configuring VLAN of OLT interface.....	228
8.2.4 Configuring VLAN of ONU UNI .....	232

8.2.5 Configuring VLAN of ONU SNI.....	234
8.2.6 Checking configurations .....	234
8.3 Configuring QinQ .....	235
8.3.1 Preparing for configurations .....	235
8.3.2 Default configurations.....	235
8.3.3 Configuring basic QinQ .....	235
8.3.4 Checking configurations .....	236
8.4 Configuring VLAN ACL.....	236
8.4.1 Preparing for configurations .....	236
8.4.2 Default configurations.....	236
8.4.3 Creating ACL .....	237
8.4.4 Configuring matching contents .....	237
8.4.5 Configuring matching actions .....	238
8.4.6 Applying ACL .....	238
8.4.7 Checking configurations .....	239
8.5 Configuring VLAN translation .....	239
8.5.1 Preparing for configurations .....	239
8.5.2 Default configurations.....	239
8.5.3 Configuring VLAN translation .....	240
8.5.4 Configuring 1:1 VLAN translation .....	240
8.5.5 Configuring N:1 VLAN translation .....	240
8.5.6 Configuring translation rules based on VLAN+CoS.....	241
8.5.7 Checking configurations .....	241
8.6 Configuring virtual interface .....	241
8.6.1 Preparing for configurations .....	241
8.6.2 Default configurations.....	242
8.6.3 Configuring VLAN of virtual interface .....	242
8.6.4 Configuring basic QinQ on virtual interface .....	242
8.6.5 Configuring VLAN translation on virtual interface .....	243
8.6.6 Checking configurations .....	243
8.7 Maintenance .....	243
8.8 Configuration examples .....	244
8.8.1 Example for configuring VLAN .....	244
8.8.2 Example for configuring VLAN translation .....	246
<b>9 Configuring spanning tree .....</b>	<b>249</b>
9.1 Overview of spanning tree .....	249
9.1.1 STP.....	249
9.1.2 RSTP .....	251
9.1.3 MSTP.....	251
9.2 Configuring STP .....	254
9.2.1 Preparing for configurations .....	254



9.2.2 Default configurations.....	255
9.2.3 Enabling STP .....	255
9.2.4 Configuring STP parameters.....	255
9.2.5 Checking configurations .....	256
9.3 Configuring MSTP .....	256
9.3.1 Preparing for configurations .....	256
9.3.2 Default configurations.....	256
9.3.3 Enabling MSTP.....	257
9.3.4 Configuring MST domain and maximum number of hops .....	257
9.3.5 Configuring root bridge and backup root bridge.....	258
9.3.6 Configuring system priority and port priority .....	259
9.3.7 Configuring switching network diameter.....	260
9.3.8 Configuring internal port path cost .....	260
9.3.9 Configuring external port path cost.....	261
9.3.10 Configuring port maximum Tx rate .....	261
9.3.11 Configuring MSTP timers .....	261
9.3.12 Configuring edge port .....	263
9.3.13 Configuring link type .....	263
9.3.14 Configuring root port protection .....	263
9.3.15 Configuring port loop protection .....	264
9.3.16 Performing mcheck operation .....	264
9.3.17 Checking configurations .....	265
9.4 Configuring ONU RSTP .....	265
9.4.1 Preparing for configurations .....	265
9.4.2 Default configurations.....	265
9.4.3 Configuring ONU RSTP.....	266
9.4.4 Configuring parameters of ONU RSTP .....	266
9.4.5 Checking configurations .....	267
9.5 Maintenance .....	267
9.6 Configuration examples .....	267
9.6.1 Example for configuring STP .....	267
9.6.2 Example for configuring MSTP.....	271
9.6.3 Example for configuring ONU RSTP .....	276
<b>10 Configuring routing .....</b>	<b>278</b>
10.1 Overview of routing .....	278
10.1.1 ARP .....	278
10.1.2 Routing.....	279
10.1.3 VRRP .....	280
10.1.4 Key-chain.....	280
10.2 Configuring ARP.....	281
10.2.1 Preparing for configurations .....	281

10.2.2 Default configurations.....	281
10.2.3 Configuring static ARP entries.....	281
10.2.4 Configuring dynamic ARP entries .....	281
10.2.5 Checking configurations .....	282
10.3 Configuring static routing .....	282
10.3.1 Preparing for configurations .....	282
10.3.2 Configuring default gateway.....	282
10.3.3 Configuring IPv4 static routing.....	283
10.3.4 Checking configurations .....	283
10.4 Configuring VRRP .....	284
10.4.1 Preparing for configurations .....	284
10.4.2 Default configurations.....	284
10.4.3 Configuring VRRP.....	284
10.4.4 Checking configurations .....	285
10.5 Configuring key-chain.....	285
10.5.1 Preparing for configurations .....	285
10.5.2 Default configurations.....	286
10.5.3 Configuring key-chain .....	286
10.5.4 Checking configurations .....	286
10.6 Configuration examples .....	287
10.6.1 Example for configuring ARP.....	287
10.6.2 Example for configuring static routing .....	288
<b>11 Configuring DHCP .....</b>	<b>290</b>
11.1 Overview of DHCP .....	290
11.1.2 DHCP packet.....	292
11.1.3 DHCP Snooping.....	293
11.1.4 DHCP Relay .....	294
11.1.5 DHCP Option 82 .....	295
11.2 Configuring DHCP Snooping.....	296
11.2.1 Preparing for configurations.....	296
11.2.2 Default configurations.....	296
11.2.3 Configuring global DHCP Snooping.....	297
11.2.4 Configuring DHCP Snooping on VLAN interface.....	298
11.2.5 Configuring DHCP Snooping trust on ONU interface .....	298
11.2.6 (Optional) configuring DHCP Snooping supporting Option 82 .....	298
11.2.7 Checking configurations .....	299
11.3 Configuring DHCP Relay.....	300
11.3.1 Preparing for configurations.....	300
11.3.2 Default configurations.....	300
11.3.3 Configuring global DHCP Relay.....	300
11.3.4 Configuring destination IP address of DHCP Relay on VLAN interface .....	301

11.3.5 Configuring DHCP Relay trust on interface.....	301
11.3.6 Configuring DHCP Relay on ONU.....	301
11.3.7 Checking configurations .....	302
11.4 Configuring DHCP Option 82.....	302
11.4.1 Preparing for configurations.....	302
11.4.2 Default configurations.....	303
11.4.3 Enabling DHCP Option 82.....	303
11.4.4 Configuring global DHCP Option attach-string .....	304
11.4.5 Configuring global DHCP Option remote-id .....	304
11.4.6 Configuring DHCP Option circuit-id on interface .....	305
11.4.7 Configuring processing policy of Option 82 packet.....	305
11.4.8 Checking configurations .....	306
11.5 Maintenance .....	306
11.6 Configuration examples .....	307
11.6.1 Example for configuring DHCP Snooping.....	307
11.6.2 Example for configuring DHCP Relay.....	308
<b>12 Configuring QoS.....</b>	<b>310</b>
12.1 Overview of QoS.....	310
12.1.1 Priority trust .....	310
12.1.2 Traffic classification.....	311
12.1.3 Traffic policy.....	312
12.1.4 Priority mapping .....	313
12.1.5 Congestion management .....	313
12.2 Configuring traffic classification.....	315
12.2.1 Preparing for configurations .....	315
12.2.2 Default configurations.....	315
12.2.3 Configuring priority trust .....	316
12.2.4 Configuring priority mapping .....	316
12.2.5 Checking configurations .....	317
12.3 Configuring traffic monitoring .....	317
12.3.1 Preparing for configurations .....	317
12.3.2 Default configurations.....	318
12.3.3 Configuring rate limiting .....	318
12.3.4 Checking configurations .....	318
12.4 Configuring congestion management.....	319
12.4.1 Preparing for configurations .....	319
12.4.2 Default configurations.....	319
12.4.3 Configuring SP scheduling.....	320
12.4.4 Configuring WRR scheduling.....	320
12.4.5 Configuring WDRR scheduling .....	320
12.4.6 Checking configurations .....	321

12.5 Configuring congestion avoidance .....	321
12.5.1 Preparing for configurations .....	321
12.5.2 Default configurations.....	321
12.5.3 Configuring WRED scheduling .....	321
12.5.4 Checking configurations .....	322
12.6 Configuring traffic shaping .....	322
12.6.1 Preparing for configurations .....	322
12.6.2 Default configurations.....	322
12.6.3 Configuring traffic shaping .....	323
12.6.4 Checking configurations .....	323
12.7 Configuring traffic policy.....	323
12.7.1 Preparing for configurations .....	323
12.7.2 Default configurations.....	323
12.7.3 Configuring traffic policy on OLT .....	324
12.7.4 Configuring traffic policy on ONU .....	324
12.7.5 Checking configurations .....	325
12.8 Configuration examples .....	326
12.8.1 Example for configuring rate limiting.....	326
12.8.2 Example for configuring queue scheduling.....	327
<b>13 Configuring system security .....</b>	<b>329</b>
13.1 Overview of system security .....	329
13.1.1 ACL.....	329
13.1.2 RADIUS.....	329
13.1.3 TACACS+ .....	330
13.1.4 Storm control .....	330
13.1.5 Interface isolation.....	330
13.1.6 IP Source Guard .....	331
13.1.7 DAI .....	331
13.2 Configuring ACL .....	332
13.2.1 Preparing for configurations .....	332
13.2.2 Default configurations.....	332
13.2.3 Configuring IP ACL .....	333
13.2.4 Configuring Layer 2 ACL .....	335
13.2.5 Configuring hybrid ACL .....	336
13.2.6 Configuring user ACL.....	339
13.2.7 Applying ACL .....	340
13.2.8 Checking configurations .....	341
13.3 Configuring RADIUS .....	342
13.3.1 Preparing for configurations .....	342
13.3.2 Default configurations.....	342
13.3.3 Configuring RADIUS authentication.....	343

13.3.4 Configuring RADIUS accounting .....	343
13.3.5 Checking configurations .....	344
13.4 Configuring TACACS+ .....	344
13.4.1 Preparing for configurations .....	344
13.4.2 Default configurations .....	344
13.4.3 Configuring TACACS+ .....	344
13.4.4 Checking configurations .....	345
13.5 Configuring storm control .....	345
13.5.1 Preparing for configurations .....	345
13.5.2 Default configurations .....	346
13.5.3 Configuring storm control .....	346
13.5.4 Checking configurations .....	347
13.6 Configuring interface isolation .....	347
13.6.1 Preparing for configurations .....	347
13.6.2 Default configurations .....	348
13.6.3 Configuring interface isolation on OLT .....	348
13.6.4 Configuring interface isolation on ONU .....	349
13.6.5 Checking configurations .....	349
13.7 Configuring attack defense .....	350
13.7.1 Preparing for configurations .....	350
13.7.2 Default configuration .....	350
13.7.3 Configuring OLT interface isolation .....	350
13.7.4 Checking configurations .....	350
13.8 Configuring IP Source Guard .....	350
13.8.1 Preparing for configurations .....	350
13.8.2 Default configuration .....	351
13.8.3 Configuring IP Source Guard .....	351
13.8.4 Checking configurations .....	352
13.9 Configuring DAI .....	352
13.9.1 Preparing for configurations .....	352
13.9.2 Default configuration .....	352
13.9.3 Configuring DAI .....	352
13.9.4 Checking configurations .....	353
13.10 Maintenance .....	353
13.11 Configuration examples .....	353
13.11.1 Example for configuring ACL .....	353
13.11.2 Example for configuring RADIUS .....	355
13.11.3 Example for configuring TACACS+ .....	356
13.11.4 Example for configuring storm control .....	357
<b>14 Configuring link security .....</b>	<b>359</b>
14.1 Overview of link security .....	359

14.1.1 Link protection on PON interface .....	359
14.1.2 Link aggregation .....	363
14.1.3 Link-state tracking .....	363
14.1.4 RRPS.....	363
14.1.5 Loopback detection .....	364
14.1.6 Interface backup .....	365
14.2 Configuring OLT backbone fiber protection (Type B) .....	366
14.2.1 Preparing for configurations .....	366
14.2.2 Default configurations.....	366
14.2.3 Configuring OLT backbone fiber protection (Type B) .....	367
14.2.4 Configuring ONU holdover .....	367
14.2.5 Checking configurations .....	368
14.3 Configuring PON full protection (Type C).....	368
14.3.1 Preparing for configurations .....	368
14.3.2 Default configurations.....	368
14.3.3 Configuring OLT PON full protection (Type C) .....	368
14.3.4 Configuring ONU PON full protection (Type C).....	369
14.3.5 Checking configurations .....	370
14.4 Configuring PON full protection (Type D) .....	370
14.4.1 Preparing for configurations .....	370
14.4.2 Default configurations.....	370
14.4.3 Configuring OLT PON full protection (Type D).....	370
14.4.4 Checking configurations .....	371
14.5 Configuring OLT hand-in-hand uplink interface protection.....	371
14.5.1 Preparing for configurations .....	371
14.5.2 Default configurations.....	371
14.5.3 Configuring OLT hand-in-hand uplink interface protection .....	371
14.5.4 Checking configurations .....	372
14.6 Configuring cross-OLT PON interface dual-homed protection (Type B) .....	372
14.6.1 Preparing for configurations .....	372
14.6.2 Default configurations.....	372
14.6.3 Configuring cross-OLT PON interface dual-homed protection (Type B) .....	372
14.6.4 Checking configurations .....	373
14.7 Configuring link aggregation .....	373
14.7.2 Default configurations.....	374
14.7.3 Configuring manual link aggregation .....	374
14.7.4 Configuring static LACP link aggregation.....	375
14.7.5 Checking configurations .....	376
14.8 Configuring link-state tracking .....	376
14.8.2 Default configurations.....	377
14.8.3 Configuring link-state tracking .....	377
14.8.4 Checking configurations .....	377

14.9 Configuring RRPS .....	378
14.9.2 Default configurations.....	378
14.9.3 Creating Ethernet ring .....	378
14.9.4 Configuring basic functions of Ethernet ring .....	379
14.9.5 Checking configurations .....	380
14.9.6 Maintenance .....	381
14.10 Configuring loopback detection .....	381
14.10.1 Preparing for configurations .....	381
14.10.2 Default configurations.....	381
14.10.3 Configuring loopback detection on OLT .....	382
14.10.4 Configuring loopback detection on ONU .....	383
14.10.5 Checking configurations .....	384
14.11 Configuring interface backup .....	384
14.11.1 Preparing for configurations.....	384
14.11.2 Default configurations.....	384
14.11.3 Creating interface backup group .....	385
14.11.4 Configuring interface backup group.....	385
14.11.5 Configuring Force Switch .....	385
14.11.6 Checking configurations .....	386
14.12 Maintenance .....	386
14.13 Configuration examples .....	386
14.13.1 Example for configuring OLT backbone fiber protection (Type B) .....	386
14.13.2 Example for configuring PON full protection (Type C).....	388
14.13.3 Example for configuring cross-OLT PON interface dual-homed protection (Type B) .....	390
14.13.4 Example for configuring manual link aggregation.....	393
14.13.5 Example for configuring static LACP link aggregation .....	394
14.13.6 Example for configuring link-state tracking .....	396
14.13.7 Example for configuring Ethernet ring .....	397
14.13.8 Example for configuring loopback detection .....	399
14.13.9 Example for configuring interface backup .....	400
<b>15 Configuring system management.....</b>	<b>403</b>
15.1 Overview of system management .....	403
15.1.1 SNMP.....	403
15.1.2 Optical module DDM.....	405
15.1.3 System log.....	405
15.1.4 Ping .....	409
15.1.5 Traceroute .....	409
15.1.6 LLDP .....	410
15.1.7 Alarm and event management .....	412
15.2 Configuring SNMP .....	413
15.2.1 Default configurations.....	413

15.2.2 Configuring basic functions of SNMP v1/v2c .....	413
15.2.3 Configuring basic functions of SNMP v3 .....	414
15.2.4 Configuring other information of SNMP .....	415
15.2.5 Configuring Trap .....	416
15.2.6 Checking configurations .....	416
15.3 Configuring RMON .....	417
15.3.1 Default configurations .....	417
15.3.2 Configuring RMON statistics .....	417
15.3.3 Configuring RMON historical statistics .....	418
15.3.4 Configuring RMON alarm group .....	418
15.3.5 Configuring RMON event group .....	419
15.3.6 Checking configurations .....	419
15.4 Configuring optical module DDM .....	419
15.4.1 Default configurations .....	419
15.4.2 Configuring optical module DDM .....	419
15.4.3 Configuring optical module alarm .....	420
15.4.4 Checking configurations .....	420
15.5 Configuring Layer 2 protocol transparent transmission .....	421
15.5.1 Preparing for configurations .....	421
15.5.2 Default configurations .....	421
15.5.3 Configuring Layer 2 protocol transparent transmission .....	422
15.5.4 Checking configurations .....	423
15.5.5 Maintenance .....	423
15.6 Configuring PPPoE agent .....	423
15.6.1 Default configuration .....	423
15.6.2 Configuring PPPoE agent parameters .....	424
15.6.3 Enabling PPPoE agent .....	424
15.6.4 Checking configurations .....	425
15.7 Configuring Watchdog .....	425
15.8 Configuring system log .....	425
15.8.1 Default configurations .....	425
15.8.2 Configuring basic information about system log .....	425
15.8.3 Configuring output direction of system log .....	426
15.8.4 Checking configurations .....	426
15.9 Configuring port mirroring .....	427
15.9.1 Default configurations .....	427
15.9.2 Configuring port mirroring on OLT .....	427
15.9.3 Configuring port mirroring on ONU .....	427
15.9.4 Checking configurations .....	428
15.10 Configuring link detection .....	428
15.10.1 Ping .....	428
15.10.2 Traceroute .....	428



15.11 Configuring LLDP .....	429
15.11.1 Default configurations .....	429
15.11.2 Configuring global LLDP .....	429
15.11.3 Configuring LLDP on interface .....	430
15.11.4 Configuring LLDP alarm .....	430
15.11.5 Checking configurations .....	430
15.12 Configuring system monitoring.....	431
15.12.1 Default configurations.....	431
15.12.2 Configuring temperature monitoring .....	431
15.12.3 Configuring fan monitoring .....	432
15.12.4 Configuring CPU monitoring.....	432
15.12.5 Configuring memory monitoring .....	432
15.12.6 Checking configurations .....	432
15.13 Configuring link monitoring .....	433
15.13.1 Default configurations.....	434
15.13.2 Configuring link monitoring .....	434
15.13.3 Checking configurations .....	436
15.14 Configuring alarm and event management.....	436
15.14.1 Default configurations.....	436
15.14.2 Configuring alarm management.....	436
15.14.3 Configuring event management .....	439
15.14.4 Checking configurations .....	440
15.15 BCMP.....	441
15.15.1 Default configurations.....	441
15.15.2 Configuring BCMP .....	441
15.15.3 Checking configurations .....	442
15.16 Maintenance .....	442
15.17 Configuration examples .....	442
15.17.1 Example for configuring SNMP .....	442
15.17.2 Example for outputting system log to host.....	444
15.17.3 Example for configuring KeepAlive Trap.....	445
<b>16 Appendix .....</b>	<b>447</b>
16.1 Terms .....	447
16.2 Acronyms and abbreviations .....	453

# Figures

Figure 1-1 Accessing the ISCOM5508 through a PC connected with Console interface.....	12
Figure 1-2 Configuring communication parameters in Hyper Terminal .....	13
Figure 1-3 Networking with the OLT as the Telnet server .....	13
Figure 1-4 Networking with the OLT as the Telnet client .....	14
Figure 1-5 Configuring out-of-band network management.....	36
Figure 1-6 Configuring in-band network management .....	37
Figure 1-7 Upgrading OLT through TFTP .....	38
Figure 1-8 Configuring ONU auto-upgrade .....	39
Figure 2-1 Principle of EPON .....	43
Figure 2-2 Downlink and uplink transmission principle of EPON .....	43
Figure 2-3 Overall management in PON+LAN .....	46
Figure 2-4 Configuring EPON Ethernet data service .....	48
Figure 2-5 Configuring ONU independent management based on IP address pool .....	51
Figure 2-6 Configuring ONU auto-registration.....	96
Figure 2-7 Configuring ONU registration in MAC-based authentication mode .....	97
Figure 3-1 Unicast transmission mode .....	100
Figure 3-2 Broadcast transmission mode .....	100
Figure 3-3 Multicast transmission mode .....	101
Figure 3-4 Mapping between an IPv4 multicast address and a multicast MAC address.....	102
Figure 3-5 Operating positions of the IGMP and Layer 2 multicast protocols.....	103
Figure 3-6 IGMP Snooping networking.....	107
Figure 3-7 Dynamic controllable multicast networking.....	110
Figure 4-1 Typical application of SIP in NGN .....	134
Figure 4-2 Position of H.248 in the network .....	135
Figure 4-3 H.248 connection model .....	136
Figure 4-4 Configuring SIP voice service (Proxy call) .....	137

Figure 4-5 Configuring SIP voice service (Direct call) .....	142
Figure 4-6 Configuring H.248 voice service .....	146
Figure 5-1 Typical triple-play networking.....	182
Figure 5-2 Configuring CATV services .....	183
Figure 6-1 SAToP encapsulation principle of TDM signals .....	186
Figure 6-2 CESoPSN encapsulation principle of TDM signals .....	187
Figure 6-3 AAL1 unstructured encapsulation principle .....	187
Figure 6-4 AAL1 structured encapsulation principle .....	188
Figure 6-5 Self-adaptive clock synchronization mechanism principle.....	189
Figure 6-6 Differential clock synchronization mechanism principle .....	190
Figure 6-7 Logical relationship between Bundle and TDM interfaces .....	191
Figure 6-8 TDMoP service networking.....	192
Figure 7-1 Unicast forwarding mode of MAC address .....	207
Figure 7-2 Broadcast forwarding mode of MAC address .....	208
Figure 7-3 Configuring dynamic MAC address.....	218
Figure 7-4 Configuring static MAC address .....	220
Figure 8-1 Structures of Ethernet frame and 802.1Q frame .....	223
Figure 8-2 Basic QinQ networking .....	226
Figure 8-3 Configuring VLAN.....	244
Figure 8-4 Configuring VLAN translation.....	247
Figure 9-1 STP (selecting a root bridge) .....	250
Figure 9-2 STP (confirming ports).....	251
Figure 9-3 MSTP.....	252
Figure 9-4 Basic concepts of MSTP.....	253
Figure 9-5 MSTIs in a MST region.....	254
Figure 9-6 STP networking .....	268
Figure 9-7 MSTP networking.....	271
Figure 9-8 ONU RSTP networking.....	277
Figure 10-1 ARP networking .....	287
Figure 10-2 Configuring static routing.....	288
Figure 11-1 Typical application of DHCP.....	291
Figure 11-2 DHCP packet structure .....	292
Figure 11-3 DHCP Snooping networking .....	294

Figure 11-4 Working principle of DHCP Relay .....	295
Figure 11-5 Working principle of DHCP Option 82.....	295
Figure 11-6 DHCP Snooping networking .....	307
Figure 11-7 DHCP Relay networking .....	308
Figure 12-1 Traffic classification process .....	311
Figure 12-2 IP packet header structure.....	311
Figure 12-3 Structures of ToS priority and DSCP priority packets .....	311
Figure 12-4 VLAN packet structure.....	312
Figure 12-5 CoS priority packet structure.....	312
Figure 12-6 SP scheduling .....	313
Figure 12-7 WRR scheduling.....	314
Figure 12-8 DRR scheduling.....	314
Figure 12-9 Configuring rate limiting based on traffic policy .....	326
Figure 12-10 Configuring queue scheduling.....	327
Figure 13-1 ACL networking .....	354
Figure 13-2 RADIUS networking.....	355
Figure 13-3 TACACS+ networking .....	356
Figure 13-4 Storm control networking.....	357
Figure 14-1 Principle of OLT backbone fiber protection (Type B) .....	360
Figure 14-2 Principle of PON full protection (Type C).....	361
Figure 14-3 Principle of PON full protection (Type D) .....	362
Figure 14-4 Principle of cross-OLT PON interface dual-homed protection (Type B).....	362
Figure 14-5 Ethernet ring in normal status.....	364
Figure 14-6 Ethernet ring in switching status.....	364
Figure 14-7 Principle of interface backup.....	365
Figure 14-8 Principle of VLAN-based interface backup.....	366
Figure 14-9 Configuring OLT backbone fiber protection (Type B) .....	387
Figure 14-10 Configuring PON full protection (Type C).....	388
Figure 14-11 Configuring cross-OLT PON interface dual-homed protection (Type B).....	390
Figure 14-12 Manual link aggregation networking.....	393
Figure 14-13 Static LACP link aggregation networking.....	394
Figure 14-14 Link-state tracking networking .....	396
Figure 14-15 Ethernet ring networking .....	397

Figure 14-16 Loopback detection networking .....	399
Figure 14-17 Interface backup networking .....	400
Figure 15-1 Working mechanism of SNMP .....	404
Figure 15-2 Working principle of Ping.....	409
Figure 15-3 Working principle of Traceroute.....	410
Figure 15-4 Structure of LLDPDU .....	410
Figure 15-5 Structure of TLV .....	411
Figure 15-6 Authentication mechanism of SNMP V3.....	414
Figure 15-7 SNMP v3 networking .....	442
Figure 15-8 Outputting system log to host.....	444
Figure 15-9 KeepAlive networking.....	445

# Tables

Table 1-1 Corresponding relationship between the CLI level and user level .....	2
Table 1-2 Shortcut keys about display features .....	8
Table 2-1 ONU authentication modes .....	44
Table 2-2 Parameters of ONU IP address pool.....	50
Table 2-3 Parameters of ONU SNMP template.....	51
Table 6-1 Configuration parameters of TDMoP service.....	192
Table 8-1 VLAN modes and packet processing modes .....	224
Table 8-2 Processing modes of Ethernet frames in VLAN Transparent mode .....	225
Table 8-3 Processing modes of Ethernet frames in VLAN Tagged mode .....	225
Table 8-4 Processing modes of Ethernet frames in VLAN Translation mode.....	225
Table 8-5 Processing modes of Ethernet frames in VLAN Trunk mode .....	226
Table 11-1 Meanings of fields in the DHCP packet .....	292
Table 15-1 Log levels .....	406
Table 15-2 Alarm fields .....	408
Table 15-3 Alarm levels .....	408
Table 15-4 TLV type .....	411

# 1 Basic configurations

---

This chapter introduces basic configurations and configuration process of the ISCOM5508, and provides related configuration examples, including the following sections:

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

## 1.1 CLI

### 1.1.1 Overview

Command Line Interface (CLI) is the path for communication between users and the ISCOM5508. You can configure, monitor, and manage the ISCOM5508 by executing related commands.

You can log in to the ISCOM5508 through a PC that runs the terminal emulation program or the CPE device. You can enter into 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 historical command by checking command history. The last 5000 historical commands can be saved on the ISCOM5508.
- Online help is available by inputting "?" 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 ISCOM5508 uses hierarchy 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, etc. 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, etc.

### User levels

Corresponding to the CLI levels, users are divided into 15 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

–	Visitor	Monitor	Operator	Administrator
<b>administrator</b>	Permitted	Permitted	Permitted	Permitted
<b>operator</b>	Permitted	Permitted	Permitted	Forbidden
<b>monitor</b>	Permitted	Permitted	Forbidden	Forbidden
<b>visitor</b>	Permitted	Forbidden	Forbidden	Forbidden



## 1.1.3 Modes

### Overview

Command line 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 ISCOM5508. If the ISCOM5508 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 function is closely related to the CLI mode.
- 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.

### Mode list

The ISCOM5508 supports the following CLI modes:

Mode	Enter method	Description
User EXEC	Log in to the ISCOM5508, and input correct username and password.	Raisecom>

Mode	Enter method	Description
Privileged EXEC	In user EXEC mode, input the <b>enable</b> command and a correct password.  <b>Note</b> Only users in level 11 or above can enter this mode.	Raisecom#
Global configuration	In privileged EXEC mode, input the <b>config</b> command.	Raisecom(config)#
GE interface configuration	In global configuration mode, input the <b>interface gigabitethernet slot-id/port-id</b> command.	Raisecom(config-if-gigabitethernet-slot-id:port-id)#
GE interface batch configuration	In global configuration mode, input the <b>interface range gigabitethernet slot-id/port-list</b> command.	Raisecom(config-if-gigabitethernet-range)#
Aggregation group interface configuration	In global configuration mode, input the <b>interface port-channel group-id</b> command.	Raisecom(config-port-channel-group-id)#
VLAN interface configuration	In global configuration mode, input the <b>interface vlanif vlan-id</b> command.	Raisecom(config-vlanif-num)#
VLAN configuration	In global configuration mode, input the <b>vlan vlan-id</b> command.	Raisecom(config-vlan-id)#
EPON interface configuration	In global configuration mode, input the <b>interface epon-olt slot-id/port-id</b> command.	Raisecom(config-if-epon-olt-slot-id:port-id)#
EPON interface batch configuration	In global configuration mode, input the <b>interface range epon-olt slot-id/port-list</b> command.	Raisecom(config-if-epon-olt-range)#
RIP configuration	In global configuration mode, input the <b>router rip</b> command.	Raisecom(config-rip)#
KeyChain configuration	In global configuration mode, input the <b>key-chain keychainname</b> command.	Raisecom(config-keychain)#
MSTP region configuration	In global configuration mode, input the <b>spanning-tree region-configuration</b> command.	Raisecom(config-region)#
EPON ONU management configuration	In global configuration mode, input the <b>onu slot-id/olt-id/onu-id</b> command.	Raisecom(config-epon-onu-slot-id/olt-id:onu-id)#

Mode	Enter method	Description
EPON ONU management batch configuration	In global configuration mode, input the <b>epon-onu range slot-id/olt-id/onu-list</b> command.	Raisecom(config-epon-onu-range)#
EPON ONU voice service configuration	In global configuration mode, input the <b>epon-onu slot-id/olt-id/onu-id voice</b> command.	Raisecom(config-epon-onu-voice-slot-id/olt-id:onu-id)#
EPON ONU UNI configuration	In global configuration mode, input the <b>epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</b> command.	Raisecom(config-epon-onu-ethernet-slot-id/olt-id/onu-id:uni-id)#
EPON ONU UNI batch configuration	In global configuration mode, input the <b>epon-onu uni ethernet range slot-id/olt-id/onu-id/uni-list</b> command.	Raisecom(config-epon-onu-ethernet-range)#
EPON ONU serial interface configuration	In global configuration mode, input the <b>epon-onu uni serial-com slot-id/olt-id/onu-id/uni-id</b> command.	Raisecom(config-epon-onu-serial-slot-id/olt-id/onu-id:ser-id)#
EPON ONU serial interface batch configuration	In global configuration mode, input the <b>epon-onu uni serial-com range slot-id/olt-id/onu-id/uni-list</b> command.	Raisecom(config-epon-onu-serial-range)#
EPON ONU SNI configuration	In global configuration mode, input the <b>epon-onu slot-id/olt-id/onu-id sni</b> command.	Raisecom(config-epon-onu-sni-slot-id/olt-id:onu-id)#
EPON ONU TDM interface configuration	In global configuration mode, input the <b>epon-onu uni elt1 slot-id/olt-id/onu-id/uni-id</b> command.	Raisecom(config-epon-onu-elt1-slot-id/olt-id/onu-id:uni-id)#
EPON ONU TDM interface batch configuration	In global configuration mode, input the <b>epon-onu uni elt1 range slot-id/olt-id/onu-id/uni-list</b> command.	Raisecom(config-epon-onu-elt1-range)#
EPON ONU TDM Bundle configuration	In global configuration mode, input the <b>epon-onu bundle slot-id/olt-id/onu-id/bundle-id</b> command.	Raisecom(config-epon-onu-bundle-slot-id/olt-id/onu-id:bundle-id)#
EPON ONU TDM Bundle batch configuration	In global configuration mode, input the <b>epon-onu bundle range slot-id/olt-id/onu-id/bundle-list</b> command.	Raisecom(config-epon-onu-bundle-range)#
EPON ONU TDM service configuration	In global configuration mode, input the <b>epon-onu slot-id/olt-id/onu-id tdm</b> command.	Raisecom(config-epon-onu-service-profile:profile-id)#

Mode	Enter method	Description
EPON ONU service template configuration	In global configuration mode, input the <b>epon-onu-service-profile</b> <i>profile-id</i> command.	Raisecom(config-epon-onu-svr-template-template-id)#
EPON partner device configuration	In global configuration mode, input the <b>partner-profile</b> <i>profile-id</i> command.	Raisecom(config-epon-onu-partner-profile:profile-id)#
EPON PSE template configuration	In global configuration mode, use the <b>pse-profile</b> <i>profile-id</i> command.	Raisecom(config-epon-onu-pse-profile:profile-id)#
EPON voice template configuration	In global configuration mode, input the <b>voip-profile</b> <i>profile-id</i> command.	Raisecom(config-epon-onu-voip-profile:profile-id)#
EPON ONU line template configuration	In global configuration mode, input the <b>epon-onu-line-profile</b> <i>profile-id</i> command.	Raisecom(config-epon-onu-line-profile:profile-id)#
EPON ONU QoS template configuration	In global configuration mode, input the <b>epon-onu qos-template</b> <i>template-id</i> command.	Raisecom(config-epon-onu-qos-template-template-id)#
L2 ACL configuration	In global configuration mode, input the <b>l2-access-list</b> <i>acl-id</i> command.	Raisecom(config-l2-acl-acl-id)#
L2 ACL sub-rule configuration	In L2 ACL configuration mode, input the <b>rule</b> <i>rule-id</i> command.	Raisecom(config-l2-acl-acl-id-rule-rule-id)#
IPv4 ACL configuration	In global configuration mode, input the <b>ip-access-list</b> <i>acl-id</i> command.	Raisecom(config-ip-acl-acl-id)#
IPv4 ACL sub-rule configuration	In IPv4 ACL configuration mode, input the <b>rule</b> <i>rule-id</i> command.	Raisecom(config-ip-acl-acl-id-rule-rule-id)#
IPv6 ACL configuration	In global configuration mode, input the <b>ipv6-access-list</b> <i>acl-id</i> command.	Raisecom(config-ipv6-acl-acl-id)#
IPv6 ACL sub-rule configuration	In IPv6 ACL configuration mode, input the <b>rule</b> <i>rule-id</i> command.	Raisecom(config-ipv6-acl-acl-id-rule-rule-id)#
Hybrid ACL configuration	In global configuration mode, input the <b>hybrid-access-list</b> <i>acl-id</i> command.	Raisecom(config-hybrid-acl-acl-id)#
Hybrid ACL sub-rule configuration	In Hybrid ACL configuration mode, input the <b>rule</b> <i>rule-id</i> command.	Raisecom(config-hybrid-acl-acl-id-rule-rule-id)#

Mode	Enter method	Description
User ACL configuration	In global configuration mode, input the <b>user-access-list</b> <i>acl-id</i> command.	Raisecom(config-user-acl-acl-id)#
User ACL sub-rule configuration	In User ACL configuration mode, input the <b>rule</b> <i>rule-id</i> command.	Raisecom(config-user-acl-acl-id-rule-rule-id)#
VLAN ACL configuration	In global configuration mode, input the <b>vlan-access-list</b> <i>acl-id</i> command.	Raisecom(config-qinq-acl-1)#

## 1.1.4 Shortcut keys

The ISCOM5508 supports following shortcut keys.

Shortcut key	Description
Up cursor key (↑)	Show previous command if there is any command input earlier; the display has no change if the current command is the earliest one in history records.
Down cursor key (↓)	Show next command if there is any newer command; the display has no change if the current command is the newest one in history records.
Left cursor key (←)	Move the cursor one character to left; the display has no change if the cursor is at the beginning of command.
Right cursor key (→)	Move the cursor one character to right; the display has no change if the cursor is at the end of command.
<b>Backspace</b>	Delete the character before the cursor; the display has no change if the cursor is at the beginning of command.
<b>Tab</b>	<p>Press <b>Tab</b> after inputting a complete keyword, cursor will automatically appear a space to the end; press <b>Tab</b> again, the system will show the follow-up inputting keywords.</p> <p>Press <b>Tab</b> after inputting an incomplete keyword, system automatically executes partial helps:</p> <ul style="list-style-type: none"> <li>• System take the complete keyword to replace input if the matched keyword is the one and only, and leave one word space between the cursor and end of keyword;</li> <li>• In case of mismatch or matched keyword is not the one and only, display prefix at first, then press <b>Tab</b> to check words circularly, no space from cursor to the end of keyword, press <b>Space</b> to input the next word;</li> <li>• If input incorrect keyword, press <b>Tab</b> will change to the next line and prompt error, the input keyword will not change.</li> </ul>
<b>Ctrl+A</b>	Move the cursor to the head of line.

Shortcut key	Description
<b>Ctrl+C</b>	Break off some running operation, such as ping, traceroute and so on.
<b>Ctrl+D</b> or <b>Delete</b>	Delete the cursor location characters
<b>Ctrl+E</b>	Move the cursor to the end of line.
<b>Ctrl+K</b>	Delete all characters behind the cursor (including cursor location).
<b>Ctrl+X</b>	Delete all characters before the cursor (except cursor location).
<b>Ctrl+Z</b>	Return to privileged EXEC mode from other modes (except user EXEC mode).
<b>Space</b> or <b>Y</b>	When the terminal printing command line information exceeds the screen, continue to show the information in next screen.
<b>Enter</b>	When the terminal printing command line information exceeds the screen, continue to show the information in next 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 <b>Space</b> or <b>Y</b>	Scroll down one screen.
Press <b>Enter</b>	Scroll down one line.
Press any letter key (except <b>Y</b> )	Stop displaying and executing commands.

### Filtering display information

The ISCOM5508 supports 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

For more commands starting with the **show** parameter, see related manuals.

The **show** command of the ISCOM5508 supports 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.

Configure page-break for the ISCOM5508 as below.

Step	Command	Description
1	Raisecom# <b>terminal page-break enable</b>	Enable page-break. By default, page-break is enabled. You can use the <b>terminal page-break disable</b> command to restore default configurations.

## 1.1.6 Command history

The ISCOM5508 supports checking or executing some historical command by using the **history** command in any command line mode.

Raisecom>**history**

Maximum number of Terminal history commands :1000				
cmdExtTime	cmdExtResult	user	cmd	
-----				
0000:00:26:51	success	raisecom	ena	
0000:00:21:05	success	raisecom	config	
0000:00:20:53	success	raisecom	interface epon-onu 1/1/1	
0000:00:20:41	success	raisecom	ex	
0000:00:20:09	success	raisecom	epon-onu uni ethernet	
1/1/1/1				
0000:00:17:20	success	raisecom	language chinese	
0000:00:08:38	success	raisecom	language english	
0000:00:08:20	success	raisecom	ex	
0000:00:08:19	success	raisecom	exit	
0000:00:07:14	success	raisecom	show epon-onu 1/1/1 uni	
ethernet snmp trap				
0000:00:06:08	success	raisecom	config	
0000:00:05:24	success	raisecom	epon-onu uni ethernet	
1/1/1/1				
0000:00:00:52	success	raisecom	ex	
0000:00:00:51	success	raisecom	exit	

## 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** 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** 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:



<0-31> IP interface number

## Incomplete help

You can acquire incomplete 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   Install a card
```

- After you enter a command, press **Space**, 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 ISCOM5508 prints 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 device through Console interface

The Console interface is the control interface for local management. You can connect the Console interface on the ISCOM5508 to the RS-232 serial interface of a PC through a specified cable, and run the terminal emulation program on the PC to locally configure the ISCOM5508.



#### Note

For technical specifications of the Console interface and the corresponding configuration cable, see *ISCOM5508 (B) Hardware Description*.

You can log in to the ISCOM5508 through the Console interface only under the following two conditions:

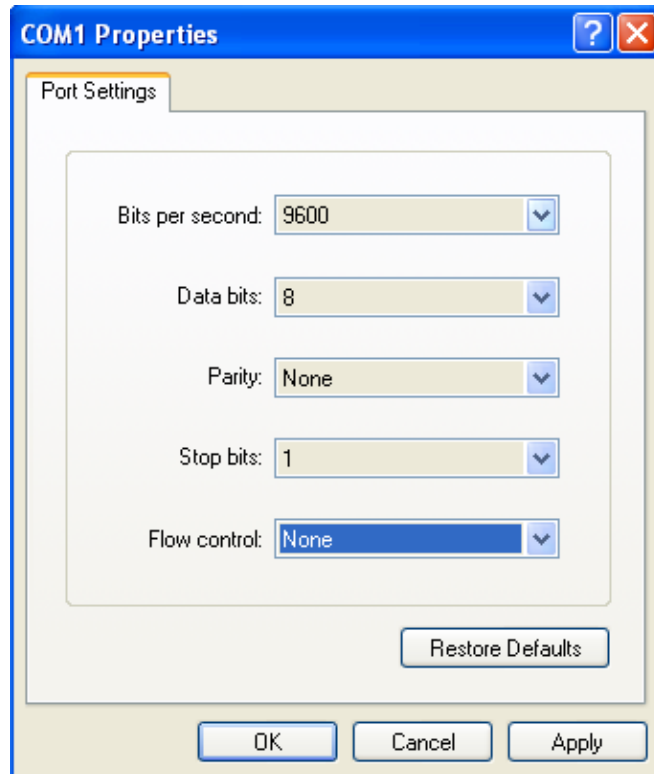
- The ISCOM5508 is configured for the first time.
- You cannot log in to the ISCOM5508 through Telnet.

If you want to access the ISCOM5508 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 ISCOM5508.

Figure 1-1 Accessing the ISCOM5508 through a PC connected with Console interface



Figure 1-2 Configuring communication parameters in Hyper Terminal



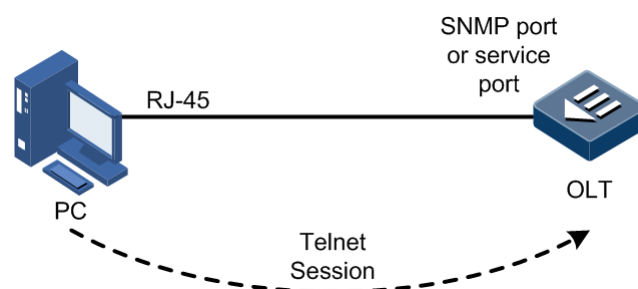
## 1.2.2 Accessing device through Telnet

To use a PC to log in to the ISCOM5508 remotely through Telnet, log in to an ISCOM5508 from the PC at first, and then Telnet other ISCOM5508 devices on the network. Thus, you do not need to connect a PC to each ISCOM5508. Moreover, you need to ensure that the ISCOM5508 can ping through the PC.

The ISCOM5508 provides the following Telnet services:

- Telnet Server: run the Telnet client program on a PC to log in to the ISCOM5508, 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



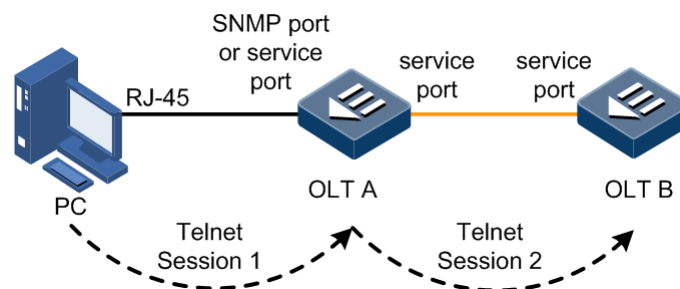
Before accessing the ISCOM5508 through Telnet, you need to log in to the ISCOM5508 through the Console interface and enable Telnet services.

Configure the ISCOM5508 working as the Telnet server as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>interface vlanif</b> <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlanif-num)# <b>ip address</b> <i>ip-address</i> [ <i>ip-mask</i> ] [ <i>vlan-id</i> ] Raisecom(config-vlanif-num)# <b>exit</b>	Configure the IP address, IP mask, and bound VLAN of the specified IP address for the ISCOM5508. The bound VLAN is the VLAN to which the interface to be enabled with Telnet services belongs.
4	Raisecom(config)# <b>telnet-server accept</b> { <b>add</b>   <b>remove</b> } <b>interface</b> { <b>gigabitethernet</b>   <b>epon-olt</b> } <i>slot-id/port-id</i>	(Optional) add/delete the interface enabled with Telnet. By default, Telnet is enabled on all interfaces.
5	Raisecom(config)# <b>telnet-server max-session</b> <i>number</i>	(Optional) configure the maximum number of Telnet sessions.
6	Raisecom(config)# <b>telnet-server close terminal-telnet</b> <i>session-number</i>	(Optional) disconnect a specified Telnet session.

- 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 ISCOM5508 working as the Telnet client as below.

Step	Command	Description
1	Raisecom# <b>telnet</b> { <i>ipv4-address</i>   <i>ipv6-address</i> [ <i>scopeid string</i> ] } [ <b>port</b> <i>port-id</i> ]	Log into other devices through Telnet.

### 1.2.3 Accessing device 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 ISCOM5508 through SSHv2, you must log in to the ISCOM5508 through the Console interface and enable the SSHv2 service.


## Default configurations

Default configurations of the SSHv2 service on the ISCOM5508 are as below.

Function	Default value
SSHv2 server status	Disable
RSA public key	N/A
SSHv2 key pair length	512 bits
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

## Configuring SSHv2

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#generate ssh-key [ key-length ]</b>	Generate the local SSHv2 server key pair. The key length can be configured.
3	<b>Raisecom(config)#ssh2 server</b>	Enable the SSHv2 server. You can use the <b>no ssh2 server</b> command to disable the SSHv2 server.
4	<b>Raisecom(config)#ssh2 server authentication { password   rsa-key   public-key }</b>	Configure the SSHv2 authentication mode and register the Public-Key function. You can use the <b>no ssh2 server authentication</b> command to restore default configurations.
5	<b>Raisecom(config)#ssh2 server authentication-timeout timeout</b>	(Optional) configure the SSHv2 authentication timeout. The ISCOM5508 refuses to authenticate and disconnects the connection when client authentication time exceeds the upper threshold. You can use the <b>no ssh2 server authentication-timeout</b> command to restore default configurations.

Step	Command	Description
6	<b>Raisecom(config)#ssh2 server authentication-retries <i>count</i></b>	(Optional) configure the allowable times for SSHv2 authentication failure. The ISCOM5508 refuses to authenticate and disconnects the connection when client authentication failure times exceed the upper threshold.
7	<b>Raisecom(config)#ssh2 server port <i>port-id</i></b>	<p>Configure the SSHv2 interception interface ID.</p> <p>You can use the <b>no ssh2 server port</b> command to restore default configurations.</p> <div>  <b>Note</b> </div> <p>When configuring the SSHv2 interception interface ID, input parameters cannot take effect immediately without rebooting the SSHv2 service.</p>
8	<b>Raisecom(config)#ssh2 server session <i>session-list</i> { enable   disable }</b>	Enable/Disable a specified SSHv2 session.

## 1.2.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show telnet-server</b>	Show interfaces supporting Telnet and the maximum number of Telnet sessions.
2	<b>Raisecom#show ssh2 server</b>	Show the SSHv2 server.
3	<b>Raisecom#show ssh2 session</b>	Show SSHv2 session.
4	<b>Raisecom#show ssh2 public-key authentication</b>	Show the SSHv2 authentication key.
5	<b>Raisecom#show ssh2 public-key rsa</b>	Show the SSHv2 RSA key.

## 1.3 Managing users

### 1.3.1 Default configurations

Default configurations of ISCOM5508 users are as below.


Function	Default value
Default user	<ul style="list-style-type: none"> <li>• User name: raisecom</li> <li>• Password: raisecom</li> <li>• User privilege: 15 (Administrator)</li> </ul>
New user privilege	15 (Administrator)



## Note

We recommend modifying the default user name and password to prevent illegal visits from breaking down the ISCOM5508.

### 1.3.2 Creating/Deleting users

Step	Command	Description
1	Raisecom# <b>user name</b> <i>username</i> <b>password</b> <i>password</i>	Create a user, or modify the user name and password.
2	Raisecom#password please input password: please input again:	Modify the password.
3	Raisecom# <b>no username</b> <i>username</i>	Delete a specified user.  <div style="text-align: center;">  <b>Caution</b>  Online users cannot be deleted. </div>



## Note

When modifying the password, you should input the same password for two times. Otherwise, the modification fails.

### 1.3.3 Managing user privileges

Step	Command	Description
1	Raisecom# <b>user name</b> <i>username</i> <b>privilege</b> <i>level</i>	(Optional) configure the user level and privilege.
2	Raisecom# <b>enable password</b>	(Optional) modify the password in privilege EXEC mode.
3	Raisecom# <b>user login</b> { <b>local-radius</b>   <b>local-user</b>   <b>radius-local</b>   <b>radius-</b> <b>user</b>   <b>tacacs-user</b>   <b>tacacs-local</b>   <b>local-tacacs</b> }	(Optional) configure the authentication mode for user login.
4	Raisecom# <b>enable login</b> { <b>local-radius</b>   <b>local-user</b>   <b>radius-local</b>   <b>radius-</b> <b>user</b>   <b>tacacs-user</b>   <b>tacacs-local</b>   <b>local-tacacs</b> }	(Optional) configure the authentication mode for login in privilege EXEC mode.

### 1.3.4 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, each of which 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.

Step	Command	Description
1	Raisecom# <b>command-set</b> <i>comsetname</i>	<p>Create a command set can enter command set configuration mode.</p> <p>You can use the <b>no command-set</b> <i>comsetname</i> command to delete the command set.</p> <div>  <h3>Note</h3> <p>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.</p> </div>
2	Raisecom(command-set:*)# <b>command</b> " <i>comkeywords</i> "	<p>You can use the keyword to add commands to the command set.</p> <p>You can use the <b>no command-set { all   comnum }</b> command to delete commands in the command set.</p>
3	Raisecom(command-set:*)# <b>end</b> Raisecom# <b>user</b> <i>username</i> { <b>allow-exeset</b>   <b>disallow-exeset</b> } <i>comsetname</i>	<p>Configure the command set privilege to allow or forbid some user to execute commands in the command set.</p> <p>You can use the <b>no user</b> <i>username</i> { <b>allow-exeset</b>   <b>disallow-exeset</b> } <i>comsetname</i> command to delete configurations of the command set privilege.</p>



## 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"
```

## 1.3.5 Checking configurations

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

## 1.4 Managing cards

### 1.4.1 Default configurations

Default configurations of cards on the ISCOM5508 are as below.

Function	Default value
Created type	<ul style="list-style-type: none"> <li>• Slots 1–3: null</li> <li>• Slots 4–5: ISCOM5508-POWER, which cannot be configured</li> <li>• Slot 6: ISCOM5508-FAN, which cannot be configured</li> </ul>
Actual type	N/A
Serial number	N/A
Card status	Not-used
Power satus	Off
Fan management mode	Auto
Fan speed level	40 at the maximum

### 1.4.2 Creating cards

The ISCOM5508 supports defining the card status through the following two types:

- Created type: the card type specified by users using the **creat card** 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.

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.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#create card slot <i>slot-id</i> type { ep4b   ge4b }</b>	Create a card on the ISCOM5508. You can use the <b>no create card slot <i>slot-id</i> [ now ]</b> command to delete the card.
3	<b>Raisecom(config)#device description <i>description</i></b>	(Optional) configure descriptions for the ISCOM5508 to identify different devices. You can use the <b>no device description</b> command to delete the descriptions.
4	<b>Raisecom(config)#slot <i>slot-id</i> description <i>description</i></b>	(Optional) configure descriptions for a specified slot. You can use the <b>no slot <i>slot-id</i> description</b> command to delete the descriptions.

## 1.4.3 Rebooting cards

Step	Command	Description
1	<b>Raisecom#reboot slot { <i>slot-id</i>   all } [ now ]</b>	Reboot the card in a specified slot or all cards.

## 1.4.4 Managing fan

The ISCOM5508 supports the intelligent fan. You can configure the speed of the fan manually.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#fan speed mode { auto   manual }</b>	Configure the fan management mode. You can use the <b>no fan speed mode</b> command to restore default configurations.
3	<b>Raisecom(config)#fan speed manual level</b>	Configure the fan speed level. You can use the <b>no fan manual</b> command to restore default configurations.

## 1.4.5 Checking configurations

No.	Command	Description
1	<b>Raisecom#show card</b>	Show information about all cards.
2	<b>Raisecom#show cpu-utilization [ dynamic ]</b>	Show the CPU utilization rate of the card.
3	<b>Raisecom#show device</b>	Show information about the ISCOM5508, including the type, MAC address, serial number, and slots on the main control card.
4	<b>Raisecom#show version slot slot-id</b>	Show version information about the card in a specified slot, including the type, hardware version, software version, bootrom version, firmware version, and CPLD version.
5	<b>Raisecom#show slot slot-id</b>	Show features of a specified slot, including the list of supported card types, descriptions, status, serial number, actual card type, and supposed card type. If the supposed card type is not specified, the value is null. If the actual card is not inserted into the slot, the value is null.
6	<b>Raisecom#show fan</b>	Show the fan status.

## 1.5 Managing interfaces

### 1.5.1 Default configurations

#### Default configurations of GE interfaces on OLT

Default configurations of GE interfaces on the ISCOM5508 are as below.

Function	Default value
Status	Enable
Rate and duplex mode	Auto-negotiation

Function	Default value
Flow control	Disable
Auto-MDI/MDIX	Normal
MTU	1522 Bytes
Interval of dynamic statistics	2s

## Default configurations of Ethernet interfaces on ONU

Default configurations of Ethernet interfaces on the ONU are as below.

Function	Default value
Status	Enable
Rate	auto
Duplex mode	auto
Flow control	Disable
MTU	1596 Bytes
Interval of dynamic statistics	2s


## 1.5.2 Enabling/Disabling interfaces

### Enabling/Disabling OLT interfaces

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <b>{ gigabitethernet   epon-olt } slot-</b> <b>id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-*-*:*)#shutdown</b>	Shut down the current interface. You can use the <b>no shutdown</b> command to enable the interface.

### Enabling/Disabling ONU interfaces

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

Step	Command	Description
2	<code>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</code>	Enter EPON ONU UNI configuration mode.
3	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)#shutdown</code>	<p>Shut down the current interface.</p> <p>You can use the <b>no shutdown</b> command to enable the interface.</p> <div>  <b>Note</b> </div> <p>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 2.15.9 Configuring ONU UNI alarm.</p>

## 1.5.3 Configuring basic properties of interfaces

### Configuring basic properties of OLT interfaces

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#system mtu size</code>	<p>Configure the global MTU.</p> <p>You can use the <b>no system mtu</b> command to restore default configurations.</p>
3	<code>Raisecom(config)#interface gigabitethernet slot-id/port-id</code>	Enter GE interface configuration mode.
4	<code>Raisecom(config-if-gigabitethernet-*/*)#speed { 100   1000   auto }</code>	Configure the interface rate.
5	<code>Raisecom(config-if-gigabitethernet-*/*)#description word</code>	<p>Configure descriptions of the interface.</p> <p>You can use the <b>no description</b> command to restore default configurations.</p>

### Configuring basic properties of ONU interfaces

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</code>	Enter EPON ONU UNI configuration mode.
3	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)#speed { 10   100   1000 } duplex { half   full }</code>	Configure the rate and duplex mode of the Ethernet interface on the ONU.
4	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)#speed auto</code>	Configure the rate and duplex mode to auto-negotiation on the Ethernet interface of ONU.

Step	Command	Description
5	<code>Raisecom(config-epon-onu-ethernet- */*/*:*)#uni name name</code>	Configure descriptions of physical interfaces.

## 1.5.4 Configuring interface statistics

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#dynamic statistics time period</code>	Configure the interval of dynamic statistics on the interface.  You can use the <b>no dynamic statistics time</b> command to restore default configurations.
3	<code>Raisecom(config)#clear interface { epon-olt   gigabitethernet } slot-id/port-id statistics</code>	Clear interface statistics saved on the ISCOM5508.

## 1.5.5 Configuring flow control on interfaces

### Configuring flow control on OLT interfaces

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface gigabitethernet slot-id/port-id</code>	Enter GE interface configuration mode.
3	<code>Raisecom(config-if- gigabitethernet-*:*)#flowcontrol { receive   send }</code>	Configure flow control on the interface and the direction of flow control.  You can use the <b>no flowcontrol { receive   send }</b> command to restore default configurations.

### Configuring flow control on ONU interfaces

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni- id</code>	Enter EPON ONU UNI configuration mode.
3	<code>Raisecom(config-epon-onu-ethernet- */*/*:*)#flowcontrol { enable   disable }</code>	Enable/Disable flow control on the physical interface.

## 1.5.6 Configuring IP interface

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlanif</b> <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	<b>Raisecom(config-vlanif-*)#ip</b> <b>address</b> <i>ip-address</i> [ <i>ip-mask</i> ] [ <i>vlan-id</i> ]	(Optional) configure the IPv4 address of VLAN interface. You can use the <b>no ip address ip-address</b> command to delete the configuration.
	<b>Raisecom(config-vlanif-*)#ipv6</b> <b>address</b> <i>ipv6-address/prefix-length</i> [ <i>eui-64</i> ] [ <i>link-local</i> ] [ <i>vlan-id</i> ]	(Optional) configure the master and slave IPv6 addresses of the VLAN interface. You can use the <b>no ipv6 address ipv6-address</b> command to delete the configuration.
4	<b>Raisecom(config-vlanif-*)#ip vlan</b> <i>vlan-id</i>	Configure mapping between the interface and VLAN. You can use the <b>no ip vlan</b> command to delete the configuration.

## 1.5.7 Configuring out-of-band network management interface

The SNMP interface is used for out-of-band network management. Before configuring out-of-band network management, you need to configure the IP address of the SNMP interface.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#management-port ip</b> <b>address</b> <i>ip-address</i> [ <i>mask</i> ]	Configure the IP address for the out-of-band management interface.
	<b>Raisecom(config)#management-port ipv6</b> <b>address</b> <i>ip-address</i> [ <i>link-local</i> ]	Configure the IPv6 address of the out-of-band management interface.



### Note

IP addresses of the out-of-band interface and the Layer 3 IP interface cannot be in the same network segment.

## 1.5.8 Cutting interface services

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

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

Step	Command	Description
2	<b>Raisecom(config)#running-config from interface gigabitethernet slot-id/port-id to interface gigabitethernet slot-id/port-id [ clear-source ]</b>	Cut the GE interface.
	<b>Raisecom(config)#running-config from interface ten-gigabitethernet slot-id/port-id to interface ten-gigabitethernet slot-id/port-id [ clear source ]</b>	Cut the 10 GE interface.
	<b>Raisecom(config)#running-config from interface epon-olt slot-id/port-id to interface epon-olt slot-id/port-id [ clear-source ]</b>	Cut the EPON interface.
	<b>Raisecom(config)#running-config from port-channel group-id to port-channel group-id [ clear-source ]</b>	Cut the LAG interface.



## Note

When enabling interface service cutting, pay attention to the following matters:

- Types of the source and destination interfaces should be consistent and they 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 cutting the EPON interface, there cannot be any online ONU under the destination PON interface.

## 1.5.9 Checking configurations

### Checking configurations of OLT interfaces

No.	Command	Description
1	<b>Raisecom#show interface { epon-olt   gigabitethernet } slot-id/olt-id</b>	Show interface status, including enabling/disabling status, rate, duplex mode, and forwarding mode.
2	<b>Raisecom#show interface { epon-olt   gigabitethernet } slot-id/olt-id description</b>	Show descriptions of a specified physical interface.
3	<b>Raisecom#show interface { epon-olt   gigabitethernet } slot-id/olt-id statistics</b>	Show interface statistics.
4	<b>Raisecom#show interface { epon-olt   gigabitethernet } slot-id/olt-id flowcontrol</b>	Show flow control information about the interface.
5	<b>Raisecom#show system mtu</b>	Show the maximum length of forwarding frame.
6	<b>Raisecom#show management-port { ip-address   ipv6-address }</b>	Show the IPv4 or IPv6 address of the out-of-band management interface.
7	<b>Raisecom#show { ip   ipv6 } interface brief</b>	Show the IPv4 or IPv6 address of the IP interface.
8	<b>Raisecom#show interface vlanif [ if-id ] statistics</b>	Show statistics of the IP interface.



## Checking configurations of ONU interfaces

No.	Command	Description
1	<b>Raisecom#show interface epon-onu [ slot-id/olt-id/onu-id ] creation-information</b>	Show creation information about the ONU.
2	<b>Raisecom#show interface epon-onu [ slot-id/olt-id/onu-id ] online-information</b>	Show online information about the ONU.
3	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id information</b>	Show information about the ONU.
4	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id name</b>	Show the name of a UNI on the ONU.
5	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id information</b>	Show information about the UNI on ONU, such as rate, duplex mode, flow control, and connection status.
6	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id isolation</b>	Show isolation status of the UNI on ONU.
7	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id auto-negotiation ability</b>	Show the auto-negotiation ability of the UNI on ONU.
8	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id statistic</b>	Show statistics of the UNI on ONU.
9	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id pon statistic</b>	Show statistics of the PON interface on ONU.
10	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uplink statistic</b>	Show statistics of the uplink interface on ONU.

## 1.6 Managing time

### 1.6.1 Default configurations

Default configurations of time management on the ISCOM5508 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

## 1.6.2 Configuring time and time zone

### Configuring time

Step	Command	Description
1	<code>Raisecom#clock set hour minute second year month day</code>	Configure the system time, including hour, minute, second, year, month, and day.

### Configuring time zone

Step	Command	Description
1	<code>Raisecom#clock timezone { +   - } hour minute</code>	Configure the time zone. You can use the <b>clock timezone</b> command to restore default configurations.

## 1.6.3 Configuring DST

Daylight Saving Time (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.

Step	Command	Description
1	<code>Raisecom#clock summer-time</code>	Enable DST. Use the <b>no clock summer-time</b> command to disable DST.
2	<code>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</code>	Configure the calculating period of DST. You can use the <b>no clock summer-time recurring</b> command to restore default configurations.



### 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 advance the clock one hour faster 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, the DST is the period from the start time this year to the end time next year.

## 1.6.4 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 ISCOM5508 can provide different applications over a unified time. Meanwhile, NTP can ensure very high accuracy, with accuracy of 10ms around.

The ISCOM5508 in support of NTP cannot only accept synchronization from other clock source, but also synchronize other devices as a clock source.

The ISCOM5508 adopts multiple NTP working modes for time synchronization:

- Server mode

In this mode, the ISCOM5508 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 ISCOM5508 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.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ntp server</b> { <i>ip-address</i>   <i>ipv6-address</i> } [ <b>version</b> <i>version-number</i> ]	(Optional) configure the IP address of the NTP server. You can use the <b>no ntp server</b> { <i>ip-address</i>   <i>ipv6-address</i> } command to restore default configurations.
3	<b>Raisecom(config)#ntp peer</b> { <i>ip-address</i>   <i>ipv6-address</i> } [ <b>version</b> <i>version-number</i> ]	(Optional) configure the IP address of the NTP symmetric peer. You can use the <b>no ntp peer</b> { <i>ip-address</i>   <i>ipv6-address</i> } command to restore default configurations.
4	<b>Raisecom(config)#ntp refclock-master</b> [ <i>clock-source</i> ]	(Optional) configure the local clock as the NTP reference clock source. You can use the <b>no ntp refclock-master</b> command to delete the configuration.



## Note

If the ISCOM5508 is configured as the NTP reference clock source, it cannot be configured as the NTP server or NTP symmetric peer; and vice versa.

## 1.6.5 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 for the ISCOM5508 to synchronize its system time with the SNTP server, thus realizing time synchronization on the whole network.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#sntp-client</b>	Enable SNTP Client. You can use the <b>no sntp client</b> command to disable this function.
3	<b>Raisecom(config)#sntp-client server { ip-address   ipv6-address }</b>	Configure the IP address of the SNTP client. You can use the <b>no sntp-client server</b> command to restore default configurations.



## Note

SNTP and NTP are mutually exclusive.

## 1.6.6 Checking configurations

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

## 1.7 Upgrade and backup

### 1.7.1 Introduction

The ISCOM5508 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.

## 1.7.2 Configuring server


The ISCOM5508 supports upgrade and backup through the FTP/TFTP server.




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

- The ISCOM5508 is connected to the FTP/TFTP server correctly.
- Configure the FTP/TFTP server and ensure the server can be accessed.
- Configure related parameters of the FTP/TFTP server on the ISCOM5508 to enable it to access the FTP/TFTP server.

Step	Command	Description
1	Raisecom# <b>ftp</b> <i>ip-address username password</i>	Configure the IPv4 parameters of the FTP.
2	Raisecom# <b>ftp</b> <i>ipv6-address [ scopeid scopeid-id ] username password</i>	Configure the IPv6 parameters of the FTP.
3	Raisecom# <b>tftp</b> <i>ip-address</i>	Configure the IPv4 parameters of the TFTP.
4	Raisecom# <b>tftp</b> <i>ipv6-address [ scopeid scopeid-id ]</i>	Configure the IPv6 parameters of the TFTP.

## 1.7.3 Upgrading OLT system files

Step	Command	Description
1	Raisecom# <b>download</b> { <b>mainrom1</b>   <b>mainrom2</b>   <b>system1</b>   <b>system2</b>   <b>cp1d</b>   <b>startup-config</b> } <b>ftp</b> <i>ip-address username password filename slot 1</i>	<p>(Optional) upgrade the system boot file or startup file through FTP.</p> <p> <b>Note</b></p> <p>Use the <b>show version</b> command to show whether the system is active before selecting system1/system2. If one system is active, you have to upgrade the other one.</p>

Step	Command	Description
	Raisecom# <b>download</b> { <b>mainrom1</b>   <b>mainrom2</b>   <b>system1</b>   <b>system2</b>   <b>cp1d</b>   <b>startup-config</b> } <b>tftp</b> <i>ip-address filename slot 1</i>	(Optional) upgrade the system boot file or startup file through TFTP.   <b>Note</b> Use the <b>show version</b> command to show whether the system is active before selecting system1/system2. If one system is active, you have to upgrade the other one.
2	Raisecom# <b>commit</b> { <b>mainrom1</b>   <b>mainrom2</b>   <b>system1</b>   <b>system2</b> }	Specify the version of the system software or startup software to be loaded.   <b>Note</b> After specifying the version, you need to reboot the ISCOM5508 to switch to the specified version.
3	Raisecom# <b>write startup-config</b>	Save the current configurations.
4	Raisecom# <b>erase startup-config</b>	(Optional) clear the current system configuration file.   <b>Caution</b> Clearing the system configuration file may lead to service interruption. Use this command with caution.

## 1.7.4 Backing up OLT system files

Step	Command	Description
1	Raisecom# <b>upload startup-config</b> { <b>ftp</b> <i>ip-address username password filename</i>   <b>tftp</b> <i>ip-address filename</i> } <b>slot 1</b>	(Optional) back up the system startup file.
2	Raisecom# <b>upload history-cmd</b> <b>ftp</b> <i>ip-address username password filename</i>	(Optional) back up the history operation file through FTP.

## 1.7.5 Upgrading ONU system files

Step	Command	Description
1	Raisecom# <b>download</b> { <b>system1</b>   <b>system2</b> } <b>ftp</b> <i>ip-address username password filename</i> <b>epon-onu</b> { <i>slot-id/olt-id/onu-list</i>   <b>all</b>   <b>slot slot-id</b> }	(Optional) upgrade ONU system files through FTP.
	Raisecom# <b>download</b> { <b>system1</b>   <b>system2</b> } <b>tftp</b> <i>ip-address filename</i> <b>epon-onu</b> { <i>slot-id/olt-id/onu-list</i>   <b>all</b>   <b>slot slot-id</b> }	(Optional) upgrade ONU system files through TFTP.

## 1.7.6 Managing ONU configuration files

Step	Command	Description
1	Raisecom# <b>download startup-config</b> { <b>ftp</b> ip-address username password filename   <b>tftp</b> ip-address filename } <b>onu</b> slot-id/olt-id/onu-id	(Optional) download ONU startup configuration files through FTP or TFTP.
	Raisecom# <b>upload startup-config</b> { <b>ftp</b> ip-address username password filename   <b>tftp</b> ip-address filename } <b>onu</b> slot-id/olt-id/onu-id [ <b>schedule-list</b> list-number ]	(Optional) upload ONU startup configuration files through FTP or TFTP.
2	Raisecom(config)# <b>config</b> Raisecom(config)# <b>epon-onu</b> slot-id/olt-id/onu-id	Enter EPON ONU remote management configuration mode.
3	Raisecom(config-epon-onu-*/*/*:*)# <b>restore startup-config</b>	(Optional) restore the ONU to default configurations.
4	Raisecom(config-epon-onu-*/*/*:*)# <b>reload startup-config</b>	(Optional) reload the ONU startup configuration file.
5	Raisecom(config-epon-onu-*/*/*:*)# <b>write</b>	Save ONU configuration files.

## 1.7.7 Configuring auto-save

The ISCOM5508 supports the auto-save feature. This feature can avoid loss of system configurations due to human carelessness, such as forgetting to save the configuration.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>auto-write</b> { <b>enable</b>   <b>disable</b> }	Enable/Disable the auto-save feature.
3	Raisecom(config)# <b>auto-write time</b> time	(Optional) configure the time for auto-save.

## 1.7.8 Configuring ONU auto-upgrade

ONU auto-upgrade refers that you can configure the ONU of specified type to automatically download files for upgrade from the specified FTP/TFTP server and complete batch upgrade, thus facilitating you to manage and maintain the ONU in batch.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>auto-upgrade</b> { <b>enable</b>   <b>disable</b> }	Enable/Disable ONU auto-upgrade.
3	Raisecom(config)# <b>auto-upgrade time</b> start-time	Configure the start time of auto-upgrade. You can use the <b>no auto-upgrade time</b> command to restore default configurations.

Step	Command	Description
4	<b>Raisecom(config)#auto-upgrade add device-type onu-type { ftp ip-address username password filename   tftp ip-address filename }</b>	Add an auto-upgrade plan based on FTP or TFTP.
5	<b>Raisecom(config)#auto-upgrade delete device-type onu-type</b>	(Optional) delete an auto-upgrade plan.
6	<b>Raisecom(config)#auto-upgrade device-type { type-name now   all }</b>	Perform auto-upgrade on the specified OUN or all ONUs.

## 1.7.9 Configuring ONU performance template

The file name of the ONU performance template in the OLT system is onu-template.ini. The template contains the manageable ONU models and remote management performance differences of those ONU models.

By upgrading the ONU performance template, you can enable the OLT to manage more ONU models.



### Note

The ONU performance template is the basis for the OLT to remotely manage the ONU. We do not recommend modifying and downloading the template.

Step	Command	Description
1	<b>Raisecom#download onu-template { ftp ip-address username password filename   tftp ip-address filename }</b>	(Optional) download the ONU performance template through FTP/TFTP.
2	<b>Raisecom#upload onu-template { ftp ip-address username password filename   tftp ip-address filename }</b>	(Optional) back up the ONU performance template through FTP/TFTP.

## 1.7.10 Checking configurations

No.	Command	Description
1	<b>Raisecom#show { ftp   tftp }</b>	Show FTP/TFTP default configuration parameters.
2	<b>Raisecom#show startup-config</b>	Show configurations loaded upon the startup of the device.
3	<b>Raisecom#show running-config</b>	Show running configurations of the device.
4	<b>Raisecom#show version</b>	Show versions of the system.
5	<b>Raisecom#show version [ slot slot-id   epon-onu slot-id/olt-id/onu-list ]</b>	Show the specified slot or ONU version.
6	<b>Raisecom#show auto-write</b>	Show configurations of auto-save.
7	<b>Raisecom#show auto-upgrade information</b>	Show configurations of auto-upgrade and operation information.



## 1.8 Task scheduling

### 1.8.1 Introduction

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

The ISCOM5508 supports realizing task scheduling by combining a schedule list to 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.

### 1.8.2 Default configurations

N/A

### 1.8.3 Configuring task scheduling

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#schedule-list</b> <i>number</i> <b>start</b> { <b>up-time</b> <i>days time</i> [ <b>every</b> <i>days time</i> [ <b>stop</b> <i>days time</i> ] ]   <b>date-time</b> <i>date time</i> [ <b>every</b> { <b>day</b>   <b>week</b>   <i>days time</i> } [ <b>stop</b> <i>date time</i> ] ] }	Add or modify entries in the schedule list, including the start time, interval, and end time of the task.  You can use the <b>no schedule-list list-no</b> command to delete the schedule list.
3	<b>Raisecom(config)#command-string</b> <b>schedule-list</b> <i>number</i>	Add commands to the schedule list.  You can use the <b>no schedule-list number command cmd-no</b> command to delete commands in the schedule list.

### 1.8.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show schedule-list</b>	Show configurations of the schedule list.

## 1.9 Maintenance

Command	Description
<b>Raisecom(config)#clear interface epon-olt</b> <b>slot-id/port-id statistics</b>	Clear statistics of the Ethernet interface.

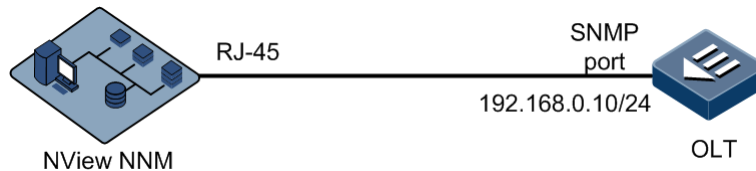
## 1.10 Configuration examples

### 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
```

Prefix	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 Layer 3 IP address 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 gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:1)#switchport trunk allowed vlan 2
Raisecom(config-if-gigabitethernet-1:1)#exit
  
```

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

```

Raisecom(config)#interface vlanif 0
Raisecom(config-vlanif-0)#ip address 192.168.0.1 255.255.255.0 2
  
```

## Checking results

Show the IP address of the Layer 3 IP interface.

```

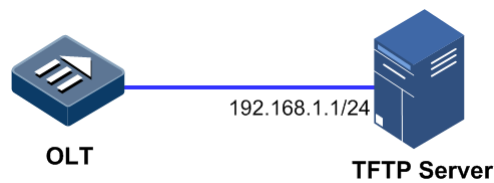
Raisecom#show interface vlanif
VRF          IF          Address
NetMask
-----
Default-IP-Routing-Table  vlan0          192.168.0.1    255.255.255.0
  
```

## 1.10.3 Example for upgrading OLT through TFTP

### Networking requirements

As shown in Figure 1-7, 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 ISCOM5508B-ROAP\_2.2.2\_20130607.

Figure 1-7 Upgrading OLT through TFTP



## Configuration steps

Step 1 Download the system startup file through TFTP.

```
Raisecom#download system1 tftp 192.168.1.1 ISCOM5508b-roap_2.2.2_20130607 slot 1
```

Step 2 Write the configured file to the memory.

```
Raisecom#write startup-config
```

Step 3 Reboot the ISCOM5508 and it will automatically load the downloaded system startup file.

```
Raisecom#reboot
```

## Checking results

Show OLT versions.

```
Raisecom#show version
Copyright (c) 2010-2012 Raisecom Technology Co., Ltd .
Slot ID: 1
Card Type       : ISCOM5508-EPSC
Product  Version : --
System1  Version : ISCOM5508B_ROAP_2.2.2_20130607 (active)
(committed)
System2  Version : ISCOM5508B_ROAP_2.2.2_20130607
Bootrom  Version : ISCOM5508B_FLASH_BOOTROM_2.0.2_20130607
Firmware1 Version : --
Firmware2 Version : --
CPLD     Version : V1.0
Mainrom1  Version : ISCOM5508B_FLASH_BOOTROM_2.0.2_20130607
(active) (committed)
Mainrom2  Version : ISCOM5508B_FLASH_BOOTROM_2.0.2_20130607
Active   Version : ISCOM5508B_ROAP_2.2.2_20130607
System   Uptime   : 0 days, 9 hours, 57 minutes
```

## 1.10.4 Example for configuring ONU auto-upgrade

### Networking requirements

As shown in Figure 1-8, the ONU auto-upgrade feature can periodically upgrade the ONU remotely according to configurations. Basic requirements are as below:

- IP address of the TFTP server: 192.168.1.1/24
- ONU type: ISCOM5304
- Auto-upgrade time: 2:00 a.m.
- Auto-upgrade system file: startup\_config

Figure 1-8 Configuring ONU auto-upgrade



### Configuration steps

Step 1 Configure the IP address of the TFTP server and add an auto-upgrade configuration program.

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

Step 2 Configure the start time of auto-upgrade to 2:00 am.

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

Step 3 Enable auto-upgrade.

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

### Checking results

Show auto-upgrade configurations and operation information.

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

## 1.10.5 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

---

This chapter introduces EPON services and configuration process of the ISCOM5508, and provides related configurations examples, including the following sections:

- Overview of EPON
- Quick configuration of EPON services
- Registration and deregistration
- Configuring ONU IP address pool
- Configuring ONU SNMP template
- Configuring ONU template
- Configuring ONU line template
- Configuring ONU service profile
- Configuring partner profile
- Configuring PSE profile
- Configuring voice profile
- Configuring ONU QoS profile
- Configuring DBA template
- Configuring EPON interface
- Configuring ONU
- Configuration examples

## 2.1 Overview of EPON

With increasing of Internet users and rapid growing of data services, such as HD video, Internet TV, and upload and download of large files, demands on network bandwidth become increasingly higher. Fiber access is undoubtedly the most effective solution and the EPON technology becomes the optimal scheme for point-to-multipoint Ethernet fiber access.

### 2.1.1 Structure of EPON system

The EPON system adopts a point-to-multipoint Ethernet topology structure. It transmits the data, voice, and video through fiber to ensure full-access and high-speed transmission.

Typical EPON is composed of three parts:

- Optical Line Terminal (OLT)

The OLT is a switch or router and a multi-service platform, which provides an optical interface connected to the PON. It is the core of an EPON system. The main functions of an OLT are as below:

- Broadcast Ethernet data to the ONU.
- Initiate and control the ranging process, and record the information.
- Allocate bandwidth for the ONU. That is, control the start time and window size for the ONU to send data.
- Manage the ONU through the OAM protocol.
- Provide others Ethernet functions.

- Optical Network Unit (ONU)

In the EPON system, the ONU adopts the Ethernet protocol, which is mature in technology and economical. It can realize low-cost Layer 2 or Layer 3 switching functions. The main functions of an ONU are as below:

- Choose to receive broadcast data from an OLT.
- Respond to the ranging command from the OLT, and make the corresponding adjustment.
- Buffer users' Ethernet data, and send them to uplink direction within the time window distributed by the OLT.
- Provide other Ethernet functions.

- Optical Distribution Network (ODN)

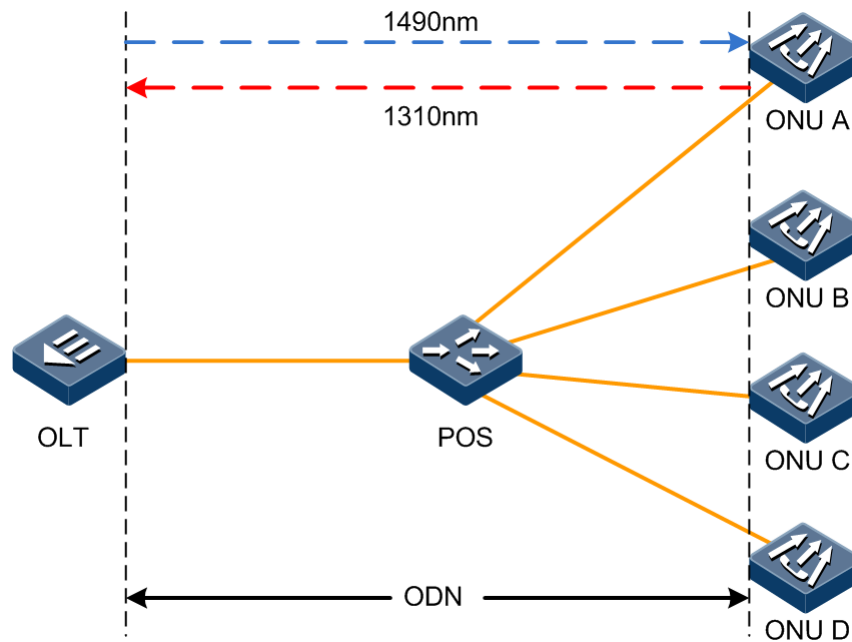
The ODN is composed of Passive Optical Splitter (POS) and fiber. POS is a passive device to connect the OLT and ONU, used to distribute downlink data and aggregate uplink data.

## 2.1.2 EPON principle

Figure 2-1 shows the principle of EPON.



Figure 2-1 Principle of EPON

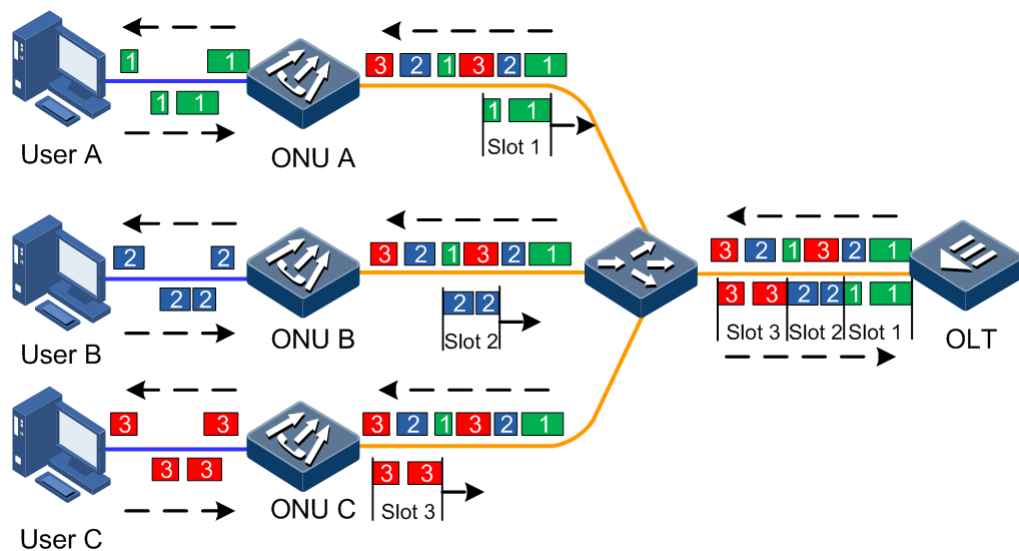


In order to separate signals of multiple users in different directions on the same fiber, the EPON system uses the following multiplexing technologies:

- Use 1490 nm wavelength in downlink direction, and use 1310 nm wavelength in uplink direction. Use CWDM to complete transmission of uplink and downlink signals on one fiber.
- Use TDM technology to transmit downlink data. Each ONU only receives its own data, and the downlink transmission rate is 1.25 Gbit/s.
- Use TDMA technology to transmit uplink data. Each ONU sends data in the distributed timeslot without conflict detection. The uplink transmission rate is 1.25 Gbit/s.

Figure 2-2 shows the downlink and uplink transmission principle of EPON.

Figure 2-2 Downlink and uplink transmission principle of EPON



## 2.1.3 Splitting ratio

The EPON adopts a point-to-multipoint transmission mode to split optical signals. The splitting ratio is a key index for the EPON system, which is in tree topology.

The splitting ratio refers to the number of ONUs connected to an EPON interface.

The ISCOM5508 supports up to 1:64 splitting ratio.



### Note

When the ISCOM5508 is used in the scenario of 1:64 splitting ratio, the two-stage splitting technology should be used, that is, "one PON interface + one 1:2 splitter + one 1:32 splitter".

## 2.1.4 ONU authentication

There are six ONU authentication modes, as listed in Table 2-1.

Table 2-1 ONU authentication modes

Authentication mode	CLI option	Description
Automatic authentication	none	The ONU can register successfully without authentication.
MAC-based authentication	mac	Only the ONU whose MAC address is listed in the MAC address table authorized by the OLT can register successfully; otherwise, the registration fails.
SN-based authentication	sn	Only the ONU whose SN is listed in the SN table authorized by the OLT can register successfully; otherwise, the registration fails.
PASSWORD-based authentication	password	Only the ONU whose local password is listed in the PASSWORD table authorized by the OLT can register successfully; otherwise, the registration fails.
Authentication based on SN+PASSWORD	sn-password	Only the ONU whose SN and local password are listed in the SN table and PASSWORD table authorized by the OLT respectively can register successfully; otherwise, the registration fails.
Hybrid authentication	hybrid	The ONU can choose either of the six authentication modes flexibly as required. The system can compare the authentication mode of the ONU with the authorized records; if matched, the ONU registers successfully; otherwise, the registration fails.

The last five authentication modes are manual ones. In these modes, you need to create the ONU device. The ONU applying for registration should match with the created ONU in aspects of MAC address, SN, password, and SN+password; otherwise, the registration fails.



### Note

- The manual authentication mode, characterized by higher security, can prevent illegal ONUs from accessing the network. So it is applicable to the public access network which has higher demands on security. The automatic authentication

mode, characterized by simpleness, flexibility, and "plug and play", is applicable to the private network.

- The hybrid authentication mode provides the PON interface of the OLT with a more flexible ONU authentication mode. In this mode, the ONU under a specified PON interface can flexibly choose the authentication mode as required.

## 2.1.5 ONU management

In the EPON system, there are two ONU management modes:

- OLT remote management
- ONU independent management

### OLT remote management

OLT remote management refers that the OLT works as the control end on the PON and the ONU works as the controlled end. The OLT manages parameters and properties of the ONU remotely through the OAM protocol packet based on 802.3ah and CTC standards.

OLT remote management adopts the point-to-multipoint control method, which makes the control end concentrated to one node, thus facilitating control of the whole network. However, it cannot manage and control lower-layer devices of the ONU and cannot realize overall management of the PON in PON+LAN scenario.

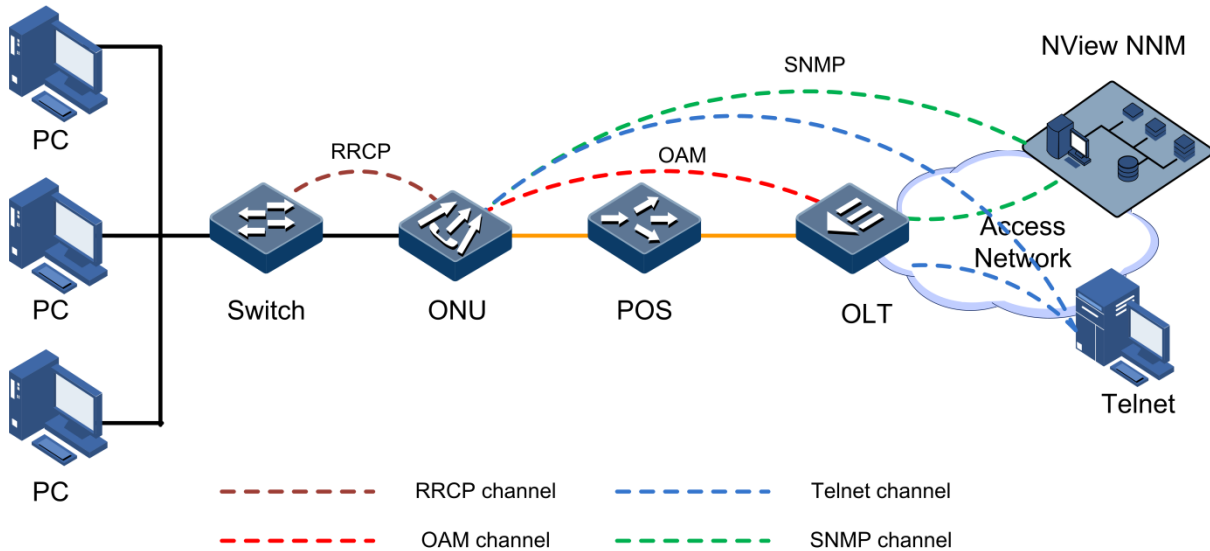
### ONU independence management

ONU independent management refers to logging in to and managing the ONU as well as configuring related network parameters and features of it through the NView NNM system or Telnet directly after configuring the management IP address and SNMP parameters of the ONU through the OLT. At this time, the ONU works as an independent device.

In ONU independent management mode, the system can directly manage network parameters and features of the lower-layer device, such as the ISCOM1000EM series switch, through the RRCP packet.

By combining OLT remote management, ONU independent management, and RRCP management, overall management of the whole PON in PON+LAN networking can be realized, as shown in Figure 2-3.

Figure 2-3 Overall management in PON+LAN



## 2.1.6 Data encryption

The EPON system adopts the broadcast mode in downlink direction, so a malicious user can easily intercept other users' data in the system. To improve confidentiality of the user data, the system supports two data encryption modes in the downlink direction: Triple Churning and AES-128. Moreover, it supports configuring different encryption modes for each Logical Link Identifier (LLID).

## 2.1.7 DBA

The EPON system adopts the Dynamic Bandwidth Allocation (DBA) mechanism to enhance uplink bandwidth utilization, ensure fairness and Quality of Service (QoS) of services, and allocate bandwidth grant according to the queue status reported by LLID.

DBA supports the following three bandwidth types:

- **Fixed Bandwidth:** the OLT periodically sends a fixed number of bandwidth grant to the ONU. Fixed bandwidth is reserved for the specified ONU or services, and cannot be used by other ONUs. Even when there is no uplink data through the ONU, the OLT still allocates grant corresponding to the fixed bandwidth for the ONU. Fixed bandwidth is usually used to transmit TDM service for the ONU or LLID to ensure a small transmission delay.
- **Assured Bandwidth:** the assured bandwidth is that surely obtained by the ONU, which is granted by the OLT according to the REPORT of the ONU. When the actual service data of the ONU do not reach the assured bandwidth, the OLT allocates the extra bandwidth to other ONUs through the DBA mechanism.
- **Best Effort Bandwidth:** when the bandwidth of the EPON interface is not occupied by services of higher priorities, the ONU can use this part of bandwidth. The OLT allocates bandwidth grant for the ONU according to the REPORT of all online ONUs in the EPON system and bandwidth occupation status of the EPON interface. The system does not ensure the quantity of bandwidth obtained by the OUN or specified services. Best-effort bandwidth is the service type of the lowest priority.

Parameters of ONU uplink bandwidth include Fixed Information Rate (FIR), Committed Information Rate (CIR), and Peak Information Rate (PIR). The relationship between different bandwidth types and these configuration parameters are as below:

- Fixed Bandwidth: FIR
- Assured Bandwidth: CIR+FIR
- Best Effort Bandwidth: PIR+CIR

The DBA algorithm in the EPON system supports the fairness mechanism to ensure the extra bandwidth to be allocated fairly according to the following three methods:

- Perform weighted allocation on extra bandwidth according to priorities.
- Perform weighted allocation on extra bandwidth according to assured bandwidth in the Service Level Agreement (SLA) signed with different users.
- Perform weighted allocation of extra bandwidth according to ONU types.

To support QoS in scenario of multi-service access, the OLT can allocate uplink bandwidth based on the report of ONU's local queue status, and the ONU can schedule uplink services according to the local queue status based on the bandwidth grant through DBA.

## 2.1.8 Layer 2 isolation

The OLT realizes Layer 2 isolation among ONUs. By default, ONUs connected to the same PON interface on the OLT cannot intercommunicate with each other at Layer 2. You can disable Layer 2 isolation by adding access entries to make ONUs intercommunicate with each other.

The ONU realizes Layer 2 isolation among User Network Interfaces (UNIs). By default, UNIs on the same ONU cannot intercommunicate with each other at Layer 2. You can disable Layer 2 isolation by executing related commands to make UNIs intercommunicate with each other.

## 2.1.9 FEC

Forward Error Correction (FEC) refers to adding error correction codes in physical layer coding of PON to increase the ODN power budget and support longer transmission distance or larger splitting ratio.

## 2.1.10 Maximum RTT

The physical distance between each ONU and OLT are not equal. The distance difference causes the loopback delay to change in microseconds. Because of different loopback delay, if there is not enough isolation interval, signals from different ONUs may reach the receiver end of the OLT at the same time (or overlapping in time), which will cause uplink signals to conflict with each other. Moreover, transmission delay of fiber may change because the temperature changes or components age. If all these changes are not corrected timely, uplink conflict may occur upon accumulation.

To avoid the above conflict, the EPON system adopts the timestamp ranging. Timestamp ranging realizes synchronization based on the timestamp in the EPON system. The difference between the Rx timestamp and timestamp of the local clock counter is calculated to realize distance ranging. The ranging result is used to obtain the Round-Trip Time (RTT), which can be used to adjust the Tx delay of the ONU and decrease the interval between the Tx window of the ONU, thus enhancing utilization of the uplink channel and reducing the delay.

Since the distance between each ONU and the OLT is different, so the RTT is different accordingly. The maximum RTT can ensure that all ONUs can register successfully in the distance range corresponding to the RTT.

## 2.2 Quick configuration of EPON services

EPON service configuration is complicated, involving many scenarios and functional configuration items. This section provides typical configuration applications so as to facilitate users to open EPON services quickly.

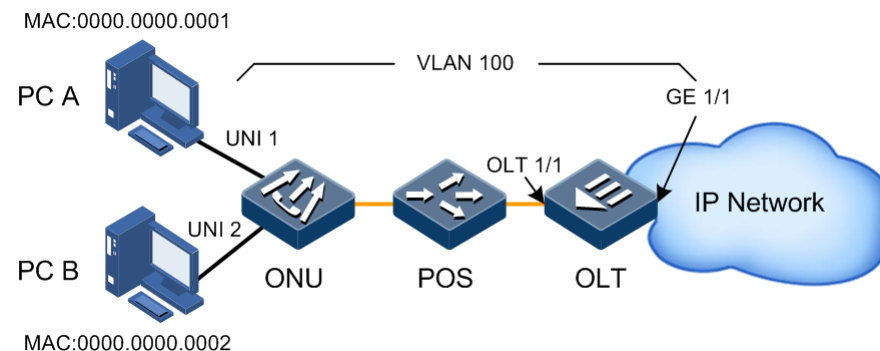
If you need to configure more EPON service functions, or require a more detailed understanding of EPON service configurations, see other sections of this chapter.

### 2.2.1 Example for configuring EPON Ethernet data service

#### Networking requirements

As shown in Figure 2-4, PC A connects ONU UNI 1, and the customer VLAN is VLAN 100. The PON interface OLT 1/1 on the ISCOM5508 connects the ONU, and GE 1/1 connects IP network. Enable data service in this network topology.

Figure 2-4 Configuring EPON Ethernet data service



#### Configuration steps

- Configure OLT.

Step 1 Create a VLAN and configure the interface VLAN mode.

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

Step 2 Configure the ONU authentication mode as **none**.

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

- Configure ONU.

Step 3 Configure the user data VLAN.

```
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 100
Raisecom(config-epon-onu-ethernet-1/1/1:1)#end
```

## Checking results

Show VLAN configurations of the interface GE 1/1 on the OLT.

```
Raisecom#show interface gigabitethernet 1/1 vlan
Port: 1/1
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 the PON interface OLT 1/1.

```
Raisecom#show interface epon-olt 1/1 vlan
Port: 1/1
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 registered ONU information.

```
Raisecom#show interface epon-onu creation-information
ONU ID      MAC Address  Mode   Creation Date   Device Type
State      Mng-mode  Description
-----
11/1/1      000e.5e07.7ac0 auto    2005-07-29,09:00:03 ISCOM5304D
active      oam       --
```

Show UNI VLAN configurations of ONU.

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

## 2.2.2 Example for configuring PON+LAN typical networking (data service+network management)

### Networking requirements

As shown in Figure 2-5, adopt the IP address pool to configure management parameters of the ONU in batch. The requirements are as below:

- Configure ONU IP address pool and SNMP parameter template on the OLT. The ONU can obtain management parameters in batch through the address pool and SNMP template.
- Configure parameters of the IP address pool as required, as shown in Table 2-2.

Table 2-2 Parameters of ONU IP address pool

Parameter	Default value
ID of IP address pool	Automatically allocated by system
Name of IP address pool	raisecom-ippool
Start IP address of IP address pool	192.168.1.11
End IP address of IP address pool	192.168.1.254
Subnet mask of IP address pool	255.255.255.0
Default gateway of IP address pool	192.168.1.1
CVLAN of management data in IP address pool	10
SVLAN of management data in IP address pool	0 (that is, the packet does not carry VLAN Tag)
Priority of management data in IP address pool	6 (the management packet requires a higher priority)

- Configure parameters of the NView NNM system as required, as shown in Table 2-3.

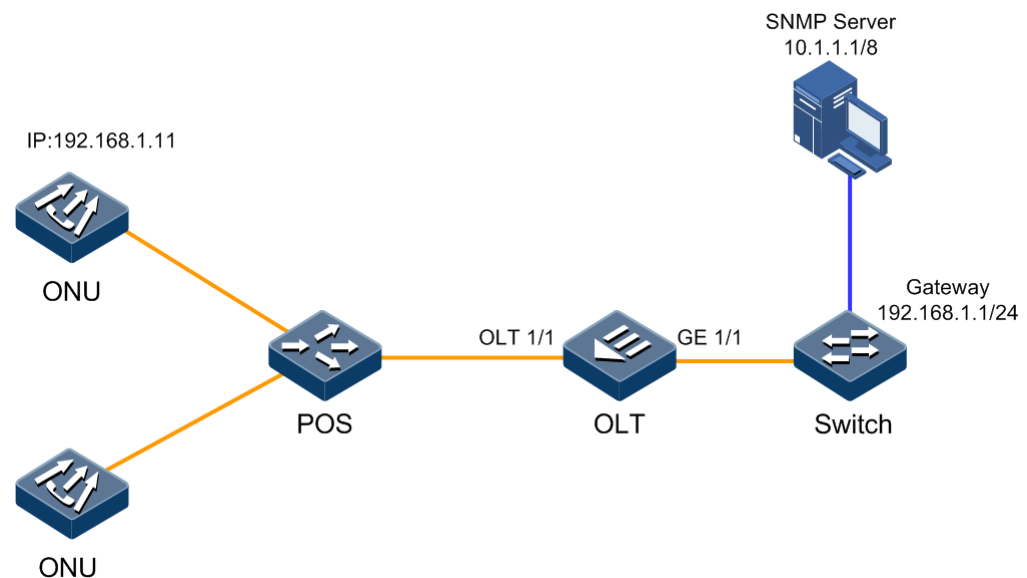


Table 2-3 Parameters of ONU SNMP template

Parameter	Default value
ID of SNMP template	Automatically allocated by system
Name of SNMP template	raisecom1
SNMP version	SNMP v2
IP address of SNMP Trap host	10.1.1.1
Trap interface ID	161
UDP port ID	162
Name of SNMP security principal	public
Name of SNMP read-only community	public
Name of SNMP write-only community	private

- Configure the ONU data service channel VLAN to VLAN 20.

Figure 2-5 Configuring ONU independent 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 Configure the PON interface binding with the IP address pool.

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

Step 3 Create the ONU SNMP template. Parameters are listed in Table 2-3.

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

Step 6 Configure the PON interface to work in Trunk mode and allow VLAN 10 to pass.

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

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

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

```
Raisecom(config-if-gigabitethernet-1:1)#switchport trunk allowed vlan 20
confirm
```

## Checking results

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

```
Raisecom#show interface epon-olt 1/1 ip-pool information
```

```
OLT ID Pool ID Pool Name
-----
1/1      1      raisecom1
```

Show ONU management information, including ONU management mode, IP address configurations, and information about the bound SNMP template.

```
Raisecom#show epon-onu 1/1/1 mng-information
```

```
ONU ID Mng-mode IP Config Mode SNMP Template ID SNMP Template Name
-----
1/1/1   SNMP      auto           1           raisecom-template
```

## 2.3 Registration and deregistration



### 2.3.1 Default configurations


Default configurations of EPON services on the ISCOM5508 are as below.

Function	Default value
ONU authentication mode	mac (MAC-based authentication mode)
ONU status	Active
Data encryption mode	Tri-churning
Data encryption	Disable
Data encryption direction	Downstream
Response timeout for triple-churning key request	300 (in unit of 0.1s)
Triple-churning key update cycle	100s
Downstream broadcast rate limiting	<ul style="list-style-type: none"> <li>• Rate: 0 Kbit/s</li> <li>• Burst value: 4095 Bytes</li> </ul>
Downstream unicast rate limiting	<ul style="list-style-type: none"> <li>• Rate: 0 Kbit/s</li> <li>• Burst value: 4095 Bytes</li> </ul>

Function	Default value
ONU uplink FIR	0 Kbit/s
ONU uplink CIR	10240 Kbit/s
ONU uplink PIR	102400 Kbit/s
ONU uplink service priority	0
FEC	Disable
Maximum RTT	14000 TQ (1 TQ = 16ns)

### 2.3.2 Configuring ONU registration

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface epon-olt slot-id/olt-id</b>	Enter EPON interface configuration mode.
3	<b>Raisecom(config-if-epon-olt-*)#authorization mode { hybrid   mac   none   password   sn   sn-password }</b>	<p>Configure the ONU authorization mode.</p> <p> <b>Note</b></p> <p>The <b>none</b> mode refers to the automatical authorization mode. In this mode, the ONU can register successfully after it is connected to the PON interface on the OLT through a physical link.</p>
4	<b>Raisecom(config-if-epon-olt-*)#create epon-onu [ onu-id ] mac mac-address [ device-type type-name ] [ suspend ] [ description name ] [ auto ]</b>	<p>(Optional) create the ONU registered based on MAC address.</p> <p>If the ONU adopts the MAC-based authorization mode, you need to use this command to create an ONU on the OLT.</p> <p> <b>Note</b></p> <p>The <b>mac mac-address</b> parameter is the MAC address of the PON interface on the ONU.</p>
	<b>Raisecom(config-if-epon-olt-*)#create epon-onu [ onu-id ] sn snstring [ device-type type-name ] [ suspend ] [ description name ]</b>	<p>(Optional) create the ONU registered based on SN.</p> <p>If the ONU adopts the SN-based authorization mode, you need to use this command to create an ONU on the OLT.</p>

Step	Command	Description
	Raisecom(config-if-epon-olt- *:*)# <b>create epon-onu</b> [ <i>onu-id</i> ] <b>password</b> <i>password</i> [ <b>device-type</b> <i>type-name</i> ] [ <b>suspend</b> ] [ <b>description</b> <i>name</i> ]	(Optional) create the ONU registered based on PASSWORD.  If the ONU adopts the PASSWORD-based authorization mode, you need to use this command to create an ONU on the OLT.   <b>Note</b> To configure the registration password for the ONU, see section 2.15.3 Configuring ONU management.
	Raisecom(config-if-epon-olt- *:*)# <b>create epon-onu</b> [ <i>onu-id</i> ] <b>sn</b> <i>snstring</i> <b>password</b> <i>password</i> [ <b>device-</b> <b>type</b> <i>type-name</i> ] [ <b>suspend</b> ] [ <b>description</b> <i>name</i> ]	(Optional) create the ONU registered based on SN+PASSWORD.  If the ONU adopts the authorization mode based on SN+PASSWORD, you need to use this command to create an ONU on the OLT.

### 2.3.3 Configuring ONU deregistration

You can make the ONU initiate the authorization request again by deregistering the ONU, which is usually used in maintenance. When you suspect that the logical link of some ONU works improperly, deregister the ONU to make it work properly.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>interface epon-onu</b> <i>slot-id/olt-id/onu-id</i>	Enter EPON ONU management configuration mode.
3	Raisecom(config-if-epon-onu-*/*:*)# <b>deregister</b>	Configure ONU deregistration.

### 2.3.4 Checking configurations

No.	Command	Description
1	Raisecom# <b>show interface epon-onu creation-information</b>	Show information about the created ONU, including creation type, ONU type, and ONU status.
2	Raisecom# <b>show epon-onu information</b>	Show information about all ONUs in the system.
3	Raisecom# <b>show interface epon-onu duplicate creation-information</b>	Show information about the created ONU with repeated MAC address on different PON interfaces.
4	Raisecom# <b>show interface epon-onu mac</b> <i>mac-address</i> <b>creation-information</b>	Retrieve the information about ONU creation according to the MAC address.
5	Raisecom# <b>show interface epon-onu</b> <i>slot-id/olt-id/onu-id</i> <b>online-information</b>	Show the ONU online information.

No.	Command	Description
6	Raisecom# <b>show interface epon-onu offline</b> [ <b>logout-date before</b> <i>mm-dd-yyyy hh:mm:ss</i> ]	Show information about offline ONUs.
7	Raisecom# <b>show interface</b> { <b>epon-olt</b>   <b>ten-giga-epon-olt</b> } <i>slot-id/olt-id illegal-onu</i>	Show information about illegally-registered ONUs on the EPON interface.
8	Raisecom# <b>show epon-onu</b> [ <i>slot-id/olt-id</i> ] <b>device statistics</b>	Count the number of ONUs according to status/type.

## 2.4 Configuring ONU IP address pool


### 2.4.1 Default configuration

N/A

### 2.4.2 Creating address pool

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>ip-pool</b> <i>pool-id pool-name begin ip-address end ip-address mask default-gw ip-address vlan svlan-id cvlan-id priority</i>	Configure the ONU IP address pool. You can use the <b>no ip-pool</b> <i>pool-id</i> command to delete the address pool.

### 2.4.3 Binding PON interface

Step	Command	Description
1	Raisecom(config)# <b>interface epon-olt</b> <i>slot-id/olt-id</i>	Enter EPON interface configuration mode.
2	Raisecom(config-if-epon-olt-*)# <b>ip-pool</b> <i>pool-id</i>	Configure the PON interface to bind with the IP address pool. You can use the <b>no ip-pool</b> command to delete the binding relationship.  <div style="display: flex; align-items: center;">  <div> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>Multiple PON interfaces can bind with the same ONU IP address pool.</li> <li>Each PON interface can bind with one ONU IP address pool only.</li> </ul> </div> </div>

## 2.4.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show ip-pool</b> [ <i>pool-id</i> ] <b>information</b>	Show configurations of IP address pool.
2	<b>Raisecom#show interface</b> { <b>epon-olt</b>   <b>ten-giga-epon-olt</b> } [ <i>slot-id/olt-list</i> ] <b>ip-pool information</b>	Show information about IP address pool binding on the EPON interface.

## 2.5 Configuring ONU SNMP template

### 2.5.1 Default configuration

N/A

### 2.5.2 Creating template and configuring it

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#snmp-template</b> <i>template-id</i> <b>template-name</b> <b>snmp-server</b> <i>ip-address</i> <b>version</b> { <b>v1</b>   <b>v2</b> } <b>trap-port</b> <i>port-id</i> <b>udp-port</b> <i>port-id</i> <b>security</b> <i>name</i> <b>community</b> <b>ro</b> <i>name</i> <b>rw</b> <i>name</i>	Create the ONU SNMP template. You can use the <b>no snmp-template</b> <i>template-id</i> command to delete the template.

### Binding ONU SNMP template

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu</b> <i>slot-id/olt-id/onu-list</i>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*//*:*)#snmp-template</b> <i>template-id</i>	Bind the ONU SNMP template with the ONU. You can use the <b>no snmp-template</b> command to delete the binding relationship.

### 2.5.3 Checking configurations

No.	Command	Description
1	<b>Raisecom#show snmp-template</b> [ <i>template-id</i> ] <b>information</b>	Show configurations of the SNMP template.

## 2.6 Configuring ONU template

### 2.6.1 Default configuration

N/A

### 2.6.2 Creating template and configuring it

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#onu-template add</b> <i>device-type</i>	Create an ONU template of new type, and configure related parameters and performance metrics according to the system prompt.
3	<b>Raisecom(config)#onu-template add</b> <i>device-type copy onu-type</i>	Copy capabilities and properties of the ONU of the specified type to the current template.
4	<b>Raisecom(config)#onu-template remove</b> <i>device-type</i>	Remove the specified ONU template.
5	<b>Raisecom(config)#onu-template modify</b> <i>device-type { common   device-type }</i>	Modify configurations of related parameters and performance metrics in the ONU performance template.
6	<b>Raisecom(config)#onu-template load</b>	Load ONU performance template to update the ONU type and update the corresponding device type when creating the ONU, in order to make the ONU type be consistent with that in the performance template.
7	<b>Raisecom(config)#onu-template restore</b>	Restore the ONU performance template to default configurations.

### 2.6.3 Binding template

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-</b> <i>id/olt-id/onu-list</i>	Enter EPON ONU management configuration mode.
3	<b>Raisecom(config-epon-onu-*//*:*)#snmp-</b> <b>template</b> <i>template-id</i>	Bind the SNMP template to the ONU. Use the <b>no snmp-template</b> command to delete the association.



## 2.6.4 Checking configurations


No.	Command	Description
1	Raisecom# <b>show onu-template</b> { <b>common</b>   <i>device-type</i> }	Show configurations of all devices or devices of a certain type in the template.
2	Raisecom# <b>show onu-template</b> { <b>common</b>   <i>device-type</i> } <b>flash</b>	Show ONU device type in the onu-template.ini file in FLASH.
3	Raisecom# <b>show onu-template default</b>	Show default configurations of device template.

## 2.7 Configuring ONU line template

### 2.7.1 Default configuration

N/A

### 2.7.2 Creating template and configuring it

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>epon-onu-line-profile</b> <i>profile-id</i>	<p>Create a line profile and enter line profile configuration mode.</p> <p>Use the <b>no epon-onu-line-profile</b> <i>profile-id</i> command to delete the profile.</p> <div>  <b>Note</b> <ul style="list-style-type: none"> <li>• If the profile exists, the system will directly enter profile configuration mode.</li> <li>• If the profile does not exist, the system will create a profile before entering profile configuration mode.</li> </ul> </div>
3	Raisecom(config-epon-onu-line-profile:*)# <b>name</b> <i>profile-name</i>	(Optional) configure profile name.
4	Raisecom(config-epon-onu-line-profile:*)# <b>fec upstream</b> { <b>enable</b>   <b>disable</b> }	(Optional) enable FEC for the uplink channel.
5	Raisecom(config-epon-onu-line-profile:*)# <b>encryption</b> { <b>enable</b>   <b>disable</b> }	(Optional) configure encryption.
6	Raisecom(config-epon-onu-line-profile:*)# <b>encryption direction</b> { <b>down</b>   <b>up-down</b> }	(Optional) configure encryption direction.
7	Raisecom(config-epon-onu-line-profile:*)# <b>dba-profile</b> <i>profile-id</i>	(Optional) bind a DBA profile.

## 2.7.3 Binding profile

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface epon-olt slot-id/olt-id</b>	Enter EPON interface configuration mode.
3	<b>Raisecom(config-if-epon-olt-*/*)#epon-onu-line-profile-id profile-id binded-onu-list onu-list</b>	Bind a profile to the ONU list.
4	<b>Raisecom(config-if-epon-olt-*/*)#epon-onu-line-profile template-id add onu-list</b>	(Optional) add an ONU to the binded ONU profile.
5	<b>Raisecom(config-if-epon-olt-*/*)#epon-onu-line-profile template-id remove onu-list</b>	(Optional) delete an ONU from the binded ONU profile.

## 2.7.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show epon-onu-line-profile { all   profile-list }</b>	Show line profile configurations.


## 2.8 Configuring ONU service profile

### 2.8.1 Default configuration

N/A

### 2.8.2 Creating profile and configuring it

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu-service-profile profile-id</b>	Enter service profile configuration mode. If the profile exists, enter the profile configuration mode. Otherwise, create a profile before entering profile configuration mode.
3	<b>Raisecom(config-epon-onu-service-profile: *)#name name</b>	(Optional) configure the name of the service profile.
4	<b>Raisecom(config-epon-onu-service-profile:*)#ip igmp immediate-leave</b>	(Optional) configure ONU IGMP immediate leave.

Step	Command	Description
5	Raisecom(config-epon-onu-service-profile: *)# <b>ip igmp mode { ctrl-multicast   proxy   snooping   transparent }</b>	(Optional) configure ONU IGMP mode.
6	Raisecom(config-epon-onu-service-profile: *)# <b>ip igmp vlan-aware { enable   disable }</b>	(Optional) configure the ONU IGMP to identify VLAN when forwarding multicast services.
7	Raisecom(config-epon-onu-service-profile: *)# <b>mac-address-table aging-time aging-time</b>	(Optional) configure the aging time of ONU MAC address table.
8	Raisecom(config-epon-onu-service-profile: *)# <b>mng-mode { snmp   oam }</b>	(Optional) configure ONU management mode.
9	Raisecom(config-epon-onu-service-profile: *)# <b>storm-control multicast { enable   disable }</b>	(Optional) configure ONU multicast storm control.
10	Raisecom(config-epon-onu-service-profile: *)# <b>uni-eth-num sensitive { enable   disable }</b>	<p>Configure consistency of the ONU service profile.</p>  <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• When consistency of the ONU service profile is enabled, the interface number of the profile should be consistent with that of the ONU. At this time, configurations of each interface on the ONU correspond to those of each interface in the profile.</li> <li>• When consistency of the ONU service profile is disabled, the interface number of the profile can be inconsistent with that of the ONU. At this time, configurations of the first interface in the profile are adopted for each interface of the ONU.</li> </ul>
11	Raisecom(config-epon-onu-service-profile: *)# <b>uplink rate-limit rate</b>	(Optional) configure the rate-limiting rate on the ONU uplink interface.
12	Raisecom(config-epon-onu-service-profile: *)# <b>downstream policy rule-list</b>	(Optional) configure the downlink traffic classification policies on the ONU.
13	Raisecom(config-epon-onu-service-profile: *)# <b>uni ethernet uni-list loopback-detection down-time { infinite   time }</b>	(Optional) configure the Down time of ONU UNI loop interface.
14	Raisecom(config-epon-onu-service-profile: *)# <b>uni ethernet uni-list mac-address-table threshold { unlimited   number }</b>	(Optional) configure the maximum capacity of ONU UNI MAC address table.

Step	Command	Description
15	Raisecom(config-epon-onu-service-profile: *)# <b>uni ethernet uni-list multicast vlan</b> <i>vlan-id</i>	(Optional) configure the multicast VLAN ID on ONU UNI interface.  Use the <b>no uni ethernet uni-list multicast vlan</b> command to delete the multicast VLAN.
16	Raisecom(config-epon-onu-service-profile: *)# <b>uni ethernet uni-list multicast vlan tag-strip</b> { <b>enable</b>   <b>disable</b> }	(Optional) configure the ONU UNI interface to strip/keep the multicast VLAN tag.
17	Raisecom(config-epon-onu-service-profile: *)# <b>uni ethernet uni-list native vlan</b> <i>vlan-id</i>	(Optional) configure the multicast VLAN ID on the ONU UNI.  Use the <b>no uni ethernet uni-list multicast vlan</b> command to delete the multicast VLAN.
18	Raisecom(config-epon-onu-service-profile: *)# <b>uni ethernet uni-list policing</b> { <b>egress</b>   <b>ingress</b> } { <b>enable</b>   <b>disable</b> }	(Optional) enable/disable ONU UNI downlink rate limiting.
19	Raisecom(config-epon-onu-service-profile: *)# <b>uni ethernet uni-list speed</b> <b>auto</b>	(Optional) configure the rate and duplex mode of ONU UNI to auto-negotiation.
20	Raisecom(config-epon-onu-service-profile: *)# <b>uni ethernet uni-list speed</b> { <b>10</b>   <b>100</b>   <b>1000</b> } <b>duplex</b> { <b>half</b>   <b>full</b> }	(Optional) configure the interface rate and duplex mode of ONU UNI.
21	Raisecom(config-epon-onu-service-profile: *)# <b>uni ethernet uni-list switchport isolation</b> { <b>disable</b>   <b>enable</b> }	(Optional) enable/disable ONU UNI isolation.
22	Raisecom(config-epon-onu-service-profile: *)# <b>uni ethernet uni-list vlan mode</b> { <b>tagged</b>   <b>transparent</b>   <b>trunk</b> }	(Optional) configure the ONU UNI VLAN mode.
23	Raisecom(config-epon-onu-service-profile: *)# <b>uni ethernet uni-list vlan trunk allowed</b> <i>vlan-list</i>	(Optional) configure VLANs that are allowed to pass by ONU UNI trunk interface.  Use the <b>no uni ethernet uni-list vlan trunk allowed</b> command to restore to default conditions.
24	Raisecom(config-epon-onu-service-profile: *)# <b>partner-profile</b> <i>profile-id</i>	(Optional) associate the partner profile with the service profile.
25	Raisecom(config-epon-onu-service-profile: *)# <b>pse-profile</b> <i>profile-id</i>	(Optional) associate the PSE profile with the service profile.
26	Raisecom(config-epon-onu-service-profile: *)# <b>voip-profile</b> <i>profile-id</i>	(Optional) associate the voice profile with the service profile.

## 2.8.3 Binding profile

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface { epon-olt   ten-giga-epon-olt } slot-id/port-id</code>	Enter EPON interface configuration mode.
3	<code>Raisecom(config-if-epon-olt-*:*)#epon-onu-service-profile profile-id binded-onu-list list</code>	Bind the profile to the ONU. Use the <b>no epon-onu-service-profile profile-id</b> command to delete the binding relation.
4	<code>Raisecom(config-if-epon-olt-*:*)#epon-onu-service-profile profile-id binded-onu-list add list</code>	(Optional) add ONUs to the binded ONU service profile.
5	<code>Raisecom(config-if-epon-olt-*:*)#epon-onu-service-profile profile-id binded-onu-list remove list</code>	(Optional) delete ONUs from the binded ONU service profile.



### Note

- When you bind the ONU service profile with the ONU list, the ONU can be bound whether it is created or not, or online or not, as long as no ONU in the list has been bound with the service profile previously. Moreover, the quantity of ONUs in the ONU list should be identical to that of the Native VLAN IDs.
- When the ONU service profile is bound with an ONU list under a PON interface, the ONU list cannot be modified. If required, you should specify the ONU list again after deleting the binding relationship.
- When the ONU in the ONU list is created, the Native VLAN ID and VLAN mode of the ONU interface will be configured according to the profile. When Native VLAN IDs (ranging from A to B) are bound with ONUs in the ONU list (ranging from M to N, which can be uncontinuous while the quantity should be identical to that from A to B), the n<sup>th</sup> Native VLAN ID is allocated to the n<sup>th</sup> ONU. For example, the ONU No. is 1, 2, 3, 5, 7, 8, 9, 10 and the Native VLAN ID ranges from 1 to 8, so the Native VLAN ID of ONU 5 is 4.
- Only when the reference count of the profile is 0, namely, the profile is not bound with any ONU, can the profile be deleted.

## 2.8.4 Checking configurations

Step	Command	Description
1	<code>Raisecom#show epon-onu-service-profile { all   profile-list }</code>	Show configurations of service profile.
2	<code>Raisecom#show interface { epon-olt   ten-giga-epon-olt } slot-id/olt-list epon-onu-service-profile</code>	Show binding information about the ONU service profile on the specified PON interface.

## 2.9 Configuring partner profile



### Note

- A partner profile is a level 2 profile of service profile. By configuring the profile ID, you can associate the subprofile with the service profile. For the association mode, see section 2.8 Configuring ONU service profile. When the service profile is bound to the ONU, the subprofile is also bound to the corresponding ONU.
- You can configure the related parameters of the ONU partner devices in batches through the partner profile, which will greatly reduce the workload.

### 2.9.1 Default configurations

N/A

### 2.9.2 Creating profile

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>create partner-profile</b> <i>profile-id</i> <b>name</b> <i>name</i> <b>partner-device-num</b> <i>num</i>	Create a partner profile and configure related parameters. You can use the <b>no create partner-profile</b> { <b>all</b>   <i>profile-list</i> } command to delete the profile.

### 2.9.3 Configuring profile

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>partner-profile</b> <i>profile-id</i>	Enter partner profile configuration mode. It is allowed to enter the profile mode if there is a profile.
3	Raisecom(config-epon-onu-partner-profile:*)# <b>name</b> <i>name</i>	(Optional) modify the name of the partner profile.
4	Raisecom(config-epon-onu-partner-profile:*)# <b>partner-device-num</b> <i>num</i>	(Optional) modify the number of partner devices.
5	Raisecom(config-epon-onu-partner-profile:*)# <b>partner discovery</b> { <b>enable</b>   <b>disable</b> }	(Optional) enable/disable partner device discovery.
6	Raisecom(config-epon-onu-partner-profile:*)# <b>partner list snmp-server community</b> <i>name</i> { <b>ro</b>   <b>rw</b> }	(Optional) configure the SNMP community name and configure the read-write/read only function.
7	Raisecom(config-epon-onu-partner-profile:*)# <b>partner list snmp-server host</b> <i>ip-address</i>	(Optional) configure the destination host address of the partner SNMP server.

Step	Command	Description
8	Raisecom (config-epon-onu-partner-profile:*)# <b>partner list snmp-server security name</b>	(Optional) configure the SNMP security name of the partner device.



### Note

A profile must be ready. The profile in use cannot be modified.

## 2.9.4 Checking configurations

Step	Command	Description
1	Raisecom# <b>show partner-profile { all   profile-id }</b>	Show configurations of partner profile.

## 2.10 Configuring PSE profile



### Note

- A power Sourcing Equipment (PSE) profile is a level 2 profile of service profile. By configuring the profile ID, you can associate the subprofile with the service profile. For the association mode, see section 2.8 Configuring ONU service profile. When the service profile is bound to the ONU, the subprofile is also bound to the corresponding ONU.
- You can configure the related parameters of the ONU PSE in batches through the PSE profile, which will greatly reduce the workload.

### 2.10.1 Default configurations

N/A

### 2.10.2 Creating profile

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>create pse-profile profile-id name name</b>	Create a PSE profile and configure related parameters. You can use the <b>no create partner-profile { all   profile-list }</b> command to delete the profile.

## 2.10.3 Configuring profile

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#pse-profile</b> <i>profile-id</i>	Enter PSE profile configuration mode. You can enter the profile if there is a profile.
3	<b>Raisecom(config-epon-onu-pse-profile:*)#name</b> <i>name</i>	(Optional) configure the name of the PSE profile.
4	<b>Raisecom(config-epon-onu-pse-profile:*)#poe pse power-management</b> <b>{ manual   auto }</b>	(Optional) configure the power sourcing management mode of the PSE.
5	<b>Raisecom(config-epon-onu-pse-profile:*)#poe pse power-threshold</b> <i>threshold</i>	(Optional) configure the PSE power threshold.
6	<b>Raisecom(config-epon-onu-pse-profile:*)#poe pse temperature-protection</b> <b>{ enable   disable }</b>	(Optional) enable/disable PSE overtemperature protection.



### Note

A profile must be ready. The profile in use cannot be modified.

## 2.10.4 Checking configurations

Step	Command	Description
1	<b>Raisecom#show pse-profile</b> <b>{ all   profile-id }</b>	Show PSE profile configurations.

## 2.11 Configuring voice profile



### Note

- A voice profile is a level 2 profile of service profile. By configuring the profile ID, you can associate the subprofile with the service profile. For the association mode, see section 2.8 Configuring ONU service profile. When the service profile is bound to the ONU, the subprofile is also bound to the corresponding ONU.
- You can configure the voice-related parameters of the ONU in batches through the voice profile, which will greatly reduce the workload.

### 2.11.1 Default configurations

N/A



## 2.11.2 Creating profile

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#create voip-profile</b> <i>profile-id name name pots pot-id</i>	Create a voice profile and configure related parameters.  You can use the <b>no create voip-profile { all   profile-list }</b> command to delete the profile.

## 2.11.3 Configuring profile

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#voip-profile</b> <i>profile-id</i>	Enter voice profile configuration mode. It is allowed to enter the profile if there is a profile.
3	<b>Raisecom(config-epon-onu-voip-profile:*)#name</b> <i>name</i>	(Optional) configure the name of the voice profile.
4	<b>Raisecom(config-epon-onu-voip-profile:*)#pots</b> <i>num</i>	(Optional) configure the number of interfaces of the voice profile.
5	<b>Raisecom(config-epon-onu-voip-profile:*)#digitmap match-mode { max   min }</b>	(Optional) configure the digitmap matching mode of the voice profile to maximum/minimum.
6	<b>Raisecom(config-epon-onu-voip-profile:*)#h248 mg digitmap { short-timer   long-timer }</b> <i>time</i>	(Optional) configure the time of the long timer/short timer of the voice profile H.248 MG digitmap.
7	<b>Raisecom(config-epon-onu-voip-profile:*)#h248 mg heartbeat cycle</b> <i>time</i>	(Optional) configure the H.248 MG heartbeat period of the voice profile.
8	<b>Raisecom(config-epon-onu-voip-profile:*)#h248 mg heartbeat timeout count</b> <i>count</i>	(Optional) configure the H.248 MG heartbeat timeout of the voice profile.
9	<b>Raisecom(config-epon-onu-voip-profile:*)#h248 pots tid name</b> <i>name pot-id</i>	(Optional) configure the H.248 interface ID of the voice profile.
10	<b>Raisecom(config-epon-onu-voip-profile:*)#h248 primary mgc ip</b> <i>ip-address [ port port-id ]</i>	(Optional) configure the H.248 primary MGC IP address of the voice profile.
11	<b>Raisecom(config-epon-onu-voip-profile:*)#h248 secondary mgc ip</b> <i>ip-address [ port port-id ]</i>	(Optional) configure the H.248 secondary MGC IP address of the voice profile.



### Note

A profile must be ready. The profile in use cannot be modified.

## 2.11.4 Checking configurations

Step	Command	Description
1	Raisecom# <b>show voip-profile</b> { <b>all</b>   <i>profile-id</i> }	Show configurations of PSE profile.

## 2.12 Configuring ONU QoS profile



### Note

The ONU QoS profile can configure QoS functions of the ONU in batch, which reduces the configuration workload on the engineers.

### 2.12.1 Default configuration


N/A

### 2.12.2 Creating profile

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>create onu-qos-template</b> <i>template-id</i> <b>name</b> <i>template-name</i>	Create the ONU QoS template. You can use the <b>no create onu-qos-template</b> <i>template-id</i> command to delete the template.

### 2.12.3 Configuring parameters of ONU QoS template

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>epon-onu qos-template</b> <i>template-id</i>	Enter QoS template configuration mode.
3	Raisecom(config-epon-onu-qos-template:*)# <b>name</b> <i>template-name</i>	(Optional) configure the name of the current template.
4	Raisecom(config-epon-onu-qos-template:*)# <b>best-effort-scheduling-scheme</b> { <b>sp</b>   <b>wrr weight</b> <i>w1 w2 w3 w4</i>   <b>sp-wrr weight</b> <i>w1 w2 w3 w4</i> <b>high-priority-boundary</b> <i>value</i> }	(Optional) configure the queue scheduling mode and weight of the queue. You can use the <b>no best-effort-scheduling-scheme</b> command to restore default configurations.

Step	Command	Description
5	<code>Raisecom(config-epon-onu-qos-template:*)#weight <i>weight-values</i></code>	(Optional) configure the weight of the queue.
6	<code>Raisecom(config-epon-onu-qos-template:*)#high-priority-boundary <i>value</i></code>	<p>(Optional) configure the boundary value of the queue priority in SP+WRR mode.</p> <p>You can use the <b>no high-priority-boundary</b> command to restore default configurations.</p> <div>  <b>Note</b> </div> <p>Perform SP scheduling on queues whose priorities are not smaller than the boundary value; perform WRR scheduling on other queues.</p>
7	<code>Raisecom(config-epon-onu-qos-template:*)#cycle-length <i>value</i></code>	<p>(Optional) configure the polling cycle of scheduling.</p> <p>You can use the <b>no cycle-length</b> command to restore default configurations.</p>
8	<code>Raisecom(config-epon-onu-qos-template:*)#queue <i>queue-id</i> type fixed fir <i>fir-value</i> [ fix-pkt <i>size</i> ]</code>	<p>(Optional) configure the fixed bandwidth.</p> <p>You can use the <b>no queue</b> command to restore default configurations.</p>
9	<code>Raisecom(config-epon-onu-qos-template:*)#queue <i>queue-id</i> type assured cir <i>cir-value</i> [ fix-pkt <i>size</i> ]</code>	<p>(Optional) configure the assured bandwidth.</p> <p>You can use the <b>no queue</b> command to restore default configurations.</p>
10	<code>Raisecom(config-epon-onu-qos-template:*)#queue <i>queue-id</i> type besteffort pir <i>pir-value</i> [ fix-pkt <i>size</i> ]</code>	<p>(Optional) configure the best-effort bandwidth.</p> <p>You can use the <b>no queue</b> command to restore default configurations.</p>
11	<code>Raisecom(config-epon-onu-qos-template:*)#queue <i>queue-id</i> type fixed-assured fir <i>fir-value</i> cir <i>cir-value</i> [ fix-pkt <i>size</i> ]</code>	<p>(Optional) configure the fixed bandwidth+assured bandwidth.</p> <p>You can use the <b>no queue</b> command to restore default configurations.</p>
12	<code>Raisecom(config-epon-onu-qos-template:*)#queue <i>queue-id</i> type { fixed-besteffort   assured-besteffort } fir <i>fir-value</i> pir <i>pir-value</i> [ fix-pkt <i>size</i> ]</code>	<p>(Optional) configure the fixed bandwidth+best-effort bandwidth.</p> <p>You can use the <b>no queue</b> command to restore default configurations.</p>
13	<code>Raisecom(config-epon-onu-qos-template:*)#queue <i>queue-id</i> type fix-assured-besteffort fir <i>fir-value</i> cir <i>cir-value</i> pir <i>pir-value</i> [ fix-pkt <i>size</i> ]</code>	<p>(Optional) configure the fixed bandwidth+assured bandwidth+best-effort bandwidth.</p> <p>You can use the <b>no queue</b> command to restore default configurations.</p>



## Note

- The template bound with the ONU cannot be modified or deleted.
- The boundary value of the queue priority can be configured in SP+WRR mode only.

- The total weight of all queues should be 100 in WRR and SP+WRR modes. In WRR mode, the weight of each queue should not be 0.
- For all queues,  $FIR \leq CIR \leq PIR$ . Total bandwidth of all queues cannot exceed the total uplink bandwidth of the ONU.
- The bandwidth type facilitates you to configure FIR, CIR, and PIR. When the bandwidth type is configured to fixed bandwidth, the assured bandwidth and best-effort bandwidth become 0 automatically. Since  $FIR = \text{fixed bandwidth}$ ,  $CIR = \text{fixed bandwidth} + \text{assured bandwidth}$ , and  $PIR = \text{fixed bandwidth} + \text{assured bandwidth} + \text{best-effort bandwidth}$ , so you only need to input the FIR and the CIR and PIR equal to FIR automatically.
- When the bandwidth type is configured to "assured bandwidth+best-effort bandwidth", the fixed bandwidth becomes 0 automatically and you only need to configure FIR and PIR.
- You can use "fixed bandwidth+assured bandwidth+best-effort bandwidth" to specify FIR, CIR, and PIR.

## 2.13 Configuring DBA template

### 2.13.1 Default configuration

There is one DBA template with ID 1 on the ISCOM5508 by default. The default configuration is as below.

Name	Default value
Template ID	1
Template name	Profile-1
Template type	Type3
Fix (fixed bandwidth)	0 kbit/s
Assure (assured bandwidth)	1000 kbit/s
Max (maximum bandwidth)	1000000 kbit/s

### 2.13.2 Creating template

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#create dba-profile</b> <i>profile-id name profile-name type1 fix fix-bandwidth</i>	Create a DBA template with fixed bandwidth. Use the <b>no create dba-profile profile-id</b> command to delete the template.
	<b>Raisecom(config)#create dba-profile</b> <i>profile-id name profile-name type2 assure assure-bandwidth</i>	Create a DBA template with assured bandwidth. Use the <b>no create dba-profile profile-id</b> command to delete the template.

Step	Command	Description
	<code>Raisecom(config)#create dba-profile profile-id name profile-name type3 assure assure-bandwidth max max-bandwidth</code>	Create a DBA template with assured bandwidth+maximum bandwidth. Use the <b>no create dba-profile profile-id</b> command to delete the template.
	<code>Raisecom(config)#create dba-profile profile-id name profile-name type4 max max-bandwidth</code>	Create a DBA template with maximum bandwidth. Use the <b>no create dba-profile profile-id</b> command to delete the template.
	<code>Raisecom(config)#create dba-profile profile-id name profile-name type5 fix fix-bandwidth assure assure-bandwidth max max-bandwidth</code>	Create a DBA template with fixed bandwidth+assured bandwidth+maximum bandwidth. Use the <b>no create dba-profile profile-id</b> command to delete the template.



### Note

It is not allowed to delete a template which is in use.

## 2.13.3 Modifying template

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#dba-profile profile-id name profile-name</code>	Modify DBA template name.
	<code>Raisecom(config)#dba-profile profile-id type1 fix fix-bandwidth</code>	Modify the DBA template with fixed bandwidth.
	<code>Raisecom(config)#dba-profile profile-id type2 assure assure-bandwidth</code>	Modify the DBA template with assured bandwidth.
	<code>Raisecom(config)#dba-profile profile-id type3 assure assure-bandwidth max max-bandwidth</code>	Modify the DBA template with assured bandwidth+maximum bandwidth.
	<code>Raisecom(config)#dba-profile profile-id type4 max max-bandwidth</code>	Modify the DBA template with maximum bandwidth.
	<code>Raisecom(config)#dba-profile profile-id type5 fix fix-bandwidth assure assure-bandwidth max max-bandwidth</code>	Modify the DBA template with fixed bandwidth+assured bandwidth+maximum bandwidth.



### Note

- The template that needs to be modified must exist.
- It is not allowed to delete a template which is in use.

## 2.13.4 Checking configurations


Step	Command	Description
1	Raisecom# <b>show dba-profile</b> { <b>all</b>   <i>profile-list</i> }	Show configurations of DBA template.

## 2.14 Configuring EPON interface

### 2.14.1 Default configuration

Function	Default value
Data encryption mode	Tri-churning
Data encryption	Disabled
Data encryption direction	Downstream
Maximum RTT	14000TQ (1TQ = 16ns)

### 2.14.2 Configuring interface

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode
2	Raisecom(config)# <b>interface</b> { <b>epon-olt</b>   <b>ten-giga-epon-olt</b> } <i>slot-id/olt-id</i>	Enter EPON interface configuration mode.
3	Raisecom(config-if-* <b>-olt-*</b> )*# <b>reset</b>	(Optional) reset the EPON interface.   <b>Note</b> When the device fails, you can use this command to reset the interface to recover services.
4	Raisecom(config-if-* <b>-olt-*</b> )*# <b>self-test</b>	(Optional) EPON interface self-test

### 2.14.3 Configuring data encryption

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

Step	Command	Description
2	<code>Raisecom(config)#<b>encryption slot</b> <i>slot-id</i> <b>triple-churning</b> { <b>key-response-timeout</b> <i>time</i>   <b>key-update-period</b> <i>period</i> }</code>	(Optional) configure key parameters of triple-churning, including response timeout for key request and key update cycle.
3	<code>Raisecom(config)#<b>interface epon-olt</b> <i>slot-id/olt-id</i></code>	Enter EPON interface configuration mode.
4	<code>Raisecom(config-if-epon-olt-:*)#<b>encryption mode</b> { <b>aes-128</b>   <b>triple-churning</b> }</code>	Configure the data encryption mode.



### Note

- At present, the ISCOM5508 supports the triple-churning encryption mode only. The AES-128 encryption mode can be configured while the configuration cannot take effect.
- At present, the ISCOM5508 supports performing data encryption in downlink direction.

## 2.14.4 Configuring maximum RTT

Step	Command	Description
1	<code>Raisecom#<b>config</b></code>	Enter global configuration mode.
2	<code>Raisecom(config)#<b>interface epon-olt</b> <i>slot-id/olt-id</i></code>	Enter EPON interface configuration mode.
3	<code>Raisecom(config-if-epon-olt-:*)#<b>rtt max</b> <i>rtt</i></code>	Configure the maximum RTT of the EPON interface. You can use the <b>no rtt max</b> command to restore default configurations.



### Note

By default, the fiber distance corresponding to the maximum RTT is about 21 km, so you do not need to modify the maximum RTT in general.

## 2.14.5 Checking configurations

Step	Command	Description
1	<code>Raisecom#<b>show interface</b> { <b>epon-olt</b>   <b>ten-giga-epon-olt</b> } [ <i>slot-id/olt-list</i> ] <b>information</b></code>	Show configurations of EPON interface.
2	<code>Raisecom#<b>show interface</b> { <b>epon-olt</b>   <b>ten-giga-epon-olt</b> } <i>slot-id/olt-id</i> <b>firmware</b></code>	Show firmware information about EPON interface.

## 2.15 Configuring ONU

### 2.15.1 Default configurations





#### Note

Because Raisecom provides various types of ONUs, features and default configurations of these ONUs may be different. The table below lists general features and default configurations for you reference.

Default configurations of ONU are as below.

Function	Default value
Name of ONU	raisecom
Management mode of ONU	OAM
Management IP address of PON interface	<ul style="list-style-type: none"> <li>• IP address: 0.0.0.0</li> <li>• Mask: 0.0.0.0</li> </ul>
Management IP address of UNI	<ul style="list-style-type: none"> <li>• IP address: 192.168.1.254</li> <li>• Mask: 255.255.255.0</li> </ul>
Name of UNI	ethernet-uni-x, where <i>x</i> refers to the serial number of the interface
Rate and duplex mode of UNI	Auto
Flow control of UNI	Disable
UNI Loss alarm	Disable
UNI status	Enable
ONU SLA	Disable
ONU SLA queue scheduling mode	SP
SLA queue parameters	<ul style="list-style-type: none"> <li>• FIR: 0 Kbit/s</li> <li>• CIR: 256 Kbit/s</li> <li>• PIR: 256 Kbit/s</li> <li>• FixPkt: 0 Byte</li> </ul>
Port mirroring	Disable
Monitor port	UNI 1
Mirroring port	N/A
DLF packet forwarding	Enable
BPDU transparent transmission	Disable
ONU partner discovery	Disable



Function	Default value
Management IP address of ONU partner	<ul style="list-style-type: none"> <li>• IP address: 192.168.2.254</li> <li>• Mask: 255.255.255.0</li> </ul>  <b>Note</b> Default configurations of different ONUs may be different.
Out-of-band management IP address of ONU partner	<ul style="list-style-type: none"> <li>• IP address: 192.168.1.100</li> <li>• Mask: 255.255.255.0</li> </ul>  <b>Note</b> Default configurations of different ONUs may be different.
Management IP address type of ONU partner	Manual
PPPoE agent	Disable
PPPoE agent user-defined	Disable
Attach-string field of PPPoE agent Circuit_ID option	N/A
Stuffing mode of PPPoE agent Remote_ID option	onumac-binary
User-defined value of PPPoE agent Remote_ID option	N/A
Power supply management mode of PSE sub-card	Auto
PSE power usage threshold percentage	99%
PSE Trap reporting	Enable
UNI PSE status	Enable
Maximum Tx power of UNI	<ul style="list-style-type: none"> <li>• IEEE 802.3af mode:15400 mW</li> <li>• IEEE 802.3at mode:30000 mW</li> </ul>
Power supply priority of interface	Low
Allow service to pass or not when the UNI is not connected with PSE	Disable

Default configurations of serial interfaces on the ONU are as below.

Function	Default value
Interface status	Enable
Interface baud rate	9600 Baud
Serial communication protocol	RS485

Function	Default value
Serial data bits	8 bits
Stop bit of serial data	1 bit
Check mode of serial data	N/A
Operation mode of serial interface	tcp_realport
Network service interface of serial interface	10990+serial interface No.
Peer service interface of serial interface	1025
Peer IP address of serial interface	0.0.0.0
Initiation condition of session connection	Always
Maximum number of sessions on serial interface	64

## 2.15.2 Basic configurations of ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*/*:*)#hostname string</b>	(Optional) configure the name of the ONU. You can use the <b>no hostname</b> command to restore default configurations.
4	<b>Raisecom(config-epon-onu-*/*:*)#reload startup-config</b>	(Optional) reload the startup configuration file.
5	<b>Raisecom(config-epon-onu-*/*:*)#restore startup-config</b>	(Optional) restore default configurations.
6	<b>Raisecom(config-epon-onu-*/*:*)#reboot [ now ]</b>	(Optional) reboot the ONU.
7	<b>Raisecom(config-epon-onu-*/*:*)#write</b>	Save configurations.



### Caution

When remotely manage and configure the ONU through the ISCOM5508, you should save configurations in ONU configuration mode; otherwise, configurations will be lost when the ISCOM5508 is rebooted.

## 2.15.3 Configuring ONU management

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

Step	Command	Description
2	<code>Raisecom(config)#<b>epon-onu</b> slot-id/olt-id/onu-id</code>	Enter EPON ONU management configuration mode.
3	<code>Raisecom(config-epon-onu-*/*:*)#<b>mng-characteristic</b> { rc   ctc2dot1   ctc3dot0 }</code>	Configure the management channel of the ONU.
4	<code>Raisecom(config-epon-onu-*/*:*)#<b>transceiver tx-power-supply</b> { primary   standby   both } reenabe</code>	Configure the working mode of the optical transceiver on the ONU PON interface.
5	<code>Raisecom(config-epon-onu-*/*:*)#<b>transceiver tx-power-supply</b> { primary   standby   both } shutdown { time   permanently }</code>	Configure the power shutdown time of the optical transceiver on the ONU PON interface.

Step	Command	Description
1	<code>Raisecom#<b>config</b></code>	Enter global configuration mode.
2	<code>Raisecom(config)#<b>interface epon-onu</b> slot-id/olt-id/onu-id</code>	Enter EPON ONU management configuration mode.
3	<code>Raisecom(config-if-epon-onu-*/*:*)#<b>password</b> password</code>	Configure the password for ONU authorization.
4	<code>Raisecom(config-if-epon-onu-*/*:*)#<b>creation-type automatic-to-manual</b></code>	Configure the ONU to transfer from the automatically created type to the manual type.
5	<code>Raisecom(config-if-epon-onu-*/*:*)#<b>mng-mode</b> { oam   snmp }</code>	Configure the management mode of the ONU.

## Configuring ONU management IP

ONU management IP includes:

- ONU management IP mode
- ONU management IP address

## Configuring ONU management IP mode

Step	Command	Description
1	<code>Raisecom#<b>config</b></code>	Enter global configuration mode.
2	<code>Raisecom(config)#<b>epon-onu</b> slot-id/olt-id/onu-id</code>	Enter EPON ONU remote management configuration mode.
3	<code>Raisecom(config-epon-onu-*/*:*)#<b>ip-config</b> { static   auto [ overlay-local-ip ] }</code>	Configure the ONU management IP mode.
4	<code>Raisecom(config-epon-onu-*/*:*)#<b>telnet</b> { enable   disable }</code>	(Optional) enable/disable Telnet.

## Configuring ONU management IP address

ONU management IP address is divided into two types:

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

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU management configuration mode.
3	<b>Raisecom(config-epon-onu-*//*:*)#mng-ip address ip-address[ mask ] default-gw default-gw vlan svlan-id cvlan-id priority</b>	(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 <b>no mng-ip address</b> command to restore default configurations.
	<b>Raisecom(config-epon-onu-*//*:*)#mng-ipv6 address ipv6-address/prefix-length default-gw default-gw vlan svlan-id cvlan-id priority</b>	(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 <b>no mng-ipv6 address</b> command to restore default configurations.
4	<b>Raisecom(config-epon-onu-*//*:*)#lan-ip address ip-address [ mask ]</b>	(Optional) configure the management IP address of the ONU UNI. Use this configuration when you perform independent management on the ONU.  You can use the <b>no lan-ip address</b> command to restore default configurations.



### Note

The management 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.

## 2.15.4 Configuring ONU management IP

ONU management IP includes:

- ONU management IP mode
- ONU management IP address

## Configuring ONU management IP mode

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*//*:*)#ip-config { static   auto [ overlay-local-ip ] }</b>	Configure the ONU management IP mode.
4	<b>Raisecom(config-epon-onu-*//*:*)#telnet { enable   disable }</b>	(Optional) enable/disable Telnet.

## Configuring ONU management IP address

ONU management IP address is divided into two types:

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

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU management configuration mode.
3	<b>Raisecom(config-epon-onu-*//*:*)#mng-ip address ip-address[ mask ] default-gw default-gw vlan svlan-id cvlan-id priority</b>	(Optional) configure ONU PON management IP address. Use this configuration when managing the ONU through SNMP. Use the <b>no mng-ip address</b> command to return to the default configuration.
4	<b>Raisecom(config-epon-onu-*//*:*)#mng-ipv6 address ipv6-address/prefix-length default-gw default-gw vlan svlan-id cvlan-id priority</b>	(Optional) configure the IPv6 management IP address on the ONU PON interface. Use this configuration when managing the ONU through SNMP. Use the <b>no mng-ipv6 address</b> command to return to the default configuration.
5	<b>Raisecom(config-epon-onu-*//*:*)#vlan-ip address ip-address [ mask ]</b>	(Optional) configure the IP address of the ONU UNI. Use this command when managing the ONU independently. Use the <b>no lan-ip address</b> command to return to the default condition.



## Note

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

### 2.15.5 Activating ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#activate epon-onu all</b>	(Optional) activate all ONUs.
3	<b>Raisecom(config)#interface epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU management configuration mode.
4	<b>Raisecom(config-if-epon-onu*/*:*)#state { active   suspend }</b>	Configure the ONU status.

### 2.15.6 Rebinding ONU

When creating the ONU, you need to specify the MAC address. When the ONU is registered on the OLT, the MAC address is regarded as the basis to judge its legality. When the original ONU is replaced, the new ONU is regarded as the illegal one since the MAC address changes. As this time, the ONU should be re-registered and the pervious configurations are lost.

Rebind the MAC address of the ONU to replace the previously authorized MAC address, you can make the new ONU become legal and remain the previous configurations.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU management configuration mode.
3	<b>Raisecom(config-if-epon-onu*/*:*)#rebind mac mac-address [ device-type onu-type ]</b>	Rebind the MAC address of the ONU and support changing the ONU type to another one of the same interface.

### 2.15.7 Configuring ONU SNMP parameters

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU management configuration mode.
3	<b>Raisecom(config-epon-onu*/*:*)#snmp-server host ip-address</b>	Configure the IP address of the ONU SNMP server. You can use the <b>no snmp-server host</b> command to restore default configurations.

Step	Command	Description
4	Raisecom(config-epon-onu- *//*:*)# <b>snmp-server version</b> { v1   v2   v3 }	Configure ONU SNMP version. You can use the <b>no snmp-server version</b> command to restore default configurations.
5	Raisecom(config-epon-onu- *//*:*)# <b>snmp-server trap-port</b> port	Configure the SNMP Trap interface ID of the ONU. You can use the <b>no snmp-server trap-port</b> command to restore default configurations.
6	Raisecom(config-epon-onu- *//*:*)# <b>snmp-server udp-port</b> port	Configure the SNMP UDP port ID of the ONU. You can use the <b>no snmp-server udp-port</b> command to restore default configurations.
7	Raisecom(config-epon-onu- *//*:*)# <b>snmp-server security</b> name	Configure the name of SNMP security principal of the ONU. You can use the <b>no snmp-server security</b> command to restore default configurations.
8	Raisecom(config-epon-onu- *//*:*)# <b>snmp-server community</b> name { ro   rw }	Configure the SNMP community name and properties of the ONU. You can use the <b>no snmp-server community</b> { ro   rw } command to restore default configurations.

## 2.15.8 Configuring ONU UNI

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</b>	Enter EPON ONU UNI configuration mode.
3	Raisecom(config-epon-onu-ethernet- *//*/*:*)# <b>uni name</b> string	(Optional) configure the UNI name. You can use the <b>no uni name</b> command to restore default configurations.
4	Raisecom(config-epon-onu-ethernet- *//*/*:*)# <b>speed</b> auto	(Optional) configure the rate and duplex mode of the UNI to <b>auto</b> .
5	Raisecom(config-epon-onu-ethernet- *//*/*:*)# <b>speed</b> { 10   100   1000 } <b>duplex</b> { full   half }	(Optional) configure the rate and duplex mode of the UNI.
6	Raisecom(config-epon-onu-ethernet- *//*/*:*)# <b>flowcontrol</b> { enable   disable }	(Optional) enable/disable flow control on the UNI.
7	Raisecom(config-epon-onu-ethernet- *//*/*:*)# <b>auto-negotiation restart</b>	(Optional) force the UNI to perform auto-negotiation again.
8	Raisecom(config-epon-onu-ethernet- *//*/*:*)# <b>shutdown</b>	(Optional) shut down the UNI. You can use the <b>no shutdown</b> to enable the UNI.

## 2.15.9 Configuring ONU UNI alarm

### Enabling/Disabling alarm

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



Step	Command	Description
15	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap down-jabber-alarm { enable   disable }</code>	(Optional) enable/disable alarm when the number of UNI downstream Jabbers exceeds the threshold.
16	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap down-jabber-warning { enable   disable }</code>	(Optional) enable/disable warning when the number of UNI downstream Jabbers exceeds the threshold.
17	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap down-oversize-alarm { enable   disable }</code>	(Optional) enable/disable alarm when the number of UNI downstream oversized packets exceeds the threshold.
18	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap down-oversize-warning { enable   disable }</code>	(Optional) enable/disable warning when the number of UNI downstream oversized packets exceeds the threshold.
19	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap down-undersize-alarm { enable   disable }</code>	(Optional) enable/disable alarm when the number of UNI downstream undersized packets exceeds the threshold.
20	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap down-undersize-warning { enable   disable }</code>	(Optional) enable/disable warning when the number of UNI downstream undersized packets exceeds the threshold.
21	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap failure { enable   disable }</code>	(Optional) enable/disable UNI failure alarm.
22	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap loopback { enable   disable }</code>	(Optional) enable/disable UNI loopback alarm.
23	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap loss { enable   disable }</code>	(Optional) enable/disable UNI LOS alarm.
24	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap status-change-times-alarm { enable   disable }</code>	(Optional) enable/disable alarm when the times of UNI status change exceed the threshold.
25	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap status-change-times-warning { enable   disable }</code>	(Optional) enable/disable warning when the times of UNI status change exceed the threshold.
26	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-crc-error-alarm { enable   disable }</code>	(Optional) enable/disable alarm when the number of UNI upstream CRC error packets exceeds the threshold.
27	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-crc-error-warning { enable   disable }</code>	(Optional) enable/disable warning when the number of UNI upstream CRC error packets exceeds the threshold.
28	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-discard-alarm { enable   disable }</code>	(Optional) enable/disable alarm when the number of UNI upstream discarded packets exceeds the threshold.
29	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-discard-warning { enable   disable }</code>	(Optional) enable/disable warning when the number of UNI upstream discarded packets exceeds the threshold.

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

## Configuring alarm threshold

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

Step	Command	Description
2	<b>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</b>	Enter EPON ONU UNI configuration mode.
3	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-crc-error-alarm threshold value</b>	(Optional) configure the alarm threshold of UNI downstream CRC error packets.
4	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-crc-error-warning threshold value</b>	(Optional) configure the warning threshold of UNI downstream CRC error packets.
5	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-discard-alarm threshold value</b>	(Optional) configure the alarm threshold of UNI downstream discarded packets.
6	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-discard-warning threshold value</b>	(Optional) configure the warning threshold of UNI downstream discarded packets.
7	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-drop-event-warning threshold value</b>	(Optional) configure the warning threshold of UNI downstream packet loss events.
8	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-drop-event-alarm threshold value</b>	(Optional) configure the alarm threshold of UNI downstream packet loss events.
9	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-error-alarm threshold value</b>	(Optional) configure the alarm threshold of UNI downstream error packets.
10	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-error-warning threshold value</b>	(Optional) configure the warning threshold of UNI downstream error packets.
11	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-fragment-alarm threshold value</b>	(Optional) configure the alarm threshold of UNI downstream Fragments.
12	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-fragment-warning threshold value</b>	(Optional) configure the warning threshold of UNI downstream Fragments.
13	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-jabber-alarm threshold value</b>	(Optional) configure the alarm threshold of UNI downstream Jabbers.
14	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-jabber-warning threshold value</b>	(Optional) configure the warning threshold of UNI downstream Jabbers.
15	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-oversize-alarm threshold value</b>	(Optional) configure the alarm threshold of UNI downstream oversized packets.
16	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-oversize-warning threshold value</b>	(Optional) configure the warning threshold of UNI downstream oversized packets.
17	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-undersize-alarm threshold value</b>	(Optional) configure the alarm threshold of UNI downstream undersized packets.
18	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap down-undersize-warning threshold value</b>	(Optional) configure the warning threshold of UNI downstream undersized packets.
19	<b>Raisecom(config-epon-onu-ethernet-*/*//*:*)#snmp trap status-change-times-alarm threshold value</b>	(Optional) configure the alarm threshold of UNI status change times.

Step	Command	Description
20	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap status-change-times-warning threshold <i>value</i></b>	(Optional) configure the warning threshold of UNI status change times
21	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-crc-error-alarm threshold <i>value</i></b>	(Optional) configure the alarm threshold of UNI upstream CRC error packets.
22	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-crc-error-warning threshold <i>value</i></b>	(Optional) configure the warning threshold of UNI upstream CRC error packets.
23	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-discard-alarm threshold <i>value</i></b>	(Optional) configure the alarm threshold of UNI upstream discarded packets.
24	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-discard-warning threshold <i>value</i></b>	(Optional) configure the warning threshold of UNI upstream discarded packets.
25	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-drop-event-warning threshold <i>value</i></b>	(Optional) configure the warning threshold of UNI upstream packet loss events.
26	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-drop-event-alarm threshold <i>value</i></b>	(Optional) configure the alarm threshold of UNI upstream packet loss events.
27	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-error-alarm threshold <i>value</i></b>	(Optional) configure the alarm threshold of UNI upstream error packets.
28	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-error-warning threshold <i>value</i></b>	(Optional) configure the warning threshold of UNI upstream error packets.
29	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-fragment-alarm threshold <i>value</i></b>	(Optional) configure the alarm threshold of UNI upstream Fragments.
30	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-fragment-warning threshold <i>value</i></b>	(Optional) configure the warning threshold of UNI upstream Fragments.
31	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-jabber-alarm threshold <i>value</i></b>	(Optional) configure the alarm threshold of UNI upstream Jabbers.
32	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-jabber-warning threshold <i>value</i></b>	(Optional) configure the warning threshold of UNI upstream Jabbers.
33	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-oversize-alarm threshold <i>value</i></b>	(Optional) configure the alarm threshold of UNI upstream oversized packets.
34	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-oversize-warning threshold <i>value</i></b>	(Optional) configure the warning threshold of UNI upstream oversized packets.
35	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-undersize-alarm threshold <i>value</i></b>	(Optional) configure the alarm threshold of UNI upstream undersized packets.
36	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)# snmp trap up-undersize-warning threshold <i>value</i></b>	(Optional) configure the warning threshold of UNI upstream undersized packets.

## 2.15.10 Configuring ONU serial interface

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu uni serial-com slot-id/olt-id/onu-id/uni-id</b>	Enter ONU serial interface configuration mode.
3	<b>Raisecom(config-epon-onu-serial-*//*/*:*)#serial-protocol { rs232   rs485 }</b>	Configure the serial communication protocol of the serial interface.
4	<b>Raisecom(config-epon-onu-serial-*//*/*:*)#baud-rate { 300   1200   2400   4800   9600   14400   19200   28800   38400   57600   115200 }</b>	Configure the baud rate of the serial interface. You can use the <b>no baud-rate</b> command to restore default configurations.
5	<b>Raisecom(config-epon-onu-serial-*//*/*:*)#data-bits bits</b>	Configure data bits of the serial interface. You can use the <b>no data-bits</b> command to restore default configurations.
6	<b>Raisecom(config-epon-onu-serial-*//*/*:*)#stop-bits { bit1   bit1dot5   bit2 }</b>	Configure the stop bit of the serial interface. You can use the <b>no stop-bits</b> command to restore default configurations.
7	<b>Raisecom(config-epon-onu-serial-*//*/*:*)#parity { none   odd   even   mark   space }</b>	Configure the check mode of the serial interface. You can use the <b>no parity</b> command to restore default configurations.
8	<b>Raisecom(config-epon-onu-serial-*//*/*:*)#loopback port-id</b>	Configure the loopback serial interface. You can use the <b>no loopback</b> command to restore default configurations.
9	<b>Raisecom(config-epon-onu-serial-*//*/*:*)#shutdown</b>	Shut down the serial interface. You can use the <b>no shutdown</b> command to enable the serial interface.
10	<b>Raisecom(config-epon-onu-serial-*//*/*:*)#work-mode { tcp-realport   tcp-client   tcp-server   udp }</b>	Configure the working mode of the serial interface. You can use the <b>no work-mode</b> command to restore default configurations.
11	<b>Raisecom(config-epon-onu-serial-*//*/*:*)#service-port port-id</b>	Configure the network service interface of the serial interface. You can use the <b>no service-port</b> command to restore default configurations.
12	<b>Raisecom(config-epon-onu-serial-*//*/*:*)#peer service-port port-id</b>	Configure the peer network service interface of the serial interface. You can use the <b>no peer service-port</b> command to restore default configurations.
13	<b>Raisecom(config-epon-onu-serial-*//*/*:*)#peerip-address ip-address</b>	Configure the IP address of the serial interface. You can use the <b>no peerip-address</b> command to restore default configurations.

Step	Command	Description
14	Raisecom(config-epon-onu-serial- *//*:*)# <b>connect-condition</b> { <b>always</b>   <b>char</b>   <b>dcd on</b>   <b>dsr on</b> }	Configure the condition to initiate a session on the serial interface.  You can use the <b>no connect-condition</b> command to restore default configurations.
15	Raisecom(config-epon-onu-serial- *//*:*)# <b>session-write-right</b> { <b>first</b>   <b>all</b> }	Configure the write right in a session on the serial interface.
16	Raisecom(config-epon-onu-serial- *//*:*)# <b>break-condition</b> { <b>none</b>   <b>dcd-off</b>   <b>dsr-off</b> }	Configure the condition to break down a session on the serial interface.  You can use the <b>no break-condition</b> command to restore default configurations.

### 2.15.11 Configuring data encryption

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>interface epon-onu</b> <i>slot-id/olt-id/onu-id</i>	Enter EPON ONU management configuration mode.
3	Raisecom(config-if-epon-onu- *//*:*)# <b>encryption</b> { <b>enable</b>   <b>disable</b> }	Enable/Disable data encryption.
4	Raisecom(config-if-epon-onu- *//*:*)# <b>encryption</b> { <b>down</b>   <b>up-down</b> }	Configure the direction of data encryption.

### 2.15.12 Configuring DBA

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>epon-onu</b> <i>slot-id/olt-id/onu-id</i>	Enter EPON ONU management configuration mode.
3	Raisecom(config-epon-onu-*//*:*)# <b>dba sla</b> { <b>enable</b>   <b>disable</b> }	Enable/Disable ONU SLA.
4	Raisecom(config-epon-onu-*//*:*)# <b>dba sla</b> <b>queue</b> <i>queue-id</i> <b>fir</b> <i>fir</i> <b>cir</b> <i>cir</i> <b>pir</b> <i>pir</i> [ <b>fix-pkt</b> <i>size</i> ]	Configure parameters of ONU SLA queue.
5	Raisecom(config-epon-onu-*//*:*)# <b>dba sla</b> <b>queue-weight</b> <i>weight0 weight1 weight2</i> <i>weight3 weight4 weight5 weight6 weight7</i>	Configure the weight of ONU SLA queue scheduling.
6	Raisecom(config-epon-onu-*//*:*)# <b>dba sla</b> <b>queue-set</b> <i>queue-list</i>	Configure the ONU SLA queue.
7	Raisecom(config-epon-onu-*//*:*)# <b>dba sla</b> <b>best-effort-scheduling</b> { <b>sp</b>   <b>sp-wrr</b>   <b>wrr</b> }	Configure the scheduling mode of best-effort bandwidth.

Step	Command	Description
8	<b>Raisecom(config-epon-onu-*//*:*)#dba sla high-priority-boundary</b> <i>priority-vlaue</i>	Configure the boundary value of the queue priority in SP+WRR mode. Perform SP scheduling on queues whose priorities are not smaller than the boundary value; perform WRR scheduling on other queues.
9	<b>Raisecom(config-epon-onu-*//*:*)#dba queue-set</b> <i>number report-bit-map queue-list</i>	(Optional) configure the queue set quantity in the Report packet sent by the ONU and the report bitmap, which are not recommended to configure by users.  You can use the <b>no dba queue-set number report-bit-map</b> command to restore default configurations.
10	<b>Raisecom(config-epon-onu-*//*:*)#dba queue-set</b> <i>number report-threshold threshold0 threshold1 threshold2 threshold3 threshold4 threshold5 threshold6 threshold7</i>	(Optional) configure the queue set quantity in the Report packet sent by the ONU and the queue threshold, which are not recommended to configure by users.  You can use the <b>no dba queue-set number report-threshold</b> command to restore default configurations.
11	<b>Raisecom(config-epon-onu-*//*:*)#dba set queue-set</b> <i>list</i>	(Optional) enable the configured queue set on the ONU. This is not recommended to configure by users.  You can use the <b>no dba set queue-set</b> command to restore default configurations.

### 2.15.13 Configuring FEC

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



#### Note

- The ISCOM5508 supports bidirectional FEC. In the receiving direction at both ends of the OLT/ONU, FEC is configured to self-adaptive receiving mode (hybrid mode). That is, the Rx end can receive related information no matter whether FEC is enabled on the Tx end or not.
- In the sending direction of OLT/ONU, FEC can be enabled or disabled.
- At present, bidirectional FEC should be enabled or disabled concurrently.

## 2.15.14 Configuring OAM remote loopback

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU management configuration mode.
3	<b>Raisecom(config-if-epon-onu-*/*:*)#oam remote-loopback</b>	Enable OAM remote loopback. You can use the <b>no oam remote-loopback</b> command to disable this function.

## 2.15.15 Configuring DLF and BPDU forwarding

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU management configuration mode.
3	<b>Raisecom(config-epon-onu-*/*:*)#dlf-pkt forwarding { enable   disable }</b>	Enable/Disable forwarding DLF packets.
4	<b>Raisecom(config-epon-onu-*/*:*)#relay bpdu { enable   disable }</b>	Configure to transparently transmit or terminate BPDUs.

## 2.15.16 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, etc. for the partner device through the OLT to manage the partner device.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU management configuration mode.
3	<b>Raisecom(config-epon-onu-*/*:*)#partner discovery { enable   disable }</b>	Enable/Disable ONU partner discovery.
4	<b>Raisecom(config-epon-onu-*/*:*)#partner partner-id mng-ip address ip-address mask mask default-gw default-gw vlan svlan-id cvlan-id priority</b>	(Optional) configure the management IP address of the ONU partner device. You can use the <b>no partner partner-id mng-ip</b> command to restore default configurations.
5	<b>Raisecom(config-epon-onu-*/*:*)#partner partner-id mng-ip address-type { dynamic   manual }</b>	(Optional) configure the management IP address type of the ONU partner device. You can use the <b>no partner partner-id mng-ip address-type</b> command to restore default configurations.



Step	Command	Description
6	<code>Raisecom(config-epon-onu-*//*:*)#partner partner-id outband default-gw default-gw</code>	(Optional) configure the default gateway for out-of-band management of the ONU partner device.  You can use the <b>no partner partner-id outband default-gw</b> command to restore default configurations.
7	<code>Raisecom(config-epon-onu-*//*:*)#partner partner-id outband ip-address ip-address mask</code>	(Optional) configure the IP address and mask for out-of-band management of the ONU partner device.  You can use the <b>no partner partner-id outband ip-address</b> command to restore default configurations.
8	<code>Raisecom(config-epon-onu-*//*:*)#partner partner-id snmp-server host ip-address</code>	(Optional) configure the IP address of the SNMP server for the ONU partner device.  You can use the <b>no partner partner-id snmp-server host</b> command to restore default configurations.
9	<code>Raisecom(config-epon-onu-*//*:*)#partner partner-id snmp-server security name</code>	(Optional) configure the security principal name the SNMP server for the ONU partner device.  You can use the <b>no partner partner-id snmp-server security</b> command to restore default configurations.
10	<code>Raisecom(config-epon-onu-*//*:*)#partner partner-id snmp-server community name { ro   rw }</code>	(Optional) configure the community name and properties for the ONU partner device.  You can use the <b>no partner partner-id snmp-server community</b> command to restore default configurations.

## 2.15.17 Configuring PPPoE agent

PPPoE agent mainly processes the specified Tag of the PPPoE packet. The Tag contains the following two fields:

- Circuit ID: stuffed with the VLAN ID, interface ID, and host name related to the interface receiving the request packet from the client
- Remote ID: stuffed with the MAC address of the client or switch

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-*//*:*)#pppoe-agent { enable   disable }</code>	Enable/Disable PPPoE agent.

Step	Command	Description
4	<code>Raisecom(config-epon-onu-*//*:*)#pppoe-agent user-define suboption { enable   disable }</code>	Enable/Disable defining PPPoE agent options by users.
5	<code>Raisecom(config-epon-onu-*//*:*)#pppoe-agent circuit-id attach-string string</code>	Configure the attach-string field in the Circuit_ID option of PPPoE agent. You can use the <b>no pppoe-agent circuit-id attach-string</b> command to restore default configurations.
6	<code>Raisecom(config-epon-onu-*//*:*)#pppoe-agent remote-id mode { onumac-binary   clientmac-binary   onumac-ascii   clientmac-ascii   user-define }</code>	Configure the stuffing mode of the Remote_ID option for PPPoE agent. You can use the <b>no pppoe-agent remote-id mode</b> command to restore default configurations.
7	<code>Raisecom(config-epon-onu-*//*:*)#pppoe-agent remote-id string string</code> <code>Raisecom(config-epon-onu-*//*:*)#exit</code>	Configure the user-defined value of the Remote_ID for PPPoE agent.
8	<code>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</code>	Enter UNI configuration mode.
9	<code>Raisecom(config-epon-onu-ethernet-*//*:*)#pppoe-agent circuit-id string string</code>	Configure the user-defined value of the Circuit_ID option for PPPoE agent. You can use the <b>no pppoe-agent circuit-id</b> command to restore default configurations.
10	<code>Raisecom(config-epon-onu-ethernet-*//*:*)#pppoe-agent policy { keep   replace }</code>	Configure the processing policy of packets carrying the Circuit_ID and Remote_ID by the interface. You can use the <b>no pppoe-agent policy</b> command to restore default configurations.

## 2.15.18 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, etc.

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 models of ONU can work as the PD or PSE.

## Enabling PoE

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

## Configuring PoE parameters

PoE parameters include interface parameters and global parameters.

Configure PoE parameters on the interface as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</b>	Enter EPON ONU UNI configuration mode.
3	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)#poe pse max-power value</b>	(Optional) configure the maximum output power of the UNI.  You can use the <b>no poe pse max-power</b> command to restore default configurations.
4	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)#poe pse power-priority { critical   high   low }</b>	(Optional) configure the powering priority of the interface.  You can use the <b>no poe pse power-priority</b> command to restore default configurations.
5	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)#poe pse-off service { enable   disable }</b>	(Optional) configure whether to allow services to pass when the ONU UNI is not connected to the PSE.
6	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)#poe pse compatibility { enable   disable }</b>	(Optional) enable/disable the interface to provide power to the non-standard FD.

Configure global PoE parameters as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU management configuration mode.
3	<b>Raisecom(config-epon-onu-*/*/*:*)#poe pse power-management { auto   manual }</b>	Configure the power management mode of the ONU.  You can use the <b>no poe pse power-management</b> command to restore default configurations.

Step	Command	Description
4	<b>Raisecom(config-epon-onu-*//*:*)#poe pse power-threshold <i>value</i></b>	(Optional) configure the power usage percentage threshold of the PSE. You can use the <b>no poe pse power-threshold</b> command to restore default configurations.
5	<b>Raisecom(config-epon-onu-*//*:*)#poe pse temperature-protection { enable   disable }</b>	(Optional) enable/disable overtemperature protection on the PSE.
6	<b>Raisecom(config-epon-onu-*//*:*)#poe pse trap { enable   disable }</b>	(Optional) enable/disable Trap report on the ONU PSE.

## 2.15.19 Checking configurations

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

No.	Command	Description
15	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id system</b>	Show system configurations of the ONU, including BPDU transparent transmission and DLF packet forwarding.
16	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id partner [ discovery ]</b>	Show the status and configurations of ONU partner discovery.
17	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id partner [ partner-id ]</b>	Show information about the ONU partner device.
18	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id partner [ partner-id ] snmp-server</b>	Show SNMP parameters of the ONU partner device.
19	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id poe pse information</b>	Show ONU power information.
20	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet [ uni-id ] poe pse information</b>	Show configurations of the PSE interface for the ONU UNI.
21	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id poe information</b>	Show ONU UNI power information.
22	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list pppoe-agent</b>	Show PPPoE configurations of the ONU.
23	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list uni ethernet [ uni-id ] pppoe-agent</b>	Show PPPoE interface configurations of the ONU.
24	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list uni ethernet [ uni-id ] pppoe-agent statistics</b>	Show PPPoE statistics of the ONU.
25	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list mng-information</b>	Show management information about the ONU.
26	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id information</b>	Show parameters of the ONU serial interface.
27	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id auto-negotiation ability</b>	Show configurations for ONU serial interface management.
28	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id name</b>	Show configurations of the ONU serial interface service.
29	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id system</b>	Show information about ONU serial interface session.
30	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list config-counter</b>	Show the value of the configuration counter at the OLT side and ONU side.
31	<b>Raisecom#show interface epon-onu slot-id/olt-id/onu-list oam loopback</b>	Show configurations of OAM remote loopback.

No.	Command	Description
32	<code>Raisecom#show interface epon-onu slot-id/olt-id/onu-list oam</code>	Show local configurations and status of the OAM channel, including mode configuration, management status, working status, MTU, configuration version, and supported functions.
33	<code>Raisecom#show interface epon-onu slot-id/olt-id/onu-list oam peer</code>	Show information about the peer device on the OAM channel.
34	<code>Raisecom#show interface epon-onu slot-id/olt-id/onu-list oam peer event</code>	Show events reported by the peer ONU, including fault and link monitoring event.
35	<code>Raisecom#show interface epon-onu slot-id/olt-id/onu-list oam statistics</code>	Show OAM statistics.
36	<code>Raisecom#show interface epon-onu slot-id/olt-id/onu-list encryption</code>	Show configurations of ONU data encryption.
37	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id dba sla</code>	Show SLA configurations of the ONU.
38	<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.
39	<code>Raisecom#show interface epon-onu slot-id/olt-id/onu-id fec</code>	Show the status of ONU FEC.
40	<code>Raisecom#show epon-onu slot-id/olt-id/onu-list environment</code>	Show the ambient temperature and power voltage of the ONU.

## 2.16 Configuration examples

### 2.16.1 Example for configuring ONU auto-registration

#### Networking requirements

As shown in Figure 2-6, configure the ONU authentication mode as **none** on OLT 1/1, so the ONU can register on the OLT automatically.

Figure 2-6 Configuring ONU auto-registration



## Configuration steps

Configure the ONU authentication mode as **none**.

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

## Checking results

Show the ONU authentication mode.

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

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

Show information about the ONU registered on the OLT.

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

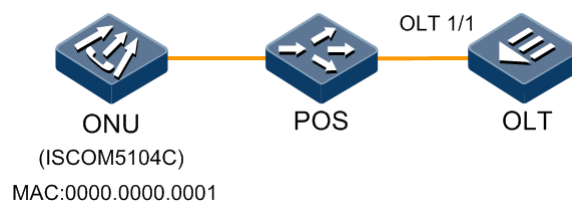
ONU ID	MAC Address	Mode	Creation Date	Device Type	State	Mng-mode
1/1/1	000e.5e0a.7a0e	auto	2000-01-01,08:00	ISCOM5304D	active	oam

## 2.16.2 Example for configuring ONU registration in MAC-based authentication mode

### Networking requirements

As shown in Figure 2-7, enable to register the ONU in MAC-based authentication mode on OLT 1/1. The ONU model is 5104c and its MAC address is 0000.0000.0001.

Figure 2-7 Configuring ONU registration in MAC-based authentication mode



## Configuration steps

Step 1 Configure the ONU authentication mode as MAC-based authentication mode.

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

Step 2 Create the ONU entries based on the MAC address.

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

## Checking results

Show the ONU authentication mode.

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

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

Show information about the ONU registered on the OLT.

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

ONU ID	MAC Address	Mode	Creation Date	Device Type	State	Mng-mode
1/1/1	0000.0000.0001	mac	2000-01-01,08:00	ISCOM5104(C)	active	oam



# 3

## Configuring multicast services

---

This chapter introduces multicast services and configuration process of the ISCOM5508, including the following sections:

- Overview of multicast services
- Quick configuration of multicast services
- Configuring static multicast
- Configuring IGMP Snooping
- Configuring IGMP Proxy
- Configuring MVR
- Configuring multicast group limit
- Configuring dynamic controllable multicast
- Configuring MLD Snooping
- Configuring MLD Proxy
- Configuring multicast VLAN
- Maintenance

### 3.1 Overview of multicast services

#### 3.1.1 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

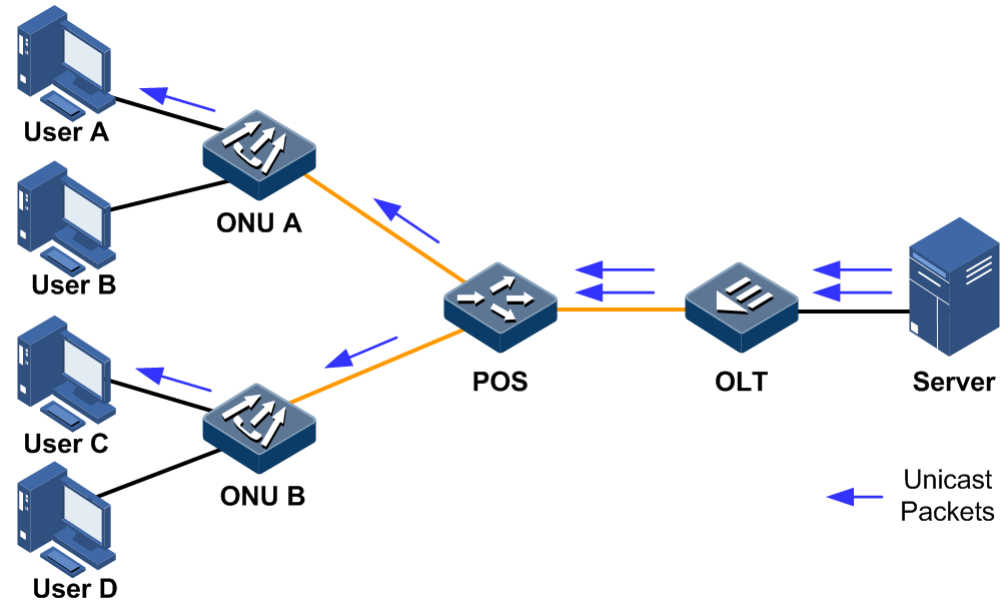
In Ethernet network, packets are transmitted in forms of unicast, broadcast, and multicast.

- 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 3-1, assume that User A and User C need a certain packet. 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.

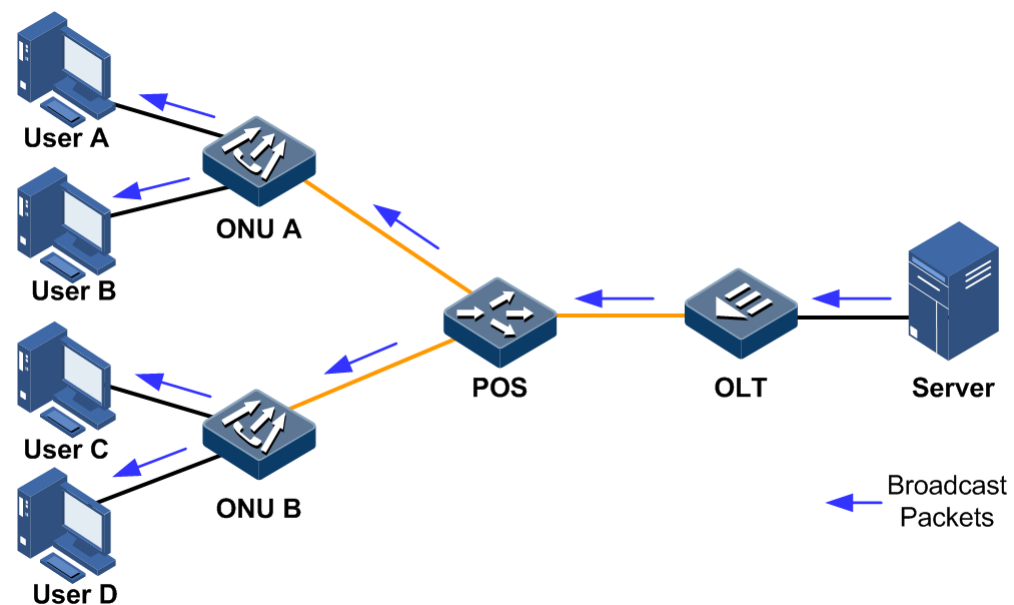
Figure 3-1 Unicast transmission mode



- 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 3-2, assume that User A and User C need a certain packet. In the broadcast transmission mode, the Server floods this packet through a router and all users (including User B) will also receive this packet. The security and non-gratuitousness of the packet cannot be ensured. In addition, network resources cannot be well utilized when few users need this packet.

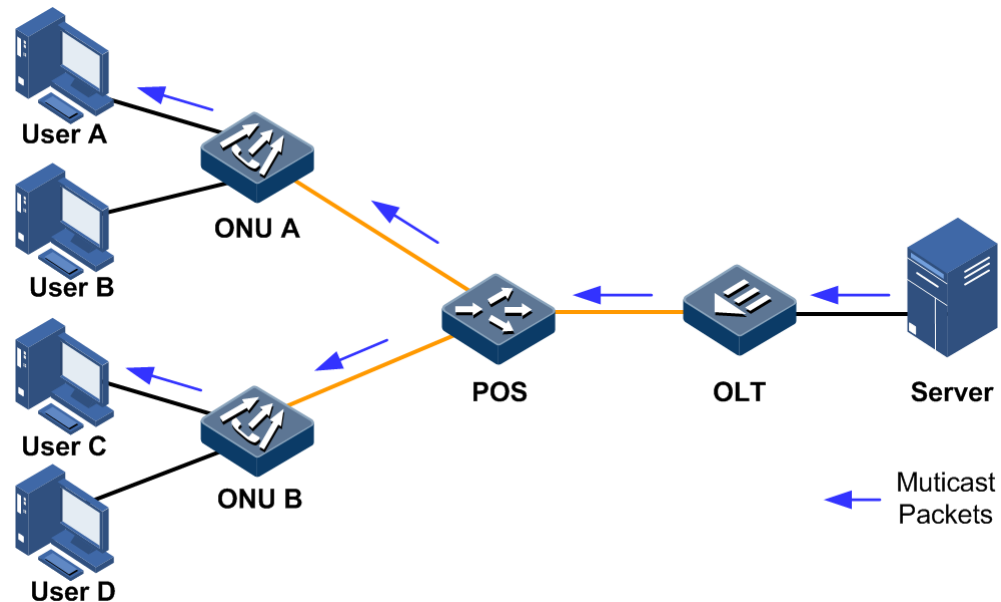
Figure 3-2 Broadcast transmission mode



- **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 3-3, 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 ISCOM5508 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 3-3 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 ISCOM5508 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, realize multicast routing, and to conduct forwarding multicast packets.

- Router interface: an interface on the ISCOM5508, 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 ISCOM5508. 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.

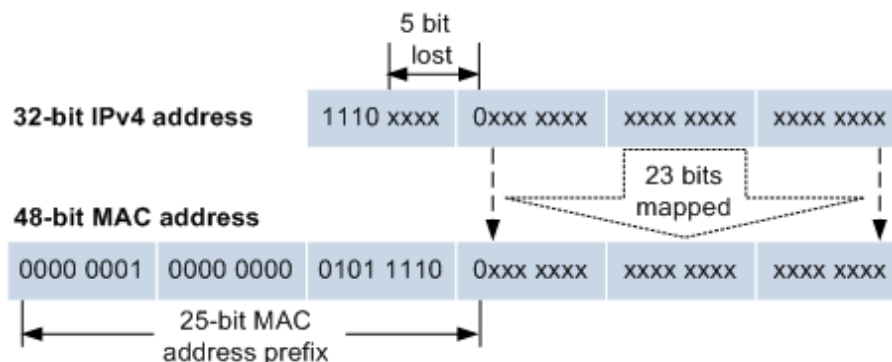
IPv6 multicast addresses are preceded with FF. The first 8 bits are set to 1. If the third hexadecimal number is set to 0, it indicates the IPv6 multicast address is a commonly-used multicast address. If it is set to 1, it indicates the IPv6 multicast address is a temporary multicast address. The fourth 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 3-4 shows the mapping between an IPv4 multicast address and a multicast MAC address.

Figure 3-4 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 ISCOM5508 will receive other multicast data. These redundant multicast data will be filtered on the upper layer of the ISCOM5508.

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

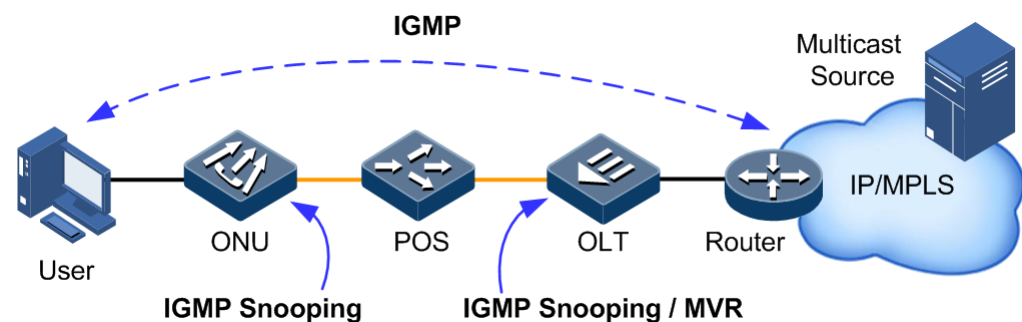
For a network that needs to realize multicast services, you need to deploy various multicast protocols at different nodes of the network. These multicast protocols cooperate with each other to realize network-based multicast services.

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 3-5 shows operating positions of the IGMP and Layer 2 multicast protocols.

Figure 3-5 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.

### 3.1.2 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 ISCOM5508 listens to an IGMP Report packet sent to a multicast group by a host, the ISCOM5508 will add the interface, which is connected to the host, to the forwarding table of the multicast group. Similarly, when the ISCOM5508 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 ISCOM5508 will delete the interface from the multicast group.

IGMP Snooping forwards multicast data through Layer 2 multicast forwarding table. When the ISCOM5508 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 either dynamically learn or manually configure the Layer 2 multicast forwarding table.

### 3.1.3 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 ISCOM5508 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.

- Interval for last member to respond

The ISCOM5508 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 ISCOM5508 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.

## 3.1.4 MVR

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

By configuring multicast VLANs, MVR adds member ports of different Customer VLAN (CVLAN) of the ISCOM5508 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.

### 3.1.5 Dynamic controllable multicast

In the EPON, dynamic controllable multicasts forward multicast services in a form of SCB+IGMP. The ISCOM5508 supports 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.

## 3.2 Quick configuration of multicast services

Configuration of multicast service is complicated, involving a number of functional configuration items. This section provides several typical configuration examples to facilitate you to quickly enable multicast services.

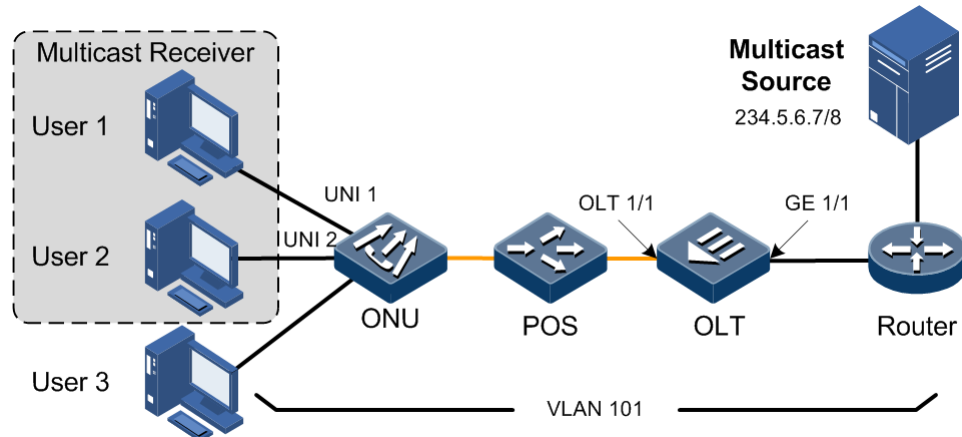
### 3.2.1 Example for configuring IGMP Snooping

#### Networking requirements

As is shown in Figure 3-6, the OLT connects to the multicast router through the uplink interface GE 1/1, and connects to the ONU through the PON interface OLT 1/1. Two Ethernet interfaces UNI 1 and UNI 2 on the ONU are respectively connected to two users. All multicast users belong to the same VLAN 101. You need to respectively configured IGMP Snooping and immediate-leave on the OLT and ONU to enable users to receive multicast data.



Figure 3-6 IGMP Snooping networking



## Configuration steps

- Configure the OLT.

Step 1 Create a multicast VLAN and configure interface properties.

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

Step 2 Configure interface roles for the multicast VLAN and enable immediate-leave.

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

Step 3 Enable global IGMP.

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

- Configure the ONU.

Step 4 Create a multicast VLAN and configure interface properties.

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

Step 5 Enable IGMP Snooping and configure immediate-leave.

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

Step 6 Configure the forwarding mode of multicast service traffic.

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

## Checking results

- Show OLT configurations.

Show IGMP configurations on the OLT.

```
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
```

Show IGMP configurations on the ONU.

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

Show multicast VLAN configurations on the ONU.

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

Show configurations of the router interface in the IGMP multicast VLAN.

```
Raisecom#show multicast-vlan 10 router
Multicast vlan      Router
-----
101                 gigabitethernet1/1
```

Show configurations of member interfaces in the IGMP multicast VLAN.

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

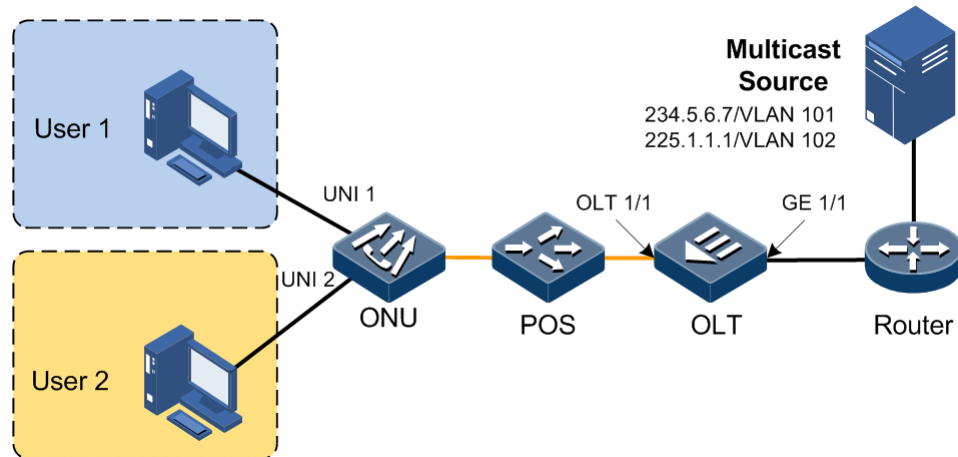
## 3.2.2 Example for configuring dynamic controllable multicast

### Networking requirements

As shown in Figure 3-7, the OLT connects to the multicast router through the interface GE 1/1, and connects to users through the PON interface OLT 1/1. Through dynamic controllable multicast, User 1 and User 2 have different access privileges to channel 1 (234.5.6.7) and channel 2 (225.1.1.1).

- User 1: be allowed to watch channel 1, and have preview privilege to channel 2 for 10 minutes.
- User 2: be forbidden to watch channel 1, but be allowed to watch channel 2.

Figure 3-7 Dynamic controllable multicast networking



## Configuration steps

- Configure 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
Raisecom(config)#exit
```

Step 2 Enable IGMP.

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

Step 3 Create the 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 packag1 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 the preview profile.

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

Step 5 Create dynamic controllable users and specify channels for the users.

```
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 1/1  
Raisecom(config-if-epon-olt-1:1)#multicast-vlan 101 member  
Raisecom(config-if-epon-olt-1:1)#multicast-vlan 102 member
```

Step 7 Configure the interface OLT 1/1.

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

- Configure the ONU.

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

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

Step 9 Configure the ONU interface.

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

## Checking results

- Show OLT configurations.

Show channel configurations of dynamic controllable multicast.

```
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 1/1/11 package1online
```

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

- Show ONU configurations.

Show the processing mode of ONU IGMP packets.

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

ONU ID: 1/1/1

IGMP Mode : ctrl-multicast

Last Member Query Count : 2

Last Member Query Interval : 2s

Aging Time : 300s

Immediate-leave Administrative : enable

## 3.3 Configuring static multicast

### 3.3.1 Preparing for configurations

#### Scenario

The ISCOM5508 supports 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

### 3.3.2 Default configurations

N/A

### 3.3.3 Configuring static multicast

The ISCOM5508 adds the member interface to the multicast routing table by identifying the IGMP packet sent by the host automatically. You can manually configure the ISCOM5508 to add member interfaces for a specified multicast routing table.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mac-address-table static multicast</b> <i>mac-address</i> <b>vlan</b> <i>vlan-id</i> <b>interface</b> { <b>epon-olt</b> <i>slot-id/olt-id</i>   <b>gigabitethernet</b> <i>slot-id/olt-id</i>   <b>port-channel</b> <i>group-id</i> }	Configure static Layer 2 multicast MAC address entries.
3	<b>Raisecom(config)#mac-address-table static multicast</b> <i>mac-address</i> <b>vlan</b> <i>vlan-id</i> { <b>add</b>   <b>remove</b> } <b>interface</b> { <b>epon-olt</b> <i>slot-id/olt-id</i>   <b>gigabitethernet</b> <i>slot-id/olt-id</i>   <b>port-channel</b> <i>group-id</i> }	(Optional) add/remove an interface to/from a Layer 2 static multicast group.

### 3.3.4 Configuring unknown multicat filter

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

Step	Command	Description
2	Raisecom(config)# <b>mac-address-table unknown-multicast filter vlanlist</b> <i>vlan-list</i>	(Optional) configure the VLAN list for unknown multicast filter.

### 3.3.5 Checking configurations

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

## 3.4 Configuring IGMP Snooping

### 3.4.1 Preparing for configurations

#### Scenario

If multiple ONU users need to receive data from the multicast source, you can enable IGMP Snooping on the ISCOM5508 or ONU, and create and maintain the multicast forwarding table 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 ISCOM5508 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.

### 3.4.2 Default configurations

Default configurations of IGMP Snooping on the ISCOM5508 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



Function	Default value
Multicast router interface	N/A
Immediate-leave	Disable
Static multicast routing table	N/A

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

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



### Note

Raisecom ONU series with a single Ethernet interface do not support being configured with the forwarding mode of multicast service traffic and do not identify the VLAN. By default, they support MAC-based packet forwarding.

## 3.4.3 Configuring IGMP Snooping

### Configuring IGMP Snooping on OLT


Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#igmp</b>	Enable global IGMP Snooping. You can use the <b>no igmp</b> 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	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU management configuration mode.
3	<b>Raisecom(config-epon-onu-*//*:*)#ip igmp mode { snooping   ctrl-multicast   transparent   proxy }</b>	Configure IGMP mode.
4	<b>Raisecom(config-epon-onu-*//*:*)#ip igmp vlan-aware{ enable   disable }</b>	(Optional) configure the forwarding mode of multicast service traffic to <b>vlan-aware</b> .
5	<b>Raisecom(config-epon-onu-*//*:*)#ip igmp last-member-query-count count</b>	(Optional) configure the timeout times to send the Last-Member query packet triggered by the leave packet. You can use the <b>no ip igmp last-member-query-count</b> command to restore default configurations.
6	<b>Raisecom(config-epon-onu-*//*:*)#ip igmp last-member-query-interval second</b>	(Optional) configure the interval to respond to the Last-Member query packet triggered by the leave packet. You can use the <b>no ip igmp last-member-query-interval</b> command to restore default configurations.
7	<b>Raisecom(config-epon-onu-ethernet-*//*:*)#multicast vlan { stripped   no-stripped }</b>	(Optional) configure the UNI whether to remove the VLAN Tag of the multicast service packet.   <b>Note</b> When ONU lower-layer devices cannot identify the VLAN, you need to configure the UNI to remove the VLAN Tag of the multicast service packet.
8	<b>Raisecom(config-epon-onu-ethernet-*//*:*)#multicast vlan vlan-list</b>	(Optional) configure the multicast VLAN list on the UNI. You can use the <b>no multicast vlan</b> command to restore default configurations.

### 3.4.4 (Optional) configuring aging time of multicast routing entries

In IGMP Snooping, when the ISCOM5508 does not receive the IGMP packet about Layer 2 multicast routing in a period of time, maybe the relevant host or router has left 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 multicast routing entries on OLT

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#igmp snooping timeout</b> <b>{ period   infinite }</b>	Configure the aging time of multicast routing entries.  You can use the <b>no igmp snooping timeout</b> command to restore default configurations.

### Configuring aging time of multicast routing entries on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-</b> <b>id/olt-id/onu-id</b>	Enter EPON ONU management configuration mode.
3	<b>Raisecom(config-epon-onu-</b> <b>*/:*)#ip igmp aging-time</b> <b>period</b>	Configure the aging time of multicast routing entries.  You can use the <b>no ip igmp aging-time</b> command to restore default configurations.

### 3.4.5 (Optional) configuring immediate-leave

When the user host sends the IGMP leave packet, the ISCOM5508 does not delete multicast route immediately, 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 immediately when the user host sends the IGMP leave packet.

At present, only IGMP v2/v3 supports this function.

### Configuring immediate-leave on OLT

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface { epon-olt</b> <b>slot-id/olt-id   gigabitethernet slot-</b> <b>id/olt-id   port-channel group-id}</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-*/:*)#igmp snooping</b> <b>immediate-leave multicast-vlan</b> <i>vlan-list</i>	Configure immediate-leave based on interface or interface+VLAN.  You can use the <b>no igmp snooping immediate-leave multicast-vlan</b> <i>vlan-list</i> command to disable this function.

## Configuring immediate-leave on ONU

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

## 3.4.6 Checking configurations

### Checking configurations of OLT

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

### Checking configurations of ONU

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

## 3.5 Configuring IGMP Proxy

### 3.5.1 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 configuration and management of the multicast router to client subnet 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.

### 3.5.2 Default configurations

Default configurations of IGMP Proxy on the ISCOM5508 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

### 3.5.3 Configuring IGMP Proxy

#### Configuring IGMP Proxy on OLT



#### 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	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#igmp proxy query-interval seconds</b>	(Optional) configure the IGMP query interval. You can use the <b>no igmp proxy query-interval</b> command to restore default configurations.
3	<b>Raisecom(config)#igmp proxy query-max-response seconds</b>	(Optional) configure the maximum response time of IGMP query. You can use the <b>no igmp proxy query-max-response</b> command to restore default configurations.
4	<b>Raisecom(config)#igmp proxy last-query-interval seconds</b>	(Optional) configure the query interval of the last member in the multicast group. You can use the <b>no igmp proxy last-query-interval</b> command to restore default configurations.

Step	Command	Description
5	<b>Raisecom(config)#igmp proxy last-query-count</b> <i>count</i>	(Optional) configure the query times of the last member in the multicast group. You can use the <b>no igmp proxy last-query-count</b> command to restore default configurations.
6	<b>Raisecom(config)#igmp proxy source-ip</b> <i>ip-address</i>	(Optional) configure the source IP address of the IGMP Proxy packet sent by the IGMP querier. You can use the <b>no igmp proxy source-ip</b> command to restore default configurations.
7	<b>Raisecom(config)#igmp proxy robustness</b> <i>robustness</i>	Configure the IGMP Proxy robustness coefficient. You can use the <b>no igmp proxy robustness</b> command to restore default configurations.

### Configuring IGMP Proxy on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU management configuration mode.
3	<b>Raisecom(config-epon-onu-*//*:*)#ip igmp proxy ip-address</b> <i>address</i>	Configure the IP address of IGMP Proxy. You can use the <b>no ip igmp proxy ip-address</b> command to delete the configuration.
4	<b>Raisecom(config-epon-onu-*//*:*)#ip igmp proxy vlan</b> <i>vlan-id</i>	(Optional) configure IGMP Proxy VLAN. You can use the <b>no ip igmp proxy vlan</b> command to delete the configuration.



#### Note

The ONU does not support IGMP Proxy.

### 3.5.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet multicast</b>	Show configurations of multicast services on the Ethernet interface of the ONU.
2	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id mac-address-table multicast</b> [ <b>uni ethernet uni</b> ]	Show multicast addresses and VLAN IDs learnt by the Ethernet interface of the ONU.

## 3.6 Configuring MVR

### 3.6.1 Preparing for configurations

#### Scenario

When multiple user hosts need to receive data from the multicast source, and when different user hosts, host and multicast router belong to different VLANs, you can configure MVR on the multicast router and the ISCOM5508 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.

### 3.6.2 Default configurations

Default configurations of MVR on the ISCOM5508 are as below.

Function	Default value
Global MVR	Disable

### 3.6.3 Configuring basic MVR

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

### 3.6.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show mvr</b>	Show MVR configurations.

## 3.7 Configuring multicast group limit

### 3.7.1 Preparing for configurations

#### Scenario

Raisecom ONU supports multicast group limit based on member interface.

#### Prerequisite

N/A

### 3.7.2 Default configurations

Default configurations of multicast group limit on the ONU are as below.

Function	Default value
Maximum number of IGMP multicast groups	64

### 3.7.3 Configuring multicast group limit on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</b>	Enter EPON ONU UNI configuration mode.
3	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)#multicast max-group-num group-number</b>	Configure the maximum number of multicast groups on the Ethernet interface of the ONU. You can use the <b>no multicast max-group-num</b> command to restore default configurations.

### 3.7.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list uni ethernet multicast</b>	Show configurations of multicast services on the Ethernet interface of the ONU.
2	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id mac-address-table multicast [ uni ethernet uni ]</b>	Show multicast addresses and VLAN IDs learnt by the Ethernet interface of the ONU.



## 3.8 Configuring dynamic controllable multicast

### 3.8.1 Preparing for configurations

#### Scenario

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

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

#### Prerequisite

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

### 3.8.2 Default configurations

Default configurations of dynamic controllable multicast on the ISCOM5508 are as below.

Function	Default value
Dynamic controllable multicast	Disable
Channel preview	Enable
Auto-reset period of preview	weekly
Aware time of preview	4s
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	5min

### 3.8.3 Configuring global function

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#multicast-ctrl</b>	Enable global dynamic controllable multicast.
3	<b>Raisecom(config)#multicast-ctrl max-non-igmp-report-duration <i>time</i></b>	(Optional) configure the maximum duration when there is no on-demand packet. You can use the <b>no multicast-ctrl max-non-igmp-report-duration</b> command to restore default configurations.

### 3.8.4 Configuring user management

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#multicast-ctrl user username source slot-id/port-id/vport-id cvlan vlan-id</b>	Create a dynamic controllable multicast user.
3	<b>Raisecom(config)#multicast-ctrl user username package packagename</b>	Configure the channel package for the specified user.

### 3.8.5 Configuring channel management

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#multicast-ctrl channel id id name channel-name group-ip ip-address</b>	Create a multicast channel. You can use the <b>no multicast-ctrl channel name</b> command to delete the configuration.
3	<b>Raisecom(config)#multicast-ctrl channel channelname cdr</b>	(Optional) enable CDR on the channel. You can use the <b>no multicast-ctrl channel channelname cdr</b> command to disable this function.
4	<b>Raisecom(config)#multicast-ctrl package packagename</b>	Create a channel package. You can use the <b>no multicast-ctrl package packagename</b> command to delete the configuration.
5	<b>Raisecom(config)#multicast-ctrlpackage packagename channel channelname { deny   permit   preview } [ preview-profile profile ]</b>	Add channels to the package. You can use the <b>no multicast-ctrl package packagename channel channelname</b> command to restore default configurations.

### 3.8.6 Configuring preview rules

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#multicast-ctrl preview</b>	Enable the preview function. You can use the <b>no multicast-ctrl preview</b> command to disable this function.
3	<b>Raisecom(config)#multicast-ctrl preview reset</b>	Configure resetting preview manually.
4	<b>Raisecom(config)#multicast-ctrl preview auto-reset-period { daily   weekly   monthly }</b>	Configure the auto-reset period of preview. You can use the <b>no multicast-ctrl preview auto-reset-period</b> command to restore default configurations.

Step	Command	Description
5	<code>Raisecom(config)#multicast-ctrl preview auto-reset-time time</code>	Configure the auto-reset time of preview. You can use the <b>no multicast-ctrl preview auto-reset</b> command to restore default configurations.
6	<code>Raisecom(config)#multicast-ctrl preview aware-time time</code>	Configure the aware time of preview. You can use the <b>no multicast-ctrl preview aware-time</b> command to restore default configurations.
7	<code>Raisecom(config)#multicast-ctrl preview-profile profile</code>	Create a preview profile. You can use the <b>nomulticast-ctrl peview-profile profile</b> command to delete the profile.
8	<code>Raisecom(config)#multicast-ctrl preview-profile profile total-time time</code>	Configure the total time for previewing a profile. You can use the <b>no multicast-ctrl peview-profile profile total-time</b> command to restore default configurations.
9	<code>Raisecom(config)#multicast-ctrl preview-profile profile count count</code>	Configure the maximum times for previewing a profile. You can use the <b>no multicast-ctrl peview-profile profile count</b> command to restore default configurations.
10	<code>Raisecom(config)#multicast-ctrl preview-profile profile duration time</code>	Configure the maximum duration for previewing a profile at one time. You can use the <b>no multicast-ctrl peview-profile profile duration</b> command to restore default configurations.
11	<code>Raisecom(config)#multicast-ctrl preview-profile profile interval time</code>	Configure the interval for previewing a profile for a second time. You can use the <b>no multicast-ctrl peview-profile profile interval</b> command to restore default configurations.

### 3.8.7 Configuring CDR

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#multicast-ctrl cdr</code>	Enable CDR management. You can use the <b>no multicast-ctrl cdr</b> command to disable this function.
3	<code>Raisecom(config)#multicast-ctrl cdr max-records number</code>	Configure the maximum number of CDR. You can use the <b>no multicast-ctrl cdr max-records</b> command to restore default configurations.
4	<code>Raisecom(config)#multicast-ctrl cdr report</code>	Configure reporting CDR manually.

Step	Command	Description
5	<code>Raisecom(config)#multicast-ctrl cdr report-interval <i>report- interval</i></code>	Configure the interval for reporting CDR manually.  You can use the <b>no multicast-ctrl cdr report-interval</b> command to restore default configurations.
6	<code>Raisecom(config)#multicast-ctrl cdr report-threshold <i>value</i></code>	Configure the threshold for reporting CDR manually.  You can use the <b>no multicast-ctrl cdr report-threshold</b> command to restore default configurations.

### 3.8.8 Checking configurations

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

## 3.9 Configuring MLD Snooping

### 3.9.1 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 realize the multicast function in an IPv6 network, you need to configure the MLD multicast function.

## Prerequisite

N/A

## 3.9.2 Default configurations

Default configurations of MLD on the ISCOM5508 are as below.

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

## 3.9.3 Configuring MLD Snooping

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mld</b>	Enable MLD Snooping. You can use the <b>no mld</b> command to disable this function.
3	<b>Raisecom(config)#mld snooping timeout { period   infinite }</b>	(Optional) configure the aging time of MLD Snooping. You can use the <b>no mld snooping timeout</b> command to restore default configurations.

## 3.9.4 Checking configurations

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

## 3.10 Configuring MLD Proxy

### 3.10.1 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 realize the multicast function in an IPv6 network, you need to configure the MLD multicast function.

#### Prerequisite

N/A

### 3.10.2 Default configurations

Default configurations of MLD on the ISCOM5508 are as below.

Function	Default value
Global MLD multicast	Disable
MLD multicast IP address	Local link address, that is, 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

### 3.10.3 Configuring MLD Proxy

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mld</b>	Enable MLD Proxy. You can use the <b>no mld</b> command to disable this function.

Step	Command	Description
3	<b>Raisecom(config)#mld proxy source-ip</b> <i>ip-address</i>	Configure the MLD Proxy multicast IP address. You can use the <b>no mld proxy source-ip</b> command to delete the configuration.
4	<b>Raisecom(config)#mld proxy query-interval</b> <i>seconds</i>	(Optional) configure the MLD Proxy query interval. You can use the <b>no mld proxy query-interval</b> command to restore default configurations.
5	<b>Raisecom(config)#mld proxy query-max-response</b> <i>seconds</i>	(Optional) configure the maximum response time of MLD Proxy query. You can use the <b>no mld proxy query-max-response</b> command to restore default configurations.
6	<b>Raisecom(config)#mld proxy last-query-interval</b> <i>seconds</i>	(Optional) configure the query interval of MLD Proxy last member. You can use the <b>no mld proxy last-query-interval</b> command to restore default configurations.
7	<b>Raisecom(config)#mld proxy last-query-count</b> <i>count</i>	(Optional) configure the times to query the MLD Proxy last member. You can use the <b>no mld proxy last-query-count</b> command to restore default configurations.
8	<b>Raisecom(config)#mld proxy source-ip</b> <i>ip-address</i>	(Optional) configure the source IP address of the query packet sent by the MLD Proxy querier. You can use the <b>no mld proxy source-ip</b> command to restore default configurations.
9	<b>Raisecom(config)#mld proxy robustness</b> <i>robustness</i>	(Optional) configure the robustness coefficient of MLD Proxy. You can use the <b>no mld proxy robustness</b> command to restore default configurations.

### 3.10.4 Checking configurations

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

## 3.11 Configuring multicast VLAN

### 3.11.1 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

### 3.11.2 Default configurations



Default configurations of multicast VLAN on the ISCOM5508 are as below.

Function	Default value
Multicast VLAN	N/A
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

### 3.11.3 Configuring multicast VLAN

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#multicast-vlan <i>vlan-id</i></b>	Create a multicast VLAN.
3	<b>Raisecom(config)#multicast-vlan <i>vlan-id</i> mode { snooping   proxy }</b>	Configure the working mode of the multicast VLAN.



Step	Command	Description
4	<code>Raisecom(config)#multicast-vlan vlan-id group { group-address [ count ]   any }</code>	Configure binding the multicast VLAN with the group address.  You can use the <b>no multicast-vlan vlan-id group { group-address [ count ]   any }</b> command to restore default configurations.
5	<code>Raisecom(config)#multicast-vlan vlan-id cvlan-forward</code>	Configure CVLAN transparent transmission.
6	<code>Raisecom(config)#multicast-vlan vlan-id upstream-priority pri</code>	Configure the priority of multicast VLAN uplink protocol packets.
7	<code>Raisecom(config)#multicast-vlan vlan-id downstream-priority pri</code>	Configure the priority of multicast VLAN downlink protocol packets.
8	<code>Raisecom(config)#interface { epon-olt slot-id/olt-id   gigabitethernet slot-id/olt-id   port-channel group-id }</code>	Enter physical interface configuration mode.
9	<code>Raisecom(config-if-* :*)#multicast-vlan vlan-id router</code>	Configure an interface as the multicast VLAN router interface.   <b>Note</b> Before you use this command to configure the interface role for the multicast VLAN, the system supports dynamically learning the interface role.
10	<code>Raisecom(config-if-* :*)#multicast-vlan vlan-id member</code>	Configure an interface as the multicast VLAN member interface.   <b>Note</b> Before you use this command to configure the interface role for the multicast VLAN, the system supports dynamically learning the interface role.

### 3.11.4 Checking configurations

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

## 3.12 Maintenance

Command	Description
<code>Raisecom(config)#clear igmp statistics</code>	Clear IGMP packet statistics.
<code>Raisecom(config)#clear interface { epon-olt slot-id/olt-id   gigabitethernet slot-id/olt-id   port-channel group-id } igmp statistics</code>	Clear IGMP packet statistics on a specified interface.
<code>Raisecom(config)#clear mld statistics</code>	Clear MLD packet statistics.
<code>Raisecom(config)#clear interface { epon-olt slot-id/olt-id   gigabitethernet slot-id/olt-id   port-channel group-id } mld statistics</code>	Clear MLD packet statistics on a specified interface.
<code>Raisecom(config)#multicast-ctrl cdr clear</code>	Clear CDR information.

# 4 Configuring VoIP services

---

This chapter introduces VoIP services and configuration process of the ISCOM5508, 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 process tone
- Configuring call emulation test
- Maintenance

## 4.1 Overview of VoIP services

### 4.1.1 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 ISCOM5508 supports Session Initiation Protocol (SIP) and H.248 protocol.

## 4.1.2 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

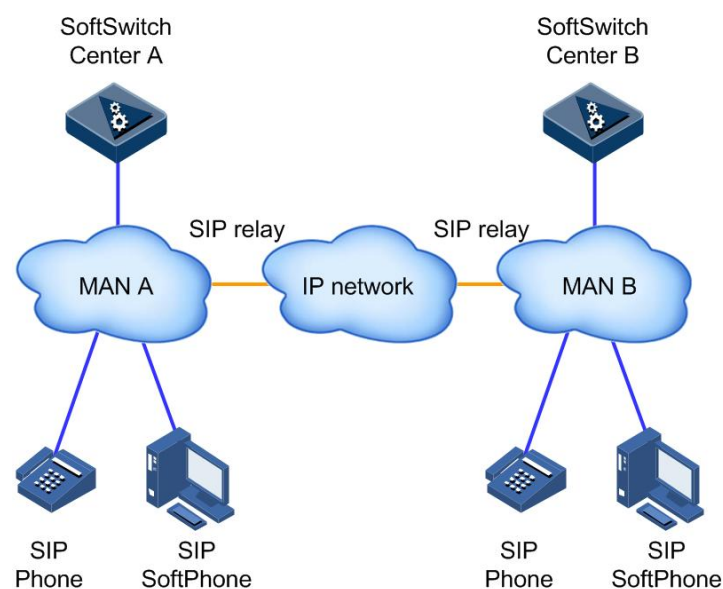
Related concepts involved in the operating environment of SIP are shown as below.

- 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 decapsulates and modify (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 and the Proxy Server/Redirect Server locate at the same place 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 4-1 shows a typical application of SIP in the Next Generation Network (NGN).

Figure 4-1 Typical application of SIP in NGN

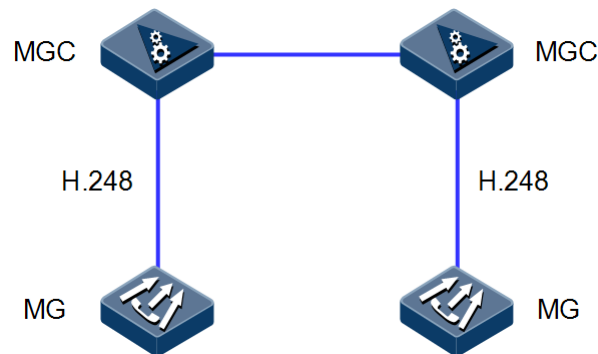


## 4.1.3 H.248

### 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 4-2.

Figure 4-2 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.

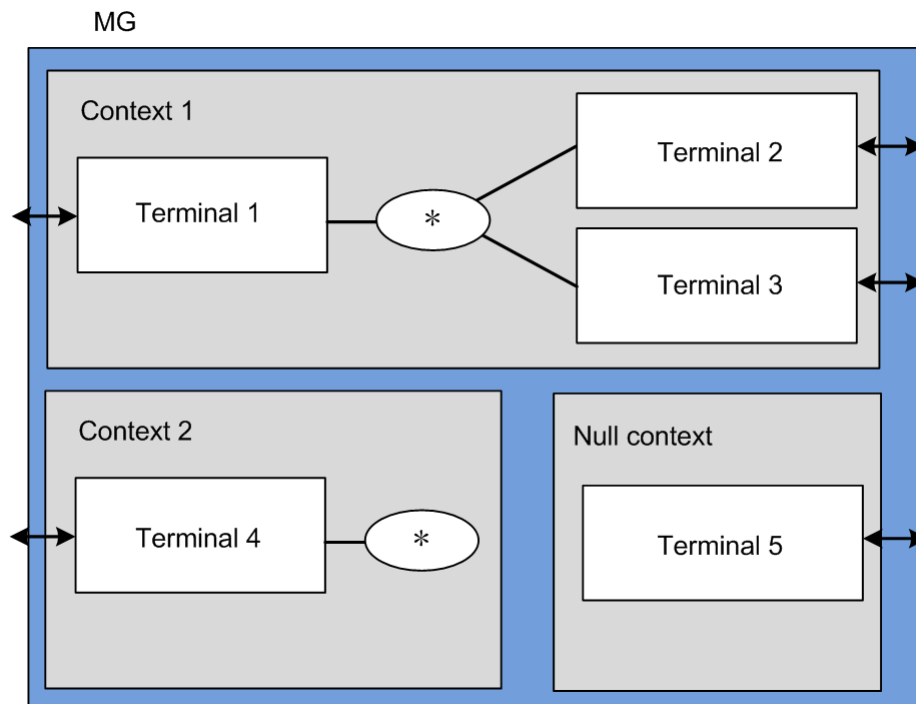
Currently, H.248 packets are transmitted through UDP. When H.248 protocol is adopted, the port number is related with the coding type. By default, port 2933 is used for text-based coding while port 2945 is used for binary coding.

### 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 information. The MGC controls connection objects within MGs. MGs reports various state information about connection objects, such as parameters and capability.

The H.248 connection model contains Terminal and Context, as shown in Figure 4-3.

Figure 4-3 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. A 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.

There is a null context. The null context is the one that 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 processes calls with Indicator for Emergency Call at first.

## 4.2 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.

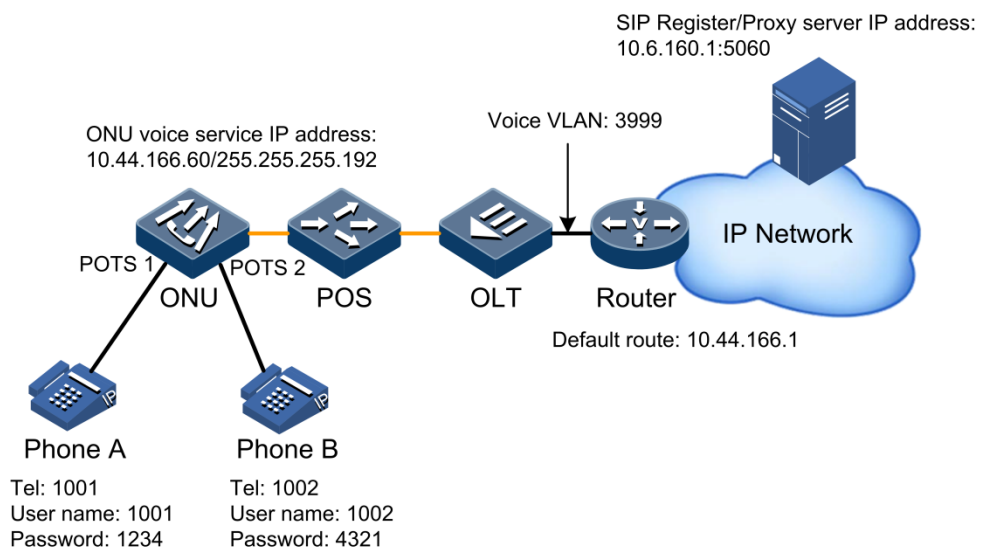
### 4.2.1 Example for configuring SIP voice service (Proxy call)

#### Networking requirements

As shown in Figure 4-4, configure SIP voice service (Proxy call) on the OLT as below:

- See section 4.5 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 4-4 Configuring SIP voice service (Proxy call)



#### Configuration steps

Step 1 Configure the VoIP signalling protocol.

```
Raisecom#config
Raisecom(config)#epon-onu 1/1/1 voice
```

```
Raisecom(config-epon-onu-voice-1/1:1)#voip-protocol sip  
Raisecom(config-epon-onu-voice-1/1:1)#exit  
Raisecom(config)#epon-onu 1/1/1  
Raisecom(config-epon-onu-1/1:1)#write  
Raisecom(config-epon-onu-1/1:1)#reboot  
Raisecom(config-epon-onu-1/1:1)#end
```



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 1/1/1 voice  
Raisecom(config-epon-onu-voice-1/1:1)#vlan mode tagged  
Raisecom(config-epon-onu-voice-1/1:1)#vlan 3999 cos 6
```

Step 3 Configure the IP address for the voice service.

```
Raisecom(config-epon-onu-voice-1/1:1)#ip address 10.44.166.60  
255.255.255.192  
Raisecom(config-epon-onu-voice-1/1:1)#ip route 0.0.0.0 0.0.0.0  
10.44.166.1
```

Step 4 Configure the phone number of POTS.

```
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 1001 1  
Raisecom(config-epon-onu-voice-1/1:1)#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-1/1:1)#sip primary proxy-server ip  
10.6.160.1  
Raisecom(config-epon-onu-voice-1/1:1)#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-1/1:1)#sip pots authentication 1001
password 1234 1
Raisecom(config-epon-onu-voice-1/1:1)#sip pots authentication 1002
password 4321 2
```

## Checking results

Check whether the route between the ONU voice node and soft switch is reachable. 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 0
Raisecom(config-vlanif-0)#ip address 10.44.166.61 255.255.255.192 3999
Raisecom(config-vlanif-0)#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 1/1/1 voice
Raisecom(config-epon-onu-voice-1/1:1)#show epon-onu 1/1/1 voice pots
```

Pots ID	Admin Status	Port Status	Service Status	CodecType
1/1/1/1	enable	registerSucceed	normal	G.711A
1/1/1/2	enable	registerSucceed	normal	G.711A

Show POTS registration information.

```
Raisecom(config-epon-onu-voice-1/1:1)#show epon-onu 1/1/1 voice sip pots
1 service
Port ID: 1/1/1:1
  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 1/1/1 voice sip pots
2 service
Port ID: 1/1/1:2
  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-1/1:1)#show epon-onu 1/1/1 voice ip
ONU ID: 1/1/1
  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 1/1/1 voice sip
primary proxy-server
ONU ID  Proxy IP      UDP Port  TCP Port  Transport
-----
1/1/1   10.6.160.1        5060     5060     udp
Raisecom(config-epon-onu-voice-1/1:1)#show epon-onu 1/1/1 voice sip
primary register-server
ONU ID  Server IP      UDP Port  TCP Port  Transport  Fresh Period(s)
-----
1/1/1   10.6.160.1        5060     5060     udp         3600

```

Show user authentication information.

```

Raisecom(config-epon-onu-voice-1/1:1)#show epon-onu 1/1/1 voice sip pots
authentication
Pots ID  Authentication Name      Authentication Password
-----
1/1/1:1  1001                    1234
1/1/1:2  1002                    4321
1/1/1:3  N/A                      *
1/1/1:4  N/A                      *

```

1/1/1:5	N/A	*
1/1/1:6	N/A	*
1/1/1:7	N/A	*
1/1/1:8	N/A	*
1/1/1:9	N/A	*
1/1/1:10	N/A	*
1/1/1:11	N/A	*
1/1/1:12	N/A	*
1/1/1:13	N/A	*
1/1/1:14	N/A	*
1/1/1:15	N/A	*
1/1/1:16	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.

## 4.2.2 Example for configuring SIP voice service (Direct call)

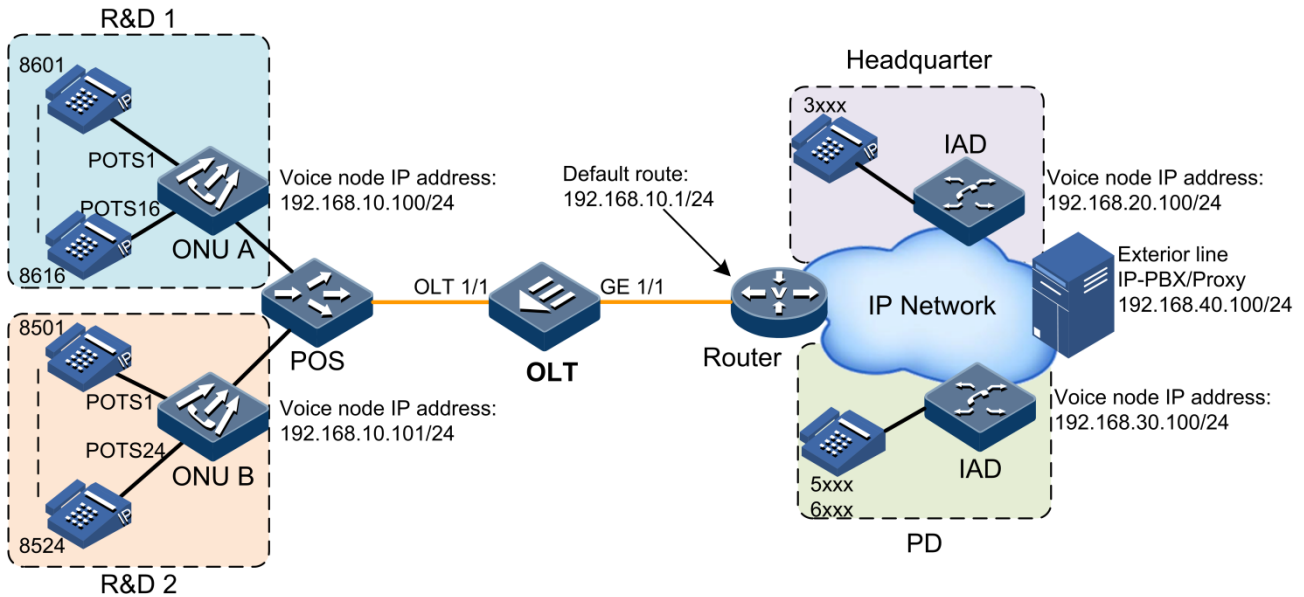
### Networking requirements

As shown in Figure 4-5, 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 can be reachable, 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 4-5 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 1/1/1 voice
Raisecom(config-epon-onu-voice-1/1:1)#voip-protocol sip
Raisecom(config-epon-onu-voice-1/1:1)#exit
Raisecom(config)#epon-onu 1/1/1
Raisecom(config-epon-onu-1/1:1)#write
Raisecom(config-epon-onu-1/1:1)#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 IP address for the voice service.

```
Raisecom#config
Raisecom#epon-onu 1/1/1 voice
Raisecom(config-epon-onu-voice-1/1:1)#ip address 192.168.10.100
Raisecom(config-epon-onu-voice-1/1:1)#ip route 0.0.0.0 0.0.0.0
192.168.10.1
```

Step 3 Configure the POTS phone number.

```
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8601 1
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8602 2
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8603 3
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8604 4
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8605 5
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8606 6
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8607 7
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8608 8
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8609 9
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8610 10
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8611 11
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8612 12
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8613 13
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8614 14
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8615 15
Raisecom(config-epon-onu-voice-1/1:1)#pots phone-number 8616 16
```

Step 4 Configure the mapping rule of SIP phone numbers.

```
Raisecom(config-epon-onu-voice-1/1:1)#sip dial-map-rule 1 86xx
192.168.10.100
Raisecom(config-epon-onu-voice-1/1:1)#sip dial-map-rule 2 85xx
192.168.10.101
Raisecom(config-epon-onu-voice-1/1:1)#sip dial-map-rule 3 3xxx
192.168.20.100
Raisecom(config-epon-onu-voice-1/1:1)#sip dial-map-rule 4 [5-6]xxx
192.168.30.100
Raisecom(config-epon-onu-voice-1/1:1)#sip dial-map-rule 5 0x.#
192.168.40.100
```

## Checking results

Show dialing rule configurations.

```
Raisecom#config
Raisecom(config)#epon-onu 1/1/1 voice
Raisecom(config-epon-onu-voice-1/1:1)#show epon-onu 1/1/1 voice sip dial-
map-rule
ONU ID: 1/1/1
```

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-1/1:1)#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-1/1:1)#end
Raisecom#config
Raisecom(config)#interface vlanif 0
Raisecom(config-vlanif-0)#ip route 0.0.0.0 0.0.0.0 192.168.10.1
Raisecom(config-vlanif-0)#ip address 192.168.10.253 255.255.255.0 1
Raisecom(config-vlanif-0)#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.

### 4.2.3 Example for configuring H.248 voice service

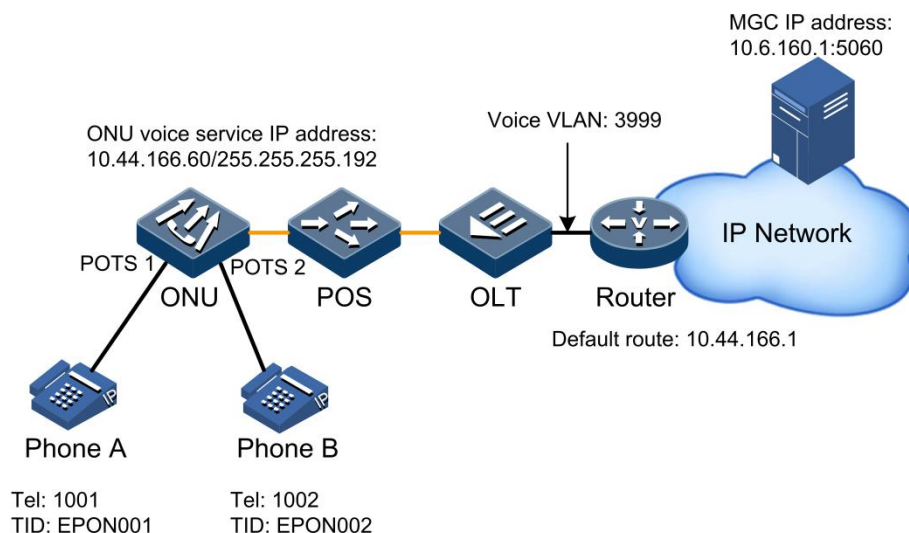
#### Networking requirements

As shown in Figure 4-6, 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 4.6 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	<ul style="list-style-type: none"> <li>• IP address: 10.44.166.60</li> <li>• Mask: 255.255.255.192</li> </ul>
Routing gateway of voice node	10.44.166.1
Voice VLAN and service priority	<ul style="list-style-type: none"> <li>• Voice VLAN: 3999</li> <li>• Service priority: 6</li> </ul>
MG registration mode	domain-name
MG name (which is not needed in IP or MAC registration mode)	raisecom
MG transmission interface ID	2944
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	<ul style="list-style-type: none"> <li>• POTS 1 TID: EPON001</li> <li>• POTS 2 TID: EPON002</li> </ul>
Prefix and digital length of MG RTP TID	<ul style="list-style-type: none"> <li>• Prefix: RTP</li> <li>• Digital length: 5</li> </ul>
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 4-6 Configuring H.248 voice service



## Configuration steps

Step 1 Choose the VoIP signalling protocol type.

```
Raisecom#config
Raisecom(config)#epon-onu 1/1/1 voice
Raisecom(config-epon-onu-voice-1/1:1)#voip-protocol h248
Raisecom(config-epon-onu-voice-1/1:1)#exit
Raisecom(config)#epon-onu 1/1/1
Raisecom(config-epon-onu-1/1:1)#write
Raisecom(config-epon-onu-1/1:1)#reboot
Raisecom(config-epon-onu-1/1:1)#exit
```

## 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 VLAN.

```
Raisecom(config)#epon-onu 1/1/1 voice
Raisecom(config-epon-onu-voice-1/1:1)#vlan mode tagged
Raisecom(config-epon-onu-voice-1/1:1)#vlan 3999 cos 6
```

Step 3 Configure the IP address for the ONU voice service.



```
Raisecom(config-epon-onu-voice-1/1:1)#ip address 10.44.166.60
255.255.255.192
Raisecom(config-epon-onu-voice-1/1:1)#ip route 0.0.0.0 0.0.0.0
10.44.166.1
```

Step 4 Configure MG information.

```
Raisecom(config-epon-onu-voice-1/1:1)#h248 mg register-mode domain-name
Raisecom(config-epon-onu-voice-1/1:1)#h248 mg name raisecom
Raisecom(config-epon-onu-voice-1/1:1)#h248 mg encode text
Raisecom(config-epon-onu-voice-1/1:1)#h248 mg transport port 2944
```

Step 5 Configure POTS TID and RTP TID.

```
Raisecom(config-epon-onu-voice-1/1:1)#h248 mg tid mode line
Raisecom(config-epon-onu-voice-1/1:1)#h248 pots tid name EPON001 1
Raisecom(config-epon-onu-voice-1/1:1)#h248 pots tid name EPON002 2
Raisecom(config-epon-onu-voice-1/1:1)#h248 mg tid rtp prefix RTP length 5
```

Step 6 Configure the MGC server.

```
Raisecom(config-epon-onu-voice-1/1:1)#h248 primary mgc ip 10.6.160.1 port
2944
Raisecom(config-epon-onu-voice-1/1:1)#no h248 primary mgc authentication
```

Step 7 Save configurations.

```
Raisecom(config-epon-onu-voice-1/1:1)#exit
Raisecom(config)#epon-onu 1/1/1
Raisecom(config-epon-onu-1/1:1)#write
```

## Checking results

Check whether the route between the ONU voice node and the MGC is reachable. 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 0
Raisecom(config-vlanif-0)#ip address 10.44.166.61 255.255.255.192 3999
Raisecom(config-vlanif-0)#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 1/1/1 voice
Raisecom(config-epon-onu-voice-1/1:1)#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-1/1:1)#show epon-onu 1/1/1 voice h248 pots
Pots ID      TID Name      Status
-----
1/1/1/1      EPON001      inservice
1/1/1/2      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.

## 4.3 Configuring VoIP

### 4.3.1 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

### 4.3.2 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	<ul style="list-style-type: none"><li>• IP address: 0.0.0.0</li><li>• Mask: 0.0.0.0</li></ul>
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

### 4.3.3 Configuring VoIP protocol type

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/:*)#voip-protocol { sip   h248 }</b>	Configure the VoIP protocol type.



#### 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.


### 4.3.4 Configuring network parameters of signalling traffic

#### Basic configurations

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/:*)#ip address ip-address [ mask ]</b>	Configure the IP address and mask for the ONU voice service.
4	<b>Raisecom(config-epon-onu-voice-*/:*)#ip route 0.0.0.0 0.0.0.0 ip-address</b>	Configure the default route for the ONU voice service.
5	<b>Raisecom(config-epon-onu-voice-*/:*)#ip dhcp client</b>	(Optional) enable DHCP Client of ONU voice service. You can use the <b>no ip dhcp client</b> command to disable this function.
6	<b>Raisecom(config-epon-onu-voice-*/:*)#ip dhcp client hostname string</b>	(Optional) configure the DHCP Client host name of ONU voice service. You can use the <b>no ip dhcp client hostname</b> command to restore default configurations.
7	<b>Raisecom(config-epon-onu-voice-*/:*)#voip register</b>	(Optional) configure the ONU to register to the soft switch system.
8	<b>Raisecom(config-epon-onu-voice-*/:*)#voip deregister</b>	(Optional) configure the ONU to deregister to the soft switch system.

Step	Command	Description
9	Raisecom(config-epon-onu-voice-*/*:*)# <b>voip reset</b>	(Optional) reset the ONU voice module.


## Other configurations

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	Raisecom(config-epon-onu-voice-*/*:*)# <b>vlan mode { transparent   tagged   stacking }</b>	Configure the VLAN mode for the ONU voice service.
4	Raisecom(config-epon-onu-voice-*/*:*)# <b>vlan vlan-id [ cos cos-value ]</b>	<p>Configure the VLAN ID and CoS priority of the ONU voice signalling traffic.</p> <p>You can use the <b>no vlan</b> command to restore default configurations.</p> <div>  <b>Note</b> </div> <p>The voice service is sensitive to delay. We recommend you to configure a higher priority for the voice service to make sure that voice packets can be scheduled preferentially.</p>
5	Raisecom(config-epon-onu-voice-*/*:*)# <b>ip dhcp client class-id class-id</b>	<p>(Optional) configure the class ID of DHCP Client for the ONU voice service.</p> <p>You can use the <b>no ip dhcp client class-id</b> command to restore default configurations.</p>
6	Raisecom(config-epon-onu-voice-*/*:*)# <b>ip dhcp client client-id client-id</b>	<p>(Optional) configure the client ID of DHCP Client for the ONU voice service.</p> <p>You can use the <b>no ip dhcp client client-id</b> command to restore default configurations.</p>
7	Raisecom(config-epon-onu-voice-*/*:*)# <b>ip qos trust { dscp   priority   tos   none }</b>	(Optional) configure the QoS trust mode for the ONU voice service.
8	Raisecom(config-epon-onu-voice-*/*:*)# <b>ip qos default-dscp dscp-value</b>	(Optional) configure the QoS trusted DSCP value for the ONU voice service.
9	Raisecom(config-epon-onu-voice-*/*:*)# <b>ip qos default-priority priority-value</b>	(Optional) configure the QoS trusted IP precedence for the ONU voice service.
10	Raisecom(config-epon-onu-voice-*/*:*)# <b>ip qos default-tos tos-value</b>	(Optional) configure the QoS trusted ToS value for the ONU voice service.

Step	Command	Description
11	<code>Raisecom(config-epon-onu-voice-*/*:*)#pppoe mode { auto   chap   pap }</code>	(Optional) configure the PPPoE mode of ONU voice service. You can use the <b>no pppoe mode</b> command to restore default configurations.
12	<code>Raisecom(config-epon-onu-voice-*/*:*)#pppoe username username</code>	(Optional) configure the user name of PPPoE. You can use the <b>no pppoe username</b> command to restore default configurations.
13	<code>Raisecom(config-epon-onu-voice-*/*:*)#pppoe password password</code>	(Optional) configure the password of PPPoE. You can use the <b>no pppoe password</b> command to restore default configurations.

### 4.3.5 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 different network parameters for the signalling and media traffic.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</code>	Enter EPON ONU voice service configuration mode.
3	<code>Raisecom(config-epon-onu-voice-*/*:*)#media vlan vlan-id [ cos cos-value ]</code>	Configure the VLAN ID and CoS priority of the ONU voice service media traffic. You can use the <b>no media vlan</b> command to restore default configurations.  <div style="display: flex; align-items: center;">  <div> <b>Note</b> <ul style="list-style-type: none"> <li>Media traffic VLAN is inconsistent with the signalling traffic VLAN.</li> <li>When configuring network parameters of media traffic, you need to configure the VLAN before configuring the IP address.</li> </ul> </div> </div>
4	<code>Raisecom(config-epon-onu-voice-*/*:*)#media ip address ip-address [ mask ]</code>	Configure the IP address and mask of the ONU voice service media traffic. You can use the <b>no media ip address</b> command to restore default configurations.
5	<code>Raisecom(config-epon-onu-voice-*/*:*)#media ip route default ip-address</code>	Configure the default route of the ONU voice service media traffic. You can use the <b>no media ip route default</b> command to restore default configurations.
6	<code>Raisecom(config-epon-onu-voice-*/*:*)#media ip qos trust { dscp   priority   tos   none }</code>	Configure the QoS trust mode of the ONU voice service media traffic.

Step	Command	Description
7	<code>Raisecom(config-epon-onu-voice-*/*:*)#media ip qos default-dscp dscp-value</code>	Configure the QoS trusted DSCP value of the ONU voice service media traffic.
8	<code>Raisecom(config-epon-onu-voice-*/*:*)#media ip qos default-priority priority-value</code>	Configure the QoS trusted IP precedence of the ONU voice service media traffic.
9	<code>Raisecom(config-epon-onu-voice-*/*:*)#media ip qos default-tos tos-value</code>	Configure the QoS trusted ToS priority of the ONU voice service media traffic.

### 4.3.6 Checking configurations

No.	Command	Description
1	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice voip-protocol</code>	Show ONU VoIP protocol type.
2	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice ip</code>	Show configurations of ONU VoIP network parameters.
3	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice ip dhcp client</code>	Show configurations of DHCP Client for the ONU voice service.
4	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice media ip</code>	Show configurations of network parameters for ONU voice service media traffic.
5	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id voice pppoe</code>	Show ONU PPPoE configurations.
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 transmission information used by ONU second dialing.
10	<code>Raisecom#show epon-onu slot-id/olt-id/onu-list voice voip-protocol</code>	Show the voice protocol used by the ONU.

## 4.4 Configuring POTS interface

### 4.4.1 Preparing for configurations

#### Scenario

POTS is 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 by user planning.

### 4.4.2 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
Echo cancellation feature of ONU POTS interface	Enable
Silence compression feature of ONU POTS interface	Diable
Comfort noise feature of ONU POTS interface	Enable
Preferred coding/decoding type of ONU line	G711A


### 4.4.3 Configuring interface properties

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.



Step	Command	Description
3	<code>Raisecom(config-epon-onu-voice-*/*:*)#pots { enable   disable } pots-list</code>	<p>Enable/Disable the POTS interface.</p> <p> <b>Note</b></p> <p>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.</p>
4	<code>Raisecom(config-epon-onu-voice-*/*:*)#pots name string pots-id</code>	<p>(Optional) configure the user name of the ONU POTS interface.</p> <p>You can use the <b>no pots name</b> command to restore default configurations.</p>

#### 4.4.4 Configuring phone number

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</code>	Enter EPON ONU voice service configuration mode.
3	<code>Raisecom(config-epon-onu-voice-*/*:*)#pots phone-number number pots-id</code>	<p>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.</p> <p>You can use the <b>no pots phone-number</b> command to restore default configurations.</p> <p> <b>Note</b></p> <p>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.</p>

#### 4.4.5 Configuring other functions

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</code>	Enter EPON ONU voice service configuration mode.
3	<code>Raisecom(config-epon-onu-voice-*/*:*)#pots echo-cancellation { enable   disable } pots-list</code>	(Optional) enable/disable the echo cancellation feature of the POTS interface.
4	<code>Raisecom(config-epon-onu-voice-*/*:*)#pots silence-compression { enable   disable } pots-list</code>	(Optional) enable/disable the silence compression feature of the POTS interface.

Step	Command	Description
5	Raisecom(config-epon-onu-voice-*/*:*)# <b>pots cng { enable   disable } pots-list</b>	(Optional) enable/disable the comfort noise feature of the POTS interface.
6	Raisecom(config-epon-onu-voice-*/*:*)# <b>pots prefer-codec { g711a   g729   g711u   g723   g726 } pots-list</b>	(Optional) configure the preferred coding/decoding type of the ONU line. You can use the <b>no pots prefer-codec</b> command to restore default configurations.
7	Raisecom(config-epon-onu-voice-*/*:*)# <b>pots caller-id mode { bellcore   etsi   ntt } pots-list</b>	(Optional) configure the encapsulation mode of CID packets for ONU call services.
8	Raisecom(config-epon-onu-voice-*/*:*)# <b>pots circuit-test pots-id</b>	(Optional) configure performing circuit test on the POTS interface.
9	Raisecom(config-epon-onu-voice-*/*:*)# <b>pots loop-line-test pots-id</b>	(Optional) configure performing loop test on the POTS interface.

## 4.4.6 Checking configurations

No.	Command	Description
1	Raisecom# <b>show epon-onu slot-id/olt-id/onu-id voice pots [ pots-id ]</b>	Show the management status of the ONU POTS interface.
2	Raisecom# <b>show epon-onu slot-id/olt-id/onu-id voice statistics call pots [ pots-id ]</b>	Show call statistics of the ONU POTS interface.
3	Raisecom# <b>show epon-onu slot-id/olt-id/onu-list voice pots [ pots-id ] service</b>	Show feature information about the ONU POTS interface.
4	Raisecom# <b>show epon-onu slot-id/olt-id/onu-list voice pots [ pots-id ] session</b>	Show the session status of the ONU POTS interface.

## 4.5 Configuring SIP

### 4.5.1 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

### 4.5.2 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	3600s
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	60s

Function	Default value
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
Call waiting service	disable
Three-way calling	disable
SIP Modem transparent transmission service	enable
Polarity reversal service	enable
Hotline service	disable
Mapping rule SIP phone numbers	min

### 4.5.3 Configuring basic functions of SIP

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip transport { udp   tcp } port port-number</b>	Configure the monitor port of SIP. You can use the <b>no sip transport { udp   tcp } port</b> command to restore default configurations.
4	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip transport tcp { enable   disable }</b>	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.

## 4.5.4 Configuring SIP Proxy/Register server

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip { primary   secondary } proxy-server ip ip-address [ { udp   tcp } port port-number ]</b>	Configure the IP address and monitor port of the primary/secondary SIP Proxy server. You can use the <b>no sip { primary   secondary } proxy-server ip</b> command to delete the configuration.
4	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip { primary   secondary } proxy-server transport { udp   tcp }</b>	Configure the transmission protocol type of the primary/secondary SIP Proxy server. You can use the <b>no sip { primary   secondary } proxy-server transport</b> command to restore default configurations.
5	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip { primary   secondary } register-server ip ip-address [ { udp   tcp } port port-number ]</b>	Configure the IP address and monitor port of the primary/secondary SIP Register server. You can use the <b>no sip { primary   secondary } register-server ip</b> command to restore default configurations.
6	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip { primary   secondary } register-server transport { udp   tcp }</b>	Configure the transmission protocol type of the primary/secondary SIP Register server. You can use the <b>sip { primary   secondary } register-server transport</b> command to restore default configurations.
7	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip proxy-swap { enable   disable }</b>	Enable/Disable SIP primary/secondary proxy swap.
8	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip register fresh-period period</b>	Configure the refresh interval for the ONU to send registration packets to the SIP Register server. You can use the <b>no sip register fresh-period</b> command to restore default configurations.
9	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip realm string</b>	Configure the SIP domain name, which works with the out-bond Proxy server. You can use the <b>no sip realm</b> command to restore default configurations.
10	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip outbound proxy-server ip ip-address [ udp port port-number ]</b>	Configure the IP address and monitor port of the Outbound Proxy server. You can use the <b>no sip outbound proxy-server ip</b> command to restore default configurations.
11	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip uri [ phonenumber   username ]</b>	Configure the information type of URI in the FROM header when performing SIP registration or calling. You can use the <b>no sip uri</b> command to restore default configurations.



## 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 ISCOM5508 should adopt TCP.

## 4.5.5 Configuring SIP heartbeat

To detect whether the ONU is connected with the SIP Proxy/Register server properly, the server sends SIP information to the ONU regularly or the ONU sends information to server regularly. The information is called "heartbeat information".

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/:*)#sip heartbeat { on   off }</b>	Enable/Disable SIP heartbeat.
4	<b>Raisecom(config-epon-onu-voice-*/:*)#sip heartbeat mode { send-option   receive-option   send-info   receive-info }</b>	(Optional) configure the detection mode of SIP heartbeat. You can use the <b>no sip heartbeat mode</b> command to restore default configurations.
5	<b>Raisecom(config-epon-onu-voice-*/:*)#sip heartbeat cycle period</b>	(Optional) configure the SIP heartbeat cycle. You can use the <b>no sip heartbeat cycle</b> command to restore default configurations.
6	<b>Raisecom(config-epon-onu-voice-*/:*)#sip heartbeat timeout count number</b>	(Optional) configure timeout times of SIP heartbeat. You can use the <b>no sip heartbeat timeout</b> command to restore default configurations.



## Note

- We recommended that the heartbeat cycle should be no less than 60s; otherwise, it brings extra burden to 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 detection feature of the device.

## 4.5.6 Configuring SIP user authentication

To avoid illegal user access, the ONU should be registered successfully on the SIP Proxy/Register server before it accesses the network. The ONU with the voice function supports two registration modes: authentication based on user name and authentication based on user name+password.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip pots authentication name [ password password ] pots-list</b>	Configure SIP user authentication information. You can use the <b>no sip pots authentication { all   pots-list }</b> command to delete the configuration.

## 4.5.7 Configuring CID

CID refers to displaying the number of the caller when the phone of the called party rings.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip pots caller-id { enable   disable } pots-list</b>	Enable/Disable CID.

## 4.5.8 Configuring call waiting

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	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip pots call-wait { enable   disable } pots-list</b>	Enable/Disable call waiting.



### 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.

## 4.5.9 Configuring three-way calling

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	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/:*)#sip pots 3-way-conference { enable   disable } pots-list</b>	Enable/Disable three-way calling.



### 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.

## 4.5.10 Configuring Modem transparent transmission

Modem transparent transmission refers that traditional Modem data services are transmitted through the IP network.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/:*)#sip modem { enable   disable }</b>	Enable/Disable SIP Modem transparent transmission.  <div data-bbox="746 1252 831 1339" data-label="Image"> </div> <div data-bbox="831 1285 938 1328" data-label="Section-Header"> <h3>Note</h3> </div> <p>When Modem transparent transmission is enabled, traditional Modem data services can be transmitted through the IP network</p>
4	<b>Raisecom(config-epon-onu-voice-*/:*)#modem transparent redundancy value</b>	(Optional) configure the redundancy for the ONU to transparently transmit Modem services.  You can use the <b>no modem transparent redundancy</b> command to restore default configurations.

## 4.5.11 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	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip pots polarity-reverse { enable   disable } pots-list</b>	Enable/Disable polarity reversal.

### 4.5.12 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	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip pots hot-line { disable   instant   delay } pots-list</b>	Configure the hotline service. You can use the <b>no sip pots hot-line { all   pots-list }</b> command to restore default configurations.
4	<b>Raisecom(config-epon-onu-voice-*/*:*)#sip pots hot-line phone-number number pots-id</b>	Configure the hotline phone number. You can use the <b>no sip pots hot-line phone-number { all   pots-list }</b> command to restore default configurations.

### 4.5.13 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	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.

Step	Command	Description
3	<code>Raisecom(config-epon-onu-voice-*/*:*)#digitmap match-mode { min   max }</code>	Configure the matching mode of the ONU digitmap. You can use the <b>no digitmap match-mode</b> command to restore default configurations.
4	<code>Raisecom(config-epon-onu-voice-*/*:*)#sip digitmap digitmap</code>	Configure the SIP digitmap. You can use the <b>no sip digitmap</b> command to delete the digitmap.



## 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 any 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.

## 4.5.14 Configuring user deregistration and re-registration

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*//*:*)#sip pots { register   deregister } pots-list</b>	<p>Deregister a user or register a user.</p> <div>  <b>Note</b> </div> <p>Both operations are mainly used for testing. You can use the <b>deregister</b> command to delete registration information about a telephone user on the Register server; you can use the <b>register</b> command to make the telephone user to initiate a new registration.</p>

## 4.5.15 Checking configurations

No.	Command	Description
1	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip transport</b>	Show information about the ONU SIP transmission protocol.
2	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip { primary   secondary } proxy-server</b>	Show configurations of the ONU SIP primary/secondary SIP Proxy server.
3	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip { primary   secondary } register-server</b>	Show configurations of the ONU SIP primary/secondary SIP Register server.
4	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip active proxy-server</b>	Show the type of the active ONU SIP server.
5	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip proxy-swap</b>	Show configurations of ONU SIP proxy swap.
6	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip realm</b>	Show information about ONU SIP domain names.
7	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip outbound proxy-server</b>	Show configurations of the ONU Outbound Proxy server.
8	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip pot service</b>	Show the SIP service information on the ONU POTS interface.
9	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip heartbeat</b>	Show SIP heartbeat configurations on the ONU POTS interface.
10	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip pots authentication</b>	Show user authentication information on the ONU POTS interface.
11	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice pots service</b>	Show feature information about the ONU POTS interface.

No.	Command	Description
12	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip dial-map-rule</b>	Show information about the ONU SIP phone number mapping rules.
13	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice modem</b>	Show ONU Modem information.
14	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip modem</b>	Show ONU SIP Modem status.
15	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip uri</b>	Show the information type of URI in the FROM header when performing SIP registration or calling.
16	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice digitmap</b>	Show matching information about the ONU digitmap.
17	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice sip digitmap</b>	Show the SIP digitmap.
18	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice statistics call pots [ pots-id ]</b>	Show calling statistics on the ONU POTS interface.
19	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice statistics sip</b>	Show ONU SIP performance statistics.

## 4.6 Configuring H.248

### 4.6.1 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

### 4.6.2 Default configurations

Default configurations of the H.248 protocol are as below.

Function	Default value
Authentication 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

Function	Default value
Transmission 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 number 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	<ul style="list-style-type: none"> <li>• g: 2</li> <li>• p: null</li> <li>• ki: null</li> </ul>
MGC initial retransmission timeout	2000ms
MGC minimum retransmission timeout	100ms
MGC maximum retransmission timeout	4000ms
Deregistration delay of H.248 POTS interface	60s
TID of H.248 POTS interface	null

### 4.6.3 Configuring basic functions of H.248

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.

Step	Command	Description
3	Raisecom(config-epon-onu-voice-*/*:*)# <b>h248 mg forced-deregister</b>	(Optional) forcedly deregister the MG.
4	Raisecom(config-epon-onu-voice-*/*:*)# <b>h248 mg register</b>	(Optional) register the MG.
5	Raisecom(config-epon-onu-voice-*/*:*)# <b>h248 mg delay-deregister</b> <i>delay-time</i>	(Optional) deregister the MG after a delay.
6	Raisecom(config-epon-onu-voice-*/*:*)# <b>h248 pots forced-deregister</b> <i>pots-list</i>	(Optional) forcedly deregister the endpoint.
7	Raisecom(config-epon-onu-voice-*/*:*)# <b>h248 pots register</b> <i>pots-list</i>	(Optional) register the endpoint.
8	Raisecom(config-epon-onu-voice-*/*:*)# <b>h248 pots delay-deregister</b> <i>delay-time pots-list</i>	(Optional) deregister the endpoint after a delay.

#### 4.6.4 Configuring H.248 authentication

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	Raisecom(config-epon-onu-voice-*/*:*)# <b>h248 create authentication</b> <i>auth-id type { national   hw   zte }</i>	Configure the MGC type in H.248 authentication. You can use the <b>no h248 create authentication</b> { <i>auth-id</i>   <b>all</b> } to delete the configuration.
4	Raisecom(config-epon-onu-voice-*/*:*)# <b>h248 create authentication</b> <i>auth-id [ g g ] [ p p ] [ ki ki ] [ mginfo mg-info ]</i>	Configure H.248 authentication parameters. You can use the <b>no h248 create authentication</b> { <i>auth-id</i>   <b>all</b> } to delete the configuration.
5	Raisecom(config-epon-onu-voice-*/*:*)# <b>h248 authentication auth-id</b> <i>type { national   hw   zte }</i>	(Optional) modify the MGC type in H.248 authentication.
6	Raisecom(config-epon-onu-voice-*/*:*)# <b>h248 authentication auth-id</b> <i>[ g g ] [ p p ] [ ki ki ] [ mginfo mg-info ]</i>	(Optional) modify H.248 authentication parameters.





#### Caution

When the ISCOM5508 is connected with the MGC, configure authentication information about the voice gateway if the MGC requires.

#### 4.6.5 Configuring MG

MG is a H.248 media gateway unit. All ONUs with the voice function can be MG objects.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg name name</b>	(Optional) configure the MG name.   <b>Note</b> 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.
4	<b>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg register-mode { ip   domain-name   device-name   mac   mid }</b>	(Optional) configure MG authentication mode. You can use the <b>no h248 mg register-mode</b> command to restore default configurations.   <b>Note</b> If the central office specifies the MG authentication mode, you need to configure this item; otherwise, you do not.
5	<b>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg max-waiting-delay time</b>	(Optional) configure the maximum waiting delay. You can use the <b>no h248 mg max-waiting-delay</b> command to restore default configurations.
6	<b>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg transport port port-number</b>	(Optional) configure the transmission interface ID of the MG. You can use the <b>no h248 mg transport port</b> command to restore default configurations.
7	<b>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg encode { text   compact-text   bin }</b>	(Optional) configure the coding type of H.248 signalling. You can use the <b>no h248 mg encode</b> command to restore default configurations.
8	<b>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg encryption { password password   authentication }</b>	(Optional) configure the encryption mode of H.248 MG signalling.




## 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.

## 4.6.6 Configuring MGC

MGC is a H.248 media gateway control unit. MGC is usually used in softswitch network.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/:*)#h248 { primary   secondary } mgc ip ip-address [ port port-number ]</b>	Configure the IP address and transmission interface ID of the primary/secondary MGC server. You can use the <b>no h248 { primary   secondary } mgc ip</b> command to restore default configurations.
4	<b>Raisecom(config-epon-onu-voice-*/:*)#h248 { primary   secondary } mgc name string</b>	(Optional) configure the name of the primary/secondary MGC server. You can use the <b>no h248 { primary   secondary } mgc name</b> command to restore default configurations.   <b>Note</b> Names of the primary and secondary MGC servers should be different.
5	<b>Raisecom(config-epon-onu-voice-*/:*)#h248 { primary   secondary } mgc authentication auth-id</b>	(Optional) configure authentication information about the primary/secondary MGC server. You can use the <b>no h248 { primary   secondary } mgc authentication</b> command to delete the configuration.
6	<b>Raisecom(config-epon-onu-voice-*/:*)#h248 mgc-swap { enable   disable }</b>	(Optional) enable/disable ONU primary/secondary MGC server swap.
7	<b>Raisecom(config-epon-onu-voice-*/:*)#h248 mgc { initial   max   min } timeout time</b>	(Optional) configure the H.248 MGC initial retransmission timeout. You can use the <b>h248 mgc { initial   max   min } timeout</b> command to restore default configurations.



### 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.

## 4.6.7 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.



## Configuring POTS TID


Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/:*)#h248 mg tid mode { auto   line   multilayer }</b>	Configure the generation mode of POTS TID. You can use the <b>no h248 mg tid mode</b> command to restore default configurations.
3	<b>Raisecom(config-epon-onu-voice-*/:*)#h248 mg tid prefix prefix name name</b>	(Optional) configure the prefix and name of the POTS TID. You can use the <b>no h248 mg tid prefix</b> command to restore default configurations.   <b>Note</b> If the POTS TID mode is auto, you need to configure this item; otherwise, you do not.
4	<b>Raisecom(config-epon-onu-voice-*/:*)#h248 pots tid name name pots-id</b>	(Optional) configure the TID on the POTS interface. You can use the <b>no h248 pots tid name { all   pots-list }</b> command to restore default configurations.



### Note

- The user interface unused does not need to be configured with TID.
- Values of TID for different user interfaces should be different.

## Configuring RTP TID

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/:*)#h248 mg tid rtp mode { align   unalign }</b>	Configure the RTP TID mode. You can use the <b>no h248 mg tid rtp number</b> command to restore default configurations.
4	<b>Raisecom(config-epon-onu-voice-*/:*)#h248 mg tid rtp prefix prefix length length</b>	(Optional) configure the prefix and digital length of the RTP TID. You can use the <b>no h248 mg tid rtp prefix</b> command to restore default configurations.   <b>Note</b> If the central office provides a RTP name which is different from the default value, you need to configure this item; otherwise you do not.

Step	Command	Description
5	<code>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg tid rtp begin value</code>	(Optional) configure the start value of the digital part of RTP TID. You can use the <b>no h248 mg tid rtp begin</b> command to restore default configurations.
6	<code>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg tid rtp number value</code>	(Optional) configure the RTP TID. You can use the <b>no h248 mg tid rtp number</b> command to restore default configurations.



### 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 interface number.

## 4.6.8 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</code>	Enter EPON ONU voice service configuration mode.
3	<code>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg heartbeat mode { disable   svc   ito   audit }</code>	Configure the MG heartbeat mode. You can use the <b>no h248 mg heartbeat mode</b> command to restore default configurations.
4	<code>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg heartbeat cycle period</code>	(Optional) configure the MG heartbeat cycle. You can use the <b>no h248 mg heartbeat cycle</b> command to restore default configurations.
5	<code>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg heartbeat timeout count number</code>	(Optional) configure timeout times of MG fault judgement. You can use the <b>no h248 mg heartbeat timeout count</b> command to restore default configurations.



### Note

- We recommended that timeout of MG heartbeat should be 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.

## 4.6.9 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	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/*:*)#h248 digitmap dm-id name string</b>	Configure the H.248 digitmap.
4	<b>Raisecom(config-epon-onu-voice-*/*:*)#digitmap match-mode { min   max }</b>	Configure the digitmap matching mode. You can use the <b>no digitmap match-mode</b> command to restore default configurations.
5	<b>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg digitmap long-timer longtime</b>	Configure the long timer used in ONU H.248 MG digitmap. You can use the <b>no h248 mg digitmap long-timer</b> command to restore default configurations.
6	<b>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg digitmap short-timer shorttime</b>	Configure the short timer used in ONU H.248 MG digitmap. You can use the <b>no h248 mg digitmap short-timer</b> command to restore default configurations.
7	<b>Raisecom(config-epon-onu-voice-*/*:*)#h248 mg digitmap start-timer starttime</b>	Configure the start timer used in ONU H.248 MG digitmap. You can use the <b>no h248 mg digitmap start-timer</b> command to restore default configurations.



### Caution

In general, you do not need to configure the digitmap. The MG uses the digitmap distributed by the MGC preferentially.

## 4.6.10 Checking configurations

No.	Command	Description
1	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 mg</b>	Show parameters of H.248 voice gateway.
2	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 mg heartbeat</b>	Show heartbeat information about the voice gateway.
3	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 pots [ pots-id ]</b>	Show POTS TID.

No.	Command	Description
4	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 mgc</b>	Show configurations of H.248 MGC on the ONU.
5	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 { primary   secondary } mgc</b>	Show configurations of the H.248 primary/secondary MGC server on the ONU.
6	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 mgc-swap</b>	Show information about ONU primary/secondary MGC server swap.
7	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 digitmap [ dm-id ]</b>	Show H.248 digitmap.
8	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 authentication</b>	Show ONU H.248 authentication information.
9	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 mg encryption</b>	Show configurations of ONU H.248 MG signalling encryption.
10	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice statistics h248</b>	Show ONU H.248 performance statistics.
11	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice h248 mg tid</b>	Show configurations of the MG TID on the ONU.
12	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id voice statistics rtp pots [ pots-id ]</b>	Show configurations of the ONU POTS ID on the ONU.

## 4.7 Configuring second dialing

### 4.7.1 Preparing for configurations

#### Scenario

Second dialing refers to dialing again after being put through, such as dialing an extension or entering the card password.

Second dialing supports transmitting dialing 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 dialing should be consistent with that of the connected device.

## 4.7.2 Default configurations

Default configurations of second dialing are as below.

Function	Default value
Transmission mode of second dialing	transparent

## 4.7.3 Configuring second dialing

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/*:*)#dtmf { rfc2833-relay   rfc2833-redundancy   sip-info   transparent }</b>	Configure the transmission mode for ONU second dialing. You can use the <b>no dtmf</b> command to restore default configurations.
4	<b>Raisecom(config-epon-onu-voice-*/*:*)#dtmf volume volume</b>	(Optional) configure DTMF volume. You can use the <b>no dtmf volume</b> command to restore default configurations.
5	<b>Raisecom(config-epon-onu-voice-*/*:*)#dtmf payload-type type</b>	(Optional) configure DTMF payload type. You can use the <b>dtmf payload-type</b> command to restore default configurations.

## 4.7.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list voice dtmf</b>	Show transmission information used by ONU second dialing.

## 4.8 Configuring fax

### 4.8.1 Preparing for configurations

#### Scenario

The voice 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

## 4.8.2 Default configurations

Default configurations of the fax service on the ONU are as below.

Function	Default value
Transmission mode of fax	transparent
T.38 fax error correction mode	redundancy
T.38 fax rate on POTS interface	14400 bit/s

## 4.8.3 Configuring fax

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*/:*)#fax transport { transparent   t38 }</b>	Configure the transmission mode of fax. You can use the <b>no fax transport</b> command to restore default configurations.
4	<b>Raisecom(config-epon-onu-voice-*/:*)#fax control mode { negotiation   auto-vbd }</b>	Configure the fax control mode of the ONU. You can use the <b>no fax control-mode</b> command to restore default configurations.
5	<b>Raisecom(config-epon-onu-voice-*/:*)#fax error-correction-mode { redundancy   fec }</b>	Configure T.38 fax error correction mode of the ONU. You can use the <b>no fax error-correction-mode</b> command to restore default configurations.
6	<b>Raisecom(config-epon-onu-voice-*/:*)#pots fax relay rate { 2400   4800   7200   9600   12000   144000 } pots-list</b>	Configure the T.38 fax rate on the POTS interface. You can use the <b>no pots fax relay rate { all   pots-list }</b> command to restore default configurations.
7	<b>Raisecom(config-epon-onu-voice-*/:*)#fax t38 data redundancy value</b>	(Optional) configure T.38 data redundancy. You can use the <b>no fax t38 data redundancy</b> command to restore default configurations.

Step	Command	Description
8	Raisecom(config-epon-onu-voice-*/*:*)# <b>fax t38 signal redundancy</b> <i>value</i>	(Optional) configure T.38 signalling redundancy. You can use the <b>no fax t38 signal redundancy</b> command to restore default configurations.
9	Raisecom(config-epon-onu-voice-*/*:*)# <b>fax transparent redundancy</b> <i>value</i>	(Optional) configure transparent transmission redundancy. You can use the <b>no transparent redundancy</b> command to restore default configurations.

## 4.8.4 Checking configurations

No.	Command	Description
1	Raisecom# <b>show epon-onu slot-id/olt-id/onu-id voice fax</b>	Show ONU fax configurations.
2	Raisecom# <b>show epon-onu slot-id/olt-id/onu-id voice pots [ pots-id ] fax</b>	Show ONU POTS fax service information.

## 4.9 Configuring call process tone

### 4.9.1 Preparing for configurations

#### Scenario

Call process tone includes the dial tone, ringback tone, busy tone, congestion tone, and call waiting tone when you dial up or answer the phone.

Customized voice requirements can be met through configuring the gain and start time of the call process tone.

#### Prerequisite

N/A

### 4.9.2 Default configurations

Default configurations of the call process tone are as below.

Function	Default value
Low frequency	450 Hz
High frequency	0 Hz
Low-frequency volume	40 dB
High-frequency volume	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

### 4.9.3 Configuring call process tone

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*//*:*)#call-progress-tone { busy   congestion   dial   ringback   waiting } { high-frequency   low-frequency } frequency</b>	Configure the low frequency and high frequency of the ONU call process tone.
4	<b>Raisecom(config-epon-onu-voice-*//*:*)#call-progress-tone { busy   congestion   dial   ringback   waiting } { high-frequency   low-frequency } volume volume</b>	Configure the volume gain of the low frequency and high frequency for the ONU.
5	<b>Raisecom(config-epon-onu-voice-*//*:*)#call-progress-tone { busy   congestion   dial   ringback   waiting } { first-signal   second-signal } on-time value off-time value</b>	Configure the start time and end time of the first ring and second ring of the ONU call process tone.



#### Note

After modifying parameters of the call process tone, you need to save the configurations and reboot the ONU to make new configurations take effect.

### 4.9.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list voice call-progress-tone [ dial   ringback   busy   congestion   waiting ] information</b>	Show parameters of the call process tone. Parameters of all types of process tone will be shown if you do not specify the type.



## 4.10 Configuring call emulation test

### 4.10.1 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

### 4.10.2 Default configurations

N/A

### 4.10.3 Configuring call emulation test

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id voice</b>	Enter EPON ONU voice service configuration mode.
3	<b>Raisecom(config-epon-onu-voice-*//*:*)#pots call-test start pots-id caller [ timeout timeout ] media { tone   loopback } phone-number number</b>	Start the outgoing call emulation test.
4	<b>Raisecom(config-epon-onu-voice-*//*:*)#pots call-test start pots-id callee [ timeout timeout ] media { tone   loopback }</b>	Start the incoming call emulation test.
5	<b>Raisecom(config-epon-onu-voice-*//*:*)#pots call-test stop pots-id</b>	End the call emulation test.
6	<b>Raisecom(config-epon-onu-voice-*//*:*)#pots call-test query { all   pots-list }</b>	Query the call emulation test.



#### Note

When the 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.

## 4.10.4 Checking configurations

N/A

## 4.11 Maintenance

Command	Description
<b>Raisecom(config-epon-onu-voice-*//*:*)#clear epon-onu slot-id/olt-id/onu-idvoice statistics sip</b>	Clear ONU SIP packet statistics.
<b>Raisecom(config-epon-onu-voice-*//*:*)#clear epon-onu slot-id/olt-id/onu-idvoice statistics call pots { all   pots-id }</b>	Clear call statistics on the ONU POTS interface.
<b>Raisecom(config-epon-onu-voice-*//*:*)#clear epon-onu slot-id/olt-id/onu-idvoice statistics h248</b>	Clear ONU H.248 protocol performance statistics.
<b>Raisecom(config-epon-onu-voice-*//*:*)#clear epon-onu slot-id/olt-id/onu-idvoice statistics rtp pots [ pots-id ]</b>	Clear ONU RTP media traffic statistics.
<b>Raisecom(config-epon-onu-voice-*//*:*)#clear epon-onu slot-id/olt-id/onu-idvoice statistics error-code</b>	Clear ONU error code statistics.
<b>Raisecom(config-epon-onu-voice-*//*:*)#clear epon-onu slot-id/olt-id/onu-idvoice statistics sdp</b>	Clear ONU SDP performance statistics.

# 5

## Configuring CATV services

---

This chapter introduces CATV services and configuration process of the ISCOM5508, and provides related configurations examples, including the following sections:

- Overview of CATV services
- Quick configuration of CATV services
- Preparing for configurations
- Configuring CATV services
- Checking configurations

### 5.1 Overview of CATV services

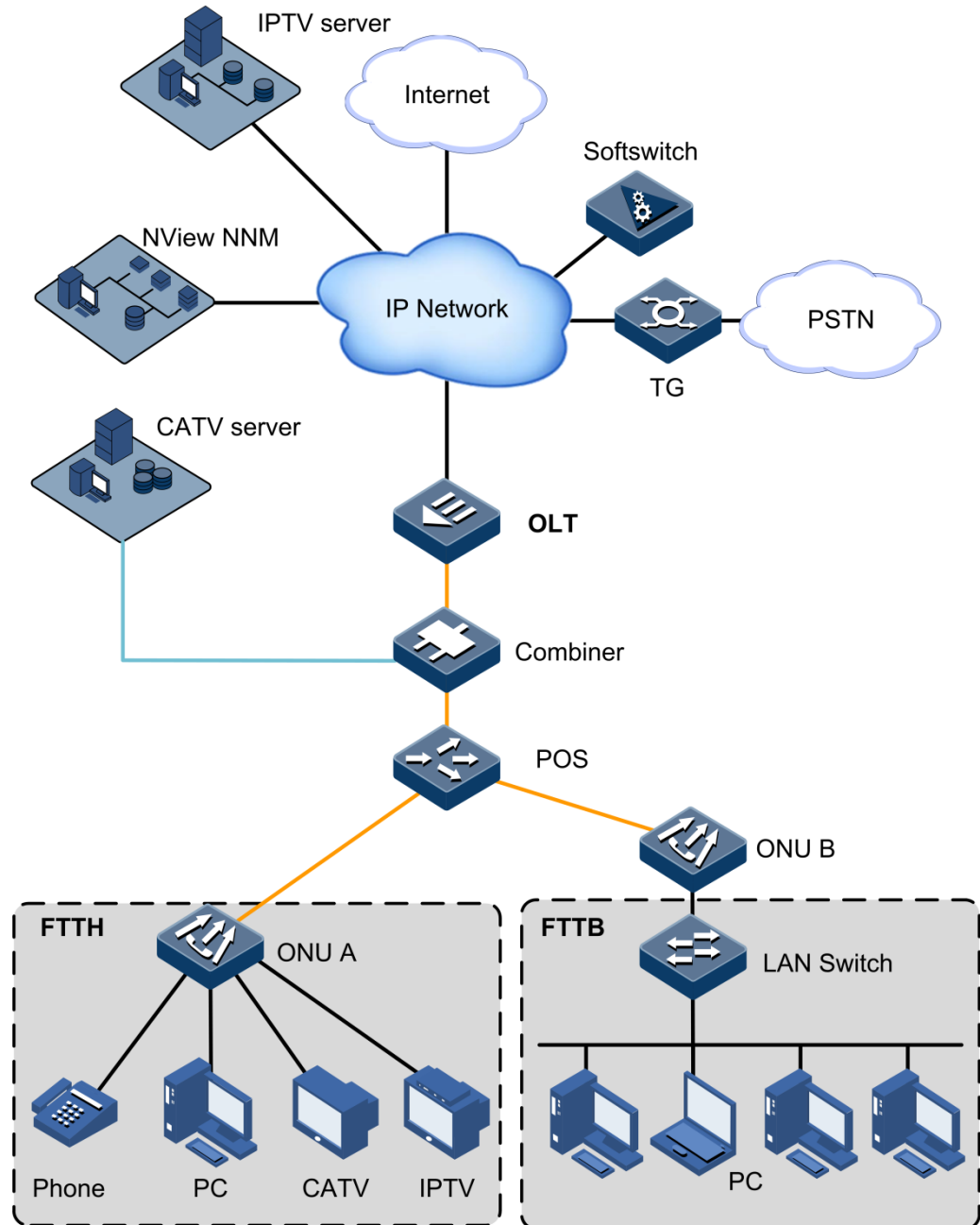
Community Antenna Television (CATV) is a cable TV system of transmitting multichannel TV signals through coaxial cables.

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 5-1 shows the typical triple-play networking.

Figure 5-1 Typical triple-play networking



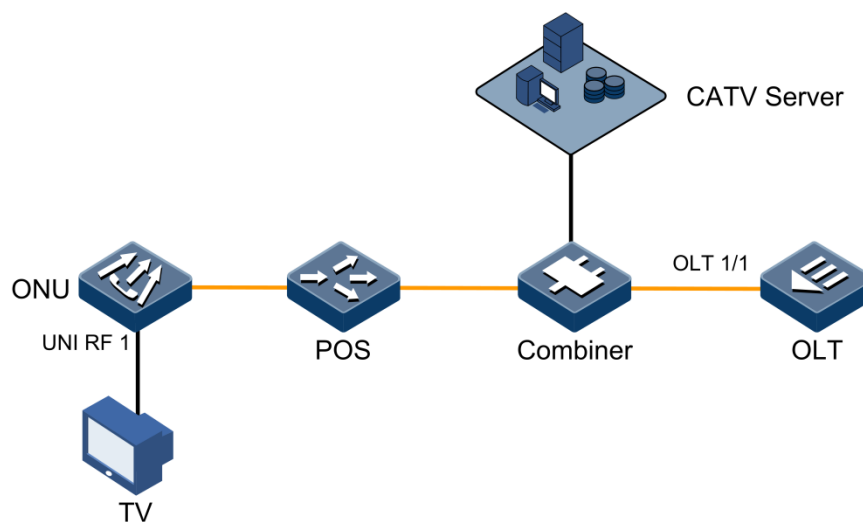
## 5.2 Quick configuration of CATV services

CATV service configuration is simple. You just need to enable the corresponding interface on the ONU which supports CATV services.

### 5.2.1 Networking requirements

As shown in Figure 5-2, the OLT is connected to the ONU through its PON interface OLT 1/1. 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 5-2 Configuring CATV services



## 5.2.2 Configuration steps

Enable CATV services on UNI RF 1.

```
Raisecom#config
Raisecom(config)#epon-onu 1/1/1
Raisecom(config-epon-onu-1/1:1)#uni rf 1 enable
```

## 5.2.3 Checking results

Show configurations of CATV services on the ONU.

```
Raisecom#show epon-onu 1/1/1 uni rf 1 information
RF UNI ID Admin State
-----
1/1/1/1 enable
```

## 5.3 Preparing for configurations

### Scenario

As shown in Figure 5-1, 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.

## 5.4 Configuring CATV services

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*/*:*)#uni rf uni-id { enable disable }</b>	Enable/Disable CATV services.

## 5.5 Checking configurations

No.	Command	Description
1	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni rf [ uni-id ] information</b>	Show information about ONU RF UNI.
2	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id nni catv [ uni-id ] information</b>	Show information about ONU CATV UNI.

# 6 Configuring TDMoP services

---

This chapter introduces TDMoP services and configuration process of the ISCOM5508, and provides related configurations examples, including the following sections:

- Overview of TDMoP services
- Quick configuration of TDMoP services
- Default configurations
- Configuring global parameters of TDMoP
- Configuring TDMoP interface mode
- Configuring TDMoP system clock
- Configuring Bundle
- Checking configurations
- Maintenance

## 6.1 Overview of TDMoP services

As the 3G era comes, data services grow fast. However, traditional Time Division Multiplex (TDM), based on the Circuit Switching Network (CSN), becomes a bottleneck due to the following disadvantages:

- Inadequate bandwidth
- Low channel utilization rate
- Poor expansibility

On the contrary, the Packet Switching Network (PSN), based on statistics multiplexing, becomes the trend of future networks with the following advantages:

- Flexible networking
- High bandwidth
- Low cost

However, PSN is not constructed within a short period. The carrier tends to adopt smooth upgrade from the CSN to PSN to cut investment on network construction. Thus, TDM still holds a predominant position and will coexist with the PSN for a long time. As a result, the Time Division Multiplex over Packet (TDMoP), which is a new technology based on TDM

and IP technology, is generated and it can transparently transmit TDM signals through the PSN.

## 6.1.1 TDMoP service encapsulation modes

Based on TDM signal types, TDMoP service encapsulation modes are classified into:

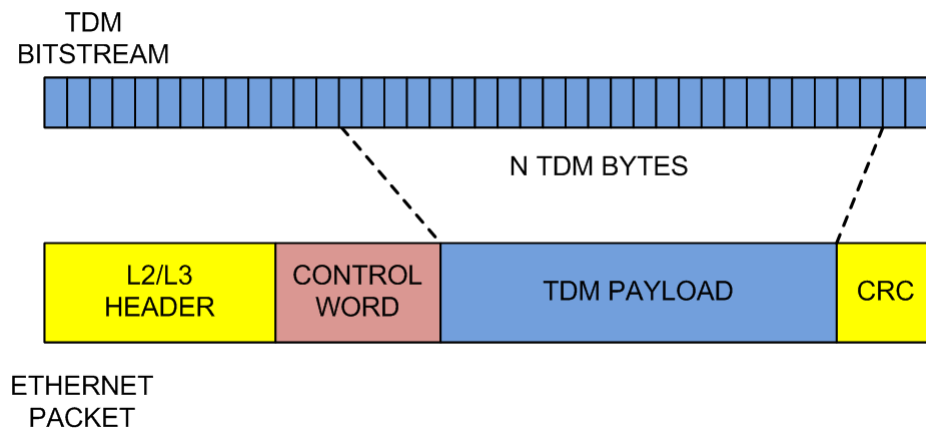
- SAToP
- CESoPSN
- TDMoIP

### SAToP

Structure-Agnostic TDM over Packet (SAToP) provides emulation for low-rate PDH circuit services, such as E1, T1, E3, and T3. It encapsulates unstructured services. It takes TDM services as a serial data flow, fragments and encapsulates it into PW packets for transmission.

Figure 6-1 shows the SAToP encapsulation principle of TDM signals.

Figure 6-1 SAToP encapsulation principle of TDM signals



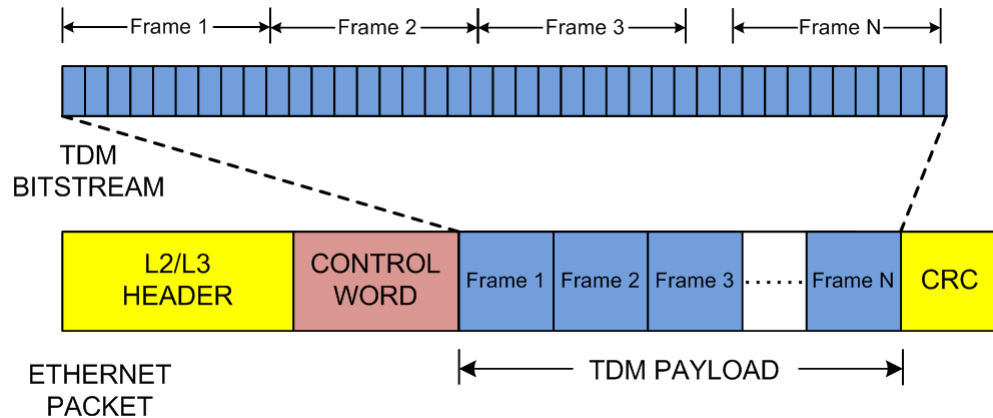
### CESoPSN

Structure-Aware TDM Circuit Emulation Service over Packet-Switched Network (CESoPSN) provides emulation for low-rate PDH circuit services, such as E1, T1, E3, and T3. It provides structured TDM emulation service transmission, has a frame structure, and can recognize and process TDM internal frame signalling.

Figure 6-2 shows the CESoPSN encapsulation principle of TDM signals.



Figure 6-2 CESoPSN encapsulation principle of TDM signals



## TDMoIP

Time Division Multiplexing over IP (TDMoIP) provides emulation for both structured and unstructured TDM services.

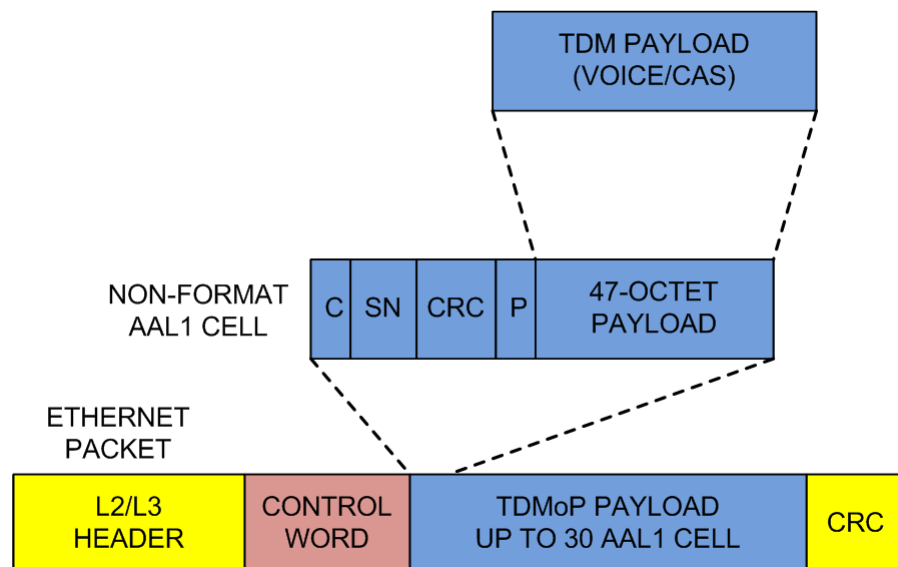
According to different types of encapsulated payload, TDMoIP encapsulation can be divided into the following three adaption modes:

- AAL1

AAL1 is commonly used for 64 Kbit/s voice services, non-compressed and constant-rate video services, and leased line services of data network. This layer is used to adapt data to 48-byte cells. AAL1 is mainly used to adapt structured, unstructured, and timeslot-occupied TDM signals.

Figure 6-3 shows the AAL1 unstructured encapsulation principle.

Figure 6-3 AAL1 unstructured encapsulation principle

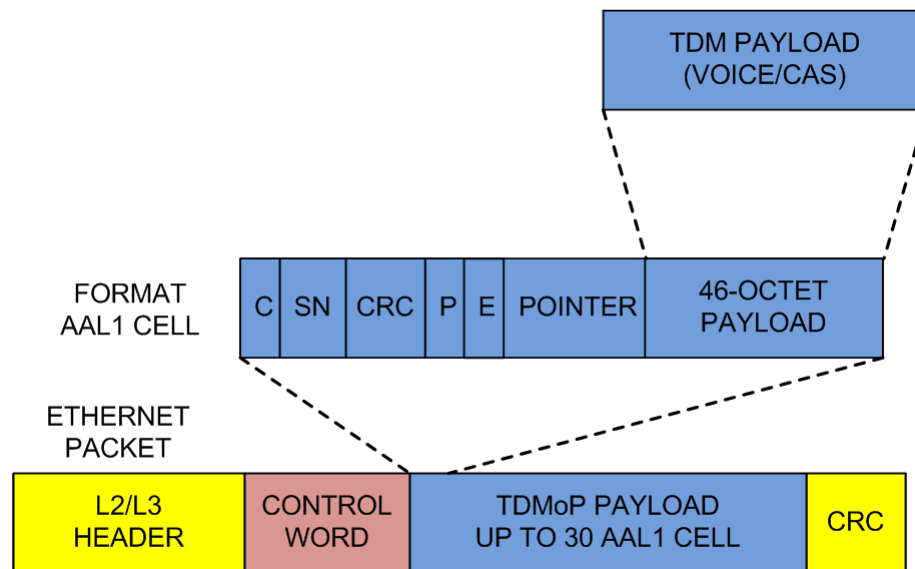


When AAL1 adapts unstructured TDM signals, it uses 47 Bytes of the TDM signal and 1 AAL1 overhead byte to form an AAL1 CELL, where

- C bit indicates whether there is a pointer. When the value is set to 0, it indicates there is no pointer. If the value is set to 1, it indicates there is a pointer. In the unstructured encapsulation mode, the value is set to 0.
- SN is a 3-bit field. It indicates the serial number of a cell. In the unstructured encapsulation mode, this field has no meaning.
- CRC is a 3-bit field. It is a Cyclic Redundancy Check (CRC) of C bit and the SN field.
- P bit is a parity check of C bit, SN field, and CRC field.

Figure 6-4 the AAL1 structured encapsulation principle.

Figure 6-4 AAL1 structured encapsulation principle



When AAL1 adapts structured TDM signals, it uses 46 Bytes of the TDM signal and 2 AAL1 overhead Bytes to form an AAL1 CELL, where

- C bit indicates whether there is a pointer. When the value is set to 0, it indicates there is no pointer. If the value is set to 1, it indicates there is a pointer.
- SN is a 3-bit field. It indicates the serial number of a cell.
- CRC is a 3-bit field. It is a CRC of C bit and the SN field.
- P bit is a parity check of C bit, SN field, and CRC field.
- E bit is a parity check of the pointer.
- POINTER field is a pointer, used to identify the begin timeslot of the first complete E1 frame in the cell.

#### • AAL2

AAL2 is commonly used for variable-rate TDM signals and transmission scenarios of compressed voice. When not all channels of a TDM link are in the active status, or when the system decides whether to use a channel based on the signalling, you can adopt AAL2 variable-rate adaptation mode. In this mode, the system dynamically assigns active channels to the TDM link to save bandwidth.



At present, the ISCOM5508 does not support AAL2 encapsulation mode.

- HDLC

High-level Data Link Control (HDLC) is mainly used to adapt Common Channel Signalling (CCS), HDLC, Point to Point Protocol (PPP), and Frame Relay (FR) signals.

## 6.1.2 TDMoP clock synchronization principles

The key to TDMoP is clock synchronization. A feature of TDM services is high realtime requirement. That is, the clocks of both the sender and the receiver must be in the same precision grade.

Packet transmission on the IP network is a best-effort service. After packets are sent out, they will be buffered, rearranged in order, or probably discarded on the transmission path. As required by TDMoP, the IP network carries TDM services, which may damage code stream and affect clock synchronization between the sender and the receiver, going against realtime transmission.

To eliminate this impact, clock synchronization is used in TDMoP to ensure transparent transmission of clock synchronization signals on the IP network, thus making the sender and the receiver synchronized.

The main clock synchronization mechanisms used by TDMoP are as below:

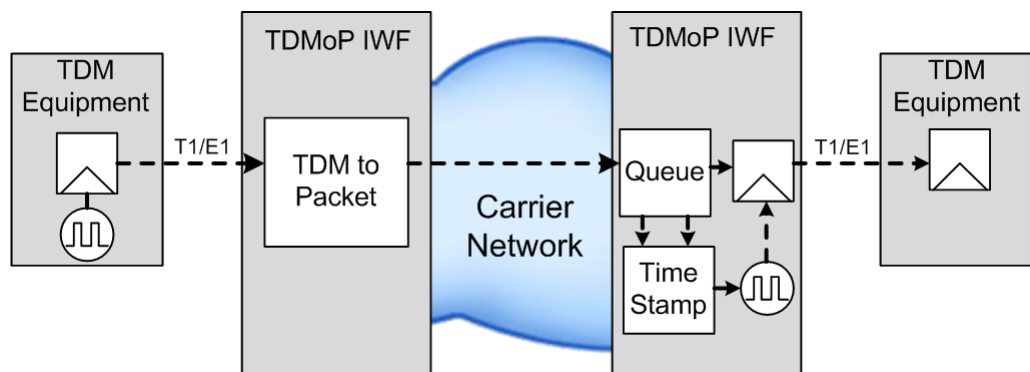
- Self-adaptive clock synchronization
- Differential clock synchronization

### Self-adaptive clock synchronization mechanism

Self-adaptive clock synchronization mechanism, based on the queue buffering technology, tracks IP Packet Delay Variation (IPDV) by the packet queue length of the receiver. It is a basis of clock synchronization between the sender and the receiver.

Figure 6-5 shows the self-adaptive clock synchronization mechanism principle.

Figure 6-5 Self-adaptive clock synchronization mechanism principle



The clock synchronization process of the self-adaptive clock synchronization mechanism is shown as below:

- Step 1 A source Inter-Working Function (IWF) device sends its source clock signals to the destination IWF device.
- Step 2 The destination IWF device buffers all received signals in a queue, and then sends them out with the local clock.

Step 3 If the source IWF clock is not synchronous with the destination IWF clock, the length of the buffering queue on the destination IWF changes, detailed descriptions are shown as follows:

- If the length increases, the destination clock runs slower than the source clock; thus advance the destination clock.
- If the length decreases, the destination clock runs faster than the source clock; thus slow down the destination clock.

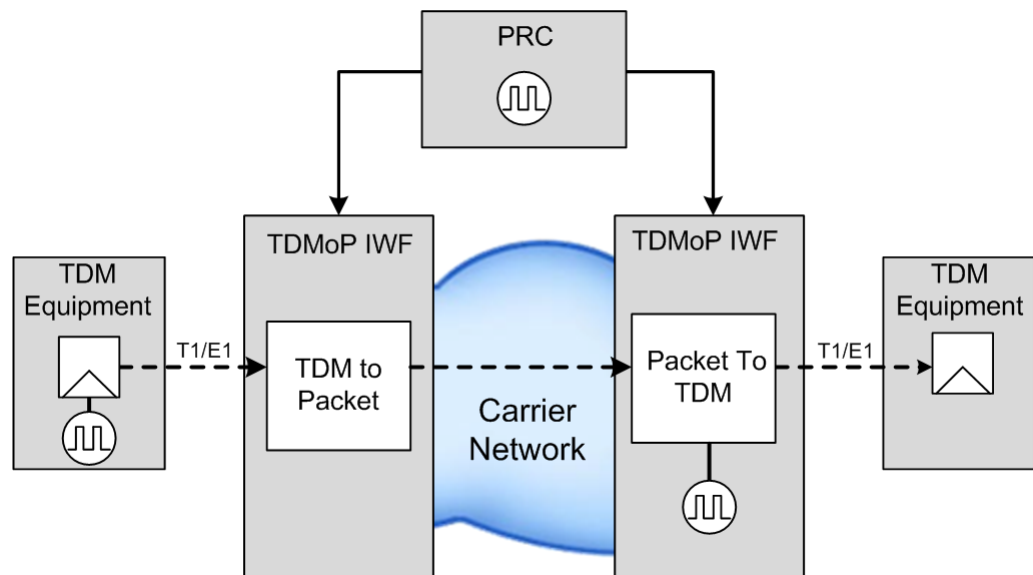
The self-adaptive clock synchronization mechanism is a passive feedback mechanism. When the clock is adjusted properly, clock synchronization between the source IWF device and the destination IWF device on the IP network is complete.

## Differential clock synchronization mechanism

Differential clock synchronization mechanism, based on the Primary Reference Clock (PRC), sends the coded differential value between the source clock the PRC to the destination. The destination compares the destination clock with the PRC and then adjusts its clock.

Figure 6-6 shows the differential clock synchronization mechanism principle.

Figure 6-6 Differential clock synchronization mechanism principle



### 6.1.3 Overview of Bundle

Bundle is a virtual channel in the PSN to emulate TDMoP services. A Bundle can be bound to different timeslots of a TDM interface. All timeslots share the identical destination, payload status host, and PSN resources.

The timeslots of a Bundle can be composed by any timeslot of a TDM frame. However, timeslots of different TDM interfaces cannot be assigned to the same Bundle.

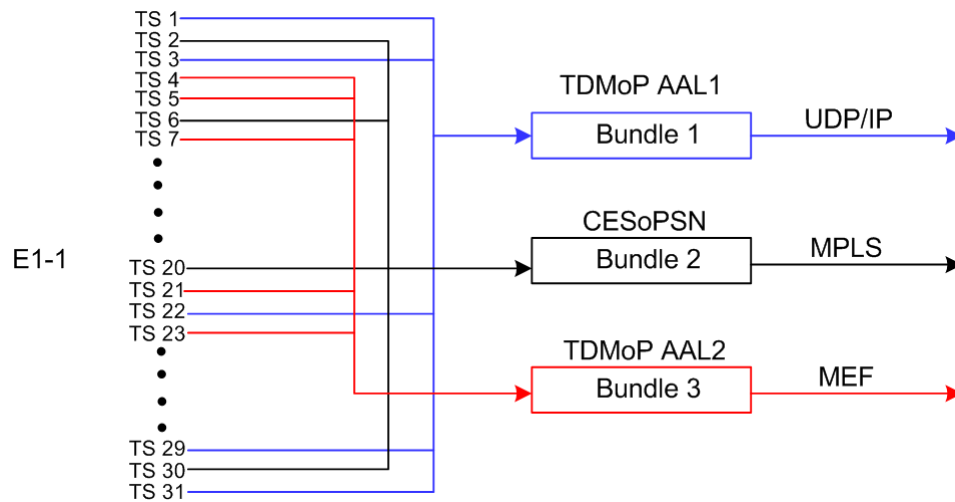
TDMoP devices communicate with each other through Bundle connection. Note the following matters when you configure Bundle.

- Bundle connection is a unidirectional connection. To implement complete full duplex communication, you must configure a Bundle connection on devices at both ends respectively.

- Connection at any direction is identified by the Bundle ID. The Bundle ID can be transmitted through UDP port ID, MPLS Label, or L2TP Session ID.
- Bundle IDs in Rx and Tx directions can be different. However, Bundle parameters of the sender and receiver must be consistent.

Figure 6-7 shows the logical relationship between Bundle and TDM interfaces.

Figure 6-7 Logical relationship between Bundle and TDM interfaces



## 6.2 Quick configuration of TDMoP services

TDMoP service configuration is complicated, involving many functional configuration items. This section provides a typical configuration application so as to facilitate users to open TDMoP services quickly.

If you need to configure more TDMoP service functions, or require a more detailed understanding of TDMoP service configurations, see other sections of this chapter.

### 6.2.1 Networking requirements

As shown in Figure 6-8, the OLT connects to the IP network router through the uplink interface GE 1/1, and connects to the ONU through the PON interface OLT 1/1. Four TDM interfaces on the ONU, namely TDM-UNI 1, TDM-UNI 2, TDM-UNI 3, and TDM-UNI 4, are connected to the TDM device. You need to configure the TDMoP feature on the ONU to realize transparent transmission of TDM services through the PSN.

Figure 6-8 TDMoP service networking

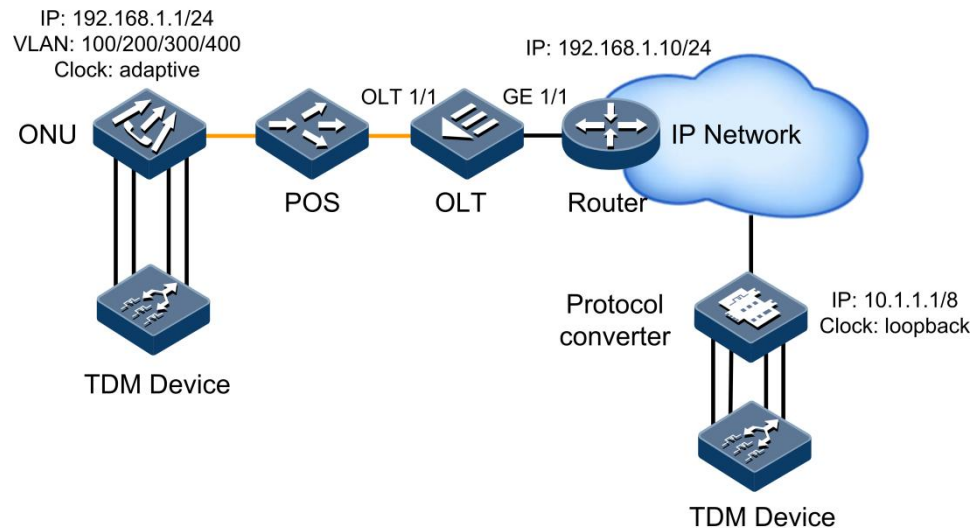


Table 6-1 lists configuration parameters of TDMoP service.

Table 6-1 Configuration parameters of TDMoP service

Parameter	Default value
IP address/mask	192.168.1.1/255.255.255.0
Clock level	stratum-3
Number of TDM signals	4
TDM-1	<ul style="list-style-type: none"> <li>• E1</li> <li>• unframed</li> <li>• clock: adaptive</li> <li>• Bundle: 1</li> </ul>
TDM-2	<ul style="list-style-type: none"> <li>• E1</li> <li>• framed</li> <li>• clock: adaptive</li> <li>• Bundle: 2</li> <li>• E1-CRC is enabled.</li> </ul>
TDM-3	<ul style="list-style-type: none"> <li>• E1</li> <li>• framed-cas (multiframe)</li> <li>• clock: adaptive</li> <li>• Bundle: 3</li> <li>• E1-CRC is enabled.</li> </ul>
TDM-4	<ul style="list-style-type: none"> <li>• E1</li> <li>• unframed</li> <li>• clock: adaptive</li> <li>• Bundle: 6</li> </ul>
Number of Bundle	6

Parameter	Default value
Bundle-1	<ul style="list-style-type: none"> <li>• Payload type: SAToP</li> <li>• PSN type: UDPIP</li> <li>• E1 interface ID: TDM-UNI 1</li> <li>• Timeslot configuration: N/A</li> <li>• Source Bundle ID: 1001</li> <li>• Destination Bundle ID: 1001</li> <li>• VLAN: 100</li> <li>• CoS: 6</li> <li>• Destination IP address: 10.1.1.1</li> <li>• Next-hop type: IP</li> <li>• Next-hop IP address: 192.168.1.10</li> </ul>
Bundle-2	<ul style="list-style-type: none"> <li>• Payload type: CESoPSN</li> <li>• PSN type: UDPIP</li> <li>• E1 interface ID: TDM-UNI 2</li> <li>• Timeslot configuration: 1-15</li> <li>• Source Bundle ID: 1002</li> <li>• Destination Bundle ID: 1002</li> <li>• VLAN: 100</li> <li>• CoS: 6</li> <li>• Destination IP address: 10.1.1.1</li> <li>• Next-hop type: IP</li> <li>• Next-hop IP address: 192.168.1.10</li> </ul>
Bundle-3	<ul style="list-style-type: none"> <li>• Payload type: AAL1</li> <li>• PSN type: UDPIP</li> <li>• E1 interface ID: TDM-UNI 2</li> <li>• Timeslot configuration: 16-31</li> <li>• Source Bundle ID: 1003</li> <li>• Destination Bundle ID: 1003</li> <li>• VLAN: 200</li> <li>• CoS: 6</li> <li>• Destination IP address: 10.1.1.1</li> <li>• Next-hop type: IP</li> <li>• Next-hop IP address: 192.168.1.10</li> </ul>
Bundle-4	<ul style="list-style-type: none"> <li>• Payload type: CESoPSN</li> <li>• PSN type: MPLS</li> <li>• E1 interface ID: TDM-UNI 3</li> <li>• Timeslot configuration: 1-5</li> <li>• Source Bundle ID: 1004</li> <li>• Destination Bundle ID: 1004</li> <li>• VLAN: 300</li> <li>• CoS: 6</li> <li>• Next-hop type: IP</li> <li>• Next-hop IP address: 192.168.1.10</li> <li>• Number of MPLS labels: 2</li> <li>• Outer MPLS label: 14</li> <li>• Inner MPLS label: 104</li> </ul>

Parameter	Default value
Bundle-5	<ul style="list-style-type: none"> <li>• Payload type: AAL1</li> <li>• PSN type: UDPIP</li> <li>• E1 interface ID: TDM-UNI 3</li> <li>• Timeslot configuration: 6-15,17-31</li> <li>• Source Bundle ID: 1005</li> <li>• Destination Bundle ID: 1005</li> <li>• VLAN: 300</li> <li>• CoS: 6</li> <li>• Destination IP address: 10.1.1.1</li> <li>• Next-hop type: IP</li> <li>• Next-hop IP address: 192.168.1.10</li> </ul>
Bundle-6	<ul style="list-style-type: none"> <li>• Payload type: AAL1</li> <li>• PSN type: MPLS</li> <li>• E1 interface ID: TDM-UNI 4</li> <li>• Timeslot configuration: 0-31</li> <li>• Source Bundle ID: 1006</li> <li>• Destination Bundle ID: 1006</li> <li>• VLAN: 400</li> <li>• CoS: 6</li> <li>• Next-hop type: IP</li> <li>• Next-hop IP address: 192.168.1.10</li> <li>• Number of MPLS labels: 2</li> <li>• Outer MPLS label: 16</li> <li>• Inner MPLS label: 106</li> </ul>

## 6.2.2 Configuration steps

Step 1 Configure global parameters.

```
Raisecom#config
Raisecom(config)#epon-onu 1/1/1 tdm
Raisecom(config-epon-onu-tdm-1/1/1)#ip-address 192.168.1.1 255.255.255.0
Raisecom(config-epon-onu-tdm-1/1/1)#source-clock-quality stratum-3
Raisecom(config-epon-onu-tdm-1/1/1)#end
```

Step 2 Configure parameters of the TDM interface.

- Configure TDM-1.

```
Raisecom#config
Raisecom(config)#epon-onu uni elt1 1/1/1/1
Raisecom(config-epon-onu-elt1-1/1/1/1)#service-type e1
Raisecom(config-epon-onu-elt1-1/1/1/1)#frame-mode unframed
Raisecom(config-epon-onu-elt1-1/1/1/1)#tx-clock-src arc
Raisecom(config-epon-onu-elt1-1/1/1/1)#adaptive-bundleid 1
Raisecom(config-epon-onu-tdm-1/1/1)#end
```



- Configure TDM-2.

```
Raisecom#config
Raisecom(config)#epon-onu uni elt1 1/1/1/2
Raisecom(config-epon-onu-elt1-1/1/1:2)#service-type e1
Raisecom(config-epon-onu-elt1-1/1/1:2)#frame-mode framed
Raisecom(config-epon-onu-elt1-1/1/1:2)#tx-clock-src arc
Raisecom(config-epon-onu-elt1-1/1/1:2)#adaptive-bundleid 2
Raisecom(config-epon-onu-elt1-1/1/1:2)#end
```

- Configure TDM-3.

```
Raisecom(config)#epon-onu uni elt1 1/1/1/3
Raisecom(config-epon-onu-elt1-1/1/1:3)#service-type e1
Raisecom(config-epon-onu-elt1-1/1/1:3)#frame-mode framed-cas
Raisecom(config-epon-onu-elt1-1/1/1:3)#tx-clock-src arc
Raisecom(config-epon-onu-elt1-1/1/1:3)#adaptive-bundleid 4
Raisecom(config-epon-onu-elt1-1/1/1:3)#end
```

- Configure TDM-4.

```
Raisecom#config
Raisecom(config)#epon-onu uni elt1 1/1/1/4
Raisecom(config-epon-onu-elt1-1/1/1:4)#service-type e1
Raisecom(config-epon-onu-elt1-1/1/1:4)#frame-mode unframed
Raisecom(config-epon-onu-elt1-1/1/1:4)#tx-clock-src arc
Raisecom(config-epon-onu-elt1-1/1/1:4)#adaptive-bundleid 6
Raisecom(config-epon-onu-elt1-1/1/1:4)#end
```

### Step 3 Configure Bundle parameters.

- Configure Bundle-1.

```
Raisecom#config
Raisecom(config)#epon-onu 1/1/1 tdm
Raisecom(config-onu-tdm-1/1:1)#create bundle 1 payload-type satop psn-
type udpip dest-bundle 1001 src-bundle 1001 port 1 time-slot 0-31
Raisecom(config-onu-tdm-1/1:1)#exit
Raisecom(config)#epon-onu bundle 1/1/1/1
Raisecom(config-epon-onu-bundle-1/1/1:1)#vlan mode tag
Raisecom(config-epon-onu-bundle-1/1/1:1)#vlan inner-vlanid 100
Raisecom(config-epon-onu-bundle-1/1/1:1)#vlan inner-cos 6
Raisecom(config-epon-onu-bundle-1/1/1:1)#udp dest-ip 10.1.1.1
Raisecom(config-epon-onu-bundle-1/1/1:1)#udp nexthop-address-type ip
Raisecom(config-epon-onu-bundle-1/1/1:1)#udp ip-address-nexthop
192.168.1.10
```

```
Raisecom(config-epon-onu-bundle-1/1/1:1)#exit
```

- Configure Bundle-2.

```
Raisecom(config)#epon-onu 1/1/1 tdm
Raisecom(config-onu-tdm-1/1:1)#create bundle 2 payload-type cesop psn-
type udpip dest-bundle 1002 src-bundle 1002 port 2 time-slot 1-15
Raisecom(config-onu-tdm-1/1:1)#exit
Raisecom(config)#epon-onu bundle 1/1/1/2
Raisecom(config-epon-onu-bundle-1/1/1:2)#vlan mode tag
Raisecom(config-epon-onu-bundle-1/1/1:2)#vlan inner-vlanid 100
Raisecom(config-epon-onu-bundle-1/1/1:2)#vlan inner-cos 6
Raisecom(config-epon-onu-bundle-1/1/1:2)#udp dest-ip 10.1.1.1
Raisecom(config-epon-onu-bundle-1/1/1:2)#udp nexthop-address-type ip
Raisecom(config-epon-onu-bundle-1/1/1:2)#udp ip-address-nexthop
192.168.1.10
Raisecom(config-epon-onu-bundle-1/1/1:1)#exit
```

- Configure Bundle-3.

```
Raisecom(config)#epon-onu 1/1/1 tdm
Raisecom(config-onu-tdm-1/1:1)#create bundle 3 payload-type aal1 psn-type
udpip dest-bundle 1003 src-bundle 1003 port 2 time-slot 16-31
Raisecom(config-onu-tdm-1/1:1)#exit
Raisecom(config)#epon-onu bundle 1/1/1/3
Raisecom(config-epon-onu-bundle-1/1/1:3)#vlan mode tag
Raisecom(config-epon-onu-bundle-1/1/1:3)#vlan inner-vlanid 200
Raisecom(config-epon-onu-bundle-1/1/1:3)#vlan inner-cos 6
Raisecom(config-epon-onu-bundle-1/1/1:3)#udp dest-ip 10.1.1.1
Raisecom(config-epon-onu-bundle-1/1/1:3)#udp nexthop-address-type ip
Raisecom(config-epon-onu-bundle-1/1/1:3)#udp ip-address-nexthop
192.168.1.10
Raisecom(config-epon-onu-bundle-1/1/1:3)#exit
```

- Configure Bundle-4.

```
Raisecom(config)#epon-onu 1/1/1 tdm
Raisecom(config-onu-tdm-1/1:1)#create bundle 4 payload-type cesop psn-
type mpls dest-bundle 1004 src-bundle 1004 port 3 time-slot 1-5
Raisecom(config-onu-tdm-1/1:1)#exit
Raisecom(config)#epon-onu bundle 1/1/1/4
Raisecom(config-epon-onu-bundle-1/1/1:4)#vlan mode tag
Raisecom(config-epon-onu-bundle-1/1/1:4)#vlan inner-vlanid 200
Raisecom(config-epon-onu-bundle-1/1/1:4)#vlan inner-cos 6
Raisecom(config-epon-onu-bundle-1/1/1:4)#mpls label-num 2
Raisecom(config-epon-onu-bundle-1/1/1:4)#mpls outer1-label 14
Raisecom(config-epon-onu-bundle-1/1/1:4)#mpls outer2-label 104
```

```
Raisecom(config-epon-onu-bundle-1/1/1:4)#udp nexthop-address-type ip
Raisecom(config-epon-onu-bundle-1/1/1:4)#udp ip-address-nexthop
192.168.1.10
Raisecom(config-epon-onu-bundle-1/1/1:4)#exit
```

- Configure Bundle-5.

```
Raisecom(config)#epon-onu 1/1/1 tdm
Raisecom(config-onu-tdm1/1:1)#create bundle 5 payload-type aal1 psn-type
udpip dest-bundle 1005 src-bundle 1005 port 3 time-slot 6-15,17-31
Raisecom(config-onu-tdm-1/1:1)#exit
Raisecom(config)#epon-onu bundle 1/1/1/5
Raisecom(config-epon-onu-bundle-1/1/1:5)#vlan mode tag
Raisecom(config-epon-onu-bundle-1/1/1:5)#vlan inner-vlanid 300
Raisecom(config-epon-onu-bundle-1/1/1:5)#vlan inner-cos 6
Raisecom(config-epon-onu-bundle-1/1/1:5)#udp dest-ip 10.1.1.1
Raisecom(config-epon-onu-bundle-1/1/1:5)#udp nexthop-address-type ip
Raisecom(config-epon-onu-bundle-1/1/1:5)#udp ip-address-nexthop
192.168.1.10
Raisecom(config-epon-onu-bundle-1/1/1:5)#exit
```

- Configure Bundle-6.

```
Raisecom(config)#epon-onu 1/1/1 tdm
Raisecom(config-onu-tdm1/1:1)#create bundle 6 payload-type aal1 psn-type
mpls dest-bundle 1006 src-bundle 1006 port 4 time-slot 0-31
Raisecom(config-onu-tdm-1/1:1)#exit
Raisecom(config)#epon-onu bundle 1/1/1/6
Raisecom(config-epon-onu-bundle-1/1/1:6)#vlan mode tag
Raisecom(config-epon-onu-bundle-1/1/1:6)#vlan inner-vlanid 400
Raisecom(config-epon-onu-bundle-1/1/1:6)#vlan inner-cos 6
Raisecom(config-epon-onu-bundle-1/1/1:6)#mpls label-num 2
Raisecom(config-epon-onu-bundle-1/1/1:6)#mpls outer1-label 16
Raisecom(config-epon-onu-bundle-1/1/1:6)#mpls outer2-label 106
Raisecom(config-epon-onu-bundle-1/1/1:6)#udp nexthop-address-type ip
Raisecom(config-epon-onu-bundle-1/1/1:6)#udp ip-address-nexthop
192.168.1.10
Raisecom(config-epon-onu-bundle-1/1/1:6)#exit
```

Step 4 Enable the TDM interface.

```
Raisecom(config)#epon-onu uni elt1 range 1/1/1/1-4
Raisecom(config-epon-onu-elt1-range)#port-admin enable
Raisecom(config-epon-onu-elt1-range)#exit
```

Step 5 Enable Bundle.

```
Raisecom(config)#epon-onu bundle range 1/1/3/1-6
Raisecom(config-epon-onu-bundle-range)#bundle enable
Raisecom(config-epon-onu-bundle-range)#end
```

## 6.2.3 Checking results

Show TDM global configurations.

```
Raisecom#show epon-onu 1/1/1 tdm information
ONU ID: 1/1/1
  IP Address       : 192.168.1.1
  Subnet Mask      : 255.255.255.0
  MAC Address      : 000c.d562.1545
  Outer TPID       : 0x9100
  UDP Multiplex Method : src-port
  OAM Frame ID     : 16383
  OOS Code         : 0x7f
  OOS Signalling   : 5
  Source Clock Quality : stratum3
```

Show configurations of the TDM interface.

```
Raisecom#show epon-onu 1/1/1 tdm port information
Port ID : 1/1/1/1
  Description      : tdm-uni-1
  Service-type     : E1
  Port-state       : Enable
  E1-frame-mode    : Unframed
  T1-frame-mode    : Unframed
  E1-crc           : Disable
  T1-signal-mode   : --
  Ts-idle-code     : 0xFF
  Signal-idle-code : 0x5
  Loopback-mode    : None
  Tx-clock-source  : Adaptive recovery clock
  Adaptive-bundle-id : 1
  LOS              : Yes
  LOF              : No
  AIS              : No
  LCV              : No
  RAI              : No
  CRC Error        : No
LOMF              : No
Port ID : 1/1/1/2
  Description      : tdm-uni-2
  Service-type     : E1
  Port-state       : Enable
  E1-frame-mode    : Framed
  T1-frame-mode    : --
  E1-crc           : Enable
```

```

T1-signal-mode      : --
Ts-idle-code        : 0xFF
Signal-idle-code    : 0x5
Loopback-mode       : None
Tx-clock-source     : Adaptive recovery clock
Adaptive-bundle-id  : 2
E1 Service          : Disable
LOS                 : Yes
LOF                 : Yes
AIS                 : No
LCV                 : No
RAI                 : No
CRC Error           : No
LOMF                : No
Port ID : 1/1/1/3
  Description        : tdm-uni-3
  Service-type       : E1
  Port-state         : Enable
  E1-frame-mode      : CAS multi-frame
  T1-frame-mode      : --
  E1-crc             : Enable
  T1-signal-mode     : --
  Ts-idle-code       : 0xFF
  Signal-idle-code   : 0x5
  Loopback-mode      : None
  Tx-clock-source    : Adaptive recovery clock
  Adaptive-bundle-id : 4
  E1 Service         : Disable
  LOS                : Yes
  LOF                : Yes
  AIS                : No
  LCV                : No
  RAI                : No
  CRC Error          : No
LOMF                : No
Port ID : 1/1/1/4
  Description        : tdm-uni-4
  Service-type       : E1
  Port-state         : Enable
  E1-frame-mode      : Unframed
  T1-frame-mode      : Unframed
  E1-crc             : Disable
  T1-signal-mode     : --
  Ts-idle-code       : 0xFF
  Signal-idle-code   : 0x5
  Loopback-mode      : None
  Tx-clock-source    : Adaptive recovery clock
  Adaptive-bundle-id : 6
  E1 Service         : Disable
  LOS                : No
  LOF                : No
  AIS                : No
  LCV                : No
  RAI                : No
  CRC Error          : No

```

LOMF :No

Show Bundle configurations.

Raisecom#**show epon-onu 1/1/1 tdm bundle**

PSN:Packet Switch Network

Bundle ID	Payload Type	PSN Type	Destination Bundle	Source Bundle	Port	Timeslot
1/1/1/1	satop	udpip	1001	1001	1	0-31
1/1/1/2	cesop	udpip	1002	1002	2	1-15
1/1/1/3	aal1	udpip	1003	1003	2	17-31
1/1/1/4	cesop	mpls	1004	1004	3	1-5
1/1/1/5	aal1	udpip	1005	1005	3	6-15,17-31
1/1/1/6	aal1	mpls	1006	1006	4	0-31

## 6.3 Default configurations


N/A

## 6.4 Configuring global parameters of TDMoP




### Note

In Raisecom EPON system, TDMoP features are realized on the ONU. Confirm whether the ONU connected with the ISCOM5508 supports the TDMoP service before configuration.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>epon-onu slot-id/olt-id/onu-id tdm</b>	Enter EPON ONU remote management TDM service configuration mode.  <div>  <b>Note</b>                      You can use the <b>tdm</b> command in EPON ONU remote management mode to enter TDM configuration mode.                 </div>
3	Raisecom(config-epon-onu-tdm-*/:*)# <b>ip-address ip-address [ ip-mask ]</b>	Configure the system source IP address and subnet mask.
4	Raisecom(config-epon-onu-tdm-*/:*)# <b>source-clock-quality { stratum-1   stratum-2   stratum-3   stratum-3e   stratum-4 }</b>	Configure the system clock source level.

Step	Command	Description
5	Raisecom(config-epon-onu-tdm-*/*:*)# <b>oam frame-id</b> <i>frame-id</i>	Configure the frame ID for transmitting OAM packets.
6	Raisecom(config-epon-onu-tdm-*/*:*)# <b>udp-multiplex-method</b> { <b>src-port</b>   <b>dest-port</b> }	Configure the position of the destination Bundle ID in the local Tx UDP packet.
7	Raisecom(config-epon-onu-tdm-*/*:*)# <b>double-tagging tpid</b> <i>tp-id</i>	Configure the outer TPID of Bundle.
8	Raisecom(config-epon-onu-tdm-*/*:*)# <b>oos-code</b> <i>code-value</i>	Configure OSS data code.
9	Raisecom(config-epon-onu-tdm-*/*:*)# <b>oos-signaling</b> <i>code-value</i>	Configure OSS signalling code.

## 6.5 Configuring TDMoP interface mode

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>epon-onu uni elt1 slot-id/olt-id/onu-id/uni-id</b>	Enter EPON ONU TDM interface configuration mode.   <b>Note</b> You can use the <b>elt1</b> command in EPON ONU management mode to enter TDM interface configuration mode.
3	Raisecom(config-epon-onu-elt1-*/*:*)# <b>port-admin</b> { <b>enable</b>   <b>disable</b> }	Enable/Disable TDM on the interface.
4	Raisecom(config-epon-onu-elt1-*/*:*)# <b>service-type</b> { <b>e1</b>   <b>t1</b> }	Configure the service type of the TDM interface.
5	Raisecom(config-epon-onu-elt1-*/*:*)# <b>frame-mode</b> { <b>unframed</b>   <b>framed</b>   <b>framed-cas</b>   <b>sf</b>   <b>esf</b> }	Configure the frame mode of the E1 interface.
6	Raisecom(config-epon-onu-elt1-*/*:*)# <b>e1-crc</b> { <b>enable</b>   <b>disable</b> }	Configure E1 CRC.
7	Raisecom(config-epon-onu-elt1-*/*:*)# <b>t1-signal-mode</b> { <b>none</b>   <b>robbed-bit</b> }	Configure T1 signalling mode.
8	Raisecom(config-epon-onu-elt1-*/*:*)# <b>ts-idle-code</b> <i>code-value</i>	Configure timeslot idled code.
9	Raisecom(config-epon-onu-elt1-*/*:*)# <b>signal-idle-code</b> <i>code-value</i>	Configure signalling idle code.
10	Raisecom(config-epon-onu-elt1-*/*:*)# <b>description</b> <i>description</i>	(Optional) configure descriptions of the TDM interface.

## 6.6 Configuring TDMoP system clock

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu uni elt1 slot-id/olt-id/onu-id/uni-id</b>	Enter EPON ONU TDM interface configuration mode.
3	<b>Raisecom(config-epon-onu-elt1-*//*/*:*)#tx-clock-src { arc   drc   loopback   system }</b>	Configure the Tx clock source.
4	<b>Raisecom(config-epon-onu-elt1-*//*/*:*)#adaptive-bundleid id</b>	Configure the clock recovery Bundle ID.

## 6.7 Configuring Bundle


### 6.7.1 Creating and enabling Bundle

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu uni elt1 slot-id/olt-id/onu-id/uni-id</b>	Enter EPON ONU TDM interface configuration mode.
3	<b>Raisecom(config-epon-onu-tdm-*//*/*:*)#exit</b> <b>Raisecom(config)#epon-onu bundle slot-id/olt-id/onu-id/bundle-id</b>	Enter EPON ONU TDM Bundle configuration mode.
4	<b>Raisecom(config-epon-onu-bundle-*//*/*:*)#bundle { enable   disable }</b>	Enable/Disable Bundle.
5	<b>Raisecom(config-epon-onu-bundle-*//*/*:*)#exit</b> <b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id tdm</b>  <b>Raisecom(config-epon-onu-tdm-*//*/*:*)#create bundle bundle-id payload-type { aal1   aal2   cesop   satop   hd1c } psn-type { udpip   mpls   12tp   mef } dest-bundle dest-bundle-id src-bundle src-bundle-id port port-index time-slot ts-list</b>	Create the TDM Bundle management table.

### 6.7.2 Configuring parameters of Bundle

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



Step	Command	Description
2	<code>Raisecom(config)#epon-onu bundle slot-id/olt-id/onu-id/bundle-id</code>	Enter EPON ONU TDM Bundle configuration mode.   <b>Note</b> You can use the <b>bundle</b> command in EPON ONU remote management mode to enter Bundle configuration mode.
3	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#description description</code>	(Optional) configure descriptions of the Bundle interface.
4	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#payload-type {aal1   aal2   cesop   satop   hdlc}</code>	(Optional) configure the payload type of Bundle.
5	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#psn-type {udpip   mpls   l2tp   mef}</code>	(Optional) configure the PSN type.
6	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#dest-bundle dest-bundle-id</code>	(Optional) configure the destination Bundle interface ID.
7	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#src-bundle src-bundle-id</code>	(Optional) configure the source Bundle interface ID.
8	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#oos-status {lbit   txoff}</code>	(Optional) configure the OSS mode.
9	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#protocol-port port-id</code>	(Optional) configure the ID of the interface which is not filled with the Bundle ID in the UDP packet.
10	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#oam-connectivity {enable   disable}</code>	(Optional) enable/disable OAM connectivity check.

### 6.7.3 Configuring parameters of E1/T1 interface

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#epon-onu bundle slot-id/olt-id/onu-id/bundle-id</code>	Enter EPON ONU TDM Bundle configuration mode.
3	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#port port-id</code>	(Optional) configure the E1/T1 interface ID corresponding to Bundle.
4	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#timeslot timeslot-list</code>	(Optional) configure the timeslot occupied by Bundle.

### 6.7.4 Configuring related information of PSN

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

Step	Command	Description
2	<code>Raisecom(config)#epon-onu bundle slot-id/olt-id/onu-id/bundle-id</code>	Enter EPON ONU TDM Bundle configuration mode.
3	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#udp dest-ip ip-address</code>	(Optional) configure the destination IP address of Bundle connection.
4	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#udp next-hop-address-type { ip   mac }</code>	(Optional) configure the next-hop address type of Bundle.
5	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#udp ip-address-nexthop ip-address</code>	(Optional) configure the next-hop IP address of Bundle.
6	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#udp mac-address-nexthop mac-address</code>	(Optional) configure the next-hop MAC address of Bundle.
7	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#mpls label-num label-num</code>	(Optional) configure the number of Bundle MPLS outer labels.
8	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#mpls outer1-label label-val</code>	(Optional) configure the value of Bundle MPLS outer label 1.
9	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#mpls outer2-label label-val</code>	(Optional) configure the value of Bundle MPLS outer label 2.
10	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#mpls exp exp-val</code>	(Optional) configure the EXP field of Bundle MPLS.
11	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#mpls ttl ttl-val</code>	(Optional) configure the TTL field of Bundle MPLS.
12	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#vlan mode { tag   double-tag   untag }</code>	(Optional) configure the VLAN mode of Bundle.
13	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#vlan inner-vlanid vlan-id</code>	(Optional) configure the inner VLAN ID of Bundle.
14	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#vlan outer-vlanid vlan-id</code>	(Optional) configure the outer VLAN ID of Bundle.
15	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#vlan inner-cos cos-val</code>	(Optional) configure the inner VLAN priority of Bundle.
16	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#vlan outer-cos cos-val</code>	(Optional) configure the outer VLAN priority of Bundle.
17	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#rtp { enable   disable }</code>	(Optional) enable/disable the RTP feature of Bundle.

## 6.7.5 Configuring packet load time and Jitter Buffer

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#epon-onu bundle slot-id/olt-id/onu-id/bundle-id</code>	Enter EPON ONU TDM Bundle configuration mode.
3	<code>Raisecom(config-epon-onu-bundle-*/*/*:*)#packet-load-time time</code>	(Optional) configure the packet load time of Bundle.

Step	Command	Description
4	<code>Raisecom(config-epon-onu-bundle- */*/*:*)#jitter-buffer buffer-size</code>	(Optional) configure the size of Jitter Buffer.

## 6.8 Checking configurations

No.	Command	Description
1	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id tdm information</code>	Show configurations of the TDM system.
2	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id tdm port port-list time-slot</code>	Show information about timeslot assignment on the TDM interface.
3	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id tdm port port-list information</code>	Show configurations of the TDM E1/T1 interface.
4	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id tdm port port-list statistics</code>	Show performance statistics of the TDM interface.
5	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id tdm bundle bundle-list</code>	Show the created TDM Bundle.
6	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id tdm bundle bundle-list information</code>	Show configurations of TDM Bundle.
7	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id tdm bundle bundle-list current-status</code>	Show the current status of TDM Bundle.
8	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id tdm bundle bundle-list udp information</code>	Show TDM Bundle UDP management information.
9	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id tdm bundle bundle-list mpls information</code>	Show TDM Bundle MPLS management information.
10	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id tdm bundle bundle-list vlan information</code>	Show TDM Bundle VLAN management information.
11	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id tdm bundle bundle-list statistics</code>	Show TDM Bundle statistics.

## 6.9 Maintenance

Command	Description
<code>Raisecom(config)#clear epon-onu slot-id/olt-id/onu-id tdm port port-list statistics</code>	Clear performance statistics of the ONU TDM interface.
<code>Raisecom(config)#clear epon-onu slot-id/olt-id/onu-id tdm bundle bundle-list statistics</code>	Clear performance statistics of Bundle.

# 7

## Configuring MAC address

---

This chapter introduces basic principles and configuration process of the MAC address table for the ISCOM5508, and provides related configuration examples, including the following sections:

- Overview of MAC address table
- Configuring dynamic MAC address
- Configuring static MAC address
- Maintenance and search
- Configuration examples

### 7.1 Overview of MAC address table

The ISCOM5508 supports 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 ISCOM5508 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

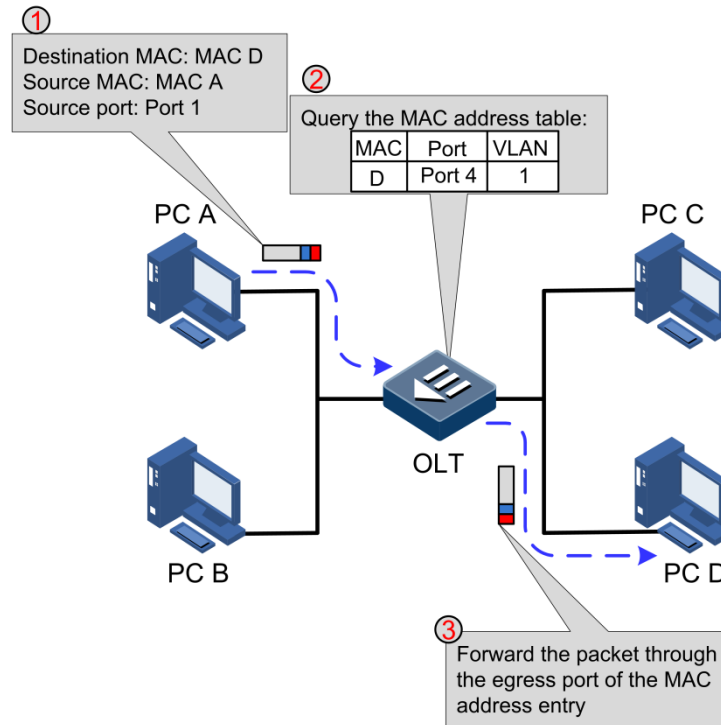
The MAC address table on the ISCOM5508 consists of two kinds of address entries:

- 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 ISCOM5508 adopts following modes:

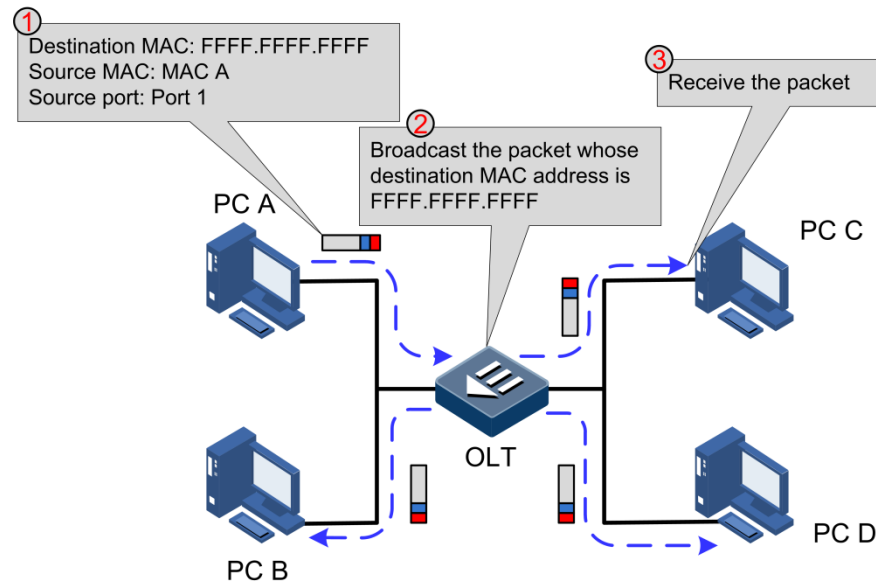
- Unicast: when a MAC address entry, which is related to the destination MAC address of a packet, is listed in the MAC address table, the ISCOM5508 will directly forward the packet through the egress interface. Otherwise, the ISCOM5508 will broadcast the packet, as shown in Figure 7-1.

Figure 7-1 Unicast forwarding mode of MAC address



- Multicast: when the ISCOM5508 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 ISCOM5508 will forward the packet through the egress interface. Otherwise, the ISCOM5508 will broadcast this packet.
- Broadcast: when the ISCOM5508 receives an all-F packet, or when the ISCOM5508 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 7-2.

Figure 7-2 Broadcast forwarding mode of MAC address



## 7.2 Configuring dynamic MAC address

### 7.2.1 Preparing for configurations

#### Scenario

Dynamic MAC address entries can be added through the MAC address learning mechanism. You can limit the number of MAC address 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 ISCOM5508 is rebooted.

#### Prerequisite

N/A

### 7.2.2 Default configurations

Default configurations of dynamic MAC address entries on the ISCOM5508 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 ONU are as below

Function	Default value
MAC address learning	Enable
Aging time of MAC address	300s
MAC address limit	Unlimited

## 7.2.3 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 realize Layer 2 forwarding.

### Configuring MAC address learning on OLT

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface { epon-olt   gigabitethernet } slot-id/olt-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-*:*:*)#mac-address-table learning</b>	Enable MAC address learning on the OLT. You can use the <b>no mac-address-table learning</b> command to disable this function.


### Configuring MAC address learning on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</b>	Enter EPON ONU UNI configuration mode.
3	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)#mac-address-table learning { enable   disable }</b>	Enable/Disable MAC address learning on the Ethernet interface of the ONU.


## 7.2.4 (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 aging time of MAC address on OLT

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mac-address-table aging-time { 0   period }</b>	<p>Configure the aging time of dynamic MAC address entries on the OLT.</p> <p>You can use the <b>no mac-address-table aging-time</b> command to restore default configurations.</p> <div>  <b>Note</b> </div> <p>The value 0 refers that the dynamic MAC address is not aged.</p>

## Configuring aging time of MAC address on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*/*:*)#mac-address-table aging-time { 0   period }</b>	<p>Configure the aging time of dynamic MAC address entries on the ONU.</p> <p>You can use the <b>no mac-address-table aging-time</b> command to restore default configurations.</p> <div>  <b>Note</b> </div> <p>The value 0 refers that the dynamic MAC address is not aged.</p>

## 7.2.5 (Optional) configuring MAC address limit

To avoid explosive increase of the MAC address table, you need to configure the MAC address limit, thus preventing lowering performance of the device due to a too large MAC address table.

### Configuring MAC address limit on OLT

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface { epon-olt   gigabitethernet } slot-id/olt-id</b>	Enter physical interface configuration mode.



Step	Command	Description
3	<b>Raisecom(config-if-epon-*/*:*)#mac-address-table threshold <i>threshold</i></b>	Configure the threshold of MAC addresses allowed to be learnt by the interface on the OLT.  You can use the <b>no mac-address-table threshold</b> command to restore default configurations.

## Configuring global MAC address limit on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface epon-onu <i>slot-id/olt-id/onu-id</i></b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-if-epon-onu-*/*:*)#mac-address-table threshold <i>threshold</i></b>	Configure the threshold of MAC addresses allowed to be learnt by the ONU.  You can use the <b>no mac-address-table threshold</b> command to restore default configurations.

## Configuring MAC address limit on ONU UNI

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu uni ethernet <i>slot-id/olt-id/onu-id/uni-id</i></b>	Enter EPON ONU UNI configuration mode.
3	<b>Raisecom(config-epon-onu-ethernet-*/*:*)#mac-address-table threshold { <b>unlimited</b>   <i>number</i> }</b>	Configure the threshold of MAC addresses allowed to be learnt by the ONU UNI.  You can use the <b>no mac-address-table threshold</b> command to restore default configurations.

## 7.2.6 Checking configurations

### Checking configurations on OLT

No.	Command	Description
1	<b>Raisecom#show interface { epon-olt   gigabitethernet } <i>slot-id/port-list</i> mac-address-table</b>	Show configurations of the MAC address table on the OLT interface.
2	<b>Raisecom#show mac-address-table 12-address [ <i>vlan vlan-id</i>   interface { epon-olt <i>slot-id/port-id</i>   gigabitethernet <i>slot-id/port-id</i>   port-channel <i>group-id</i> } ]</b>	Show MAC address entries on the OLT interface.

No.	Command	Description
3	<b>Raisecom#show mac aging-time</b>	Show the aging time of MAC addresses on the OLT.

## Checking configurations on ONU

No.	Command	Description
1	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id mac-address-table l2-address [ uni ethernet uni-id ] { all   dynamic   static } [ count ]</b>	Show configurations of the MAC address table on the ONU UNI.
2	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list mac-address-table aging-time</b>	Show the aging time of MAC addresses on the ONU.
3	<b>Raisecom#show interface epon-onu slot-id/olt-id/onu-list mac-address-table threshold</b>	Show the threshold of MAC addresses allowed to be learnt by the ONU.
4	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id mac-address-table l2-address [ uni ethernet uni-id ] { all   dynamic   static } [ count ]</b>	Show the MAC address entry of the ONU or the specified ONU UNI.
5	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet [ uni-id ] mac-address-table</b>	Show configurations of the MAC address table on the ONU UNI.

## 7.3 Configuring static MAC address

### 7.3.1 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

### 7.3.2 Default configurations

N/A

### 7.3.3 Configuring static unicast MAC address

Static MAC address can be set for fixed servers, special persons (manager, financial staff, etc.) 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 address on OLT

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>mac-address-table static unicast</b> <i>mac-address</i> <b>vlan</b> <i>vlan-id</i> <b>interface</b> { <b>epon-olt</b> <i>slot-id/port-id</i>   <b>gigabitethernet</b> <i>slot-id/port-id</i>   <b>port-channel</b> <i>group-id</i> }	Configure static unicast MAC address entries on the OLT.  You can use the <b>no mac-address-table static unicast</b> <i>mac-address</i> <b>vlan</b> <i>vlan-id</i> command to delete the configuration.

## Configuring static unicast MAC address on ONU

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>epon-onu</b> <i>slot-id/olt-id/onu-id</i>	Enter EPON ONU remote management configuration mode.
3	Raisecom(config-epon-onu-*/*:*)# <b>mac-address-table static unicast</b> <i>mac-address</i> <b>uni ethernet</b> <i>uni-id</i>	Configure static unicast MAC address entries on the ONU.  You can use the <b>no mac-address-table static unicast</b> <i>mac-address</i> command to delete the configuration.

## 7.3.4 Configuring static multicast MAC address

### Configuring static multicast MAC address on OLT

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>mac-address-table static multicast</b> <i>mac-address</i> <b>vlan</b> <i>vlan-id</i> { <b>add</b>   <b>remove</b> } <b>interface</b> { <b>epon-olt</b> <i>slot-id/port-id</i>   <b>gigabitethernet</b> <i>slot-id/port-id</i>   <b>port-channel</b> <i>group-id</i> }	Configure static multicast MAC address entries on the OLT.  You can use the <b>no mac-address-table static multicast</b> <i>mac-address</i> <b>vlan</b> <i>vlan-id</i> <b>port-list</b> <i>port-list</i> command to delete the configuration.

### Configuring static multicast MAC address on ONU

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

Step	Command	Description
2	<code>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</code>	Enter EPON ONU remote management configuration mode.
3	<code>Raisecom(config-epon-onu-*/*:*)#mac-address-table static multicast mac-address vlan vlan-id uni ethernet uni-list</code>	Configure static multicast MAC address entries on the ONU.  You can use the <b>no mac-address-table static multicast { mac-address   all }</b> command to delete the configuration.

### 7.3.5 Configuring MAC address flapping

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface { epon-olt   gpon-olt   gigabitethernet   ten-gigabitethernet } slot-id/olt-id</code>	Enter physical interface configuration mode.
3	<code>Raisecom(config-if-*-*:*)#mac-address-table station move</code>	Configure MAC address flapping.

### 7.3.6 Checking configurations

#### Checking configurations on OLT

No.	Command	Description
1	<code>Raisecom#show mac-address-table static unicast [ vlan vlan-id   interface { epon-olt slot-id/port-id   gigabitethernet slot-id/port-id   port-channel group-id } ]</code>	Show the static unicast MAC address of the OLT.
2	<code>Raisecom#show mac-address-table statistics unicast [ vlan vlan-id   interface { epon-olt slot-id/port-id   gigabitethernet slot-id/port-id   port-channel group-id } ]</code>	Show statistics of the static unicast MAC address of the OLT.
3	<code>Raisecom#show mac-address-table multicast [ statistics ]</code>	Show the static multicast MAC address of the OLT.

#### Checking configurations on ONU

No.	Command	Description
1	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id mac-address-table static [ uni ethernet uni-id ]</code>	Show the static MAC address table on the ONU UNI.

No.	Command	Description
2	Raisecom# <b>show epon-onu slot-id/olt-id/onu-id mac-address-table multicast</b> [ <b>uni ethernet uni-id</b> ]	Show the multicast MAC address table on the ONU.
3	Raisecom# <b>show epon-onu slot-id/olt-id/onu-id mac-address-table static multicast</b> [ <b>vlan vlan-id</b> ]	Show all static multicast MAC address entries on the ONU or those of the specified VLAN.

## 7.4 Maintenance and search

### 7.4.1 Preparing for configurations

#### Scenario

The ISCOM5508 supports clearing the Layer 2 MAC address table, including:

- Clear all MAC address entries.
- Clear dynamically learnt MAC address entries.
- Clear statically configured MAC address entries.

Use the **search** command, you can search for the content of the MAC address entry and related information.

#### Prerequisite

N/A

### 7.4.2 Default configurations

N/A

### 7.4.3 Clearing MAC address

#### Clearing MAC address on OLT

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>clear</b> [ <b>interface</b> { <b>epon-olt</b>   <b>gigabitethernet</b> } <b>slot-id/port-id</b> ] <b>mac-address-table unicast</b> [ <b>dynamic</b>   <b>static</b> ] [ <b>vlan vlan-id</b> ]	Clear entries in the unicast MAC address table on the OLT.

## Clearing MAC address on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#clear epon-onu slot-id/olt-id/onu-id mac-address-table { all   dynamic   static }</b>	Clear entries of the specified type in the MAC address table on the ONU.

## 7.4.4 Searching MAC address

### Searching MAC address on OLT

Step	Command	Description
1	<b>Raisecom#search mac-address mac-address</b>	Search for information about a specified MAC address in the MAC address table on the OLT.

### Searching MAC address on ONU

Step	Command	Description
1	<b>Raisecom#search epon-onu slot-id/olt-id/onu-id mac-address-table mac-address</b>	Search for information about a specified MAC address in the MAC address table on the ONU.

## 7.4.5 Tracing MAC address

Step	Command	Description
1	<b>Raisecom#trace mac-address mac-address</b>	Trace a specified MAC address.

## 7.4.6 Checking configurations

### Checking configurations on OLT

No.	Command	Description
1	<b>Raisecom#show interface { epon-olt   gigabitethernet } slot-id/port-list mac-address-table</b>	Show configurations of the MAC address table on the OLT.
2	<b>Raisecom#show mac-address-table 12-address [ vlan vlan-id   interface { epon-olt slot-id/port-id   gigabitethernet slot-id/port-id   port-channel group-id } ]</b>	Show information about the MAC address table on the OLT interface.

No.	Command	Description
3	<b>Raisecom#show mac-address-table multicast [ statistics ]</b>	Show information about the multicast MAC address entries on the OLT.
4	<b>Raisecom#show mac-address-table static unicast [ vlan <i>vlan-id</i>   interface { epon-olt <i>slot-id/port-id</i>   gigabitethernet <i>slot-id/port-id</i>   port-channel <i>group-id</i> } ]</b>	Show information about the static unicast MAC address entries on the OLT.
5	<b>Raisecom#show mac-address-table statistics unicast [ vlan <i>vlan-id</i>   interface { epon-olt <i>slot-id/port-id</i>   gigabitethernet <i>slot-id/port-id</i>   port-channel <i>group-id</i> } ]</b>	Show statistics on the static unicast MAC address entries on the OLT.

## Checking configurations on ONU

No.	Command	Description
1	<b>Raisecom#show interface epon-onu mac <i>mac-address</i> creation-information</b>	Show creation information about the specified entry in the MAC address table on the ONU.
2	<b>Raisecom#show epon-onu <i>slot-id/olt-id/onu-id</i> mac-address-table <i>l2-address</i> [ uni ethernet <i>uni-id</i> ] { all   dynamic   static } [ count ]</b>	Show the MAC address of the ONU or the specified ONU UNI.
3	<b>Raisecom#show epon-onu <i>slot-id/olt-id/onu-id</i> mac-address-table multicast [ uni ethernet <i>uni-id</i> ]</b>	Show the multicast MAC address table on the ONU.
4	<b>Raisecom#show epon-onu <i>slot-id/olt-id/onu-id</i> mac-address-table static multicast [ vlan <i>vlan-id</i> ]</b>	Show the static multicast MAC address table on the ONU.
5	<b>Raisecom#show epon-onu <i>slot-id/olt-id/onu-id</i> mac-address-table static [ uni ethernet <i>uni-id</i> ]</b>	Show the static MAC address table on the specified ONU UNI.
6	<b>Raisecom#show epon-onu <i>slot-id/olt-id/onu-id</i> uni ethernet [ <i>uni-id</i> ] mac-address-table</b>	Show configurations of the MAC address table on the ONU UNI.

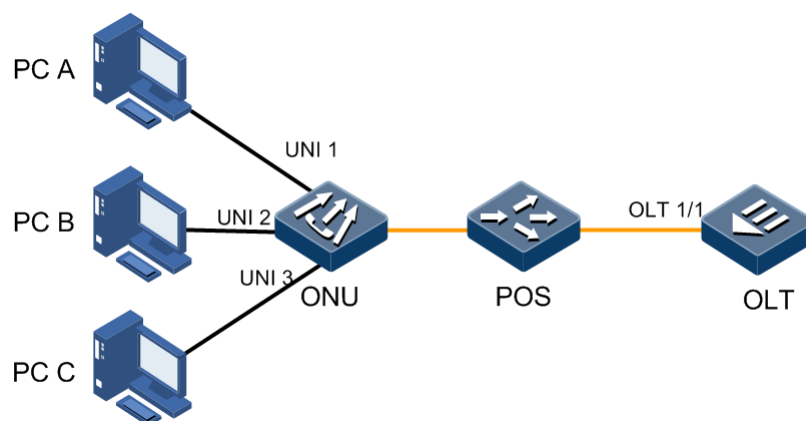
## 7.5 Configuration examples

### 7.5.1 Example for configuring dynamic MAC address

#### Networking requirements

As shown in Figure 7-3, the ONU is connected uplink to multiple hosts. To avoid explosive increase of the MAC address table on the ONU, you need to configure the aging time of the dynamic MAC address table to 100s (the configuration takes effect only when MAC address learning is enabled), and configure the maximum number of MAC address allowed to be learnt by ONU UNI 2 to 128. Meanwhile, you need to configure the aging time of the dynamic MAC address table on the OLT to 500s.

Figure 7-3 Configuring dynamic MAC address



## Configuration steps

- Configure the dynamic MAC address on the OLT.

Step 1 Enable MAC address learning on the PON interface OLT 1/1.

```
Raisecom#config
Raisecom(config)#interface epon-olt 1/1
Raisecom(config-if-epon-olt-1:1)#mac-address-table learning
Raisecom(config-if-epon-olt-1:1)#exit
```

Step 2 Configure the aging time of dynamic 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 1/1/1/1
Raisecom(config-epon-onu-ethernet-1/1/1:1)#mac-address-table learning
enable
Raisecom(config-epon-onu-ethernet-1/1/1:1)#exit
Raisecom(config)#epon-onu uni ethernet 1/1/1/2
Raisecom(config-epon-onu-ethernet-1/1/1:2)#mac-address-table learning
enable
Raisecom(config-epon-onu-ethernet-1/1/1:2)#exit
Raisecom(config)#epon-onu uni ethernet 1/1/1/3
Raisecom(config-epon-onu-ethernet-1/1/1:3)#mac-address-table learning
enable
Raisecom(config-epon-onu-ethernet-1/1/1:3)#end
```



Step 4 Configure the aging time of dynamic MAC addresses on the ONU.

```
Raisecom#config
Raisecom(config)#epon-onu 1/1/1
Raisecom(config-epon-onu-1/1:1)#mac-address-table aging-time 500
Raisecom(config-epon-onu-1/1:1)#exit
```

Step 5 Configure the threshold of MAC addresses allowed to be learnt by ONU UNI 2 to 128.

```
Raisecom(config)#epon-onu uni ethernet 1/1/1/2
Raisecom(config-epon-onu-ethernet-1/1/1:2)#mac-address-table threshold
128
```

## Checking results

- Check results on the OLT.

Show the MAC address learning status and aging time on the OLT.

```
Raisecom#show interface epon-olt 1/1 mac-address-table
Port ID  MAC-learning  MAC-threshold
-----
epon-olt1/1    Enable          0

Raisecom#show mac aging-time
Aging time: 500 seconds
```

- Check results on the ONU.

Show the MAC address learning status and aging time on the ONU.

```
Raisecom#show epon-onu 1/1/1 uni ethernet mac-address-table
Port ID    Learning  Threshold
-----
1/1/1/1    enable    no limit
1/1/1/2    enable    128
1/1/1/3    enable    no limit

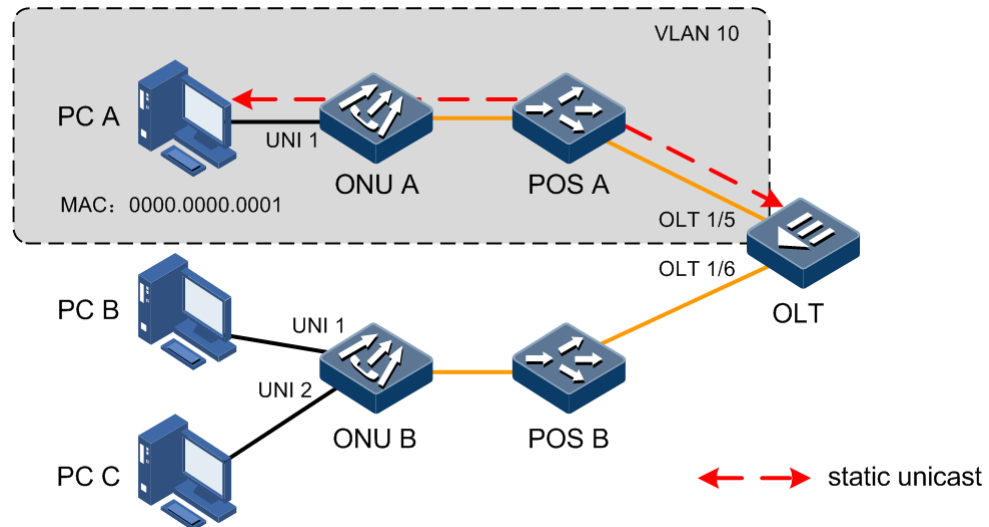
Raisecom#config
Raisecom(config)#show epon-onu 1/1/1 mac-address-table aging-time
ONU ID     AgingTime(s)
-----
1/1/1      100
```

## 7.5.2 Example for configuring static MAC address

### Networking requirements

As shown in Figure 7-4, the position of PC A is fixed and important. Configure a static unicast MAC address for PC A on ONU A and the OLT. The MAC address of PC A is 0000.0000.0001. PC A belongs to VLAN 10.

Figure 7-4 Configuring static MAC address



### Configuration steps

- Configure the 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 1/1
Raisecom(config-if-epon-olt-1:1)#switchport mode trunk
Raisecom(config-if-epon-olt-1:1)#switchport trunk allowed vlan 10
Raisecom(config-if-epon-olt-1:1)#exit
```

Step 2 Configure the static unicast MAC address on the OLT.

```
Raisecom(config)#mac-address-table static unicast 0000.0000.0001 vlan 10
interface epon-olt 1/1
Raisecom(config)#end
```

- Configure the static unicast MAC address on the ONU.

Step 3 Create a VLAN and configure the interface mode on the ONU.

```
Raisecom#config
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 10
Raisecom(config-epon-onu-ethernet-1/1/1:1)#exit
Raisecom(config)#epon-onu uplink
Raisecom(config-epon-onu-uplink)#vlan mode transparent
Raisecom(config-epon-onu-uplink)#exit
```

Step 4 Configure the static unicast MAC address on the ONU.

```
Raisecom(config)#epon-onu 1/1/1
Raisecom(config-epon-onu-1/1:1)#mac-address-table static unicast
0000.0000.0001 uni ethernet 1
```

## Checking results

- Check results on the OLT.

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-olt1/1      10    Static
```

- Check results on the ONU.

Show information about the static unicast MAC address on the ONU.

```
Raisecom#show epon-onu 1/1/1 mac-address-table static uni ethernet 1
Port ID      Static Mac Address
-----
1/1/1/1      0000.0000.0001
```

# 8 Configuring VLAN

---

This chapter introduces the VLAN features and configuration process of the ISCOM5508, and provides related configuration examples, including the following sections:

- Overview of VLAN
- Configuring VLAN
- Configuring QinQ
- Configuring VLAN ACL
- Configuring VLAN translation
- Configuring virtual interface
- Maintenance
- Configuration examples

## 8.1 Overview of VLAN

### 8.1.1 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 be collapsed. 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.

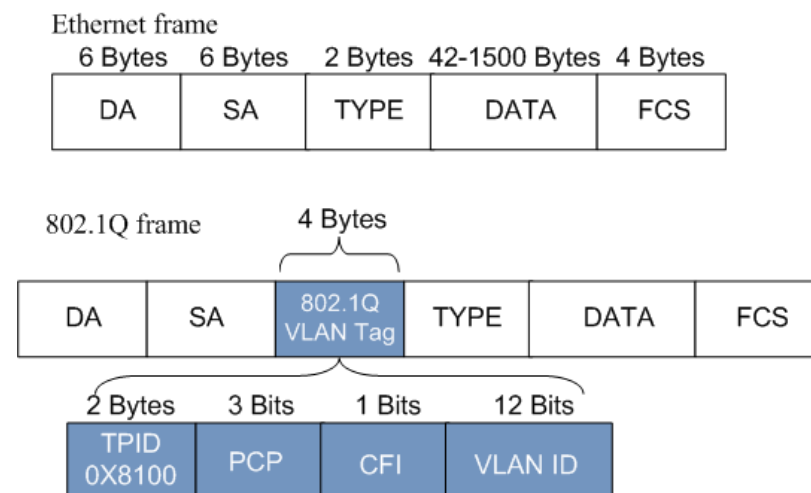
When a frame is sent to the ingress interface of a device, the device will query the VLAN where the ingress interface is and then query the MAC address table to which the VLAN is related. If the destination MAC address of the frame is listed in the MAC address table, the frame will be forwarded. Otherwise, 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 8-1 shows structures of Ethernet frame and 802.1Q frame.

Figure 8-1 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 ISCOM5508 sends packets with higher priorities first.

## VLAN modes of OLT interface

The interface on the ISCOM5508 supports two modes: Access mode and Trunk mode.

Table 8-1 lists compassion of VLAN modes and packet processing modes.

Table 8-1 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.	<ul style="list-style-type: none"> <li>• If the VLAN ID for a packet is identical to the Access VLAN, receive the packet.</li> <li>• If the VLAN ID for a packet is not identical to the Access VLAN, discard the packet.</li> </ul>	If the VLAN ID for a packet is identical to the Access VLAN ID, send the packet after removing the Tag.
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.	<ul style="list-style-type: none"> <li>• If the VLAN ID for a packet is in the VLAN ID list on an interface, receive the packet.</li> <li>• If the VLAN ID for a packet is not in the VLAN ID list on an interface, discard the packet.</li> </ul>	<ul style="list-style-type: none"> <li>• If the VLAN ID for a packet is identical to the Native VLAN ID, send the packet after removing the Tag.</li> <li>• 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.</li> </ul>

## 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 8-2 lists how ONU interfaces to process Ethernet frames in VLAN Transparent mode.

Table 8-2 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 8-3 lists how ONU interfaces to process Ethernet frames in VLAN Tagged mode.

Table 8-3 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).
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 8-4 lists how ONU interfaces to process Ethernet frames in VLAN Translation mode.

Table 8-4 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 8-5 lists how ONU interfaces to process Ethernet frames in VLAN Trunk mode.

Table 8-5 Processing modes of Ethernet frames in VLAN Trunk mode

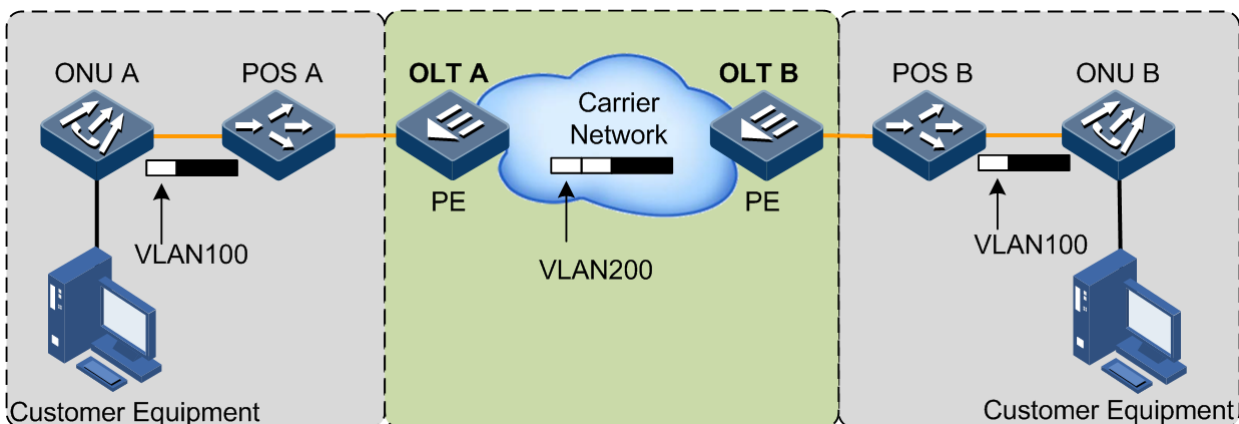
Direction	With/Without Tag	Processing mode
Uplink	With VLAN Tag	If VLANs carried by Ethernet packets are in allowed VLAN list of the interface, forward these Ethernet packets. Otherwise, discard these Ethernet packets.
	Without VLAN Tag	Forward Ethernet packets by adding native VLANs to Untagged packets.
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.

## 8.1.2 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 8-2 Basic QinQ networking



As shown in Figure 8-2, 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.

### 8.1.3 VLAN translation

VLAN translation is mainly used to replace the private VLAN Tags of Ethernet packets with Carrier's VLAN Tags, making packets 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 translation, 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 translation rules. If success, the private VLAN Tags are replaced according to configured VLAN translation rules. VLAN translation provides the following modes:

- 1:1 VLAN translation: the VLAN Tag carried by a packet from a specified VLAN is replaced with a new VLAN Tag.
- N:1 VLAN translation: different VLAN Tags carried by packets from two or more VLANs are replaced with the same VLAN Tag

## 8.2 Configuring VLAN

### 8.2.1 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. The VLANs logically divide the hosts connected to the device. 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 same department has different locations, but hosts in the same department 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 cannot communicate. If hosts in different VLANs need to communicate, use the Layer 3 device such as a router.

## Prerequisite

N/A

## 8.2.2 Default configurations

Default configurations of VLAN on the ISCOM5508 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	<ul style="list-style-type: none"> <li>• Uplink: Access</li> <li>• Downlink: Access</li> </ul>
New priority used by the interface to add VLAN Tag to data	<ul style="list-style-type: none"> <li>• Uplink: 0</li> <li>• Downlink: 0</li> </ul>
Enable/Disable the interface to use a new priority when adding VLAN Tag to data	<ul style="list-style-type: none"> <li>• Uplink: disable</li> <li>• Downlink: disable</li> </ul>
VLAN ID used by the interface to add VLAN Tag to data	<ul style="list-style-type: none"> <li>• Uplink: 1</li> <li>• Downlink: 1</li> </ul>


Default configurations of VLAN on the ONU are as below.

Function	Default value
VLAN mode of UNI	Transparent
Default VLAN of UNI	1
Default priority of UNI	0
VLAN mode of uplink interface	Transparent

## 8.2.3 Configuring VLAN of OLT interface

### Creating VLAN

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#create vlan <i>vlan-id</i> { active   suspend }</b>	<p>Create a VLAN.</p> <p>You can use the <b>no vlan { all   <i>vlan-id</i> }</b> command to delete the VLAN.</p>

Step	Command	Description
3	Raisecom(config)# <b>vlan</b> <i>vlan-id</i>	(Optional) enter VLAN configuration mode.   <b>Note</b> 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.
4	Raisecom(config-vlan)# <b>name</b> <i>name</i>	(Optional) configure the VLAN name. You can use the <b>no name</b> command to restore default configurations.
5	Raisecom(config-vlan)# <b>state</b> { <b>active</b>   <b>suspend</b> }	(Optional) configure the VLAN to be in active or suspended status.



### 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 delete/add interfaces and set VLAN name, etc. The configurations will be saved by the system. Once the VLAN is activated, the configurations will take effect in the system.

## Configuring VLAN modes

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>interface</b> { <b>gigabitethernet</b>   <b>epon-olt</b> } <i>slot-id/port-id</i>	Enter physical interface configuration mode.
3	Raisecom(config-if- <i>*-*:*</i> )# <b>switchport mode</b> { <b>access</b>   <b>trunk</b> }	Configure the VLAN mode of the interface to Access or Trunk. You can use the <b>no switchport mode</b> command to restore default configurations.

## Configuring VLAN of Access interface

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

Step	Command	Description
2	Raisecom(config)# <b>interface</b> { <b>gigabitethernet</b>   <b>epon-olt</b> } <i>slot-id/port-id</i>	Enter physical interface configuration mode.
3	Raisecom(config-if-**-*)# <b>switchport mode access</b>	Configure the VLAN mode of the interface to Access.
4	Raisecom(config-if-**-*)# <b>switchport access vlan</b> <i>vlan-id</i>	Configure the default VLAN for the interface in Access mode.  You can use the <b>no switchport access vlan</b> command to restore default configurations.
5	Raisecom(config-if-**-*)# <b>vlan drop-untagged</b>	(Optional) configure the interface to discard the untagged packet.  You can use the <b>no vlan drop-untagged</b> command to restore default configurations.



### 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 VLAN of Trunk interface

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>interface</b> { <b>gigabitethernet</b>   <b>epon-olt</b> } <i>slot-id/port-id</i>	Enter physical interface configuration mode.
3	Raisecom(config-if-**-*)# <b>switchport mode trunk</b>	Configure the VLAN mode of the interface to Trunk.
4	Raisecom(config-if-**-*)# <b>switchport trunk native vlan</b> <i>vlan-id</i>	Configure the Native VLAN of the interface. You can use the <b>no switchport trunk native vlan</b> command to restore default configurations.
5	Raisecom(config-if-**-*)# <b>switchport trunk allowed vlan</b> { <b>all</b>   [ <b>add</b>   <b>remove</b> ] <i>vlan-list</i> } [ <b>confirm</b> ]	Configure the VLAN allowed to pass by the Trunk interface. You can use the <b>no switchport trunk allowed vlan</b> command to restore default configurations.  <div data-bbox="853 1787 941 1870" data-label="Image"> </div> <b>Note</b> By default, the Trunk interface allows all VLANs to pass.

Step	Command	Description
6	<code>Raisecom(config-if-*:*:*)#switchport trunk untagged vlan { all   [ add   remove ] vlan-list } [ confirm ]</code>	(Optional) configure the untagged VLAN on the Trunk egress interface. You can use the <b>no switchport trunk untagged vlan</b> command to restore default configurations.
7	<code>Raisecom(config-if-*:*:*)#vlan drop-untagged</code>	(Optional) configure the interface to discard the untagged packet. You can use the <b>no vlan drop-untagged</b> command to restore default configurations.



### 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.

## Configuring VLAN ACL

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface { gigabitethernet   ten-gigabitethernet   epon-olt   ten-giga-epon-olt   gpon-olt } slot-id/port-id</code>	Enter physical interface configuration mode.
3	<code>Raisecom(config-if-*:*:*)#switchport vlan-access-list list rule rule-id add { inner   outer } vlan-id</code>	Add VLNA ID for VLAN ACL.
4	<code>Raisecom(config-if-*:*:*)#switchport vlan-access-list list rule rule-id remove inner</code>	Delete the external VLAN ID of VLAN ACL.
5	<code>Raisecom(config-if-*:*:*)#switchport vlan-access-list list rule rule-id translate { inner   outer } vlan to vlan-id</code>	Translate the VLAN ID of VLAN ACL.

## 8.2.4 Configuring VLAN of ONU UNI

### Configuring VLAN modes

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</b>	Enter ONU UNI configuration mode.
3	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)#vlan mode { tagged   translation   transparent   trunk   aggregation }</b>	Configure the VLAN mode of ONU UNI. You can use the <b>no vlan mode</b> command to restore default configurations.

### Configuring VLAN translation rules

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#vlan translation-rule rule-id old vlan-id priority new vlan-id priority</b>	Create the VLAN translation rule. You can use the <b>no vlan translation-rule { rule-id   all }</b> command to delete the VLAN translation rule.
3	<b>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</b>	Enter ONU UNI configuration mode.
4	<b>Raisecom(config-epon-onu-ethernet-*/*/*:*)#vlan translation-rule rule-list</b>	Apply the VLAN translation rule on the ONU UNI. You can use the <b>no vlan translation-rule</b> command to restore default configurations.



#### Note

- The ID and content of a translation rule should be unique.
- The translation rule cannot be modified after being created. If required, you should delete the created translation rule and recreate a new one.
- The translation rule applied on the UNI cannot be deleted. If required, you should cancel the application relationship first.

### Configuring VLAN aggregation rules

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#vlan aggregation-rule rule-id [ name name ] vlan-list vlan-list target vlan-id</b>	Create the VLAN aggregation rule. You can use the <b>no vlan aggregation-rule { all   rule-list }</b> command to delete the configuration.

Step	Command	Description
3	<code>Raisecom(config)#vlan aggregation-rule rule-id name name [ vlan-list vlan-list target vlan-id ]</code>	Configure the name of the VLAN aggregation rule. You can use the <b>no vlan aggregation-rule { all   rule-list }</b> command to delete the configuration.
4	<code>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</code>	Enter ONU UNI configuration mode.
5	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)#vlan aggregation -rule rule-list</code>	Apply the VLAN aggregation rule on the ONU UNI. You can use the <b>no vlan aggregation-rule</b> command to restore default configurations.



### Note

- The ID and content of the translation rule should be unique.
- The translation rule cannot be modified after being created. If required, you should delete the created translation rule and recreate a new one.
- The translation rule applied on the UNI cannot be deleted. If required, you should cancel the application relationship first.

## Configuring default VLAN of UNI

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</code>	Enter ONU UNI configuration mode.
3	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)#native vlan vlan-id [ priority ]</code>	Configure the default VLAN and priority of the ONU UNI. You can use the <b>no native vlan</b> command to restore default configurations.  <div data-bbox="798 1451 890 1538" data-label="Image"> </div> <b>Note</b> This command takes effect only when the VLAN mode is <b>tagged</b> , <b>trunk</b> , or <b>translation</b> .

## Configuring Trunk VLAN

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</code>	Enter ONU UNI configuration mode.

Step	Command	Description
3	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)#vlan trunk allowed <i>vlan-list</i></code>	Configure the allowed VLAN list on the ONU UNI in Trunk mode.  You can use the <b>no vlan trunk allowed</b> command to restore default configurations.

## Configuring QinQ on UNI

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 remote management configuration mode.
3	<code>Raisecom(config-epon-onu-*/*:*)#vlan double-tagging { enable   disable }</code>	Enable/Disable VLAN double tagging of the ONU.
4	<code>Raisecom(config-epon-onu-*/*:*)#vlan double-tagging tpid <i>tpid</i></code>	Configure the TPID of the outer VLAN Tag.

## 8.2.5 Configuring VLAN of ONU SNI

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#epon-onu slot-id/olt-id/onu-id sni</code>	Enter EPON ONU SNI configuration mode.
3	<code>Raisecom(config-epon-onu-sni-*/*:*)#vlan mode { transparent   trunk }</code>	Configure the VLAN mode of the ONU SNI.  You can use the <b>no vlan mode</b> command to restore default configurations.
4	<code>Raisecom(config-epon-onu-sni-*/*:*)#vlan trunk allowed <i>vlan-list</i></code>	Configure the allowed VLAN list on the ONU SNI in Trunk mode.  You can use the <b>no vlan trunk allowed</b> command to restore default configurations.

## 8.2.6 Checking configurations

No.	Command	Description
1	<code>Raisecom#show vlan [ <i>vlan-list</i>   static   dynamic ]</code>	Show VLAN configurations.
2	<code>Raisecom#show vlan [ <i>vlan-list</i> ] member-port</code>	Show information about the VLAN member interface and untagged interface.
3	<code>Raisecom#show epon-onu slot-id/olt-id/onu-list vlan</code>	Show configurations of VLAN Stacking on the ONU.



No.	Command	Description
4	<b>Raisecom#show onu-remote vlan translation-rule [ rule-list ]</b>	Show the created VLAN translation rule on the ONU.
5	<b>Raisecom#show onu-remote vlan aggregation-rule [ rule-list ]</b>	Show the created aggregation rule on the ONU.
6	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uplink vlan</b>	Show VLAN configurations of the uplink interface on the ONU.
7	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet [ uni-id ] vlan</b>	Show VLAN configurations of the Ethernet interface on the ONU.
8	<b>Raisecom#show interface { epon-olt slot-id/olt-id   gigabitethernet slot-id/olt-id   ten-giga-epon-olt slot-id/olt-id } switchport vlan-access-list</b>	Show configurations of VLAN ACL on physical interfaces.

## 8.3 Configuring QinQ

### 8.3.1 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 take transparent transmission without conflicting with the VLAN ID in the Internet Service Provider (ISP)'s network.

#### Prerequisite

N/A

### 8.3.2 Default configurations

Default configurations of QinQ on the ISCOM5508 are as below.

Function	Default value
TPID of outer Tag	0x8100
Basic QinQ	Disable

### 8.3.3 Configuring basic QinQ

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

Step	Command	Description
2	<code>Raisecom(config)#interface { gigabitethernet   epon-olt } slot-id/port-id</code>	Enter physical interface configuration mode.
3	<code>Raisecom(config-if-*:*:*)#vlan dot1q-tunnel</code>	Enable basic QinQ on the interface. You can use the <b>no vlan dot1q-tunnel</b> to disable this function.
4	<code>Raisecom(config-if-*:*:*)#vlan tpid</code>	Configure the TPID of the outer VLAN. You can use the <b>no vlan tpid</b> command to restore default configurations.



### Note

- After QinQ is enabled, the interface processes the received Tagged packets as Untagged packets, namely, add outer VLAN Tags on original packets.
- After QinQ is enabled, configurations for the outer VLAN are the same with those for the general VLAN. For details, see section 8.2.3 Configuring VLAN of OLT interface.

## 8.3.4 Checking configurations

No.	Command	Description
1	<code>Raisecom#show interface [ gigabitethernet   epon-olt ] slot-id/olt-id vlan-mapping</code>	Show QinQ configurations on the interface.

## 8.4 Configuring VLAN ACL

### 8.4.1 Preparing for configurations

#### Scenario

Through the VLAN ACL technology, you can configure the matching rules to flexibly match the source MAC address, SVLAN, CVLAN, CoS, and Ethernet type for Layer 2 packets, and the source IPv4 address, destination IPv4 address, and IP type for Layer 3 packets. Moreover, you can take different operations on packets based on the match, such as adding outer VLAN and modifying inner VLAN.

#### Prerequisite

N/A

### 8.4.2 Default configurations

N/A

### 8.4.3 Creating ACL

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#vlan-access-list</b> <i>list-number</i>	Create a VLAN ACL and enter VLAN ACL configuration mode. You can use the <b>no vlan-access-list</b> <i>acl-number</i> command to delete the ACL.
3	<b>Raisecom(config-vlan-acl)#description</b> <i>desc-string</i>	(Optional) configure descriptions of the VLAN ACL. You can use the <b>no description</b> command to restore default configurations.
4	<b>Raisecom(config-vlan-acl)#rule</b> <i>rule-number</i>	Create a VLAN ACL sub-rule and enter VLAN ACL sub-rule configuration mode. You can use the <b>no rule</b> <i>rule-number</i> command to delete the sub-rule.
5	<b>Raisecom(config-qinq-acl-* rule-*)#access-type</b> { <b>permit</b>   <b>deny</b> }	Configure the access type of the sub-rule.

### 8.4.4 Configuring matching contents

Step	Command	Description
1	<b>Raisecom(config-qinq-acl-* rule-*)#match mac source</b> <i>mac-address</i> [ <i>mask</i> ]	(Optional) match the source MAC address.
2	<b>Raisecom(config-qinq-acl-* rule-*)#match</b> { <b>svlan</b> <i>vlan-id</i>   <b>svlan-cos</b> <i>cos</i> }	(Optional) match the SVLAN ID and CoS value.
3	<b>Raisecom(config-qinq-acl-* rule-*)#match</b> { <b>cvlan</b> <i>vlan-id</i>   <b>cvlan-cos</b> <i>cos</i> }	(Optional) match the CVLAN ID and CoS value.
4	<b>Raisecom(config-qinq-acl-* rule-*)#match ethertype</b> { <i>frame-type frame- type-mask</i>   <b>arp</b>   <b>eapol</b>   <b>flowcontrol</b>   <b>ip</b>   <b>ipv6</b>   <b>loopback</b>   <b>mpls</b>   <b>mpls- mcast</b>   <b>pppoe</b>   <b>pppoedisc</b>   <b>x25</b>   <b>x75</b> }	(Optional) match the protocol type of the Layer 2 frame head.
5	<b>Raisecom(config-qinq-acl-* rule-*)#match ip</b> { <b>destination-address</b>   <b>source-address</b> } <i>ip-address</i> [ <i>mask</i> ]	(Optional) match the source and destination IP address.
6	<b>Raisecom(config-qinq-acl-* rule-*)#match ip protocol</b> { <i>protocol-num</i>   <b>ahp</b>   <b>esp</b>   <b>gre</b>   <b>icmp</b>   <b>igmp</b>   <b>igrp</b>   <b>ipinip</b>   <b>ospf</b>   <b>pcp</b>   <b>pim</b>   <b>tcp</b>   <b>udp</b> }	(Optional) match the IP upper protocol type.


Step	Command	Description
7	Raisecom(config-qinq-acl-* -rule-*)#match ip tcp { destination-port   source-port } { port-id   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/source interface ID of the TCP packet. You can use the <b>no match ip tcp { destination-port   source-port }</b> command to delete the configuration.
8	Raisecom(config-qinq-acl-* -rule-*)#match ip udp { destination-port   source-port } { port-id   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/source interface ID of the UDP packet. You can use the <b>no match ip udp { destination-port   source-port }</b> command to delete the configuration.

### 8.4.5 Configuring matching actions

Step	Command	Description
1	Raisecom(config-qinq-acl-* -rule-*)#add { outer   inner } vlan-id	(Optional) add a VLAN. You can use the <b>no add { outer   inner }</b> command to delete the configuration.
2	Raisecom(config-qinq-acl-* -rule-*)#remove inner	(Optional) remove a VLAN. You can use the <b>no remove inner</b> command to delete the configuration.
3	Raisecom(config-qinq-acl-* -rule-*)#translate { outer   inner } vlan to vlan-id	(Optional) translate a VLAN. You can use the <b>no translate { outer   inner } vlan</b> command to delete the configuration.
4	Raisecom(config-qinq-acl-* -rule-*)#translate outer cos to cos	(Optional) modify the CoS value. You can use the <b>no translate outer cos</b> command to delete the configuration.

### 8.4.6 Applying ACL

Step	Command	Description
1	Raisecom(config)#interface { gigabitethernet   epon-olt } slot-id/port-id	Enter physical interface configuration mode.

Step	Command	Description
2	<code>Raisecom(config-if-*:*:*)#vlan-access-list list-num</code>	<p>Apply the VLAN ACL to an interface.</p> <p>You can use the <b>no vlan-access-list list-num</b> command to delete the VLAN ACL.</p> <div>  <b>Note</b> </div> <p>Applying the VLAN ACL on an interface refers to processing packets on the ingress interface only without affecting packets on the egress interface.</p>

## 8.4.7 Checking configurations

No.	Command	Description
1	<code>Raisecom#show vlan-access-list { all   acl-num }</code>	Show VLAN ACL configurations.
2	<code>Raisecom#show interface [ gigabitethernet   epon-olt ] slot-id/olt-id vlan-access-list</code>	Show the applied VLAN ACL on the interface.

## 8.5 Configuring VLAN translation

### 8.5.1 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.

### 8.5.2 Default configurations

Default configurations of VLAN translation on the ISCOM5508 are as below.

Function	Default value
VLAN translation	Enable

### 8.5.3 Configuring VLAN translation

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <b>{ gigabitethernet   epon-olt }</b> <i>slot-id/port-id</i>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-**-*)#vlan-</b> <b>mapping cos-aware</b>	Configure CoS-aware VLAN translation, that is, VLAN+CoS translation.  You can use the <b>no vlan-mapping cos-aware</b> command to disable this function.
4	<b>Raisecom(config-if-**-*)#vlan-</b> <b>mapping { egress   ingress }</b> <b>drop-unmatched</b>	Drop packets unmatched with VLAN translation rules.  You can use the <b>no vlan-mapping { egress   ingress }</b> <b>drop-unmatched</b> command to disable this function.

### 8.5.4 Configuring 1:1 VLAN translation

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <b>{ gigabitethernet   epon-olt }</b> <i>slot-</i> <i>id/port-id</i>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-**-*)#vlan-</b> <b>mapping{ ingress   egress } outer</b> <i>before-outer translate outer after-</i> <i>outer inner { add vlan-id   remove  </i> <i>vlan-id   unchange }</i>	Configure 1:1 VLAN translation rules based on the ingress/egress interface (only the outer VLAN Tag is translated).
4	<b>Raisecom(config-if-**-*)#vlan-</b> <b>mapping{ ingress   egress } outer</b> <i>before-outer inner before-inner</i> <b>translate outer after-oute inner</b> <i>{ vlan-id   remove }</i>	Configure 1:1 VLAN translation rules based on the ingress/egress interface (both the outer and inner VLAN Tags are translated).

### 8.5.5 Configuring N:1 VLAN translation

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <b>{ gigabitethernet   epon-olt }</b> <i>slot-</i> <i>id/port-id</i>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-**-*)#vlan-mapping</b> <b>outer before-vlan aggregate outer after-</b> <i>vlan inner { add vlan-id   unchange }</i>	Configure N:1 VLAN translation rules based on interface (the outer VLAN Tag is translated and the inner VLAN Tag is added).

Step	Command	Description
	<b>Raisecom(config-if-*:*)#vlan-mapping outer before-outer inner before-innerlist aggregate outer after-outer inner { vlan- id   remove }</b>	Configure N:1 VLAN translation rules based on interface (both the outer and inner VLAN Tags are translated).

## 8.5.6 Configuring translation rules based on VLAN+CoS

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface { gigabitethernet   epon-olt } slot- id/port-id</b>	Enter physical interface configuration mode.
3	<b>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 }</b>	Configure VLAN translation rules based on VLAN+CoS and the ingress interface.  You can use the <b>no vlan-mapping { ingress   egress } cos-aware outer before-outer before-cos translate</b> command to cancel this application.

## 8.5.7 Checking configurations

No.	Command	Description
1	<b>Raisecom#show interface { epon-olt   gigabitethernet } slot-id/port-id vlan-mapping { ingress   egress } translate</b>	Show 1:1 VLAN translation rules on the egress interface.
2	<b>Raisecom#show interface { epon-olt   gigabitethernet } slot-id/port-id vlan-mapping aggregate</b>	Show N:1 VLAN translation rules based on interface.
3	<b>Raisecom#show interface { epon-olt   gigabitethernet } slot-id/port-id vlan-mapping cos- aware aggregate</b>	Show translation rules based on VLAN+CoS on the interface.

## 8.6 Configuring virtual interface

### 8.6.1 Preparing for configurations

#### Scenario

VLAN translation is different from QinQ. Through VLAN translation, the VLAN Tag is changed instead of adding multiple layers of VLAN Tags. So the length of the packet is not increased and the packet can be transmitted according to the VLAN forwarding rule of the carrier. VLAN translation can be used in the following scenarios:

- Translate the VLAN ID of the user service to that of the carrier.
- Translate VLAN IDs of multiple user services to the same VLAN ID of the carrier.

## Prerequisite

N/A

## 8.6.2 Default configurations

Default configurations of the virtual interface on the ISCOM5508 are as below.

Function	Default value
VLAN mode of virtual interface	Transparent
Native VLAN	VLAN 1

## 8.6.3 Configuring VLAN of virtual interface

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface epon-onu slot-id/port-id/onu-id</b>	Enter EPON ONU remote management mode.
3	<b>Raisecom(config-if-epon-onu-*/*:*)#vlan mode { transparent   trunk }</b>	Configure the VLAN mode of the virtual interface.  You can use the <b>no vlan-mode</b> command to restore default configurations.
4	<b>Raisecom(config-if-epon-onu-*/*:*)#native vlan vlan-id</b>	Configure the Native VLAN of the virtual interface.  You can use the <b>no vlan native</b> command to restore default configurations.

## 8.6.4 Configuring basic QinQ on virtual interface

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface epon-onu slot-id/port-id/onu-id</b>	Enter EPON ONU remote management mode.
3	<b>Raisecom(config-if-epon-onu-*/*:*)#vlan dot1q-tunnel</b>	Enable basic QinQ on the virtual interface.  You can use the <b>no vlan dot1q-tunnel</b> command to disable this function.



## 8.6.5 Configuring VLAN translation on virtual interface

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface epon-onu slot-id/port-id/onu-id</b>	Enter EPON ONU remote management mode.
3	<b>Raisecom(config-if-epon-onu-*//*:*)#vlan-mapping { ingress   egress } outer vlan-id translate outer vlan-id</b>	Configure 1:1 VLAN translation on the virtual interface.  You can use the <b>no vlan-mapping { ingress   egress } outer vlan-id translate</b> command to delete the configuration.
4	<b>Raisecom(config-if-epon-onu-*//*:*)#vlan-mapping outer vlan-id aggregate outer vlan-id</b> <b>Raisecom(config-if-epon-onu-*//*:*)#vlan-mapping outer form vlan-id to vlan-id aggregate outer vlan-id [ inner copy-form-outer ]</b>	Configure N:1 VLAN translation on the virtual interface.  You can use the <b>no vlan-mapping { ingress   egress } outer vlan-id translate</b> command to delete the configuration.

## 8.6.6 Checking configurations

No.	Command	Description
1	<b>Raisecom#show interface epon-onu slot-id/port-id/onu-list vlan</b>	Show configurations of the virtual interface.
2	<b>Raisecom#show interface epon-onu slot-id/port-id/vport-list vlan-mapping { ingress   egress } translate</b>	Show 1:1 VLAN translation rules on the virtual interface.
3	<b>Raisecom#show interface epon-onu slot-id/port-id/vport-list vlan-mapping aggregate</b>	Show N:1 VLAN translation rules on the virtual interface.

## 8.7 Maintenance

Command	Description
<b>Raisecom(config)#clear epon-onu slot-id/olt-id/onu-id uni ehernet uni-id statistic</b>	Clear statistics on the ONU UNI.

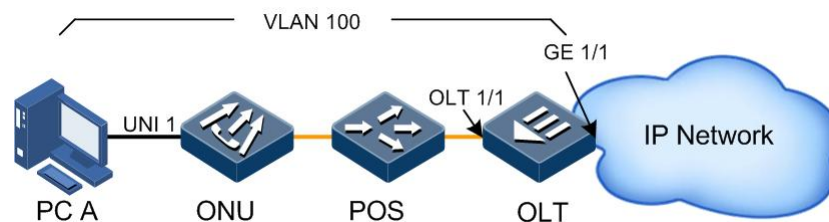
## 8.8 Configuration examples

### 8.8.1 Example for configuring VLAN

#### Networking requirements

As shown in Figure 8-3, the user connects the ONU through the interface UNI 1, and the user VLAN is 100. The OLT connects the IP network through the interface GE 1/1, and connects the ONU through the PON interface OLT 1/1. Under this network topology structure, open the data service.

Figure 8-3 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 GE interface VLAN.

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

Step 3 Configure the PON interface VLAN.

```
Raisecom(config)#interface epon-olt 1/1  
Raisecom(config-if-epon-olt-1:1)#switchport mode trunk  
Raisecom(config-if-epon-olt-1:1)#switchport trunk allowed vlan 100  
Raisecom(config-if-epon-olt-1:1)#end
```

Step 4 Configure ONU auto-registration.

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

- Configure the ONU.

Step 5 Configure user data VLAN.

```
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 100
Raisecom(config-epon-onu-ethernet-1/1/1:1)#end
```

## Checking results

Show VLAN configurations of the interface GE 1/1 and PON interface on the OLT respectively.

```
Raisecom#show interface gigabitethernet 1/1 vlan
Port: 1/1
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 1/1 vlan
Port: 1/1
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					
-----					
1/1/1	000e.5e0a.7a0e	auto	2000-01-01,08:00	ISCOM5104(C)	active
oam					

Show UNI VLAN configurations on the ONU.

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

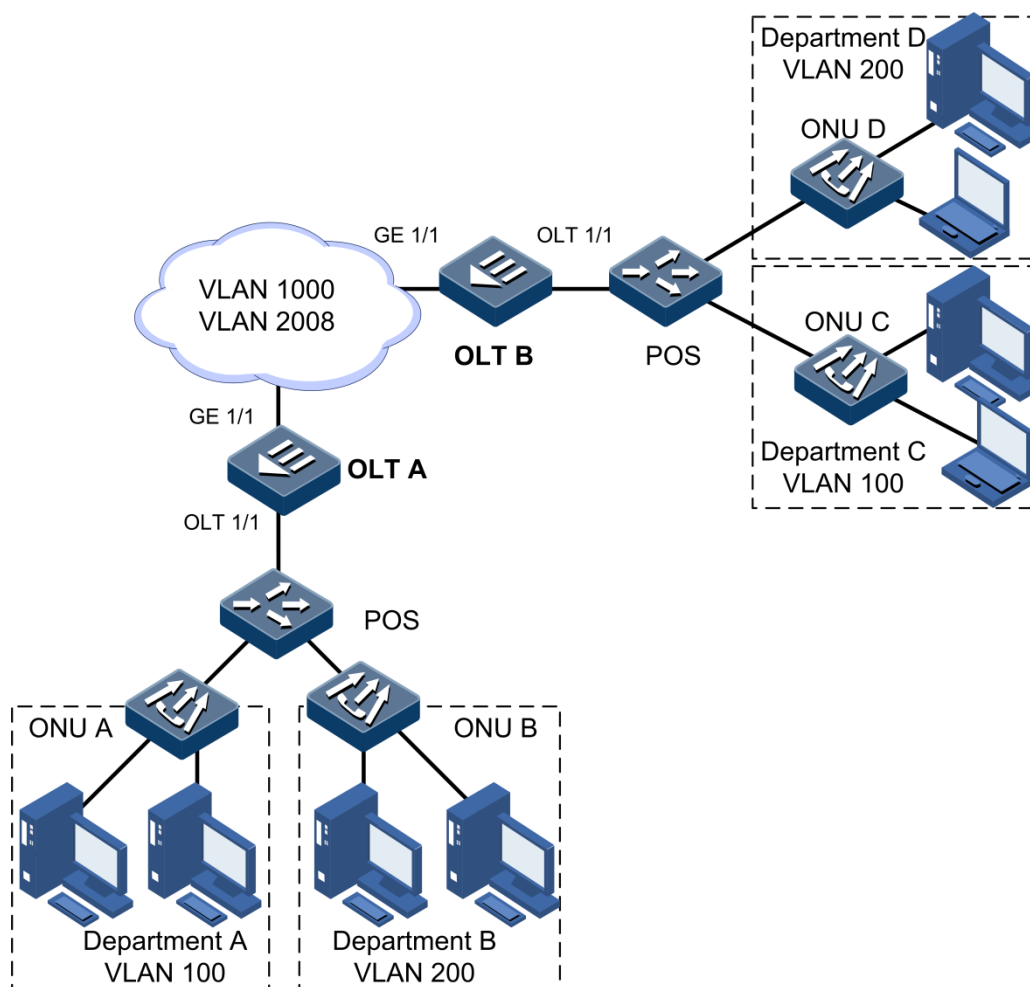
## 8.8.2 Example for configuring VLAN translation

### Networking requirements

As shown in Figure 8-4, OLT A connects Department A in VLAN 100 and Department B in VLAN 200 through the interface OLT 1/1; OLT B connects Department C in VLAN 100 and Department D in VLAN 200 through the interface OLT 1/1. 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 translation on OLT A and OLT B to realize proper communication between the PC user or terminal user, and the server.

Figure 8-4 Configuring VLAN translation



## 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 the uplink interface GE 1/1 to Trunk mode and allow VLAN 1000 and VLAN 2008 to pass.

```
Raisecom(config)#interface gigabitethernet 1/1  
Raisecom(config-if-gigabitethernet-1:1)#switchport mode trunk  
Raisecom(config-if-gigabitethernet-1:1)#switchport trunk allowed vlan 1000,2008 confirm  
Raisecom(config-if-gigabitethernet-1:1)#exit
```

- Step 3 Configure the interface OLT 1/1 to Trunk mode and allow VLAN 100 and VLAN 200 to pass, and enable VLAN translation.

```
Raisecom(config)#interface epon-olt 1/1
Raisecom(config-if-epon-olt-1:1)#switchport mode trunk
Raisecom(config-if-epon-olt-1:1)#switchport trunk allowed vlan 100,200
confirm
Raisecom(config-if-*-*:*)#vlan-mapping ingress outer 1000 inner 100 outer
translate 1000 inner unchanged
Raisecom(config-if-*-*:*)#vlan-mapping egress outer 1000 inner 100 outer
translate 1000 inner unchanged
Raisecom(config-if-*-*:*)#vlan-mapping ingress outer 2008 inner 200 outer
translate 2008 inner unchanged
Raisecom(config-if-*-*:*)#vlan-mapping egress outer 2008 inner 200 outer
translate 2008 inner unchanged
```

## Checking results

Use the **show interface epon-olt slot-id/olt-id vlan-mapping { ingress | egress }** command to show 1:1 VLAN translation configurations.

```
Raisecom#show interface epon-olt 1/1 vlan-mapping egress
```

	old		New		IVLAN
Port ID	OVID	IVID	OVID	IVID	Mapping Action
epon-olt1/1	1000	100	1000	100	unchanged

```
Raisecom#show interface epon-olt 1/1 vlan-mapping ingress
```

	old		New		IVLAN
Port ID	OVID	IVID	OVID	IVID	Mapping Action
epon-olt1/1	1000	100	1000	100	add

# 9 Configuring spanning tree

---

This chapter introduces the spanning tree feature and configuration process of the ISCOM5508, and provides related configuration examples, including the following sections:

- Overview of spanning tree
- Configuring STP
- Configuring MSTP
- Configuring ONU RSTP
- Maintenance
- Configuration examples

## 9.1 Overview of spanning tree

### 9.1.1 STP

When you establish a network, you often need to create a redundant topology at a specified location to provide link backup and improve reliability. In addition, loops are generated in a network due to redundant links.

After a loop topology is generated between two devices, when these 2 devices send broadcast packets, these broadcast packets will be transmitted in the loop topology, resulting in a broadcast storm. The broadcast storm can reduce network performance, even worse, making the whole network collapsed.

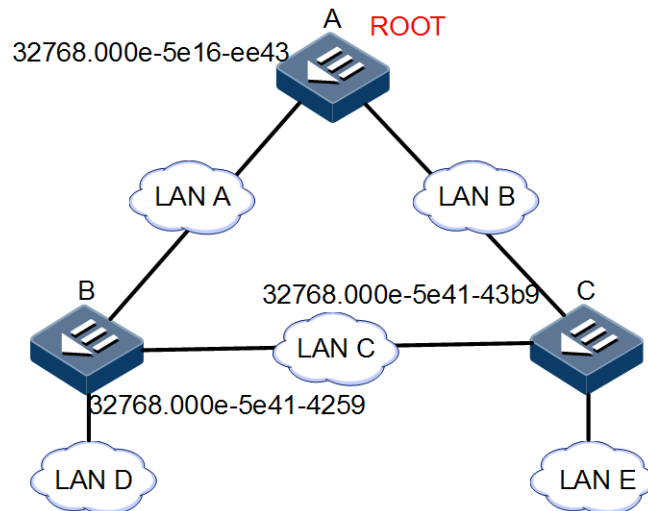
Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology and data link backup. Devices, where STP runs, learn related parameters about each other by exchanging Bridge Protocol Data Units (BPDUs) and logically block loops with specified STP algorithm to prevent broadcast storm. When an unblocked link fails, the previously-blocked link is re-activated to act as a backup link.

The working process of STP is divided into the following steps:

- Select a root bridge. The device selects a root bridge based on bridge IDs. The root bridge is the bridge with the smallest bridge ID. The bridge ID contains both bridge priority and the MAC address. By default, the bridge priority is set to 32768. The administrator can modify the bridge priority. To select a root bridge, the priority is compared first. The bridge with the smaller priority is the root bridge. If two bridges have equal priority, then the MAC addresses are compared. The bridge with the smaller

MAC address is the root bridge. As shown in Figure 9-1, by comparing bridge IDs (bridge priority + MAC address) of all devices, Device A is selected as a root bridge.

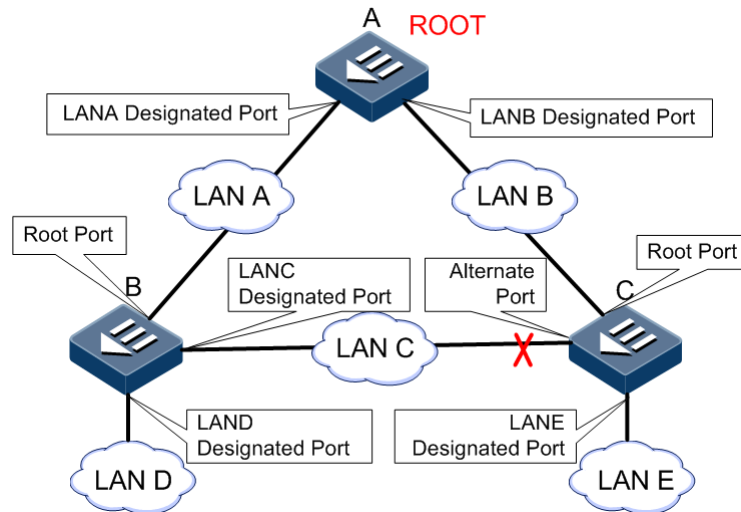
Figure 9-1 STP (selecting a root bridge)



- Select a root port. STP selects a root port on each non-root bridge. The root port can send and receive data flow. STP selects the port with the smallest cost (a least-cost path) as the root port. When path costs of multiple ports are identical, STP selects the port with smaller bridge ID as the root port. If bridges IDs are identical, STP selects the port with smaller port identifier as the root port. As described above, the uplink ports of Device B and Device C in Figure 9-2 shows root ports.
- Select a designated port. STP selects a designated port at each network segment. Ports on the root bridge are designated ports. STP selects a designated port based on the following items in order: path cost, bridge ID, and port identifier. STP selects the port with the smallest cost (a least-cost path) as the designated port. When path costs are identical, STP selects a designated port based on bridge IDs and then based on port identifier. As shown in Figure 9-2, the port at the right side of Device B is selected as a designated port.
- Block an alternate port. Alternate ports are ports that are not the root port or designated ports. Alternated ports are in blocked status and cannot forward data. As shown in Figure 9-2, the port at the left side of Device C is selected as an alternate port, which will be blocked.



Figure 9-2 STP (confirming ports)



## 9.1.2 RSTP

Rapid Spanning Tree Protocol (RSTP) can be seen as an evolution of the 8STP. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this. RSTP was designed to be backwards-compatible with standard STP.

## 9.1.3 MSTP

With quick development and wide application of VLAN technology, defects of the STP/RSTP are exposed gradually. STP/RSTP regards the whole network as a single spanning tree, leading to following problems:

- Some blocked links do not carry any traffic, consuming bandwidth.
- After a link is blocked, packets of some VLANs may not be forwarded.

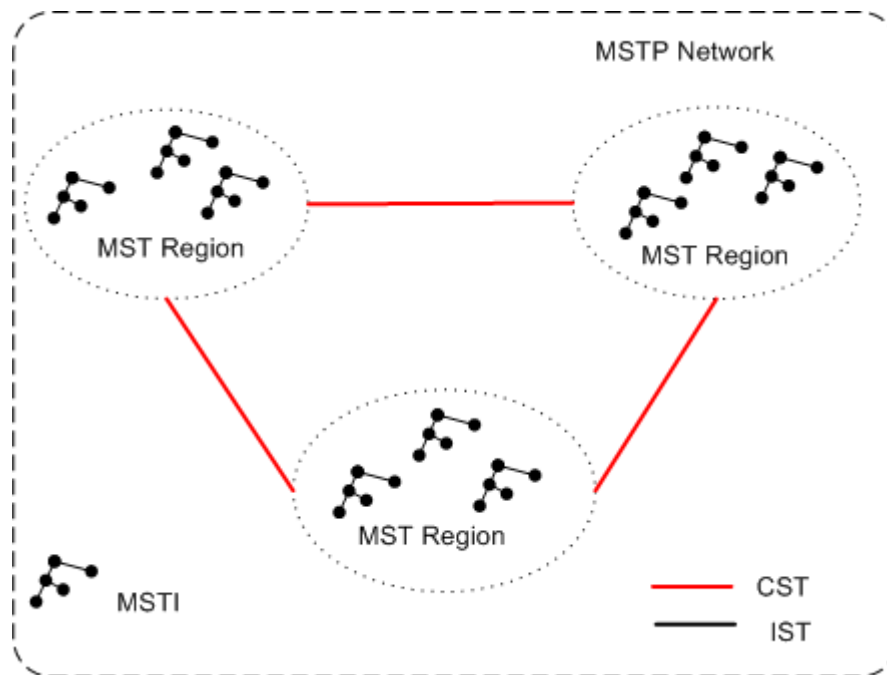
To solve the above problems, IEEE defines the 802.1s Multiple Spanning Tree Protocol (MSTP). The MSTP provides significantly faster spanning tree convergence. In addition, the MSTP ensures traffic in different VLANs being forwarded along their own paths. It provides good load sharing mechanism.

The MSTP partitions a switching network into multiple regions, which are called MST regions. Each MST region can have multiple spanning trees, which are independent. Each spanning tree is called a Multiple Spanning Tree Instance (MSTI). MST regions are interconnected through a single spanning tree. This single spanning tree is called a Common Spanning Tree (CST). CST is used to ensure a loop-free and connected network.

You can map different VLANs to different MSTIs as required. The MSTP relates VLANs to MSTIs through the VLAN translation table (the relationship table of VLANs and MSTIs).

In each MST region, there is an MSTI whose ID is set to 0. This MSTI and CST make up of a Common Internal Spanning Tree (CIST). The CIST makes MST regions, bridges and network segments in these MST regions a fully-connected and loop-free tree. Figure 9-3 shows the relationship among MST regions, MSTIs, and CSTs.

Figure 9-3 MSTP

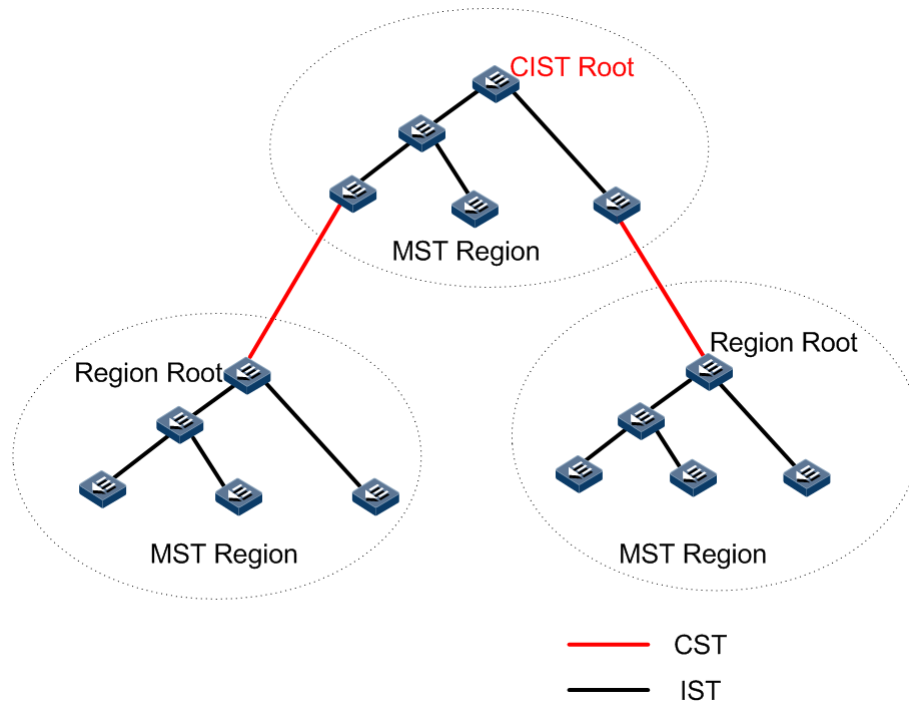


## Related concepts of MSTP

The MSTP introduces multiple new concepts and names. Figure 9-4 shows locations of related names.

- CST: a spanning tree used to connect all MST regions in a network
- IST: a spanning tree in a MST region. IST is a special MSTI. In general, it is MSTI0.
- CIST: a single spanning tree that is generated through STP/RSTP. It is used to connect all devices in a switching network. ISTs in all MST regions and CST compose a complete single spanning tree.
- Single Spanning Tree (SST): when only one device is in a MST region, this device is a SST. When you take a MST region as a device, the MSTP network is a SST.
- MST region: a MST region is composed by multiple devices in a LAN and network segments among these devices. In a LAN, there can be multiple MST regions. These MST regions are directly/indirectly connected in physical. You can partition multiple devices into a MST region through MSTP configuration commands.
- VLAN translation table: the MSTP connects VLANs and MSTIs by configuring a VLAN translation table (the relationship table of VLANs and MSTIs).
- MSTI: a spanning tree is a MST region. MSTIs are independent. A MSTI can relate to one or more VLANs. However, a VLAN is related to a MSTI only.
- Region root: consists of an IST region root and a MSTI region root. IST region root refers to the device with smallest path cost to the root device in ISTs. MSTI region roots refer to roots of all MSTIs.
- Master bridge: a device that is most closed to the root bridge in a MST region. If the root device is in the MST region, the root device is the master bridge of the MST region.

Figure 9-4 Basic concepts of MSTP



## Port roles of MSTP

Ports of a device where MSTP is enabled work as one of the following roles:

- Root port: on a non-root device, the port with the smallest path cost to the root device is a root port of the device. The root port is used to forward data to the root device.
- Designated port: for a non-root device, the designated port is a port (except for the root port) that has the least-cost to the root bridge. All ports on the root bridge are designated ports.
- Edge port: if a designated port is located at the edge of a region and is not connected to any device, this port is called an edge port. In general, the edge port is directly connected to user devices.
- Alternate port: in terms of sending BPDUs, the Alternate port is a port that is blocked because of learning BPDUs sent by other devices. In terms of forwarding traffic, the Alternate port provides a backup path between a designated device and a root device. The Alternative port is backup port of the root port. If the root port is blocked, the Alternative port will become a new root port.
- Backup port: a loop is generated when two ports of a device is connected. The device will block one port. The backup port is the one that is blocked. In terms of sending BPDUs, the Backup port is a port that is blocked because of learning BPDUs sent by itself. In terms of forwarding traffic, as a backup of the designated port, the Backup port provides a backup path between a root device and a leaf node.
- Master port: a port that is on the shortest path of all paths connecting the MST region and the root device. It is a port that is used to connect a MST region and the root device.
- Region edge port: a port that locates at the edge of a MST region and that is used to connect other MST regions. Or it is a port that is used to connect related regions where STP/RSTP runs.

When you perform MSTP computation, roles of region edge ports on MSTI and CIST should be consistent. If the region edge port on the CIST is a master port (the port used to connect the region to the root device), it acts as a master port on all MSTIs in the region.



## Note

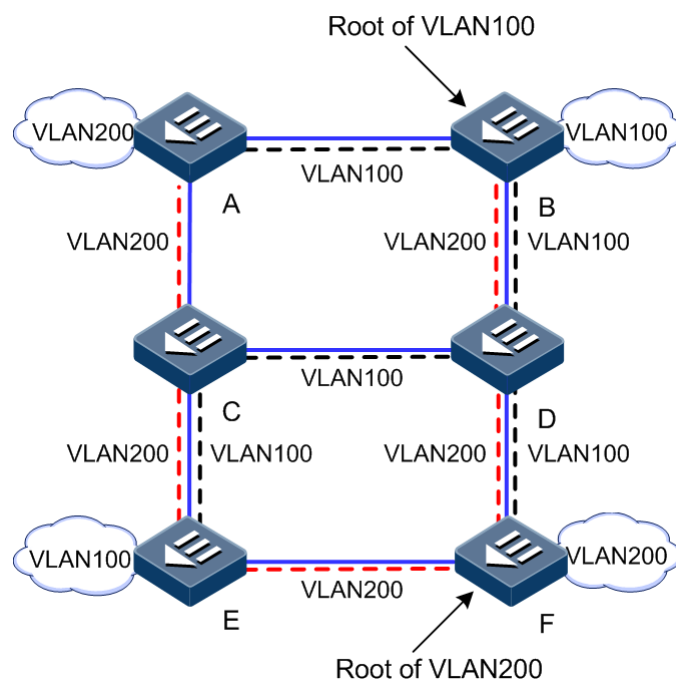
Each VLAN is related to one MSTI only. It means data of the same VLAN can be transmitted in a MSTI only. However, one MSTI can be related to multiple VLANs.

After applying MSTP to a network as shown in Figure 9-5, 2 spanning trees are generated after computation:

- MSTI 1 takes Device B as the root device, forwarding packets with VLAN 100.
- MSTI 2 takes Device F as the root device, forwarding packets with VLAN 200.

Therefore, devices in a VLAN can communicate with each other. In addition, packets of different VLANs are forwarded along different paths. It helps realize load sharing.

Figure 9-5 MSTIs in a MST region



## 9.2 Configuring STP

### 9.2.1 Preparing for configurations

#### Scenario

In a large-scale LAN, multiple devices are cascaded together to meet the need to access each other. You can enable STP on these devices to avoid loops due to device cascade, MAC address learning faults, and broadcast storm caused by quick copy and transmission of data

frames. Through the STP calculation, you can block some interface in a loop to ensure that there is only one path from data flow to destination host.

## Prerequisite

Configure physical parameters of the interface and make the interface Up at the physical layer.

## 9.2.2 Default configurations

Default configurations of STP on the ISCOM5508 are as below.

Function	Default value
Global STP	Disable
Port STP	Enable
System STP priority	32768
Port STP priority	128
Port path cost	0

## 9.2.3 Enabling STP

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree mode stp</b>	Configure the spanning tree mode to STP.
3	<b>Raisecom(config)#spanning-tree</b>	Enable global STP. You can use the <b>no spanning-tree</b> command to disable this function.
4	<b>Raisecom(config)#interface gigabitethernet slot-id/port-id</b>	Enter physical interface configuration mode.
5	<b>Raisecom(config-if-gigabitethernet-*)#spanning-tree</b>	(Optional) enable port STP.

## 9.2.4 Configuring STP parameters

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree [ instance instance-id ] priority priority</b>	(Optional) configure system priority. You can use the <b>no spanning-tree [ instance instance-id ] priority</b> command to restore default configurations.

Step	Command	Description
3	Raisecom(config)# <b>spanning-tree</b> [ <b>instance</b> <i>instance-id</i> ] <b>root</b> { <b>primary</b>   <b>secondary</b> }	(Optional) configure the device as the root device or backup root device. You can use the <b>no spanning-tree</b> [ <b>instance</b> <i>instance-id</i> ] <b>root</b> command to restore default configurations.
4	Raisecom(config)# <b>interface</b> <b>gigabitethernet</b> <i>slot-id/port-id</i>	Enter physical interface configuration mode.
5	Raisecom(config-if-gigabitethernet- *:*)# <b>spanning-tree</b> [ <b>instance</b> <i>instance-id</i> ] <b>priority</b> <i>priority-value</i>	(Optional) configure the port priority. You can use the <b>no spanning-tree</b> [ <b>instance</b> <i>instance-id</i> ] <b>priority</b> command to restore default configurations.
6	Raisecom(config-if-gigabitethernet- *:*)# <b>spanning-tree</b> [ <b>instance</b> <i>instance-id</i> ] <b>inter-path-cost</b> <i>cost-value</i>	(Optional) configure the internal port path cost. You can use the <b>no spanning-tree</b> [ <b>instance</b> <i>instance-id</i> ] <b>inter-path-cost</b> command to restore default configurations.
7	Raisecom(config-if-gigabitethernet- *:*)# <b>spanning-tree</b> <b>extern-path-cost</b> <i>cost-value</i>	(Optional) configure the external port path cost. You can use the <b>no spanning-tree</b> <b>extern-path-cost</b> command to restore default configurations.

## 9.2.5 Checking configurations

No.	Command	Description
1	Raisecom# <b>show spanning-tree</b> [ <b>instance</b> <i>instance-id</i> ] [ <b>detail</b> ]	Show STP basic configurations.

## 9.3 Configuring MSTP

### 9.3.1 Preparing for configurations

#### Scenario

In a large-scale LAN or community aggregation network, aggregation devices make up a ring for link backup, which avoids loopback and realize service load sharing at the same time. The MSTP can select different and unique forwarding path for each VLAN or a group of VLANs.

#### Prerequisite

Configure physical parameters of the interface and make the interface Up at the physical layer.

### 9.3.2 Default configurations

Default configurations of MSTP on the ISCOM5508 are as below.

Function	Default value
Global MSTP	Disable
Port MSTP	Enable
Maximum number of hops in MST domain	20
System priority	32768
Port priority	128
Port path cost	0
Maximum number of packets sent within in a Hello time	3
Max-Age timer	20s
Hello-Time timer	2s
Forward-Delay timer	15s
Revision level of MST domain	0

### 9.3.3 Enabling MSTP

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree mode mstp</b>	Configure the spanning tree mode to MSTP.
3	<b>Raisecom(config)#spanning-tree</b>	Enable global MSTP.
4	<b>Raisecom(config)#interface gigabitethernet slot-id/port-id</b>	Enter physical interface configuration mode.
5	<b>Raisecom(config-if-gigabitethernet- *:*)#spanning-tree</b>	(Optional) enable port MSTP.

### 9.3.4 Configuring MST domain and maximum number of hops

You can configure domain information for the device when it is running in MSTP mode. The MST domain depends on the domain name, VLAN mapping table, and MSTP revision level. You can configure current device to a specific MST domain through following configurations.

The maximum number of hops confines the scale of the MST domain. Starting from the root bridge in the domain, the BPDU reduces 1 hop once it is forwarded through a device; the BPDU will be discarded when the number of hop is 0. In this case, the device out of the maximum number of hops cannot take part in spanning tree calculation, thus defining the scale of the MST domain.

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

Step	Command	Description
2	<b>Raisecom(config)#spanning-tree max-hops</b> <i>hops-value</i>	(Optional) configure the maximum number of hops of the MST domain.  You can use the <b>no spanning-tree max-hops</b> command to restore default configurations.
3	<b>Raisecom(config)#spanning-tree region-configuration</b>	Enter MST domain configuration mode.
4	<b>Raisecom(config-region)#name</b> <i>name</i>	(Optional) configure the MST domain name.  You can use the <b>no name</b> command to restore default configurations.
5	<b>Raisecom(config-region)#revision-level</b> <i>level-value</i>	(Optional) configure the revision level of the MST domain.  You can use the <b>no revision-level</b> command to restore default configurations.
6	<b>Raisecom(config-region)#instance</b> <i>instance-id</i> <b>vlan</b> <i>vlan-list</i>	(Optional) configure mapping between the MST domain VLAN and the instance.  You can use the <b>no instance</b> <i>instance-id</i> [ <b>vlan</b> <i>vlan-list</i> ] command to restore default configurations.



## Note

Only when the device is the domain root, the configured maximum number of hops is that of the MST domain; configurations on non-domain root bridges do not take effect.

### 9.3.5 Configuring root bridge and backup root bridge

Two modes for MSTP root bridge selection: one is to configure the system priority and confirm the STP root bridge or backup root bridge through STP calculation; the other is to assign the root bridge or backup root bridge directly by commands.

When the root bridge fails or is powered off, the backup root bridge can replace the root bridge for related instances. In this case, if you have configured a new root bridge, the backup bridge will recover from the root bridge. If you have configured multiple backup bridges for a spanning tree instance, once the root bridge stops working, MSTP will choose the backup root bridge with the smallest bridge ID (composed by system priority and MAC address) as the root bridge.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree [ instance</b> <i>instance-id</i> <b>] root { primary   secondary }</b>	Configure the device as the root bridge or backup root bridge.  You can use the <b>no panning-tree [ instance</b> <i>instance-id</i> <b>] root</b> command to restore default configurations.



## Caution

We recommend that you had better not modify the system priority of any device in the network if you adopt the mode of assigning the root bridge directly; otherwise, the assigned root bridge or backup root bridge may be invalid.

## Note

- You can make sure the effective instance of a root bridge or backup root bridge through the instance-id parameter. If the value of the instance-id is 0 or this parameter is omitted, the current device will be designated as the root bridge or backup root bridge of CIST.
- The device root types in instances are independent mutually. That is, they not only can be the root bridge or backup root bridge of one instance, but also the root bridge or backup root bridge of other spanning tree instances. However, in the same spanning tree instance, the same device cannot be used as both root bridge and backup root bridge simultaneously.
- You cannot assign two or more root bridges for one spanning tree instance, but can assign multiple backup bridges for one spanning tree. Generally, we recommend you to assign one root bridge and multiple backup root bridges for one spanning tree.

### 9.3.6 Configuring system priority and port priority

Whether a port is selected as the root port depends on its priority if the path cost to the root bridge is identical. The smaller the port priority is, the more preferentially the port is selected as the root port. A port may have different priorities and play different roles in different instances.

The device Bridge ID decides whether it can be selected as the root of a spanning tree. Configure a smaller priority to get a smaller device Bridge ID and reach the purpose to designate some device as the root of a spanning tree. If the priority is identical, the device with smaller MAC address will be selected as the root.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree [ instance instance-id ] priority priority-value</b>	Configure the system priority. You can use the <b>no spanning-tree [ instance instance-id ] priority</b> command to restore default configurations.
3	<b>Raisecom(config)#interface gigabitethernet slot-id/port-id</b>	Enter physical interface configuration mode.
4	<b>Raisecom(config-if-gigabitethernet-*:*)#spanning-tree [ instance instance-id ] priority priority-value</b>	Configure the port priority. You can use the <b>no spanning-tree [ instance instance-id ] priority</b> command to restore default configurations.



## Note

The priority must be a multiple of 4096, such as 0, 4096, and 8192, and the default value is 32768.

### 9.3.7 Configuring switching network diameter

Network diameter refers to the number of nodes on the path with the most devices in a switching network. In MSTP, the network diameter is valid only to CIST, but not to the MSTI. In the same domain, no matter how many nodes in a path, it is considered as just one node to calculate. Actually, the network diameter should be defined as the number of domains in the path crossing the most domains. The network diameter is 1 if there is only one domain in the whole network.

The maximum number of hops of the MST domain is used to indicate the scale of the domain, while the network diameter is used to indicate the scale of the whole network. The bigger the network diameter is, the bigger the network scale is.

Similar to maximum number of hops of the MST domain, the configuration takes effect only when the configured device serves as the CIST root device. When you configure the network diameter parameters, the MSTP will set Hello Time, Forward Delay, and Max Age to an optimal value automatically through calculation.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree bridge-diameter <i>bridge-diameter-value</i></b>	Configure the switching network diameter. You can use the <b>no spanning-tree bridge-diameter</b> command to restore default configurations.

### 9.3.8 Configuring internal port path cost

When selecting the root port and designated port, the smaller the port path cost is, the easier it is selected as the root port or designated port. Internal port path cost is mutually independent in different instances.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface gigabitethernet <i>slot-id/port-id</i></b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-gigabitethernet-<i>*:*</i>)#spanning-tree [ instance <i>instance-id</i> ] inter-path-cost <i>cost-value</i></b>	Configure the internal port path cost for a spanning tree instance. You can use the <b>no spanning-tree [ instance <i>instance-id</i> ] inter-path-cost</b> command to restore default configurations.

### 9.3.9 Configuring external port path cost

External path cost is the path cost from the device to CIST root device, and the external path cost in the same domain is the same.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface gigabitethernet <i>slot-id/port-id</i></b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-gigabitethernet-<i>*:*</i>)#spanning-tree extern-path-cost <i>cost-value</i></b>	Configure the external port path cost. You can use the <b>no spanning-tree extern-path-cost</b> command to restore default configurations.

### 9.3.10 Configuring port maximum Tx rate

The maximum Tx rate refers to the maximum number of BPDUs allowed to be transmitted by MSTP in each Hello Time. In a Hello Time period, the number of Tx packets cannot exceed transit-limit+1 to avoid network oscillation from causing the frequent change of network topology, which makes the device transmit BPDUs frequently. This parameter is a relative value with no unit. The bigger the parameter is configured, the more packets are permitted to be transmitted in a Hello Time, the more device resource it consumes. The configuration takes effect on the root device only.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree transit-limit <i>value</i></b>	Configure the port maximum Tx rate. You can use the <b>no spanning-tree transit-limit</b> command to restore default configurations.

### 9.3.11 Configuring MSTP timers

There are three MSTP timers:

- Hello Time timer: the interval of the device to send bridge configuration information (BPDU) regularly to detect whether the link fails or not. The device sends hello packets to other devices around every Hello Time to check if there is any failure in the link. The default value is 2s, and you can adjust the interval according to network conditions. Reduce the interval when the network link changes frequently to enhance the robustness of STP; on the contrary, increasing interval value will reduce the system CPU resource occupation rate for STP.
- Forward Delay timer: the time parameter to ensure safe status transition of the device. Link fault initiates the network to recalculate spanning tree, but the new configuration recalculated cannot be transmitted to the whole network immediately. There may be temporary loop if the new root port and designated port start transmitting data at once. This protocol adopts a status transition mechanism: before the root port and designated port start forwarding data, it experiences a medium status (learning status), after a

Forward Delay, it enters the forwarding status. The delay guarantees the new configuration to be transmitted through whole network. You can adjust the delay according to actual conditions. That is, you can reduce it when the network topology changes infrequently and increase it otherwise.

- Max Age timer: the bridge configuration information used by STP has a life time, which is used to judge whether the configuration information is outdated. The device will discard outdated information and STP will recalculate spanning tree. Too small age value may cause frequent recalculation of spanning tree, while too big age value will make STP not adapt to the network topology change timely.

All devices in the whole switching network adopt the three time parameters on the CIST root device, so only the configuration on the root device is valid.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree hello-time <i>value</i></b>	Configure the Hello Time timer. You can use the <b>no spanning-tree hello-time</b> command to restore default configurations.
3	<b>Raisecom(config)#spanning-tree forward-delay <i>value</i></b>	Configure the Forward Delay timer. You can use the <b>no spanning-tree forward-delay</b> command to restore default configurations.
4	<b>Raisecom(config)#spanning-tree max-age <i>value</i></b>	Configure the Max Age timer. You can use the <b>no spanning-tree max-age</b> command to restore default configurations.



## Note

The values of Forward Delay and Max Age will change after you modify the value of Hello Time. The formula is as below:

- $\text{Max Age} = (4 + \text{network diameter}/2) \times \text{Hello Time} + \text{network diameter} - 1 - ((\text{Hello Time} + 1)/2) \times ((\text{network diameter} + 1)/2)$ , and if the Max Age < 6, the MaxAge = 6; if the MaxAge > 40, the Max Age = 40.
- If  $((\text{Hello Time} + 1) \times \text{network diameter})/2 = 0$ , the Forward Delay =  $2 \times \text{Hello Time} + ((\text{HelloTime} + 1) \times \text{network diameter})/2$ ; otherwise, the ForwardDelay =  $2 \times \text{Hello Time} + ((\text{HelloTime} + 1) \times \text{network diameter})/2 + 1$ ; and if the ForwardDelay < 4, the Forward Delay = 4; if the Forward Delay > 30, the Forward Delay = 30.

In addition, the value of Forward Delay will change after you modify the value of Max Age. The formula is as below:

- If  $3/4 \times \text{Max Age} < 4$ , the Forward Delay = 4.
- If  $3/4 \times \text{Max Age} > 30$ , the Forward Delay = 30.
- Otherwise, the Forward Delay =  $3/4 \times \text{HelloTime}$ .

Return operation fails and the system will prompt error information when the configured value exceeds the range between  $6 \leq \text{Max Age} \leq 40$  and  $\text{Max Age} \geq 2 \times \text{Hello Time} + 1$ .

Return operation fails and the system will prompt error information when the configured value exceeds the range between  $4 \leq \text{Forward Delay} \leq 30$  and  $\text{Forward Delay} \geq \text{Max Age}/2 + 1$ .

### 9.3.12 Configuring edge port

Edge port refers to the port neither connects to any devices directly nor connects to any device indirectly via network.

Configuring the edge port can change the port to the forwarding status quickly without any wait time. For the Ethernet port connected to the user terminal directly, you can configure it as the edge port to make it change to forwarding status quickly.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface gigabitethernet slot-id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-gigabitethernet- *:*)#spanning-tree edged-port { auto   force-true   force-false }</b>	Configure edge port properties.

### 9.3.13 Configuring link type

The two ports connected by a point-to-point link can change to the forwarding status quickly by transmitting synchronous packets, thus reducing unnecessary forwarding delay. By default, the MSTP configure the port link type according to the duplex mode. The full-duplex port is considered as a point-to-point link; half-duplex port is considered as a shared link.

You can configure the current Ethernet port to connect a point-to-point link by force, but the system will fail if the link is not a point-to-point one. Generally, we recommend you to configure this item in automatical status. In this case, the system will automatically detect whether the port is connected to a point-to-point link.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface gigabitethernet slot-id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-gigabitethernet- *:*)#spanning-tree link-type { point-to- point   shared   auto }</b>	Configure the port link type. You can use the <b>no spanning-tree link-type</b> command to restore default configurations.

### 9.3.14 Configuring root port protection

When a bridge receives the packet with a higher priority, the bridge will be reselected. Reselection affects the network connectivity and consumes CPU resources. For the network enabled with the MSTP function, if someone sends the BPDU with a higher priority to attack the network, the network becomes unstable due to the continuous selection. Generally, the priority of each bridge has already been configured in the stage of network planning. The nearer to the edge the bridge is, the lower priority it has. So downlink ports cannot receive packets with priorities higher than the bridge priority (except the bridge reselection on the MSTP network caused by wrong connection of a device with a higher priority or hostile attacks). For these downlink ports, you can enable root port protection to refuse to deal with

packets with priorities higher than the bridge priority and block the port for a period if it receives the packet with a higher priority, in order to prevent the attack source from damaging the upper layer link.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface gigabitethernet slot-id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-gigabitethernet- *:*)#spanning-tree rootguard</b>	Configure root port protection. You can use the <b>no spanning-tree rootguard</b> command to disable this function.

### 9.3.15 Configuring port loop protection

Spanning tree provides two functions: loop protection and link backup. Loop protection requires carving up the network topology into the tree structure. There must be redundant links in the topology to perform link backup. Spanning tree can avoid loops by blocking the redundant links and enable link backup by enabling redundant links when the link breaks down.

Spanning tree modules exchange packets periodically. The link is considered to fail if it has not received packets in a period. Then a new link will be reselected and the backup port is enabled. In actual network applications, the packets cannot be received may not because of link failure; then at this time, enabling the backup port may lead to loop.

The purpose of loop protection is to keep the port in its original status without reselection when it cannot receive packets in a period. You should note that loop protection and link backup is mutually exclusive. That is, the trade-off of loop protection is disabling link backup.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface gigabitethernet slot-id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-gigabitethernet- *:*)#spanning-tree loopguard</b>	Configure port loop protection. You can use the <b>no spanning-tree loopguard</b> command to disable this function.

### 9.3.16 Performing mcheck operation

There are two working modes for ports on the device supporting the MSTP function: STP compatible mode and MSTP mode. Suppose the port of a MSTP device in a switching network is connected to a device running STP, the port will change to work in STP compatible mode automatically. But the port cannot change to work in MSTP mode if the STP device is removed, i.e. the port still works in STP compatible mode. You can perform the mcheck operation to force the port to work in MSTP mode. Of course, if the port receives new STP packets again, it will return to STP compatible mode.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface gigabitethernet slot-id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-gigabitethernet- *:*)#spanning-tree mcheck</b>	Perform the mcheck operation to forcibly return the port to MSTP mode.

### 9.3.17 Checking configurations

No.	Command	Description
1	<b>Raisecom#show spanning-tree [ instance instance-id ] [ detail ]</b>	Show spanning tree configurations.
2	<b>Raisecom#show interface gigabitethernet slot-id/port-id spanning-tree [ instance instance-id ] [ detail ]</b>	Show spanning tree configurations on the interface.
3	<b>Raisecom#show spanning-tree region-configuration</b>	Show MST domain configurations.
4	<b>Raisecom#show spanning-tree region-operation</b>	Show MST domain operation information.

## 9.4 Configuring ONU RSTP

### 9.4.1 Preparing for configurations

#### Scenario

To prevent network loopback from causing broadcast storm or paralyzing the network, you can configure RSTP on the ONU to form a tree network topology between the ONU UNI and user network, through which the loopback port is blocked, thus avoiding the loss caused by network loopback.

#### Prerequisite

The RSTP function is mutually exclusive with loopback detection and BPDU transparent transmission. So note the following prerequisites when enabling RSTP:

- Disable loopback detection on all ONU Ethernet interfaces.
- Configure the BPDU transparent transmission mode to termination.

### 9.4.2 Default configurations

Default configurations of RSTP on the ONU are as below.

Function	Default value
ONU RSTP	Disable
System priority of RSTP	32768
Port priority of RSTP	128
Whether the UNI is an edge port	Yes
Path cost	0

### 9.4.3 Configuring ONU RSTP

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*/:*)#spanning-tree</b>	Enable ONU RSTP. You can use the <b>no spanning-tree</b> to disable this function.

### 9.4.4 Configuring parameters of ONU RSTP

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config-epon-onu-*/:*)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*/:*)#spanning-treepriority priority-value</b>	Configure the system priority of ONU RSTP. You can use the <b>no spanning-tree priority</b> command to restore default configurations.
4	<b>Raisecom(config-epon-onu-*/:*)#exit</b> <b>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</b>	Enter EPON ONU UNI configuration mode.
5	<b>Raisecom(config-epon-onu-ethernet-*/:*)#spanning-tree priority priority-value</b>	Configure the port priority of RSTP. You can use the <b>no spanning-tree priority</b> command to restore default configurations.
6	<b>Raisecom(config-epon-onu-ethernet-*/:*)#spanning-tree edged-port</b>	Configure the UNI as an edge port. You can use the <b>no spanning-tree edged-port</b> command to restore default configurations.



Step	Command	Description
7	<code>Raisecom(config-epon-onu-ethernet- */*/*:*)#spanning-tree path-cost value</code>	Configure the path cost of ONU RSTP bridge port.  You can use the <b>no spanning-tree path-cost</b> command to restore default configurations.

## 9.4.5 Checking configurations

No.	Command	Description
1	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id spanning-tree</code>	Show configurations of spanning tree on the ONU.
2	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet [ uni-id ] spanning-tree [ statistics ]</code>	Show configurations and statistics of spanning tree on the UNI.
3	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id spanning-tree non-forwarding port</code>	Show ports in non-forwarding status.

## 9.5 Maintenance

Command	Description
<code>Raisecom(config)#clear epon-onu slot-id/olt-id/onu-id uni ethernet uni-id spanning-tree statistic</code>	Clear spanning tree statistics on ONU UNI.

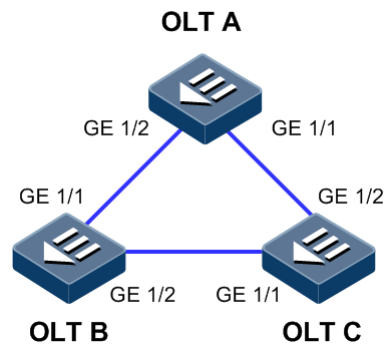
## 9.6 Configuration examples

### 9.6.1 Example for configuring STP

#### Networking requirements

As shown in Figure 9-6, three devices OLT A, OLT B, and OLT C form a ring network. To solve the loop problem in a physical link ring, you need to enable STP on the three devices, and configure the priority of OLT A as 0 and the cost from OLT B to OLT A as 10.

Figure 9-6 STP networking



## Configuration steps

Step 1 Enable STP on OLT A.

```
Raisecom#config
Raisecom(config)#spanning-tree
Raisecom(config)#spanning-tree mode stp
```

Step 2 Configure port mode for OLT A.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:2)#exit
```

Step 3 Configure the OLT A spanning tree priority and port path cost.

```
Raisecom(config)#spanning-tree priority 0
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#spanning-tree extern-path-cost 10
Raisecom(config-if-gigabitethernet-1:2)#exit
```

Configurations of OLT B and OLT C are identical with those of OLT A, so refer to OLT A configurations for related configuration.

## Checking results

Show the bridge status.

- OLT A

```
Raisecom#show spanning-tree
MSTP Admin State: Enable
Protocol Mode: STP
BridgeId:    Mac 000E.5E7B.C557 Priority 0
Root:        Mac 000E.5E7B.C557 Priority 0    RootCost 0
Operational: HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:  HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
```

- OLT B

```
Raisecom#show spanning-tree
MSTP Admin State: Enable
Protocol Mode: STP
BridgeId:    Mac 000E.5E83.ABD1 Priority 32768
Root:        Mac 000E.5E7B.C557 Priority 0    RootCost 10
Operational: HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:  HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
```

- OLT C

```
Raisecom#show spanning-tree
MSTP Admin State: Enable
Protocol Mode: STP
BridgeId:    Mac 000E.5E83.ABD5 Priority 32768
Root:        Mac 000E.5E7B.C557 Priority 0    RootCost 20000
Operational: HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:  HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
```

Show the port status.

- OLT A

```
Raisecom#show interface gigabitethernet 1/1-2 spanning-tree
Port ID: gigabitethernet1/1
PortEnable: admin: enable
oper: enable
Rootguard: disable
Loopguard: disable
ExternPathCost:10
Partner MSTP Mode: stp
Bpdus send:    279 (TCN<0>    Config<279> RST<0> MST<0>)
Bpdus received:13 (TCN<13>    Config<0> RST<0> MST<0>)
State:forwarding Role:designated    Priority:128    Cost: 20000
Root:          Mac 000E.5E7B.C557 Priority 0    RootCost 0
DesignatedBridge: Mac 000E.5E7B.C557 Priority 0    DesignatedPort 32777

Port ID: gigabitethernet1/2
PortEnable: admin: enable
```

```
oper: enable
Rootguard: disable
Loopguard: disable
ExternPathCost:20000
Partner MSTP Mode: stp
Bpdus send: 279 (TCN<0> Config<279> RST<0> MST<0>)
Bpdus received:6 (TCN<6> Config<0> RST<0> MST<0>)
State:forwarding Role:designated Priority:128 Cost: 20000
Root: Mac 000E.5E7B.C557 Priority 0 RootCost 0
DesignatedBridge: Mac 000E.5E7B.C557 Priority 0 DesignatedPort 32778
```

- OLT B

```
Raisecom#show interface gigabitethernet 1/1-2 spanning-tree
Port ID: gigabitethernet1/1
PortEnable: admin: enable
oper: enable
Rootguard: disable
Loopguard: disable
ExternPathCost:10
Partner MSTP Mode: stp
Bpdus send: 357 (TCN<0> Config<357> RST<0> MST<0>)
Bpdus received:13 (TCN<12> Config<1> RST<0> MST<0>)
State:forwarding Role:designated Priority:128 Cost: 20000
Root: Mac 000E.5E7B.C557 Priority 0 RootCost 10
DesignatedBridge: Mac 000E.5E7B.C558 Priority 0 DesignatedPort 32777
```

```
Port ID: gigabitethernet1/2
PortEnable: admin: enable
oper: enable
Rootguard: disable
Loopguard: disable
ExternPathCost:20000
Partner MSTP Mode: stp
Bpdus send: 36 (TCN<13> Config<23> RST<0> MST<0>)
Bpdus received:335 (TCN<0> Config<335> RST<0> MST<0>)
State:forwarding Role:root Priority:128 Cost: 20000
Root: Mac 000E.5E7B.C557 Priority 0 RootCost 20000
DesignatedBridge: Mac 000E.5E83.ABD1 Priority 32768 DesignatedPort
32777
```

- OLT C

```
Raisecom#show interface gigabitethernet 1/1-2 spanning-tree
Port ID: gigabitethernet1/1
PortEnable: admin: enable
oper: enable
Rootguard: disable
Loopguard: disable
ExternPathCost:20000
```

```

Partner MSTP Mode: stp
Bpdus send: 22 (TCN<12> Config<10> RST<0> MST<0>)
Bpdus received:390 (TCN<0> Config<390> RST<0> MST<0>)
State:blocking Role:non-designated Priority:128 Cost: 20000
Root: Mac 000E.5E7B.C557 Priority 0 RootCost 20000
DesignatedBridge: Mac 000E.5E83.ABD1 Priority 32768 DesignatedPort
32777

Port ID: gigabitethernet1/2
PortEnable: admin: enable
oper: enable
Rootguard: disable
Loopguard: disable
ExternPathCost:20000
Partner MSTP Mode: stp
Bpdus send: 38 (TCN<6> Config<32> RST<0> MST<0>)
Bpdus received:368 (TCN<0> Config<368> RST<0> MST<0>)
State:forwarding Role:root Priority:128 Cost: 20000
Root: Mac 000E.5E7B.C557 Priority 0 RootCost 0
DesignatedBridge: Mac 000E.5E7B.C557 Priority 0 DesignatedPort 32778

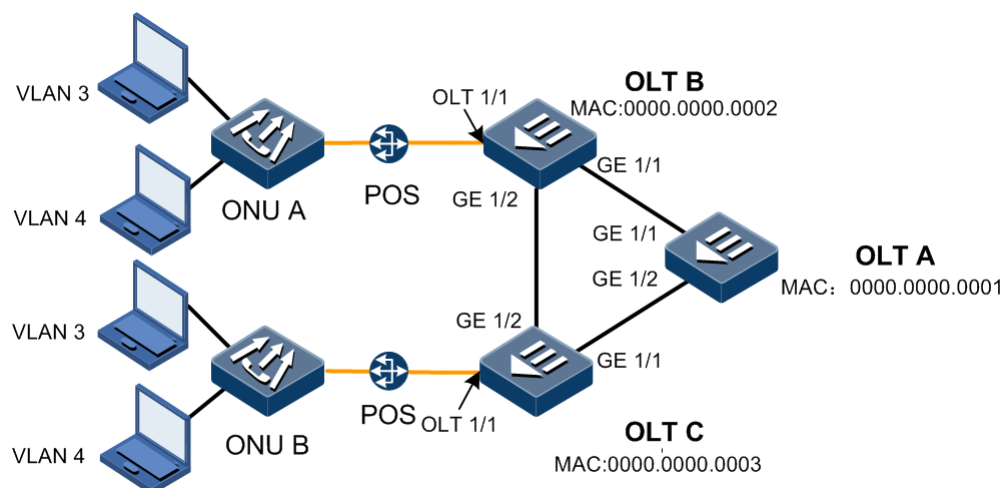
```

## 9.6.2 Example for configuring MSTP

### Networking requirements

As shown in Figure 9-7, three devices OLT A, B, C form a ring network and run the MSTP protocol with a domain name aaa. OLT B and OLT C connect with two PCs respectively which belong to VLAN 3 and VLAN 4 respectively. Instance 3 associates with VLAN 3 and instance 4 associates with VLAN 4. You can configure the path cost for instance 3 of OLT B to forward two VLAN packets in two paths respectively, in which way to realize loop protection and load sharing.

Figure 9-7 MSTP networking



### Configuration steps

Step 1 Create VLAN 3 and VLAN 4 on three OLT devices respectively and activate them.

- Configure OLT A.

```
Raisecom#config
Raisecom(config)#create vlan 3-4 active
Raisecom(config)#end
```

- Configure OLT B.

```
Raisecom#config
Raisecom(config)#create vlan 3-4 active
Raisecom(config)#end
```

- Configure OLT C.

```
Raisecom#config
Raisecom(config)#create vlan 3-4 active
Raisecom(config)#end
```

Step 2 Uplink ports GE 1/1 and GE 1/2 of OLT A, OLT B, and OLT C work in Trunk mode to allow all VLANs to pass. Downlink ports OLT 1/1 of OLT B and OLT C work in Trunk mode to allow VLAN 3 and VLAN 4 to pass.

- Configure OLT A.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:2)#exit
```

- Configure OLT B.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:2)#exit
Raisecom(config)#interface epon-olt 1/1
Raisecom(config-if-epon-olt-1:1)#switchport mode trunk
Raisecom(config-if-epon-olt-1:1)#switchport trunk allowed vlan 3,4
Raisecom(config-if-epon-olt-1:1)#exit
```

- Configure OLT C.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:2)#exit
Raisecom(config)#interface epon-olt 1/1
Raisecom(config-if-epon-olt-1:1)#switchport mode trunk
Raisecom(config-if-epon-olt-1:1)#switchport trunk allowed vlan 3,4
```

Step 3 Configure OLT A, OLT B, and OLT C to MSTP mode and enable STP. Enter MSTP configuration mode and configure the domain name as aaa, the revision version as 0, instance 3 mapping VLAN 3, and instance 4 mapping VLAN 4.

- Configure OLT A.

```
Raisecom(config)#spanning-tree mode mstp
Raisecom(config)#spanning-tree
Raisecom(config)#spanning-tree region-Command
Raisecom(config-region)#name aaa
Raisecom(config-region)#revision-level 0
Raisecom(config-region)#instance 3 vlan 3
Raisecom(config-region)#instance 4 vlan 4
Raisecom(config-region)#exit
```

- Configure OLT B.

```
Raisecom(config)#spanning-tree mode mstp
Raisecom(config)#spanning-tree
Raisecom(config)#spanning-tree region-Command
Raisecom(config-region)#name aaa
Raisecom(config-region)#revision-level 0
Raisecom(config-region)#instance 3 vlan 3
Raisecom(config-region)#instance 4 vlan 4
Raisecom(config-region)#exit
```

- Configure OLT C.

```
Raisecom(config)#spanning-tree mode mstp
Raisecom(config)#spanning-tree
Raisecom(config)#spanning-tree region-Command
Raisecom(config-region)#name aaa
Raisecom(config-region)#revision-level 0
Raisecom(config-region)#instance 3 vlan 3
```

```
Raisecom(config-region)#instance 4 vlan 4
Raisecom(config-region)#exit
```

Step 4 On OLT B, modify the internal path cost of port GE 1/1 in spanning tree instance 3 as 500000.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#spanning-tree instance 3 inter-
path-cost 500000
```

## Checking results

Show MST domain configurations.

```
Raisecom#show spanning-tree region-operation
Operational:
-----
Name: aaa
Revision level: 0          Instances running: 3
Digest: 0x024E1CF7E14D5DBBD9F8E059D2C683AA
Instance      vlans Mapped
-----
0             1,2,5-4094
3             3
4             4
```

Show information about MSTI 3.

- OLT A

```
Raisecom#show spanning-tree instance 3
MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 3
-----
BridgeId:   Mac 0000.0000.0001 Priority 32768
RegionalRoot: Mac 0000.0000.0001 Priority 32768 InternalRootCost 0
PortId PortState PortRole PathCost PortPriority LinkType TrunkPort
-----
gigabitethernet1/1 forwarding designated 20000 128 point-
to-point no
gigabitethernet1/2 forwarding designated 20000 128 point-
to-point no
```

- OLT B



**Raisecom#show spanning-tree instance 3**

MSTP Admin State: Enable  
Protocol Mode: MSTP  
MST ID: 3

```
-----  
BridgeId:    Mac 0000.0000.0002 Priority 32768  
RegionalRoot: Mac 0000.0000.0001 Priority 32768 InternalRootCost  
500000  
PortId PortState PortRole PathCost PortPriority LinkType TrunkPort  
-----  
gigabitethernet1/1      discarding alternate 500000 128      point-  
to-point no  
gigabitethernet1/2      forwarding root      20000 128      point-  
to-point no  
epon-olt1/1      forwarding designated 20000 128      point-to-point  
no
```

- OLT C

**Raisecom#show spanning-tree instance 3**

MSTP Admin State: Enable  
Protocol Mode: MSTP  
MST ID: 3

```
-----  
BridgeId:    Mac 0000.0000.0003 Priority 32768  
RegionalRoot: Mac 0000.0000.0001 Priority 32768 InternalRootCost 20000  
PortId PortState PortRole PathCost PortPriority LinkType TrunkPort  
-----  
gigabitethernet1/1      forwarding root      20000 128      point-  
to-point no  
gigabitethernet1/2      forwarding designated 20000 128      point-  
to-point no  
epon-olt1/1      forwarding designated 20000 128      point-to-point  
no
```

Show information about MSTI 4.

- OLT A

**Raisecom#show spanning-tree instance 4**

MSTP Admin State: Enable  
Protocol Mode: MSTP  
MST ID: 4

```
-----  
BridgeId:    Mac 0000.0000.0001 Priority 32768  
RegionalRoot: Mac 0000.0000.0001 Priority 32768 InternalRootCost 0  
PortId PortState PortRole PathCost PortPriority LinkType TrunkPort  
-----  
gigabitethernet1/1      forwarding designated 20000 128      point-  
to-point no
```

```
gigabitethernet1/2    forwarding designated 20000    128        point-
to-point no
```

- OLT B

Raisecom#**show spanning-tree instance 4**

MSTP Admin State: Enable

Protocol Mode: MSTP

MST ID: 4

```
-----
BridgeId:    Mac 0000.0000.0002 Priority 32768
RegionalRoot: Mac 0000.0000.0001 Priority 32768 InternalRootCost 20000
PortId PortState PortRole PathCost PortPriority LinkType TrunkPort
-----
gigabitethernet1/1    forwarding root      200000    128        point-
to-point no
gigabitethernet1/2    forwarding designated 20000    128        point-
to-point no
epon-olt1/1           forwarding designated 20000    128        point-
to-point no
```

- OLT C

Raisecom#**show spanning-tree instance 4**

MSTP Admin State: Enable

Protocol Mode: MSTP

MST ID: 4

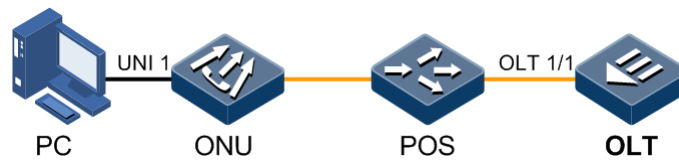
```
-----
BridgeId:    Mac 0000.0000.0003 Priority 32768
RegionalRoot: Mac 0000.0000.0001 Priority 32768 InternalRootCost 20000
PortId PortState PortRole PathCost PortPriority LinkType TrunkPort
-----
gigabitethernet1/1    forwarding root      20000    128        point-
to-point no
gigabitethernet1/2    discarding alternate 200000    128        point-
to-point no
epon-olt1/1           forwarding designated 20000    128        point-
to-point no
```

## 9.6.3 Example for configuring ONU RSTP

### Networking requirements

As shown in Figure 9-8, the user PC is connected to the ONU through UNI 1 and the ONU is connected to the OLT through OLT 1/1. To avoid loopback in the user network, you need to enable RSTP on the ONU to prevent broadcast storm.

Figure 9-8 ONU RSTP networking



## Configuration steps

Enable ONU RSTP.

```
Raisecom#config
Raisecom(config)#epon-onu 1/1/1
Raisecom(config-epon-onu-1/1:1)#spanning-tree
Raisecom(config-epon-onu-1/1:1)#exit
```

## Checking results

Show RSTP configurations on the ONU.

```
Raisecom(config)#show epon-onu 1/1/1 spanning-tree
ONU ID: 1/1/1
  Admin state      : enable
  Mode             : RSTP
  Priority          : 32768
  Max-age-time     : 0s
  Bridge max-age-time : 20s
  Hello time       : 0s
  Bridge hello time : 2s
  Hold time        : 0s
  Forward delay    : 0s
  Bridge forward delay : 15s
  Root bridge ID   : 0-000E.5E7B.C557(priority-MAC)
  Root port ID     : 0
  Root cost        : 0
  Default path cost version: stp8021t2001
  Max transmission limit : 3(per hello time)
  Protocol specification : ieee8021d
  Time since topology change: 0 days 0 hours 0 minutes
  Topology change times  : 0
```

# 10 Configuring routing

---

This chapter introduces the routing feature and configure process of the ISCOM5508, and provides related configuration examples, including the following sections:

- Overview of routing
- Configuring ARP
- Configuring static routing
- Configuring VRRP
- Configuring key-chain
- Configuration examples

## 10.1 Overview of routing

### 10.1.1 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, you must learn the physical address of the destination host. It means that you 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, helping 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 ISCOM5508.
  - Dynamic ARP entries are aged when the aging time is exceeded, if dynamic ARP entries are not used.

The ISCOM5508 supports **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.

## 10.1.2 Routing

The 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 follows:

- Interface routing or directly-connected routing: routes discovered by link-layer protocols
- Static routing: routes manually configured by the administrator
- Dynamic routing: 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 routing

The default routing is a type of special routing. It takes effect when no other route can be matched in the routing table. In the routing table, the default routing is designated as 0.0.0.0/0. If the destination IP address of a packet mismatches any entry in the routing table, this packet will select the default routing.

If no default routing 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 the destination address or network is unreachable.

### Static routing

Static routing refers to a type of routing that is manually configured. The static routing has the following advantages:

- Do not consume network bandwidth.
- Cannot be aged.
- Can accurately control the direction of data packets.

However, the static routing has some disadvantages:

- Be configured manually.
- Add workload of the administrator.

The static routing is mainly applied to small- and medium-sized network.

## 10.1.3 VRRP

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerance protocol.

Generally, all hosts in the network are configured with default routes. Packets, with destination addresses beyond this network segment, sent by the host will be forwarded by the default router, thus enabling the host to communicate with the external network. However, when the default router fails, all hosts in this network segment will fail to communicate with the external network, thus generating a single point of failure. To solve this problem, VRRP which is designed for the LAN with multicast or broadcast capabilities (such as Ethernet) is introduced.

Working process of VRRP

- After enabled with VRRP, the router will confirm its role in the backup group based on its priority. The router with the highest priority serves as the primary router while the ones with lower priorities will serve as backup routers. The primary router will send VRRP advertisement packets periodically to inform other routers in the backup group of its working status. The backup routers are enabled with a timer to wait for the VRRP advertisement packets.
- In different preemptive modes, the replacement method of the primary role is different. In preemptive mode, when receiving the VRRP advertisement packet, the primary router will compare its priority with that in the advertisement packet. If its priority is higher than the one in the advertisement packet, it will become the primary router. Otherwise, it will remain standby. In non-preemptive mode, as long as the primary router works properly, the routers in the backup group will remain active or standby. They will not become the primary router even being configured with higher priorities.
- If the backup router did not receive the VRRP advertisement packets from the primary router until its timer times out, it will assume that the primary router fails. In this case, the backup router will consider itself as a primary router and sends VRRP advertisement packets out. The routers in the backup group will elect a primary router based on priorities for forwarding packets.

## 10.1.4 Key-chain

For the sake of network security, you need to change the authentication information in the application layer constantly. You can use the authentication algorithm and shared key to check whether information is changed during transport on an unsecure network. However, the receiver and the sender should share the security key and authentication algorithm while using the above-mentioned way to authenticate data. In addition, the secret key cannot be transported in the network.

If each application layer protocol maintains a set of authentication rules (authentication algorithm and secret key), a large number of applications will adopt the same authentication mode, which will result in the duplication and modification of authentication information. Similarly, if each application adopts a fixed authentication secret key, then each modification shall be done by the administrator manually. However, it is difficult to modify the password or authentication algorithm, so it is with changing passwords of all routers without packet loss.

Therefore, the system is required to centralize the management of all authentication processing and change authentication algorithms and passwords without manual intervention. Fortunately, what Key-chain implements is exactly this function. Key-chain can provide authentication for all application layers and dynamically change the password chain without losing packets.

## 10.2 Configuring ARP

### 10.2.1 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

### 10.2.2 Default configurations

Default configurations of ARP on the ISCOM5508 are as below.

Function	Default value
Static ARP entries	N/A
Dynamic ARP learning mode	learn-all

### 10.2.3 Configuring static ARP entries



#### Caution

- The IP address of a static ARP entry must be in the same IP network segment with the Layer 3 interface.
- You need to add or delete static ARP entries manually.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#arp <i>ip-address mac-address</i></b>	Configure static ARP entries. You can use the <b>no arp <i>ip-address</i></b> command to delete the entry.

### 10.2.4 Configuring dynamic ARP entries

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#arp aging-time <i>time</i></b>	Configure the aging time of dynamic ARP entries.

## 10.2.5 Checking configurations

No.	Command	Description
1	Raisecom# <b>show arp</b>	Show all entries in the ARP address table.
2	Raisecom# <b>show arp</b> [ <i>ip-address</i> ]	Show information about an ARP entry of a specified IP address.
3	Raisecom# <b>show arp static</b>	Show information about static ARP entries.
4	Raisecom# <b>show arp summary</b>	Show statistics on ARP table.

## 10.3 Configuring static routing

### 10.3.1 Preparing for configurations

#### Scenario

Configure static routing for simple topology networks. You need to configure static routing manually to create an interconnected network.

#### Prerequisite

Configure the IP address of the Layer 3 interface correctly.

### 10.3.2 Configuring default gateway

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>ip route</b> <b>0.0.0.0 0.0.0.0</b> <i>ip-address</i>	Configure the IPv4 default gateway.



#### Note

When the packet to be forwarded does not have a corresponding route, you can use the **ip route** command to configure the default next-hop IP address (default gateway) to enable the packet to be forwarded to the default gateway. The IP address of the default gateway and the local IP address are in the same network segment.



### 10.3.3 Configuring IPv4 static routing

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip routing</b>	Enable routing. You can use the <b>no ip routing</b> command to disable this function.
3	<b>Raisecom(config)#router id ip-address</b>	(Optional) configure the router ID. You can use the <b>no router id</b> command to delete the configuration.
4	<b>Raisecom(config)#ip route ip-address mask nexthopip</b> [ <b>distancevalue</b> ] [ <b>description description</b> ] [ <b>tag tag-id</b> ]	Configure IPv4 static routing. You can use the <b>no ip route ip-address mask nexthopip</b> command to delete the configuration.
5	<b>Raisecom(config)#ip route static distance value</b>	(Optional) configure the default management distance of IPv4 static routing. You can use the <b>no ip route static distance</b> command to restore default configurations.

### 10.3.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show ip route [ detail ]</b>	Show routing details.
2	<b>Raisecom#show ip route ip-address [ ip-mask ] [ longer-prefixes ] [ detail ]</b>	Show routing to a specified IP address.
3	<b>Raisecom#show ip route start-ip-address ip-mask end-ip-address ip-mask [ detail ]</b>	Show routing information about a specified address range.
4	<b>Raisecom#show ip route protocol { static   direct   ospf }</b>	Show routing information about a specified protocol.
5	<b>Raisecom#show ip route statistics</b>	Show routing statistics.
6	<b>Raisecom#show ip route protocol { direct   static   ospf   rip }</b>	Show configurations of the routing protocol.
7	<b>Raisecom#show router id</b>	Show the router ID.

## 10.4 Configuring VRRP

### 10.4.1 Preparing for configurations

#### Scenario

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant protocol.

In general, all hosts in the network are configured with a default route. Packets, whose destination address is not in the network segment, are sent through the default router. Therefore, hosts can communicate with the external network. However, if the default router fails, hosts will fail to communicate with the external network and a single-point fault occurs. VRRP can resolve this problem. VRRP is designed for the Local Area Network with multicast or broadcast capability (such as Ethernet).

#### Prerequisite

Configure the IP address of the Layer 3 interface.

### 10.4.2 Default configurations

Default configurations of VRRP on the ISCOM5508 are as below.

Function	Default value
VRRP alarm	Enable
VRRP	Enable
VRRP backup group	N/A

### 10.4.3 Configuring VRRP

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#vrrp ping</b>	(Optional) enable VRRP.
3	<b>Raisecom(config)#vrrp trap</b>	(Optional) enable VRRP alarm.
4	<b>Raisecom(config)#interface vlanif <i>vlan-id</i></b>	Enter VLAN interface configuration mode.
5	<b>Raisecom(config-vlanif-*)#vrrp <i>id</i> description <i>text</i></b>	Configure descriptions about the VRRP backup group. You can use the <b>no vrrp <i>id</i> description <i>text</i></b> command to delete the configuration.
6	<b>Raisecom(config-vlanif-*)#vrrp <i>id</i> { <b>enable</b>   <b>disable</b> }</b>	Enable/Disable the VRRP backup group.

Step	Command	Description
7	Raisecom(config-vlanif-*)# <b>vrrp id ip ip-address</b>	Configure the IP address of the VRRP backup group. You can use the <b>no vrrp id ip ip-address</b> command to delete the configuration.
8	Raisecom(config-vlanif-*)# <b>vrrp id preempt [ delay-time time ]</b>	Configure VRRP preemption and delay time. You can use the <b>no vrrp id preempt [ delay-time time ]</b> command to delete the configuration.
9	Raisecom(config-vlanif-*)# <b>vrrp id priority value</b>	Configure the VRRP priority. You can use the <b>no vrrp id priority value</b> command to delete the configuration.
10	Raisecom(config-vlanif-*)# <b>vrrp id timer advertise-interval time</b>	Configure the timer for sending VRRP notification packets. You can use the <b>no vrrp id timer advertise-interval time</b> command to delete the configuration.
11	Raisecom(config-vlanif-*)# <b>vrrp id track interface vlanif vlan-id [ reduced value ]</b>	Check VRRP.

## 10.4.4 Checking configurations

No.	Command	Description
1	Raisecom# <b>show vrrp</b>	Show VRRP configurations.

## 10.5 Configuring key-chain

### 10.5.1 Preparing for configurations

#### Scenario

For the sake of network security, you need to change the authentication information in the application layer constantly. You can use the authentication algorithm and shared key to check whether information is changed during transport on an unsecure network. However, the receiver and the sender should share the security key and authentication algorithm when using the above-mentioned way to authenticate data. In addition, the secret key cannot be transported in the network.

If each application layer protocol maintains a set of authentication rules (authentication algorithm and secret key), a large number of applications will adopt the same authentication mode, which will result in the duplication and modification of authentication information. Similarly, if each application adopts a fixed authentication secret key, then each modification

shall be done by the administrator manually. However, it is difficult to modify the password or authentication algorithm, so it is with changing passwords of all routers without packet loss.

Therefore, the system is required to intensively manage all authentication processing and change authentication algorithms and passwords without manual intervention. Fortunately, what Key-chain implements is exactly this function. Key-chain can provide authentication for all application layers and dynamically change the password chain without losing packets.

## Prerequisite

N/A

## 10.5.2 Default configurations

N/A

## 10.5.3 Configuring key-chain

No.	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#key-chain <i>string</i></b>	Create a secret key chain and enter KEYCHAIN configuration mode. You can use the <b>no key-chain <i>string</i></b> command to delete the configuration.
3	<b>Raisecom(config-keychain)#key <i>key-id</i> key-string [ 0   7 ] <i>string</i></b>	Configure the secret key and key string.
4	<b>Raisecom(config-keychain)#key <i>key-id</i> accept-lifetime <i>start-time</i> { <b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>duration-time</i> }</b>	(Optional) configure the receiving time of secret key. You can use the <b>no key <i>key-id</i> accept-lifetime</b> command to restore default configuration.
5	<b>Raisecom(config-keychain)#key <i>key-id</i> send-lifetime <i>start-time</i> { <b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>duration-time</i> }</b>	(Optional) configure the sending time of the secret key. You can use the <b>no key <i>key-id</i> send-lifetime</b> command to restore default configuration.
6	<b>Raisecom(config-keychain)#accept-tolerance { <i>time</i>   <b>infinite</b> }</b>	(Optional) configure the receiving tolerance time of the secret key chain. You can use the <b>no accept-tolerance</b> command to restore default configuration.

## 10.5.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show key-chain [ <i>chainname</i> [ <b>key</b> <i>key-id</i> ] ]</b>	Show information about key chain.

## 10.6 Configuration examples

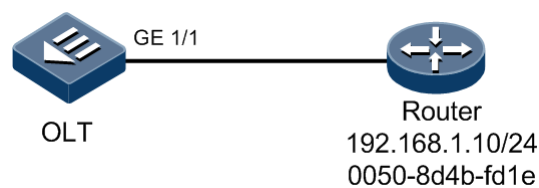
### 10.6.1 Example for configuring ARP

#### Networking requirements

As shown in Figure 10-1, the OLT device connects the host, and connects the upper layer router through the interface GE 1/1. The IP address of the router is 192.168.1.10/24, and the MAC address is 0050.8d4b.fd1e.

You need to configure corresponding static ARP entries on the OLT to increase the communication security between the OLT and router.

Figure 10-1 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

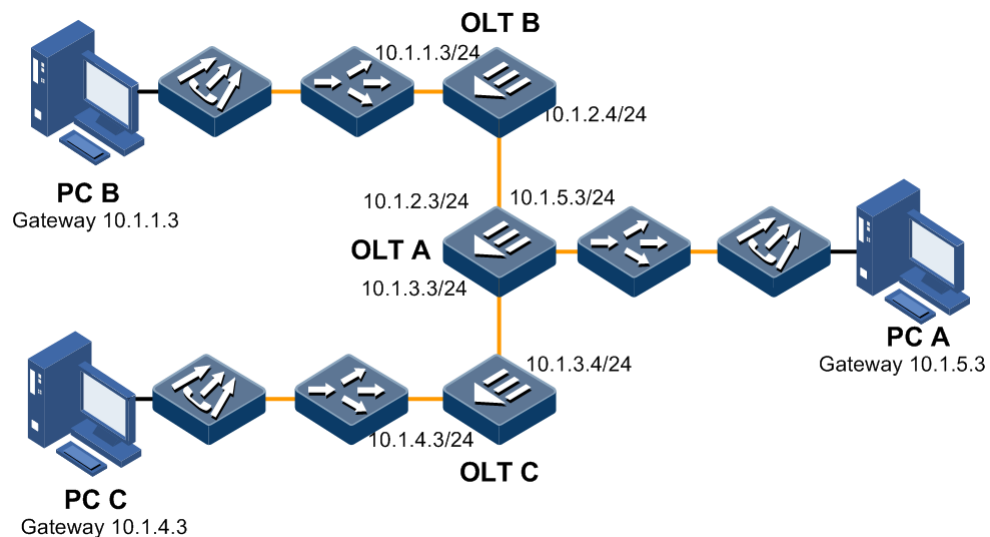
Dynamic: 0

## 10.6.2 Example for configuring static routing

### Networking requirements

As shown in Figure 10-2, configure static routing to enable any two PCs or OLTs can ping through each other. IP addresses of two interfaces on OLT B are 10.1.1.3/24 and 10.1.2.4/24 respectively; IP addresses of three interfaces on OLT A are 10.1.2.3/24, 10.1.5.3/24, and 10.1.3.3/24 respectively; IP addresses of two interfaces on OLT C are 10.1.3.4/24 and 10.1.4.3/24 respectively.

Figure 10-2 Configuring static routing



### Configuration steps

Step 1 Configure the IP address of each device. Detailed configurations are omitted.

Step 2 Enable routing on OLT A and configure static routing.

```
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 routing.

```
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 routing.

```
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 as 10.1.5.3. Detailed configurations are omitted.
- Configure the default gateway of PC B as 10.1.1.3. Detailed configurations are omitted.
- Configure the default gateway of PC C as 10.1.4.3. Detailed configurations are omitted.

## Checking results

Perform the following operation on any OLT to show whether all devices are interconnected.

```
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
```

# 11 Configuring DHCP

---

This chapter introduces the DHCP feature and configuration process of the ISCOM5508, and provides related configuration examples, including the following sections:

- Overview of DHCP
- Configuring DHCP Snooping
- Configuring DHCP Relay
- Configuring DHCP Option 82
- Maintenance
- Configuration examples

## 11.1 Overview of DHCP

With development of Internet, it is more complex to manage IP addresses in the network.

- The number of PCs in the network increases dramatically, which consumes a lot of human resources to manually configure and modify their IP addresses.
- There are multiple laptops in the network, whose IP addresses are frequently changed. The administrator must modify IP configurations frequently.
- To improve IP management efficiency, the administrator must perform centralized management on IP addresses.

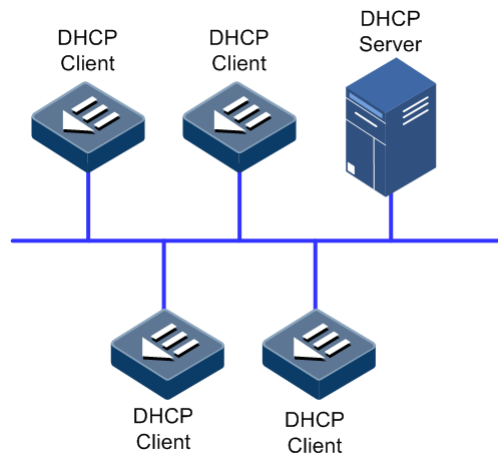
Dynamic Host Configuration Protocol (DHCP) can be used to solve the above problems. DHCP can automatically allocate IP addresses for all clients in the network. It helps reduce workload of the administration, realizing centralized management of IP addresses.

DHCP works in a Client/Server mode. The Client sends an IP request to the Server. The Server provides an IP address and related configurations for the Client, once receiving the IP request.

A typical DHCP application contains at least a DHCP server and multiple DHCP clients (including PCs and laptops), as shown in Figure 11-1.



Figure 11-1 Typical application of DHCP



## Working principles of DHCP

The DHCP server provides IP configurations for a DHCP client by flowing the below steps:

- IP request: a DHCP client broadcasts a DHCP Discover packet to query DHCP servers of the network segment for acquiring an IP address and related configurations.
- IP offer: all DHCP servers in the network segment broadcast a DHCP Offer packet after receiving the DHCP Discover packet. The DHCP Offer packet contains an IP address and related configurations provided for the DHCP client. In addition, the packet contains the identifier of the DHCP server.
- IP selection: the DHCP client selects one IP as its IP address after receiving DHCP Offer packet(s). At the same time, the DHCP client broadcasts a DHCP Request packet to tell other DHCP servers the selected configurations and ask other DHCP servers to withdraw their configurations.
- IP acknowledgement: the DHCP server sends a DHCP Ack packet for acknowledgement after receiving the DHCP Request packet.

Then, the DHCP server implements allocating an IP address and related configurations for the DHCP client.

## DHCP lease renewal

After a DHCP client obtains an IP address from the DHCP server, it cannot use this IP address permanently. The IP address has a fixed usage period, which is called a lease. The lease interval can be assigned by users. If the DHCP client uses the IP address and related configurations permanently, it must ask the DHCP server to renew the lease for the client. The DHCP renewal process is shown as below.

- When 50% lease expires, the DHCP client sends a DHCP Request packet to the DHCP server for renewing the lease. If success, the lease becomes a complete one. Otherwise, a DHCP Request is sent again when 87.5% lease expires.
- When 87.5% lease expires, the DHCP client sends another DHCP Request packet to the DHCP server for renewing the lease. If success, the lease becomes a complete one. Otherwise, lease renewal fails. In addition, the IP address and related configurations are withdrawn.

## Scenarios of DHCP

In general, the DHCP server allocates IP addresses in the following scenarios:

- It is the heavy workload for manually configuring IP addresses in a large network.
- The number of PCs is greater than the number of available IP addresses in a network. The administrator cannot assign a fixed IP address to each PC. In addition, the number of PCs accessing the network is limited.
- A few PCs need a fixed IP address in the network.

### 11.1.2 DHCP packet

Figure 11-2 shows the DHCP packet structure.

Figure 11-2 DHCP packet structure

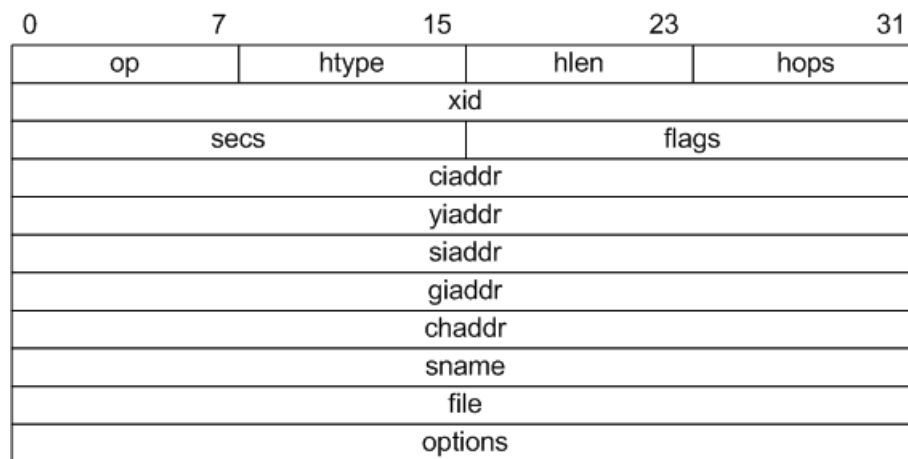


Table 11-1 lists meanings of fields in the DHCP packet.

Table 11-1 Meanings of fields in the DHCP packet

Name	Length (B)	Description
op	1	Packet type <ul style="list-style-type: none"> <li>• 1: request packet</li> <li>• 2: response packet</li> </ul>
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 once 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.

Name	Length (B)	Description
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 <ul style="list-style-type: none"> <li>• 0: unicast</li> <li>• 1: broadcast</li> </ul> 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 route information of 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).

### 11.1.3 DHCP Snooping

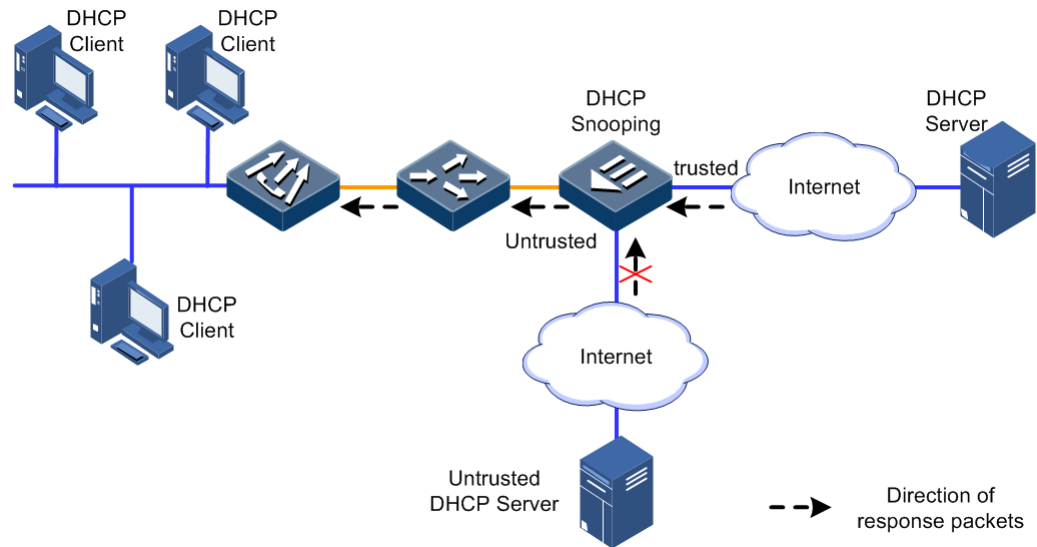
#### Overview of DHCP Snooping

The DHCP Snooping is a security feature of the DHCP, supporting the following functions:

- Ensuring 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 11-3. To ensure 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 11-3 DHCP Snooping networking



- Recording 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 realize the following functions:

- 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 realize security and accounting control of DHCP clients.

If the ISCOM5508 is enabled with DHCP Snooping supporting Option, it takes the following two actions when receiving a DHCP packet.

- When the ISCOM5508 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 ISCOM5508 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.

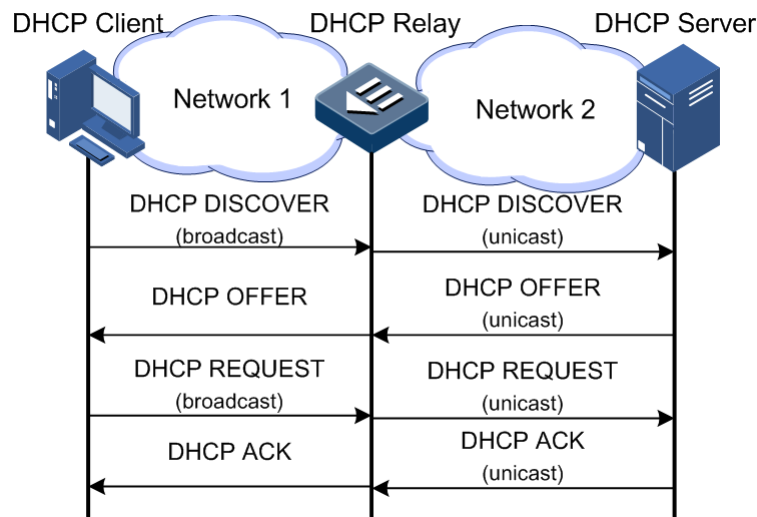
### 11.1.4 DHCP Relay

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 11-4 shows the working principle of DHCP Relay.

Figure 11-4 Working principle of DHCP Relay



As shown in Figure 11-4, 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.

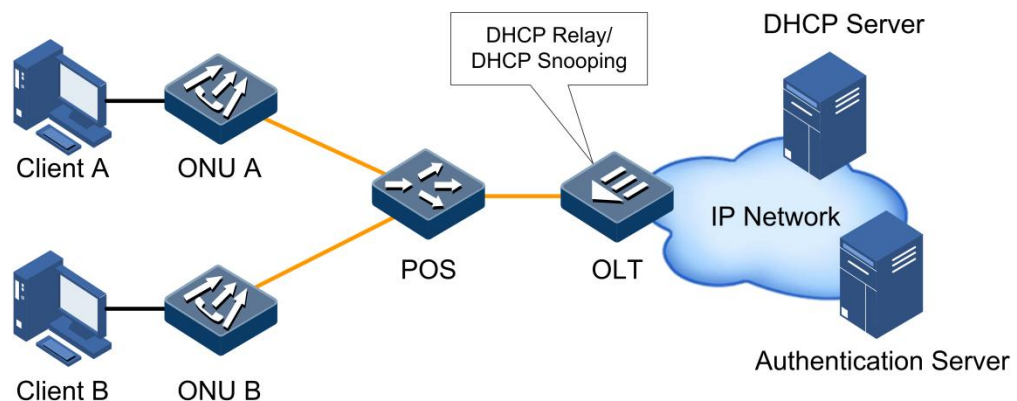
### 11.1.5 DHCP Option 82

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 11-5 Working principle of DHCP Option 82



As shown in Figure 11-5, the working process of DHCP Option 82 is as below.

- Step 1 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 2 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 3 After the authentication server authenticates the client's legality, it sends an authentication response packet to the client, informing the client's authority.
- Step 4 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 5 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 ISCOM5508 can perform policy route based on the source IP address. Therefore, users with different IP addresses have various routing rules and authorities.

## 11.2 Configuring DHCP Snooping

### 11.2.1 Preparing for configurations

#### Scenario

DHCP Snooping is a DHCP security feature, being used to guarantee the DHCP client to get IP addresses 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 ISCOM5508 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.

### 11.2.2 Default configurations

Default configurations of DHCP Snooping on the ISCOM5508 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 ONU 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	Disable

## 11.2.3 Configuring global DHCP Snooping

### Configuring global DHCP Snooping on OLT

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#{ ip   ipv6 } dhcp snooping</b>	Enable global DHCP Snooping. You can use the <b>no ip dhcp snooping</b> command to disable this function.

### Configuring global DHCP Snooping on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*/*:*)#ip dhcp snooping { enable   disable }</b>	Enable/Disable global DHCP Snooping.

## 11.2.4 Configuring DHCP Snooping on VLAN interface

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlanif <i>vlan-id</i></b>	Enter VLAN interface configuration mode.
3	<b>Raisecom(config-vlanif-*)#ip dhcp snooping</b>	Enable DHCP Snooping on the VLAN interface. You can use the <b>no ip dhcp snooping</b> command to disable this function.

## 11.2.5 Configuring DHCP Snooping trust on ONU interface

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</b>	Enter EPON ONU UNI configuration mode.
3	<b>Raisecom(config-epon-onu-ethernet- */*/*:*)#ip dhcp snooping trust { enable   disable }</b>	Enable/Disable DHCP Snooping trust on ONU interface.



### Note

Generally, you need to make sure that the device connected interface at the legal DHCP server side is in trusted status, while the interface at the DHCP client side is in untrusted status.

## 11.2.6 (Optional) configuring DHCP Snooping supporting Option 82

### Configuring DHCP Snooping supporting Option 82 on OLT

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip dhcp information option</b>	Configure DHCP Snooping supporting Option 82. You can use the <b>no ip dhcp information option</b> command to disable this function.



## Configuring DHCP Snooping supporting Option 82 on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*//*:*)#ip dhcp snooping information option82 user-defined { enable   disable }</b>	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.

## 11.2.7 Checking configurations

### Checking configurations on OLT

No.	Command	Description
1	<b>Raisecom#show ip dhcp snooping</b>	Show DHCP Snooping configurations.
2	<b>Raisecom#show ip dhcp snooping binding</b>	Show information about the DHCP Snooping binding table.
3	<b>Raisecom#show ip dhcp snooping statistics</b>	Show statistics on DHCP Snooping.

### Checking configurations on ONU

No.	Command	Description
1	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id ip dhcp snooping</b>	Show DHCP Snooping configurations.
2	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list ip dhcp snooping binding</b>	Show information about the DHCP Snooping binding table.
3	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list uni ethernet [uni-id] ip dhcp snooping</b>	Show DHCP Snooping configurations on the interface.
4	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list uni ethernet [uni-id] ip dhcp snooping statistics</b>	Show statistics of DHCP packets on the interface.

## 11.3 Configuring DHCP Relay

### 11.3.1 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.

### 11.3.2 Default configurations

Default configurations of DHCP Relay on the ISCOM5508 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

### 11.3.3 Configuring global DHCP Relay

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip dhcp relay</b>	Enable global DHCP Relay. You can use the <b>no ip dhcp relay</b> command to disable this function.

### 11.3.4 Configuring destination IP address of DHCP Relay on VLAN interface

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlanif num</b>	Enter VLAN interface configuration mode.
3	<b>Raisecom(config-vlanif-0)#ip dhcp relay</b>	Enable DHCP Relay on VLAN interfaces. You can use the <b>no ip dhcp relay</b> command to disable this function.
4	<b>Raisecom(config-vlanif-0)#ip dhcp relay target-ip ip-address</b>	(Optional) configure the destination IP address of DHCP Relay.



#### Note

- Each 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.

### 11.3.5 Configuring DHCP Relay trust on interface

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface { gigabitethernet   epon-olt } slot-id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-*/*:*)#ip dhcp relay information trusted</b>	Configure an interface as DHCP Relay trusted interface. You can use the <b>no ip dhcp relay information trusted</b> command to restore default configurations.



#### Note

Interface trust can take effect only when DHCP Relay supports DHCP Option 82.

### 11.3.6 Configuring DHCP Relay on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*/*:*)#ip dhcp relay { enable   disable }</b>	Enable/Disable global DHCP Relay on the ONU.

Step	Command	Description
4	<b>Raisecom(config-epon-onu-*//*:*)#ip dhcp relay information option82 user-defined { enable   disable }</b>	Enable/Disable customizing DHCP Relay Option 82 on the ONU.
5	<b>Raisecom(config-epon-onu-*//*:*)#ip dhcp relay ip-if ip-list target-ip ip-address</b>	Configure the destination IP address of the interface enabled with DHCP Relay on the ONU.
6	<b>Raisecom(config-epon-onu-*//*:*)#exit</b> <b>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</b>	Enter EPON ONU UNI configuration mode.
7	<b>Raisecom(config-epon-onu-ethernet-*//*:*)#ip dhcp relay trust { enable   disable }</b>	Enable/Disable DHCP Relay trust on the ONU interface.
8	<b>Raisecom(config-epon-onu-ethernet-*//*:*)#ip dhcp relay option82 policy { drop   keep   replace }</b>	Configure the processing policy of DHCP Relay request packets. You can use the <b>no ip dhcp relay option82 policy</b> command to restore default configurations.

### 11.3.7 Checking configurations

No.	Command	Description
1	<b>Raisecom#show ip dhcp relay</b>	Show DHCP Relay configurations.
2	<b>Raisecom#show ip dhcp relay statistics</b>	Show DHCP Relay statistics.
3	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list ip dhcp relay</b>	Show DHCP Relay configurations on the ONU.
4	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet [uni-id] ip dhcp relay</b>	Show DHCP Relay configurations on the ONU interface.
5	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list ip dhcp relay ip-if</b>	Show configurations of the IP interface enabled with DHCP Relay on the ONU.
6	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet [uni-id] ip dhcp relay statistics</b>	Show DHCP Relay statistics on the ONU interface.

## 11.4 Configuring DHCP Option 82

### 11.4.1 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 11.2.6 (Optional) configuring DHCP Snooping supporting Option 82.

## 11.4.2 Default configurations

Default configurations of DHCP Option 82 on the ISCOM5508 are as below.

Function	Default value
Global DHCP Option 82	Disable
Global DHCP Option attach-string	N/A
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 ONU are as below.

Function	Default value
Global DHCP Option 82	Disable
Global DHCP Option attach-string	N/A
Global remote-id mode	onumac
Circuit-id of interface	N/A

## 11.4.3 Enabling DHCP Option 82

### Enabling DHCP Option 82 on OLT

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip dhcp information option</b>	Enable DHCP Option 82 on the OLT. You can use the <b>no ip dhcp information option</b> command to disable this function.

## Enabling DHCP Option 82 on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*/*:*)#ip dhcp information option [ enable   disable ]</b>	Enable/Disable DHCP Option 82 on the ONU.

## 11.4.4 Configuring global DHCP Option attach-string

### Configuring global DHCP Option attach-string on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*/*:*)#ip dhcp information option82 attach-string attach-string</b>	Configure the attach-string of Option 82. You can use the <b>no ip dhcp information option82 attach-string</b> command to restore default configurations.

## 11.4.5 Configuring global DHCP Option remote-id

### Configuring global DHCP Option remote-id on OLT

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip dhcp information option remote-id { switch-mac   client-mac   switch-mac-string   client-mac-string   hostname   string string }</b>	Configure the remote ID of Option 82. You can use the <b>no ip dhcp information option remote-id</b> command to restore default configurations.

### Configuring global DHCP Option remote-id on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.

Step	Command	Description
3	<b>Raisecom(config-epon-onu-*//*:*)#ip dhcp information option82 remote-id string <i>string</i></b>	Configure the remote ID of Option 82. You can use the <b>no ip dhcp information option82 remote-id string</b> command to restore default configurations.
4	<b>Raisecom(config-epon-onu-*//*:*)#ip dhcp information option82 remote-id mode { client-mac   client-mac-string   hostname   onu-mac   onu-mac-string   user-defined <i>string</i> }</b>	Configure the filling mode of Option 82 remote ID. You can use the <b>no ip dhcp information option82 remote-id mode</b> command to restore default configurations.

## 11.4.6 Configuring DHCP Option circuit-id on interface

### Configuring DHCP Option circuit-id on OLT interface

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface { gigabitethernet   epon-olt } slot-id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-*//*:*)#ip dhcp information option circuit-id <i>string</i></b>	Configure the circuit ID of Option 82 on the OLT interface. You can use the <b>no ip dhcp information option circuit-id</b> command to restore default configurations.

### Configuring DHCP Option circuit-id on ONU interface

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</b>	Enter EPON ONU UNI configuration mode.
3	<b>Raisecom(config-epon-onu-ethernet-*//*:*)#ip dhcp information option82 circuit-id <i>string</i></b>	Configure the circuit ID of Option82 on the ONU interface. You can use the <b>no ip dhcp informaion option82 circuit-id</b> command to restore default configurations.

## 11.4.7 Configuring processing policy of Option 82 packet

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

Step	Command	Description
2	Raisecom(config)# <b>interface</b> { <b>gigabitethernet</b>   <b>epon-olt</b> } <i>slot-id/port-id</i>	Enter physical interface configuration mode.
3	Raisecom(config-if-**-*)# <b>ip</b> <b>dhcp information option</b> <b>overwrite-policy</b> { <b>drop</b>   <b>transparent</b> }	Configure the processing policy to the DHCP request packet containing Option 82 on the interface. You can use the <b>no ip dhcp information option overwrite-policy</b> command to restore default configurations.
4	Raisecom(config-if-**-*)# <b>ip</b> <b>dhcp information option</b> <b>overwrite-policy circuit-id</b> <b>replace</b> { <b>length</b> <i>len</i> }	Configure the processing policy to the circuit ID of the DHCP request packet containing Option 82. You can use the <b>no ip dhcp information option overwrite-policy</b> command to restore default configurations.

## 11.4.8 Checking configurations

### Checking configurations on OLT

No.	Command	Description
1	Raisecom# <b>show ip dhcp information option</b>	Show DHCP Option configurations.

### Checking configurations on ONU

No.	Command	Description
1	Raisecom# <b>show epon-onu</b> <i>slot-id/olt-id/onu-id</i> <b>ip dhcp information option82</b>	Show global DHCP Option82 configurations.
2	Raisecom# <b>show epon-onu</b> <i>slot-id/olt-id/onu-id</i> <b>uni ethernet uni-id ip dhcp information</b> <b>option82</b>	Show DHCP Option82 configurations on the interface.

## 11.5 Maintenance

Command	Description
Raisecom(config)# <b>clear epon-onu</b> <i>slot-id/olt-id/onu-id</i> <b>uni ethernet uni-id ip dhcp snooping statistics</b>	Clear DHCP Snooping statistics on the ONU interface.
Raisecom(config)# <b>clear epon-onu</b> <i>slot-id/olt-id/onu-id</i> <b>uni ethernet [ uni ] ip dhcp relay statistics</b>	Clear DHCP Relay statistics on the ONU interface.



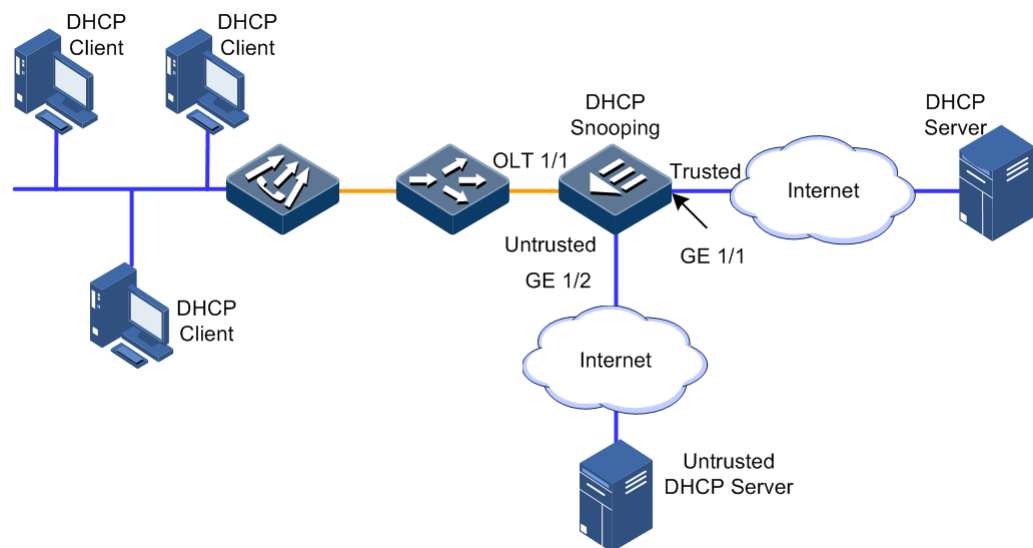
## 11.6 Configuration examples

### 11.6.1 Example for configuring DHCP Snooping

#### Networking requirements

As shown in Figure 11-6, 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 1/1 as raisecom, and filling information of the Remote ID sub-option as user 01.

Figure 11-6 DHCP Snooping networking



#### Configuration steps

Step 1 Configure global DHCP Snooping.

```
Raisecom#config  
Raisecom(config)#ip dhcp snooping
```

Step 2 Configure the trusted interface.

```
Raisecom(config)#interface gigabitethernet 1/1  
Raisecom(config-if-gigabitethernet-1/1)#ip dhcp snooping trust  
Raisecom(config-if-gigabitethernet-1/1)#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 1/1
Raisecom(config-if-epon-olt-1:1)#ip dhcp information option circuit-id
raisecom
```

## Checking results

Use the **show ip dhcp information option** command to show DHCP client configurations.

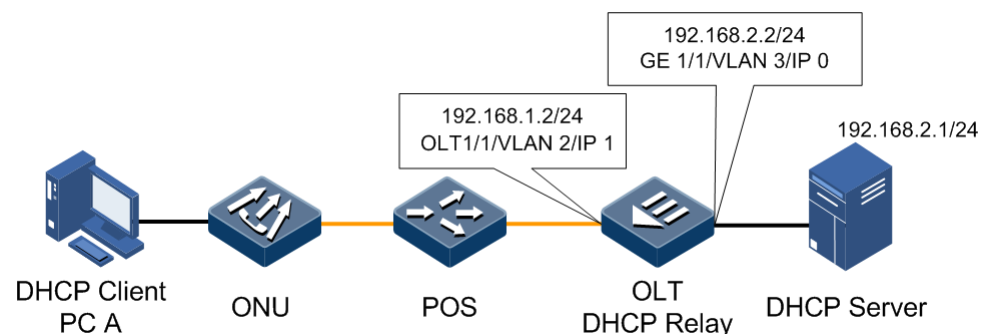
```
Raisecom#show ip dhcp information option
DHCP Option Config Information
Option 82: Enabled
Remote-ID Mode: string
Remote-ID String: user01
Port                               Op82Policy          CircuitId
-----
gigabitethernet1/1                replace              --
epon-olt1/1                        replace              raisecom
```

## 11.6.2 Example for configuring DHCP Relay

### Networking requirements

As shown in Figure 11-7, 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 11-7 DHCP Relay networking



### Configuration steps

Step 1 Configure global DHCP Relay.

```
Raisecom#config
Raisecom(config)#ip dhcp relay
```

Step 2 Configure the destination IP address of IP interface 1.

```
Raisecom(config)#ip dhcp relay ip-list 1 target-ip 192.168.2.1
```

Step 3 Configure supporting DHCP Option82.

```
Raisecom(config)#ip dhcp information option
```

Step 4 Configure interface GE 1/1 as the DHCP Relay trust interface.

```
Raisecom(config)#interface gigabitethernet 1/1  
Raisecom(config-if-gigabitethernet-1:1)#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	--
1	Enabled	--
2	Enabled	--
3	Enabled	--
4	Enabled	--
5	Enabled	192.168.2.1
6	Enabled	--
7	Enabled	--
8	Enabled	--
9	Enabled	--
10	Enabled	--
11	Enabled	--
12	Enabled	--
13	Enabled	--
14	Enabled	--

# 12 Configuring QoS

---

This chapter introduces the QoS feature and configuration process of the ISCOM5508, and provides related configuration examples, including the following sections:

- Overview of QoS
- Configuring traffic classification
- Configuring traffic monitoring
- Configuring congestion management
- Configuring congestion avoidance
- Configuring traffic shaping
- Configuring traffic policy
- Configuration examples

## 12.1 Overview of QoS

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 to transmit packets 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 the whole network runs high-efficiently.

### 12.1.1 Priority trust

Priority trust refers 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.

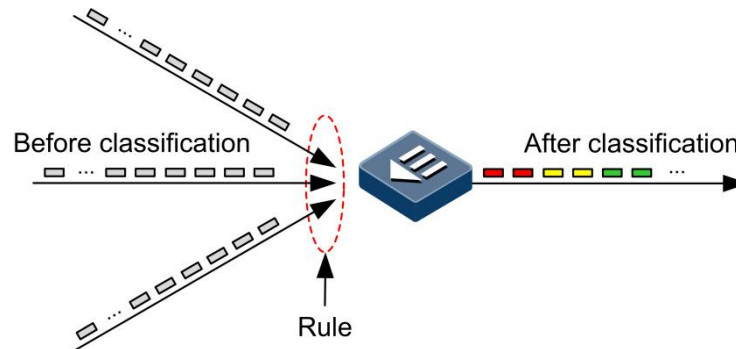
The ISCOM5508 supports port-based priority trust. The priorities are divided into priority based on Differentiated Services Code Point (DSCP) of IPv4 packets, priority based on Class of Service (CoS) of VLAN packets, and priority based on Traffic Class (TC) of IPv6 packets.

## 12.1.2 Traffic classification

Traffic classification is a process that recognizes specified packets according to some certain rule. All resulting packets can be treated differently to differentiate the service implied to users.

The ISCOM5508 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 12-1 shows the traffic classification process.

Figure 12-1 Traffic classification process



### ToS priority and DSCP priority

Figure 12-2 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 12-3 shows structures of ToS and DSCP priority packets.

Figure 12-2 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			

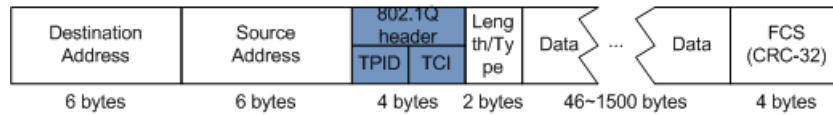
Figure 12-3 Structures of ToS priority and DSCP priority packets

Bits:	0	1	2	3	4	5	6	7
RFC1349:	Precedence		Type of Service			0		
RFC2474:	DSCP						Unused	

### CoS priority

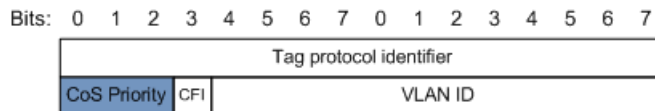
IEEE802.1Q-based VLAN packets are a modification of Ethernet packets. A 4-bit 802.1Q header is added between the source MAC address and protocol type, as shown in Figure 12-4. The 802.1Q header consists a 2-bit Tag Protocol Identifier (TPID, valuing 0x8100) field and a 2-bit Tag Control Information (TCI) field.

Figure 12-4 VLAN packet structure



The first 3 bits of TCI field represent the CoS priority, which ranges from 0 to 7, as shown in Figure 12-5. The bigger the number is, the higher the CoS priority is. CoS priority is used for ensuring service quality in Layer 2 network.

Figure 12-5 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, is 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.

### 12.1.3 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 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.

### 12.1.4 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.

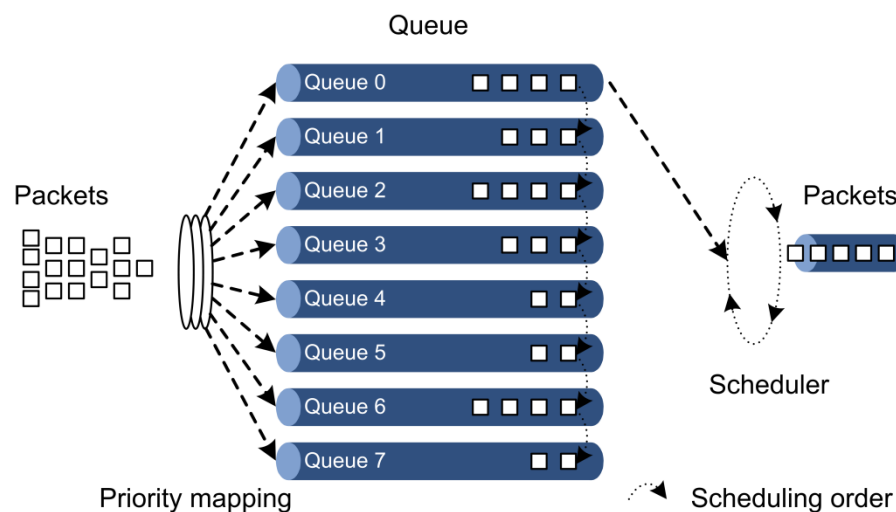
### 12.1.5 Congestion management

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 ISCOM5508 include Strict Priority (SP), Weight Round Robin (WRR), Deficit Round Robin (DRR), SP+WRR, and SP+DRR. All scheduling algorithms are designed for addressing specified traffic problems. And they have different effects on bandwidth distribution, delay, and jitter.

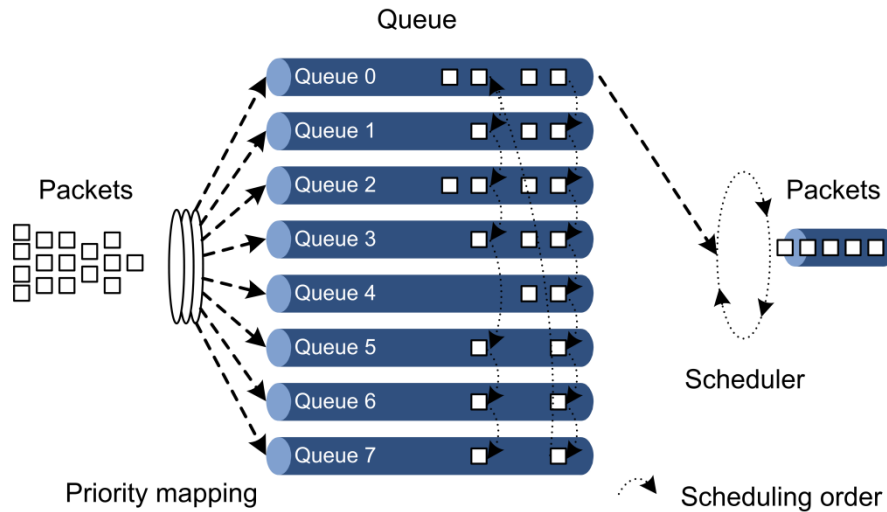
- SP: the device strictly schedules packets in a descending order of priority. Packets with lower priority cannot be scheduled until packets with higher priority are scheduled, as shown in Figure 12-6.

Figure 12-6 SP scheduling



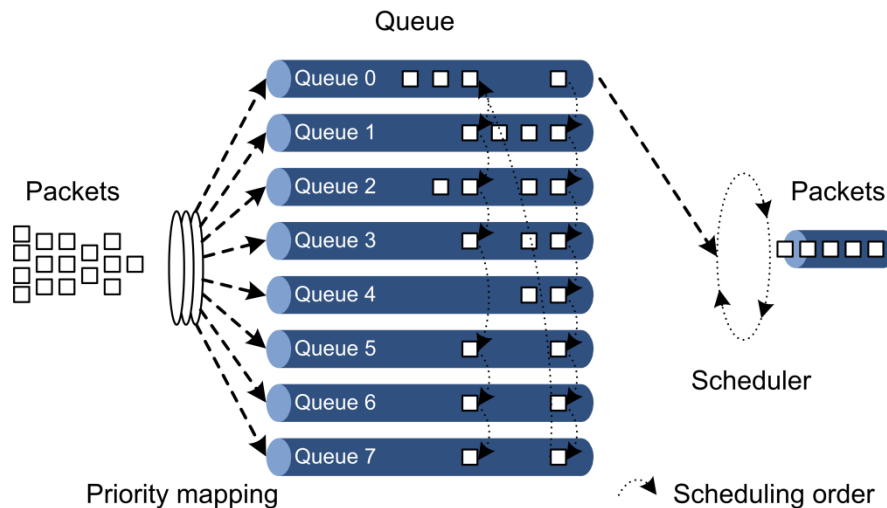
- WRR: on the basis of scheduling packets in a polling manner according to the priority, the device schedules packets according to the weight of the queue, as shown in Figure 12-7.

Figure 12-7 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 12-8.

Figure 12-8 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 queues where SP scheduling/WRR scheduling is performed.
- SP+DRR: a scheduling mode combining the SP scheduling and the DRR scheduling together. In this mode, queues on a port are divided into 2 groups. You can specify the queues where SP scheduling/DRR scheduling is performed.



## 12.2 Configuring traffic classification

### 12.2.1 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

### 12.2.2 Default configurations

#### Priority trust

Default configurations of priority trust are as below.

Function	Default value
Priority trust type on OLT	CoS
Default priority of OLT interface	0
Priority trust status of ONU UNI	Untrusted

#### Priority mapping

Mapping among the CoS priority, local priority, and queue on the ISCOM5508 is as below.

<b>CoS priority</b>	0	1	2	3	4	5	6	7
<b>Local priority</b>	0	1	2	3	4	5	6	7
<b>Queue</b>	0	1	2	3	4	5	6	7



Mapping among the DSCP priority, local priority, and queue on the ISCOM5508 is as below.

<b>DSCP priority</b>	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
<b>Local priority</b>	0	1	2	3	4	5	6	7
<b>Queue</b>	0	1	2	3	4	5	6	7

Mapping between the CoS priority and queue on the ONU is as below.

<b>CoS</b>	0	1	2	3	4	5	6	7
<b>Queue</b>	0	0	1	1	2	2	3	3

### 12.2.3 Configuring priority trust

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <b>{ gigabitethernet   epon-</b> <b>olt } slot-id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-*/-*/-*)#mls</b> <b>qos trust dscp</b>	<p>Configure trusting the DSCP field.</p> <p>You can use the <b>no mls qos trust</b> command to restore default configurations.</p> <div>  <b>Note</b> <ul style="list-style-type: none"> <li>For IPv4 packets, this command refers to trusting the DSCP field. For IPv6 packets, this command refers to trusting the Traffic Class field.</li> <li>By default, interfaces on the device trust the CoS priority. Therefore, when you need to configure trusting the CoS priority, use the <b>no</b> form of this command to restore default configurations.</li> </ul> </div>
4	<b>Raisecom(config-if-</b> <b>gigabitethernet-*/-*/-*)#mls qos</b> <b>priority value</b>	<p>Configure the default priority of the interface.</p> <p>You can use the <b>no mls qos priority</b> command to restore default configurations.</p> <div>  <b>Note</b> <p>For packets without the 802.1p field, use the default priority.</p> </div>

### 12.2.4 Configuring priority mapping

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

Step	Command	Description
2	<code>Raisecom(config)#mls qos mapping cos <i>cos-value</i> to localpriority <i>local-priority</i></code>	(Optional) configure mapping between the CoS priority and local priority. You can use the <b>no mls qos mapping cos</b> command to restore default configurations.
3	<code>Raisecom(config)#mls qos mapping dscp <i>dscp-value</i> to localpriority <i>local-priority</i></code>	(Optional) configure mapping between the DSCP priority and local priority. You can use the <b>no mls qos mapping dscp</b> command to restore default configurations.
4	<code>Raisecom(config)#mls qos mapping localpriority <i>local-priority</i> to queue <i>queue-id</i></code>	(Optional) configure mapping between the local priority and queue. You can use the <b>no mls qos mapping localpriority</b> command to restore default configurations.

## 12.2.5 Checking configurations

No.	Command	Description
1	<code>Raisecom#show interface { gigabitethernet   epon-olt } <i>slot-id/port-id</i> mls qos</code>	Show QoS configurations on the interface, including interface trust mode, queue scheduling mode, and default CoS value.
2	<code>Raisecom#show mls qos mapping cos</code>	Show mapping between the CoS priority and local priority.
3	<code>Raisecom#show mls qos mapping dscp</code>	Show mapping between the DSCP priority and local priority.
4	<code>Raisecom#show mls qos mapping local-priority</code>	Show mapping between the local priority and queue.

## 12.3 Configuring traffic monitoring

### 12.3.1 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 method for traffic measurement 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. In addition, there are two algorithm modes for the token bucket: color-blind and color-sensitive. So there are six algorithm modes in total:

- Single-rate single-token bucket (color-blind and color-sensitive)
- Single-rate dual-token bucket (color-blind and color-sensitive)
- Dual-rate dual-token bucket (color-blind and color-sensitive)

## Prerequisite

N/A

## 12.3.2 Default configurations

N/A

## 12.3.3 Configuring rate limiting

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>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 } ]</code>	Create rate limiting rules and specify the action to take when the rate exceeds the threshold (single-token bucket monitoring)
3	<code>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 ]</code>	Create rate limiting rules and specify the action to take when the rate exceeds the threshold (dual-token bucket monitoring)



### Note

When you configure the PIR parameter, the rate limiting policer works in dual-token bucket mode. Otherwise, it works in single-token bucket mode.

## 12.3.4 Checking configurations

No.	Command	Description
1	<code>Raisecom#show mls qos policer [ policer-id ]</code>	Show configurations of the rate limiting policer.

## 12.4 Configuring congestion management

### 12.4.1 Preparing for configurations

#### Scenario

Congestion management refers to allocating and controlling bandwidth when the network is congested. Congestion management adopts the queue technology to buffer 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

### 12.4.2 Default configurations

#### Scheduling mode

Default configurations of the queue scheduling mode are as below.

Function	Default value
Queue scheduling mode of OLT	SP
Queue scheduling mode of ONU	SP

#### Queue weight

Default weights of WDRR and WRR queues on the ISCOM5508 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

Default weights of queues on the ONU are as below (the bigger the weight is, the higher the priority is. However, the queue whose weight is 0 has the highest priority).

Queue	0	1	2	3	4	5	6	7
Weight	1	2	4	8	0	0	0	0

### 12.4.3 Configuring SP scheduling

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <b>{ gigabitethernet   epon-olt } slot-</b> <b>id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-*:*:*)#mls qos</b> <b>queue scheduler sp</b>	Configure the queue scheduling mode to SP. You can use the <b>no mls qos queue scheduler</b> command to restore default configurations.

### 12.4.4 Configuring WRR scheduling

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <b>{ gigabitethernet   epon-olt } slot-</b> <b>id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-*:*:*)#mls qos queue</b> <b>scheduler wrr</b>	Configure the queue scheduling mode to WRR. You can use the <b>no mls qos queue scheduler</b> command to restore default configurations.
4	<b>Raisecom(config-if-*:*:*)#mls qos queue</b> <b>wrr value0 value1 value2 value3 value4</b> <b>value5 value6 value7</b>	Configure the weight of each queue in WRR scheduling mode.

### 12.4.5 Configuring WDRR scheduling

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <b>{ gigabitethernet   epon-olt } slot-</b> <b>id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-*:*:*)#mls qos queue</b> <b>scheduler wdr</b>	Configure the queue scheduling mode to WDRR. You can use the <b>no mls qos queue scheduler</b> command to restore default configurations.
4	<b>Raisecom(config-if-*:*:*)#mls qos queue</b> <b>wdr value0 value1 value2 value3 value4</b> <b>value5 value6 value7</b>	Configure the weight of each queue in WDRR scheduling mode.

## 12.4.6 Checking configurations

No.	Command	Description
1	<code>Raisecom#show interface { gigabitethernet   epon-olt } slot-id/port-id mls qos</code>	Show QoS configurations on the interface, including interface trust mode, queue scheduling mode, and default CoS value.
2	<code>Raisecom#show interface { gigabitethernet   epon-olt } slot-id/port-id mls qos queue</code>	Show configurations of queue weights.

## 12.5 Configuring congestion avoidance

### 12.5.1 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, for TCP packets, if a number of packets are dropped, it 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

### 12.5.2 Default configurations

N/A

### 12.5.3 Configuring WRED scheduling

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface { gigabitethernet   epon-olt } slot-id/port-id</code>	Enter physical interface configuration mode.

Step	Command	Description
3	<code>Raisecom(config-if-*:*:*)#mls qos wred [ queue <i>queue-id</i> ] [ red   green   yellow ] low-limit <i>value</i> high-limit <i>value</i> drop-probability <i>value</i></code>	Configure WRED scheduling parameters.

## 12.5.4 Checking configurations

No.	Command	Description
1	<code>Raisecom#show interface { gigabitethernet   epon-olt } slot-id/port-id mls qos queue wred</code>	Show WRED configurations.

## 12.6 Configuring traffic shaping

### 12.6.1 Preparing for configurations

#### Scenario

Traffic shaping aims to eliminate the burst traffic to make it output smoothly. Traffic shaping is usually used on the egress interface.

Similar to traffic monitoring, traffic shaping also adopts the token bucket to measure traffic. Different from traffic monitoring, traffic shaping 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

### 12.6.2 Default configurations

Default configurations of traffic shaping are as below.

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



Queue	CIR (Kbit/s)	CBS (Kbit/s)	Gts-buffer (Byte)
7	0	0	1000

### 12.6.3 Configuring traffic shaping

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <b>{ gigabitethernet   epon-olt } slot-</b> <b>id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-*:*:*)#mls qos shaping</b> <b>[ queue queue-id ] cir cir cbs cbs [ gts-</b> <b>buffer size ]</b>	Configure traffic shaping.

### 12.6.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show interface { gigabitethernet  </b> <b>epon-olt } slot-id/port-id mls qos queue</b> <b>shaping</b>	Show configurations of traffic shaping.

## 12.7 Configuring traffic policy

### 12.7.1 Preparing for configurations

#### Scenario

After traffic classification, you need to perform different operations on packets of different types, for example, redirect some specified traffic to other physical interfaces.


#### Prerequisite

N/A

### 12.7.2 Default configurations

N/A

### 12.7.3 Configuring traffic policy on OLT

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#{ ip-access-list list-number   ipv6-access-list list-number   l2-access-list list-number   hybrid-access-list list-number   user-access-list list-number }</b>	Create an ACL and enter ACL configuration mode.
3	<b>Raisecom(config-*-acl-*)#rule rule-id</b>	Create an ACL sub-rule and enter ACL sub-rule configuration mode.
4	<b>Raisecom(config-*-acl-*-*rule-*)#set { ip dscp value   ip precedence value   cos cos   vlan vlan-id }</b>	Remark the data traffic.  <div>  <b>Note</b>            Remarking the data traffic complies with the backward effective principle.         </div>
5	<b>Raisecom(config-*-acl-*-*rule-*)#redirect-to interface { gigabitethernet   epon-olt } slot-id/port-id</b>	Redirect the data traffic to other interfaces.
6	<b>Raisecom(config-*-acl-*-*rule-*)#mirror-to interface { gigabitethernet   epon-olt } slot-id/port-id</b>	Mirror the data traffic to other interfaces.
7	<b>Raisecom(config-*-acl-*-*rule-*)#policer policer-id</b>	Bind the rate limiting policer to limit the rate of data traffic.

### 12.7.4 Configuring traffic policy on ONU

Traffic classification and traffic policy refers to classifying packets into different traffic according to the service requirement and packet characteristics to provide differentiated services. Traffic filtering on the interface refers to forwarding or discarding traffic which meets the requirement.

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

Step	Command	Description
2	Raisecom(config)# <b>create class</b> <i>rule-id</i> <b>match</b> { <b>cos</b> <i>cos-vlaue</i>   <b>dip</b> <i>ip-address</i>   <b>sip</b> <i>ip-address</i>   <b>dmac</b> <i>mac-address</i>   <b>smac</b> <i>mac-address</i>   <b>l4-dport</b> <i>port-number</i>   <b>l4-sport</b> <i>port-number</i>   <b>dscp</b> <i>dscp-value</i>   <b>eth-type</b> <i>type-vlaue</i>   <b>protocol</b> { <i>hh</i>   <b>icmp</b>   <b>igmp</b>   <b>tcp</b>   <b>udp</b> }   <b>vlan</b> <i>vlan-id</i>   <b>ipv6-dscp</b> <i>dscp-value</i>   <b>flow-label</b> <i>label-value</i>   <b>ip-vision</b> <i>vision-value</i>   <b>dipv6</b> <i>ipv6-address</i>   <b>sipv6</b> <i>ipv6-address</i>   <b>dipv6-prefix</b> <i>prefix-value</i>   <b>sipv6-prefix</b> <i>prefix-value</i>   <b>nexthead</b> { <i>protocol-number</i>   <b>icmp</b>   <b>igmp</b>   <b>tcp</b>   <b>udp</b> } } { <b>always-match</b>   <b>equal</b>   <b>exist</b>   <b>greater-equal</b>   <b>less-equal</b>   <b>never-match</b>   <b>not-equal</b>   <b>not-exist</b> }	Define the classification rule of data traffic.  You can use the <b>no class</b> { <b>all</b>   <i>rule-id</i> } command to delete the classification rule.
3	Raisecom(config)# <b>create policy</b> <i>rule-id</i> <b>class</b> <i>rule-list</i> <b>queue-map</b> <i>queue-id</i> <b>pri-marking</b> <i>priority</i> [ <b>weight</b> <i>weight-value</i> ]	Create the traffic policy.  You can use the <b>no policy</b> { <b>all</b>   <i>rule-id</i> } command to delete the traffic policy.
4	Raisecom(config)# <b>epon-onu uni ethernet</b> <i>slot-id/olt-id/onu-id/uni-id</i>	Enter EPON ONU UNI configuration mode.
5	Raisecom(config-epon-onu-ethernet- <i>*//*/*.*</i> )# <b>policy</b> <i>rule-list</i>	Apply the traffic policy on the UNI.  You can use the <b>no policy</b> command to delete the traffic policy from the UNI.
6	Raisecom(config-epon-onu-ethernet- <i>*//*/*.*</i> )# <b>filter</b> { <b>permit</b> / <b>deny</b> } { <b>match-all</b> / <b>match-any</b> } <i>policy rule-list</i>	(Optional) filter traffic entered into the Ethernet interface on the ONU.  You can use the <b>no filter</b> command to delete the filtering rule from the ONU.

## 12.7.5 Checking configurations

### Checking configurations on OLT

No.	Command	Description
1	Raisecom# <b>show mls qos policer</b>	Show rate limiting configurations

### Checking configurations on ONU

No.	Command	Description
1	Raisecom# <b>show onu-remote class</b> { <b>all</b>   <i>rule-list</i> }	Show configurations of traffic classification on the ONU.
2	Raisecom# <b>show onu-remote policy</b> { <b>all</b>   <i>rule-list</i> }	Show configurations of traffic policy on the ONU.

No.	Command	Description
3	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet [ uni-id ] policy</b>	Show the traffic policy applied on the UNI.
4	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet [ uni-id ] filter</b>	Show the filtering rules applied on the UNI.
5	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id queue</b>	Show the queue scheduling mode on the ONU.

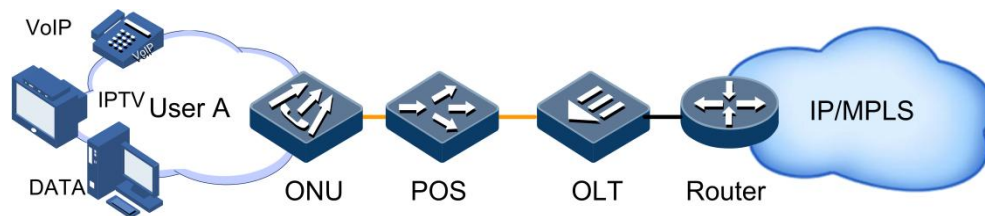
## 12.8 Configuration examples

### 12.8.1 Example for configuring rate limiting

#### Networking requirements

As shown in Figure 12-9, User A belongs to VLAN 2 and connects to the OLT through an ONU. According to users' requirements, provide a bandwidth of 25 Mbit/s for User A. The burst traffic is 100 Bytes. Excessive traffic is dropped.

Figure 12-9 Configuring rate limiting based on traffic policy



#### Configuration steps

Step 1 Create rate limiting rules.

```
Raisecom#config
Raisecom(config)#mls qos single-policer 1 cir 25000 cbs 100 red drop
green drop
```

Step 2 Bind the filter rule to the policy.

```
Raisecom(config)#12-access-list 1
Raisecom(config-12-acl-1)#rule 1
Raisecom(config-12-acl-1-rule-1)#policer 1
Raisecom(config-12-acl-1-rule-1)#set vlan 2
Raisecom(config-12-acl-1-rule-1)#exit
Raisecom(config-12-acl-1)#exit
```

Step 3 Apply the ACL to the ISCOM5508.

```
Raisecom(config)#filter 12-access-list 1
```

## Checking results

Show rate limiting configurations.

```
Raisecom#show mls qos policer 1
```

ID	Type	Rate	Burst	Exceed	Action	New DSCP	Ref. Times
1	single	25000	100	drop	--		

## 12.8.2 Example for configuring queue scheduling

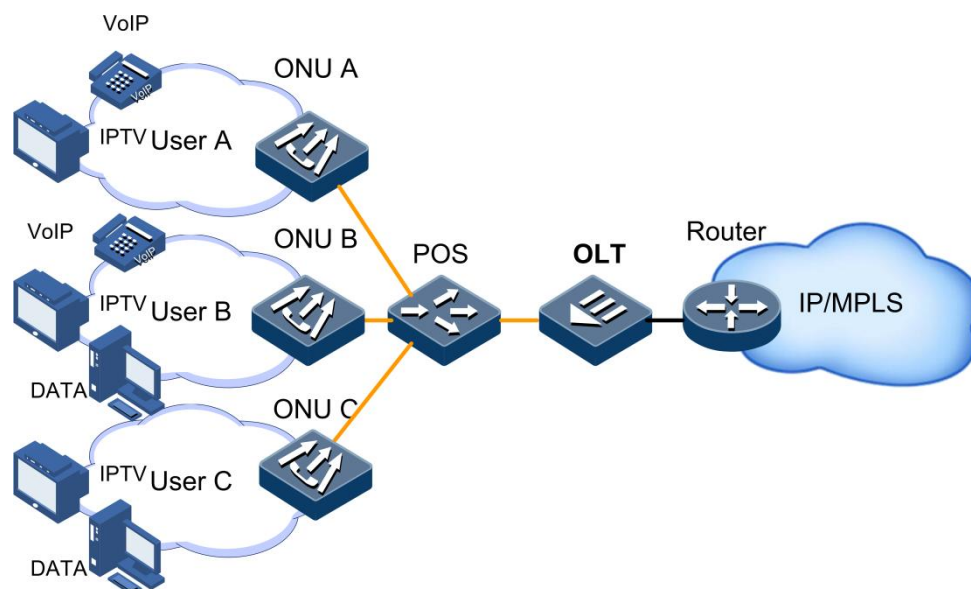
### Networking requirements

As shown in Figure 12-10, 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 12-10 Configuring queue scheduling



## Configuration steps

Step 1 Configure interface priority trust.

```
Raisecom#config
Raisecom(config)#interface epon-olt 1/1
Raisecom(config-if-epon-olt-1:1)#no mls qos trust dscp
Raisecom(config-if-epon-olt-1:1)#exit
```

Step 2 Configure mapping between the CoS priority and local priority.

```
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 epon-olt 1/1
Raisecom(config-if-epon-olt-1:1)#mls qos queue scheduler wrr
Raisecom(config-if-epon-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
```

# 13 Configuring system security

---

This chapter introduces the system security feature and configuration process of the ISCOM5508, and provides related configuration examples, including the following sections:

- Overview of system security
- Configuring ACL
- Configuring RADIUS
- Configuring TACACS+
- Configuring storm control
- Configuring interface isolation
- Configuring attack defense
- Configuring IP Source Guard
- Configuring DAI
- Maintenance
- Configuration examples

## 13.1 Overview of system security

### 13.1.1 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.

### 13.1.2 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.

### 13.1.3 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.

### 13.1.4 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 occurring when broadcast packets increase sharply on the network. Therefore, it makes sure that unicast packets can be properly forwarded.

### 13.1.5 Interface isolation

Interface isolation adopts the isolation group method to realize data isolation among multiple interfaces on the device, thus enhancing network access security.

The ISCOM5508 supports the following three types of interface isolation:

- OLT physical interface isolation: include isolation among different interfaces on the same interface card and isolation among different interfaces on different interface cards.
- OLT VLAN interface isolation: one VLAN contain multiple isolation groups. Interfaces in the same isolation group cannot communicate. Interfaces of different isolation groups



can communicate with each other. Interfaces in the VLAN, which are not in the isolation group, can communicate with any interface in the same VLAN.

- ONU UNI isolation

### 13.1.6 IP Source Guard

IP Source Guard uses a binding table to defend against IP Source spoofing and solve IP address embezzlement without identity authentication. IP Source Guard can cooperate with DHCP Snooping to generate dynamic binding. In addition, you can configure static binding manually. DHCP Snooping filters untrusted DHCP packets by establishing and maintaining the DHCP binding database.

#### IP Source Guard binding entry

IP Source Guard is used to match packet characteristics, including source IP address, source MAC address, and VLAN Tags, and can support the interface to be combined with the following characteristics (hereinafter referred to as binding entries):

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

According to the generation mode of binding entries, IP Source Guard can be divided into static binding and dynamic binding:

- Static binding: configure binding information manually and generate binding entry to complete the interface control, which fits for the case where the number of hosts is small or where you need to perform separate binding on a single host.
- Dynamic binding: obtain binding information automatically from DHCP Snooping to complete the interface control, which fits for the case where there are many hosts and you need to adopt DHCP to perform dynamic host configurations. Dynamic binding can effectively prevent IP address conflict and embezzlement.

#### Principles of IP Source Guard

Principles of IP Source Guard are to create an IP source binding table on the ISCOM5508. The IP source binding table is taken as the basis for each interface to test received data packets.

- If the received IP packets meet the corresponding relation of Port/IP/MAC/VLAN binding entries in IP source binding table, the device will forward these packets.
- If the received IP packets are DHCP data packets, the device will forward these packets.
- Otherwise, the device will discard these packets.

Before forwarding IP packets, the ISCOM5508 compares the source IP address, source MAC address, interface, and VLAN of the IP packets with information in the binding table. If the information matches, it indicates that the user is legal and the packets are permitted to be forwarded normally. Otherwise, the user is an attacker and the IP packets are discarded.

### 13.1.7 DAI

Dynamic ARP Inspection (DAI) binds the IP address with MAC address and establishes binding relations dynamically. DAI is based on DHCP Snooping binding table. For servers

which are not enabled with DHCP, you can add ARP access-list statically. DAI can be configured according to VLAN. For interfaces in the same VLAN, you can enable/disable DAI. The number of ARP request packets on certain interface can be controlled through DAI, thus preventing DoS attacks.

## 13.2 Configuring ACL

### 13.2.1 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 corresponding packets to pass according to the configured policy.

ACL can be divided into the following types.

- IP ACL: according to the source or destination address, used TCP or UDP port ID, and other data packet attributes carried by the IP head to formulate classification rules.
- IPv6 ACL: according to the source or destination address, used TCP or UDP port ID, and other data packet attributes carried by the IP head to formulate classification rules.
- Layer 2 ACL: 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 head to formulate classification rules.
- Hybrid ACL: according to information about the IP head and Layer 2 frame head to formulate classification rules. This type of ACL mixes characteristics of IP ACL and Layer 2 ACL.
- IPv6 hybrid ACL: according to information about the IPv6 head and Layer 2 frame head to formulate classification rules. 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

### 13.2.2 Default configurations

N/A

## 13.2.3 Configuring IP ACL

### Configuring IPv4 ACL

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip-access-list</b> <i>list-number</i>	Create an IPv4 ACL and enter IPv4 ACL configuration mode.  You can use the <b>no ip-access-list { all   list-number }</b> command to delete the ACL.
3	<b>Raisecom(config-ip-acl-*)#description</b> <i>desc-string</i>	(Optional) configure descriptions of the IPv4 ACL.
4	<b>Raisecom(config-ip-acl-*)#rule</b> <i>rule-number</i>	Configure the number of the IPv4 ACL sub-rule.
5	<b>Raisecom(config-ip-acl-*--rule-*)#access-type</b> { <b>permit</b>   <b>deny</b> }	Configure the access type of the IPv4 ACL sub-rule.
6	<b>Raisecom(config-ip-acl-*--rule-*)#match ip destination-address</b> <i>ip-address</i> [ <i>mask</i> ]	Configure the destination IP address of the IPv4 ACL sub-rule.
7	<b>Raisecom(config-ip-acl-*--rule-*)#match ip source-address</b> <i>ip-address</i> [ <i>mask</i> ]	Configure the source IP address of the IPv4 ACL sub-rule.
8	<b>Raisecom(config-ip-acl-*--rule-*)#match ip precedence</b> { <i>pri</i>   <b>routine</b>   <b>priority</b>   <b>immediate</b>   <b>flash</b>   <b>flash-override</b>   <b>critical</b>   <b>internet</b>   <b>network</b> }	Configure matching the IPv4 ACL sub-rule with the source IP precedence.
9	<b>Raisecom(config-ip-acl-*--rule-*)#match ip tos</b> { <i>service-value</i>   <b>normal</b>   <b>min-monetary-cost</b>   <b>min-delay</b>   <b>max-reliability</b>   <b>max-throughput</b> }	Configure matching the IPv4 ACL sub-rule with the IP ToS.
10	<b>Raisecom(config-ip-*--rule-*)#match ip dscp</b> { <i>diff-service-code</i>   <b>af11</b>   <b>af12</b>   <b>af13</b>   <b>af21</b>   <b>af22</b>   <b>af23</b>   <b>af31</b>   <b>af32</b>   <b>af33</b>   <b>af41</b>   <b>af42</b>   <b>af43</b>   <b>cs1</b>   <b>cs2</b>   <b>cs3</b>   <b>cs4</b>   <b>cs5</b>   <b>cs6</b>   <b>cs7</b>   <b>ef</b>   <b>default</b> }	Configure matching the IPv4 ACL sub-rule with IP DSCP.
11	<b>Raisecom(config-ip-acl-*--rule-*)#match ip</b> { <b>fragments</b>   <b>no-fragments</b> }	Configure matching the IPv4 ACL sub-rule with the fragmented or non-fragmented packet.
12	<b>Raisecom(config-ip-*--rule-*)#match ip protocol</b> { <i>protocol-num</i>   <b>ahp</b>   <b>esp</b>   <b>gre</b>   <b>icmp</b>   <b>igmp</b>   <b>igrp</b>   <b>ipinip</b>   <b>ospf</b>   <b>pcp</b>   <b>pim</b>   <b>tcp</b>   <b>udp</b> }	Configure matching the IPv4 ACL sub-rule with the IP upper protocol type.

Step	Command	Description
13	<code>Raisecom(config-ip-*<b>-rule</b>-*)#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 }</code>	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.
14	<code>Raisecom(config-ip-*<b>-rule</b>-*)#match ip tcp { ack   fin   psh   rst   syn   urg }</code>	Configure matching the IPv4 ACL sub-rule with the TCP packet flag.
15	<code>Raisecom(config-ip-*<b>-rule</b>-*)#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 }</code>	Configure matching the IPv4 ACL sub-rule with the destination/source interface ID of the UDP packet.

## Configuring IPv6 ACL

Step	Command	Description
1	<code>Raisecom#<b>config</b></code>	Enter global configuration mode.
2	<code>Raisecom(config)#<b>ipv6-access-list list-number</b></code>	Create an IPv6 ACL and enter IPv6 ACL configuration mode. You can use the <b>no ipv6-access-list { all   list-number }</b> command to delete the ACL.
3	<code>Raisecom(config-ipv6-acl-*<b>-rule</b>-*)#<b>description desc-string</b></code>	(Optional) configure descriptions of the IPv6 ACL.
4	<code>Raisecom(config-ipv6-acl-*<b>-rule</b>-*)#<b>rule rule-number</b></code>	Configure the number of the IPv6 ACL sub-rule.
5	<code>Raisecom(config-ipv6-acl-*<b>-rule</b>-*)#<b>access-type { permit   deny }</b></code>	Configure the access type of the IPv6 ACL sub-rule.
6	<code>Raisecom(config-ipv6-acl-*<b>-rule</b>-*)#<b>match ip destination-address ipv6-address/prefix-length</b></code>	Configure the destination IP address of the IPv6 ACL sub-rule.
7	<code>Raisecom(config-ipv6-acl-*<b>-rule</b>-*)#<b>match ip source-address ipv6-address/prefix-length</b></code>	Configure the source IP address of the IPv6 ACL sub-rule.
8	<code>Raisecom(config-ipv6-acl-*<b>-rule</b>-*)#<b>match ip traffic-class user-level</b></code>	Configure the IPv6 ACL sub-rule matching with the user level of the IPv6 packet.
9	<code>Raisecom(config-ipv6-acl-*<b>-rule</b>-*)#<b>match ip protocol ipv6-protocol-num</b></code>	Configure the IPv6 ACL sub-rule matching with IP upper protocol type.

Step	Command	Description
10	Raisecom(config-ipv6-acl- <i>rule</i> -*)# <b>match ip tcp</b> { <b>destination-port</b>   <b>source-port</b> } { <i>port-num</i>   <b>bgp</b>   <b>domain</b>   <b>echo</b>   <b>exec</b>   <b>finger</b>   <b>ftp</b>   <b>ftp-data</b>   <b>gopher</b>   <b>hostname</b> / <b>ident</b>   <b>irc</b>   <b>klogin</b>   <b>kshell</b>   <b>login</b>   <b>lpd</b>   <b>nntp</b>   <b>pim-auto-rp</b>   <b>pop2</b>   <b>pop3</b>   <b>smtp</b>   <b>sunrpc</b>   <b>syslog</b>   <b>tacacs</b>   <b>talk</b>   <b>telnet</b>   <b>time</b>   <b>uucp</b>   <b>whois</b>   <b>www</b> }	Configure matching the IPv6 ACL sub-rule with the destination/source interface ID of the TCP packet.
11	Raisecom(config-ipv6-acl- <i>rule</i> -*)# <b>match ip tcp</b> { <b>ack</b>   <b>fin</b>   <b>psh</b>   <b>rst</b>   <b>syn</b>   <b>urg</b> }	Configure matching the IPv6 ACL sub-rule with the TCP packet flag.
12	Raisecom(config-ipv6-acl- <i>rule</i> -*)# <b>match ip flow-label</b> <i>label-num</i>	Configure matching the IPv6 ACL sub-rule with the flow label of the IPv6 packet.
13	Raisecom(config-ip-acl- <i>rule</i> -*)# <b>match ip udp</b> { <b>destination-port</b>   <b>source-port</b> } { <i>port-num</i>   <b>biff</b>   <b>bootpc</b>   <b>bootps</b>   <b>domain</b>   <b>echo</b>   <b>mobile-ip</b>   <b>netbios-dgm</b>   <b>netbios-ns</b>   <b>netbios-ss</b>   <b>ntp</b>   <b>pim-auto-rp</b>   <b>rip</b>   <b>snmp</b>   <b>snmptrap</b>   <b>sunrpc</b>   <b>syslog</b>   <b>tacacs</b>   <b>talk</b>   <b>tftp</b>   <b>time</b>   <b>who</b> }	Configure matching the IPv6 ACL sub-rule with the destination/source interface ID of the UDP packet.

### 13.2.4 Configuring Layer 2 ACL

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>l2-access-list</b> <i>list-number</i>	Create a Layer 2 ACL and enter Layer 2 ACL configuration mode.  You can use the <b>no l2-access-list acl-number</b> command to delete the ACL.
3	Raisecom(config-l2-acl-*)# <b>description</b> <i>desc-string</i>	(Optional) configure descriptions of the Layer 2 ACL.
4	Raisecom(config-l2-acl-*)# <b>rule</b> <i>rule-number</i>	Configure the number of the Layer 2 ACL sub-rule.
5	Raisecom(config-l2-acl- <i>rule</i> -*)# <b>access-type</b> { <b>permit</b>   <b>deny</b> }	Configure the access type of the Layer 2 ACL sub-rule.
6	Raisecom(config-l2-acl- <i>rule</i> -*)# <b>match mac destination</b> <i>mac</i> [ <i>mac-mask</i> ]	Configure the destination MAC address of the Layer 2 ACL sub-rule.
7	Raisecom(config-l2-acl- <i>rule</i> -*)# <b>match mac source</b> <i>mac</i> [ <i>mac-mask</i> ]	Configure the source MAC address of the Layer 2 ACL sub-rule.
8	Raisecom(config-l2-acl- <i>rule</i> -*)# <b>match vlan</b> <i>vlan-id</i>	Configure matching the Layer 2 ACL sub-rule with the source VLAN ID.

Step	Command	Description
9	<code>Raisecom(config-l2-acl-* -rule-*)#match svlan-cos <i>svlan-cos</i></code>	Configure matching the Layer 2 ACL sub-rule with the SVLAN CoS.
10	<code>Raisecom(config-l2-acl-* -rule-*)#match cvlan <i>cvlan-id</i></code>	Configure matching the Layer 2 ACL sub-rule with the source CVLAN ID.
11	<code>Raisecom(config-l2-acl-* -rule-*)#match cvlan-cos <i>cvlan-cos</i></code>	Configure matching the Layer 2 ACL sub-rule with the CVLAN CoS.
12	<code>Raisecom(config-l2-acl-* -rule-*)#match ethertype <i>frame-type</i> <i>frame-type-mask</i></code>	Configure matching the Layer 2 ACL sub-rule with the frame type in the Layer 2 frame head.
13	<code>Raisecom(config-l2-acl-* -rule-*)#match ethertype { arp   eapol   flowcontrol   ip   ipv6   loopback   mpls   mpls-mcast   pppoe   pppoedisc   x25   x75 }</code>	Configure matching the Layer 2 ACL sub-rule with the protocol type in the Layer 2 frame head.

## 13.2.5 Configuring hybrid ACL

### Configuring IPv4 hybrid ACL

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#hybrid-access-list <i>list-number</i></code>	Create a hybrid ACL and enter hybrid ACL configuration mode.  You can use the <b>no hybrid-access-list { all   list-number }</b> command to delete the ACL.
3	<code>Raisecom(config-hybrid-acl-*)#description <i>desc-string</i></code>	(Optional) configure descriptions of the hybrid ACL.
4	<code>Raisecom(config-hybrid-acl-*)#rule <i>rule-number</i></code>	Configure the number of the hybrid ACL sub-rule.
5	<code>Raisecom(config-hybrid-acl-* -rule-*)#access-type { permit   deny }</code>	Configure the access type of the hybrid ACL sub-rule.
6	<code>Raisecom(config-hybrid-acl-* -rule-*)#match mac destination <i>mac</i> [ <i>mac-mask</i> ]</code>	Configure the destination MAC address of the hybrid ACL sub-rule.
7	<code>Raisecom(config-hybrid-acl-* -rule-*)#match mac source <i>mac</i> [ <i>mac-mask</i> ]</code>	Configure the source MAC address of the hybrid ACL sub-rule.
8	<code>Raisecom(config-hybrid-acl-* -rule-*)#match svlan <i>svlan-id</i></code>	Configure matching the hybrid ACL sub-rule with the source SVLAN ID.
9	<code>Raisecom(config-hybrid-acl-* -rule-*)#match svlan-cos <i>svlan-cos</i></code>	Configure matching the hybrid ACL sub-rule with the SVLAN CoS.
10	<code>Raisecom(config-hybrid-acl-* -rule-*)#match cvlan <i>cvlan-id</i></code>	Configure matching the hybrid ACL sub-rule with the source CVLAN ID.

Step	Command	Description
11	<code>Raisecom(config-hybrid-acl-*--rule-*)#match cvlan-cos <i>cvlan-cos</i></code>	Configure matching the hybrid ACL sub-rule with the CVLAN CoS.
12	<code>Raisecom(config-hybrid-acl-*--rule-*)#match ethertype <i>frame-type frame-type-mask</i></code>	Configure matching the hybrid ACL sub-rule with the frame type in the hybrid frame head.
13	<code>Raisecom(config-hybrid-acl-*--rule-*)#match ethertype { arp   eapol   flowcontrol   ip   ipv6   loopback   mpls   mpls-mcast   pppoe   pppoe-disc   x25   x75 }</code>	Configure matching the hybrid ACL sub-rule with the protocol type in the hybrid frame head.
14	<code>Raisecom(config-hybrid-acl-*--rule-*)#match ip destination-address <i>ip-address</i> [ <i>mask</i> ]</code>	Configure the destination IP address of the hybrid ACL sub-rule.
15	<code>Raisecom(config-hybrid-acl-*--rule-*)#match ip source-address <i>ip-address</i> [ <i>mask</i> ]</code>	Configure the source IP address of the hybrid ACL sub-rule.
16	<code>Raisecom(config-hybrid-acl-*--rule-*)#match ip precedence { pri   routine   priority   immediate   flash   flash-override   critical   internet   network }</code>	Configure matching the hybrid ACL sub-rule with the source IP precedence.
17	<code>Raisecom(config-hybrid-acl-*--rule-*)#match ip tos { service-type   normal   min-monetary-cost   min-delay   max-reliability   max-throughput }</code>	Configure matching the hybrid ACL sub-rule with the IP ToS.
18	<code>Raisecom(config-hybrid-acl-*--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 }</code>	Configure matching the hybrid ACL sub-rule with IP DSCP.
19	<code>Raisecom(config-hybrid-acl-*--rule-*)#match ip { fragments   no-fragments }</code>	Configure matching the hybrid ACL sub-rule with the fragmented or non-fragmented packet.
20	<code>Raisecom(config-hybrid-acl-*--rule-*)#match ip protocol { protocol-num   ahp   esp   gre   icmp   igmp   igmp   ipinip   ospf   pcp   pim   tcp   udp }</code>	Configure matching the hybrid ACL sub-rule with the IP upper protocol type.
21	<code>Raisecom(config-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 }</code>	Configure matching the hybrid ACL sub-rule with the destination/source interface ID of the TCP packet.
22	<code>Raisecom(config-hybrid-acl-*--rule-*)#match ip tcp { ack   fin   psh   rst   syn   urg }</code>	Configure matching the hybrid ACL sub-rule with the TCP packet flag.

Step	Command	Description
23	Raisecom(config-hybrid-acl- <i>rule-number</i> )# <b>match ip udp</b> { <b>destination-port</b>   <b>source-port</b> } { <i>port-num</i>   <b>biff</b>   <b>bootpc</b>   <b>bootps</b>   <b>domain</b>   <b>echo</b>   <b>mobile-ip</b>   <b>netbios-dgm</b>   <b>netbios-ns</b>   <b>netbios-ss</b>   <b>ntp</b>   <b>pim-auto-rp</b>   <b>rip</b>   <b>snmp</b>   <b>snmptrap</b>   <b>sunrpc</b>   <b>syslog</b>   <b>tacacs</b>   <b>talk</b>   <b>tftp</b>   <b>time</b>   <b>who</b> }	Configure matching the hybrid ACL sub-rule with the destination/source interface ID of the UDP packet.

## Configuring IPv6 hybrid ACL

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>ipv6-hybrid-access-list</b> <i>list-number</i>	Create an IPv6 hybrid ACL and enter the hybrid ACL configuration mode. You can use the <b>no ipv6-hybrid-access-list { all   list-number }</b> command to delete the ACL.
3	Raisecom(config-ipv6-hybrid-acl- <i>rule-number</i> )# <b>description</b> <i>desc-string</i>	(Optional) configure descriptions of the IPv6 hybrid ACL.
4	Raisecom(config-ipv6-hybrid-acl- <i>rule-number</i> )# <b>rule</b> <i>rule-number</i>	Configure the number of the IPv6 hybrid ACL sub-rule.
5	Raisecom(config-ipv6-hybrid-acl- <i>rule-number</i> )# <b>access-type</b> { <b>permit</b>   <b>deny</b> }	Configure the access type of the IPv6 hybrid ACL sub-rule.
6	Raisecom(config-ipv6-hybrid-acl- <i>rule-number</i> )# <b>match mac destination</b> <i>mac</i> [ <i>mac-mask</i> ]	Configure the destination MAC address of the IPv6 hybrid ACL sub-rule.
7	Raisecom(config-ipv6-hybrid-acl- <i>rule-number</i> )# <b>match mac source</b> <i>mac</i> [ <i>mac-mask</i> ]	Configure the source MAC address of the IPv6 hybrid ACL sub-rule.
8	Raisecom(config-ipv6-hybrid-acl- <i>rule-number</i> )# <b>match svlan</b> <i>svlan-id</i>	Configure matching the IPv6 hybrid ACL sub-rule with the source SVLAN ID.
9	Raisecom(config-ipv6-hybrid-acl- <i>rule-number</i> )# <b>match svlan-cos</b> <i>svlan-cos</i>	Configure matching the IPv6 hybrid ACL sub-rule with the SVLAN CoS.
10	Raisecom(config-ipv6-hybrid-acl- <i>rule-number</i> )# <b>match cvlan</b> <i>cvlan-id</i>	Configure matching the IPv6 hybrid ACL sub-rule with the source CVLAN ID.
11	Raisecom(config-ipv6-hybrid-acl- <i>rule-number</i> )# <b>match cvlan-cos</b> <i>cvlan-cos</i>	Configure matching the IPv6 hybrid ACL sub-rule with the CVLAN CoS.
12	Raisecom(config-ipv6-hybrid-acl- <i>rule-number</i> )# <b>match ethertype</b> <i>frame-type</i> <i>frame-type-mask</i>	Configure matching the IPv6 hybrid ACL sub-rule with the frame type in the Layer 2 frame head.



Step	Command	Description
13	Raisecom(config-ipv6-hybrid-acl- <i>rule</i> )*# <b>match</b> <b>ethertype</b> { <b>arp</b>   <b>eapol</b>   <b>flowcontrol</b>   <b>ip</b>   <b>ipv6</b>   <b>loopback</b>   <b>mpls</b>   <b>mpls-mcast</b>   <b>pppoe</b>   <b>pppoedisc</b>   <b>x25</b>   <b>x75</b> }	Configure matching the IPv6 hybrid ACL sub-rule with the protocol type in the Layer 2 frame head.
14	Raisecom(config-ipv6-hybrid-acl- <i>rule</i> )*# <b>match ip destination-address</b> <i>ip-address</i> [ <i>mask</i> ]	Configure the destination IP address of the IPv6 hybrid ACL sub-rule.
15	Raisecom(config-ipv6-hybrid-acl- <i>rule</i> )*# <b>match ip source-address</b> <i>ip-address</i> [ <i>mask</i> ]	Configure the source IP address of the IPv6 hybrid ACL sub-rule.
16	Raisecom(config-ipv6-hybrid-acl- <i>rule</i> )*# <b>match ip traffic-class</b> <i>user-level</i>	Configure the IPv6 hybrid ACL sub-rule matching with the user level of the IPv6 packet.
17	Raisecom(config-ipv6-hybrid-acl- <i>rule</i> )*# <b>match ip protocol</b> <i>protocol-num</i>	Configure the IPv6 hybrid ACL sub-rule matching with IP upper protocol type.
18	Raisecom(config-ipv6-hybrid-acl- <i>rule</i> )*# <b>match ip tcp</b> { <b>destination-port</b>   <b>source-port</b> } { <i>port-num</i>   <b>bgp</b>   <b>domain</b>   <b>echo</b>   <b>exec</b>   <b>finger</b>   <b>ftp</b>   <b>ftp-data</b>   <b>gopher</b>   <b>hostname</b>   <b>ident</b>   <b>irc</b>   <b>klogin</b>   <b>kshell</b>   <b>login</b>   <b>lpd</b>   <b>nntp</b>   <b>pim-auto-rp</b>   <b>pop2</b>   <b>pop3</b>   <b>smtp</b>   <b>sunrpc</b>   <b>syslog</b>   <b>tacacs</b>   <b>talk</b>   <b>telnet</b>   <b>time</b>   <b>uucp</b>   <b>whois</b>   <b>www</b> }	Configure matching the IPv6 hybrid ACL sub-rule with the destination/source interface ID of the TCP packet. The packet type refers to the classical interface ID.
19	Raisecom(config-ipv6-hybrid-acl- <i>rule</i> )*# <b>match ip udp</b> { <b>destination-port</b>   <b>source-port</b> } { <i>port-num</i>   <b>biff</b>   <b>bootpc</b>   <b>bootps</b>   <b>domain</b>   <b>echo</b>   <b>mobile-ip</b>   <b>netbios-dgm</b>   <b>netbios-ns</b>   <b>netbios-ss</b>   <b>ntp</b>   <b>pim-auto-rp</b>   <b>rip</b>   <b>snmp</b>   <b>snmptrap</b>   <b>sunrpc</b>   <b>syslog</b>   <b>tacacs</b>   <b>talk</b>   <b>tftp</b>   <b>time</b>   <b>who</b> }	Configure matching the IPv6 hybrid ACL sub-rule with the destination/source interface ID of the UDP packet.

### 13.2.6 Configuring user ACL

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>user-access-list profile field</b> <i>field-id</i> <b>layer</b> { <b>12</b>   <b>13</b>   <b>14</b> } <b>offset</b> <i>offset-value</i>	Configure customized ACL match objects.
3	Raisecom(config)# <b>user-access-list</b> <i>list-number</i>	Create a customized ACL and enter user ACL configuration mode.  You can use the <b>no user-access-list { all   list-number }</b> command to delete the ACL.

Step	Command	Description
3	<code>Raisecom(config-user-acl-*)#description desc-string</code>	(Optional) configure descriptions of the user ACL. You can use the <b>no description</b> command to delete the description.
4	<code>Raisecom(config-user-acl-*)#rule rule-number</code>	Configure the number of the user ACL sub-rule.
5	<code>Raisecom(config-user-acl-*--rule-*)#access-type { permit   deny }</code>	Configure the access type of the user ACL sub-rule.
6	<code>Raisecom(config-user-acl-*--rule-*)#match field field-id content mask</code>	Configure the content of the ACL match field.
7	<code>Raisecom(config-user-acl-*--rule-*)#match tag-type { double-tag   s-tagged   untagged }</code>	Configure matching the user ACL with packets of different Tag types.

### 13.2.7 Applying ACL



#### Note

The ACL takes effect only when it is added into the filter. Multiple ACL matching rules can be added into the filter to form multiple filtering rules. Priorities of the rules depend on the order of adding ACL matching rules. That is, the first added ACL matching rule has the highest priority. If multiple rules conflict with each other in matching calculation, the rule with a higher priority prevails. We recommend arranging the order of the rules reasonably to filter packets correctly.

#### Applying ACL based on whole device


Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#filter { 12-access-list / ip-access-list / ipv6-access-list / hybrid-access-list / ipv6-hybrid-access-list / user-access-list } acl-num [ statistics ]</code>	Configure applying filtering rules based on the whole device. If you have configured the <b>statistics</b> parameter, the system takes statistics according to the filtering rules.  You can use the <b>no filter acl-num</b> command to delete the application relationship of the filtering rules.

#### Applying ACL based on uplink and downlink of interface

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

Step	Command	Description
2	<code>Raisecom(config)#filter { 12-access-list   ip-access-list   ipv6-access-list   hybrid-access-list   ipv6-hybrid-access-list   user-access-list } acl-num egress interface { epon-olt   gigabitethernet } slot-id/port-list [ statistics ]</code>	Configure applying ACL filtering rules based on the downlink of the interface. If you have configured the <b>statistics</b> parameter, the system takes statistics according to the filtering rules.
3	<code>Raisecom(config)#filter { 12-access-list   ip-access-list   ipv6-access-list   hybrid-access-list   ipv6-hybrid-access-list   user-access-list } acl-num ingress interface { epon-olt slot-id/port-list   gigabitethernet slot-id/port-list   port-channel group-id } [ statistics ]</code>	Configure applying ACL filtering rules based on the uplink of the interface. If you have configured the <b>statistics</b> parameter, the system takes statistics according to the filtering rules.

### Applying ACL based on traffic from ingress interface to egress interface

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#filter { 12-access-list   ip-access-list   ipv6-access-list   hybrid-access-list   ipv6-hybrid-access-list   user-access-list } acl-num from interface { epon-olt   gigabitethernet } slot-id/port-list to interface { epon-olt   gigabitethernet } slot-id/port-list [ statistics ]</code>	<p>Configure applying ACL filtering rules based on traffic from the ingress interface to egress interface. If you have configured the <b>statistics</b> parameter, the system takes statistics according to the filtering rules.</p> <p> <b>Note</b> When you use this command, the ingress and egress interfaces should be on the same card or sub-card.</p>

## 13.2.8 Checking configurations

No.	Command	Description
1	<code>Raisecom#show ip-access-list [ list-number ]</code>	Show IPv4 ACL configurations.
2	<code>Raisecom#show ipv6-access-list [ list-number ]</code>	Show IPv6 ACL configurations.
3	<code>Raisecom#show 12-access-list [ list-number ]</code>	Show Layer 2 ACL configurations.
4	<code>Raisecom#show hybrid-access-list [ list-number ]</code>	Show hybrid ACL configurations.
5	<code>Raisecom#show ipv6-hybrid-access-list [ list-number ]</code>	Show IPv6 hybrid ACL configurations.
6	<code>Raisecom#show user-access-list [ list-number ]</code>	Show user ACL configurations.

No.	Command	Description
7	<b>Raisecom#show user-access-list profile</b>	Show the customized ACL match field.
8	<b>Raisecom#show interface vlanif ip-access-list</b>	Show ACL configurations on the VLAN interface.
9	<b>Raisecom#show filter [ filter-number ] statistics</b>	Show filter statistics.
10	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet uni-id filter</b>	Show filters configured on the ONU interface.

## 13.3 Configuring RADIUS

### 13.3.1 Preparing for configurations

#### Scenario

You can deploy the RADIUS server on the network to perform authentication and accounting to control users to access to the ISCOM5508 and network. The ISCOM5508 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

### 13.3.2 Default configurations

Default configurations of RADIUS on the ISCOM5508 are as below.

Function	Default value
RADIUS accounting	Disable
IP address of RADIUS authentication server	0.0.0.0
UDP port ID of RADIUS authentication server	1812
IP address of RADIUS accounting server	0.0.0.0
UDP port ID of RADIUS accounting server	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

### 13.3.3 Configuring RADIUS authentication

Step	Command	Description
1	<b>Raisecom#radius [ backup ] ip-address [ auth-port slot-id/port-id ]</b>	Specify the IPv4 address and interface ID of the RADIUS authentication server. You can use the <b>backup</b> parameter to specify the backup RADIUS authentication server.
	<b>Raisecom#radius [ backup ] ipv6-address [ scopeid string ] [ auth-port slot-id/port-id ]</b>	Specify the IPv6 address and interface ID of the RADIUS authentication server. You can use the <b>backup</b> parameter to specify the backup RADIUS authentication server.
2	<b>Raisecom#radius-key word</b>	Configure the shared key of RADIUS authentication.

### 13.3.4 Configuring RADIUS accounting

Step	Command	Description
1	<b>Raisecom#aaa accounting login enable</b>	Enable RADIUS accounting. You can use the <b>aaa accounting login disable</b> command to disable this function.
2	<b>Raisecom#radius [ backup ] accounting-server ip-address [ acct-port port-id ]</b>	Specify the IPv4 address and UDP port ID of the RADIUS accounting server. You can use the <b>backup</b> parameter to specify the backup RADIUS accounting server.
	<b>Raisecom#radius [ backup ] accounting-server ipv6-address [scopeid string ] [ acct-port port-id ]</b>	Specify the IPv6 address and UDP port ID of the RADIUS accounting server. You can use the <b>backup</b> parameter to specify the backup RADIUS accounting server.
3	<b>Raisecom#radius accounting-server key string</b>	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.
4	<b>Raisecom#aaa accounting fail { online   offline }</b>	Configure the processing policy upon accounting failure.
5	<b>Raisecom#aaa accounting update period</b>	Configure the period to send accounting update packets. If it is configured to 0, accounting update packets will not be sent.  <div data-bbox="710 1697 903 1780" data-label="Image"> <b>Note</b> </div> Through the accounting start packet, update packet, and end packet, the RADIUS accounting server records the access time and operations of each user.

## 13.3.5 Checking configurations

No.	Command	Description
1	Raisecom# <b>show radius-server</b>	Show RADIUS server configurations.
2	Raisecom# <b>show aaa accounting</b>	Show RADIUS accounting server running conditions.

## 13.4 Configuring TACACS+

### 13.4.1 Preparing for configurations

#### Scenario

You can deploy the TACACS+ server on the network to perform authentication and accounting to control users to access to the ISCOM5508 and network. TACACS+ is safer and more reliable than RADIUS. The ISCOM5508 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

### 13.4.2 Default configurations

Default configurations of TACACS+ on the ISCOM5508 are as below.

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
Privileged login mode	local-user

### 13.4.3 Configuring TACACS+

Step	Command	Description
1	Raisecom# <b>tacacs-server</b> [ <b>backup</b> ] <i>ip-address</i>	Specify the IPv4 address of the TACACS+ authentication server.  You can use the <b>backup</b> parameter to specify the backup TACACS+ authentication server.

Step	Command	Description
	<code>Raisecom#tacacs-server [ backup ] ipv6-address [scopeid string]</code>	(Optional) specify the IPv6 address of the TACACS+ authentication server.  You can use the <b>backup</b> parameter to specify the backup TACACS+ authentication server.
2	<code>Raisecom#tacacs [ backup ] accounting-server ip-address</code>	Specify the IPv4 address of the TACACS+ accounting server.  You can use the <b>backup</b> parameter to specify the backup TACACS+ accounting server.
	<code>Raisecom#tacacs [ backup ] accounting-server ipv6-address [scopeid string]</code>	(Optional) specify the IPv6 address of the TACACS+ accounting server.  You can use the <b>backup</b> parameter to specify the backup TACACS+ accounting server.
3	<code>Raisecom#tacacs-server key string</code>	Configure the shared key of TACACS+ authentication.
4	<code>Raisecom#enable login tacacs- local [ server-no-response ]</code>	(Optional) configure login mode in privileged EXEC mode.

## 13.4.4 Checking configurations

No.	Command	Description
1	<code>Raisecom#show tacacs-server</code>	Show TACACS+ server configurations.

## 13.5 Configuring storm control

### 13.5.1 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.

### 13.5.2 Default configurations

Default configurations of storm control on the ISCOM5508 are as below.

Function	Default value
Broadcast storm control	Enable
Multicast storm control	Disable
DLF storm control	Disable
Rate threshold	1024 Kbit/s
Burst length	512 KBytes

Default configurations of storm control on the ONU are as below.

Function	Default value
Broadcast storm control	Enable
Multicast storm control	Enable
DLF storm control	Disable
Rate threshold	1000 Kbit/s
Burst length threshold	4 Bytes
Packet rate threshold	1000 pps

### 13.5.3 Configuring storm control

#### Configuring storm control on OLT

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <b>{ gigabitethernet   epon-olt } slot-</b> <b>id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-**-*)#storm-control</b> <b>{ all   broadcast   dlf   multicast }</b>	Enable storm control on broadcast, multicast, and DLF traffic.
4	<b>Raisecom(config-if-**-*)#storm-control</b> <b>bps value burst</b>	(Optional) configure the rate threshold of storm control.



## Configuring storm control on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*//*:*)#storm-control { broadcast   dlf   multicast   all } { enable   disable }</b>	Enable/Disable storm control on broadcast traffic, multicast traffic, and DLF traffic.
4	<b>Raisecom(config-epon-onu-*//*:*)#storm-control bps rate [ burst ]</b>	(Optional) configure the rate and burst length thresholds of storm control.
5	<b>Raisecom(config-epon-onu-*//*:*)#storm-control pps rate</b>	(Optional) configure the packet rate threshold of storm control.

## 13.5.4 Checking configurations

### Checking configurations on OLT

No.	Command	Description
1	<b>Raisecom#show [ interface { epon-olt   gigabitethernet } slot-id/port-id ] storm-control</b>	Show storm control configurations on the OLT.

### Checking configurations on ONU

No.	Command	Description
1	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id storm-control</b>	Show storm control configurations on the ONU.

## 13.6 Configuring interface isolation

### 13.6.1 Preparing for configurations

#### Scenario

Interface isolation is a Layer 2 isolation mode, which adopts the isolate group to realize data isolation among multiple interfaces on the device. You can isolate different physical interfaces and interfaces in the same VLAN by creating create the isolate group to enhance safety of network access.

## Prerequisite

N/A

### 13.6.2 Default configurations

Default configurations of interface isolation are as below.

Function	Default value
Layer 2 isolation on OLT	Be enabled. That is, ONUs connected to the same OLT PON interface isolate from each other on Layer 2
Layer 2 isolation on ONU	Be enabled. That is, UNIs on the same ONU isolate from each other.

### 13.6.3 Configuring interface isolation on OLT

#### Configuring physical interface isolation

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface { epon-olt slot-id/port-id   gigabitethernet slot-id/port-id   port-channel group-id }</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-**-*)#isolate-group group-id</b>	Create the isolation group for physical interfaces. If a specified isolation group exists, add interfaces to the group.  You can use the <b>no isolate-group group-id</b> command to delete the isolation group or interfaces in the group.

#### Configuring VLAN interface isolation

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface { epon-olt   gigabitethernet } slot-id/olt-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-**-*)#vlan vlan-id isolate-group group-id</b>	Create the isolation group in the VLAN. If a specified isolation group exists, add interfaces to the group.  You can use the <b>no vlan vlan-id isolate-group group-id</b> command to delete the isolation group or interfaces in the group.

## 13.6.4 Configuring interface isolation on ONU

### Configuring P2P access control

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode of EPON system.
2	<b>Raisecom(config)#interface epon-onu slot-id/olt-id/onu-id</b>	Enter ONU configuration mode.
3	<b>Raisecom(config-if-epon-onu-*/*:*)#p2p-access { add   remove } onu-list</b>	Configure the ONU list of which ONUs can access each other on the same PON interface.



#### Note

- When you configure P2P access control, services will be interrupted for 25ms.
- P2P is targeted at unicast services only. PTP for unknown unicast, broadcast, or multicast services is not supported.

### Configuring ONU UNI isolation

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode of EPON system.
2	<b>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</b>	Enter ONU UNI configuration mode.
3	<b>Raisecom(config-epon-onu-ethernet-*/*:*)#switchport isolation { enable   disable }</b>	Enable/Disable UNI isolation, which belongs to ONU Layer 2 isolation.

## 13.6.5 Checking configurations

No.	Command	Description
1	<b>Raisecom#show isolate-group [ group-id ]</b>	Show configurations of physical interface isolation.
2	<b>Raisecom#show vlan-isolate-group vlan vlan-id [ group-id ]</b>	Show configurations of the VLAN isolation group.
3	<b>Raisecom#show interface epon-onu slot-id/olt-id/onu-id p2p-access</b>	Show information about ONU Layer 2 isolation.
4	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id uni ethernet isolation</b>	Show information about ONU UNI isolation.

## 13.7 Configuring attack defense

### 13.7.1 Preparing for configurations

#### Scenario

To prevent attack packets, you can use this command to filter excess packets.

#### Prerequisite

N/A

### 13.7.2 Default configuration

N/A

### 13.7.3 Configuring OLT interface isolation

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#attack-defense land</b>	(Optional) prevent LAND attacks.
3	<b>Raisecom(config)#attack-defense large-icmp [ size size ]</b>	(Optional) prevent large ICMP attacks.
4	<b>Raisecom(config)#attack-defense smurf</b>	(Optional) prevent SMURF attacks.
5	<b>Raisecom(config)#attack-defense urpf</b>	(Optional) prevent URPF attacks.

### 13.7.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show attack-defense</b>	Show configurations of attack defense.

## 13.8 Configuring IP Source Guard

### 13.8.1 Preparing for configurations

#### Scenario

IP Source Guard uses a binding table to defend against IP source spoofing, which prevents IP address embezzlement without ID authentication.

## Prerequisite

N/A

## 13.8.2 Default configuration

N/A

## 13.8.3 Configuring IP Source Guard

### Configuring IP Source Guard static binding

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip verify source static</b>	Enable static binding. You can use the <b>no ip verify source static</b> command to disable this function.
3	<b>Raisecom(config)#interface { epon-olt   gigabitethernet } slot-id/port-id</b>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config-if-**-*)#ipv4 source binding ip-address mask mask [ mac-address ] vlan vlan id</b>	(Optional) configure IP Source Guard static binding. You can use the <b>no ipv4 source binding ip-address mask mask [ mac-address ] vlan vlan id</b> command to delete the static binding relation.
5	<b>Raisecom(config-if-**-*)#ip verify source trust</b>	(Optional) enable interface trust. You can use the <b>no ip verify source dhcp-snooping</b> command to disable this function.

### Configuring IP Source Guard dynamic binding

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip verify source dhcp-snooping</b>	Enable IP Source Guard dynamic binding.
3	<b>Raisecom(config)#interface { epon-olt   gigabitethernet } slot-id/port-id</b>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config-if-**-*)#ip verify source trust</b>	(Optional) enable interface trust. You can use the <b>no ip verify source dhcp-snooping</b> command to disable this function.

## 13.8.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show ip verify source</b>	Show configurations of attack defense.
2	<b>Raisecom#show ipv4 verify source binding [ port slot-id / port-id ]</b>	Show IP Source Guard binding table.

## 13.9 Configuring DAI

### 13.9.1 Preparing for configurations

#### Scenario

DAI binds IP address and MAC address and establish binding relations dynamically.

#### Prerequisite

N/A

### 13.9.2 Default configuration

N/A

### 13.9.3 Configuring DAI

#### Configuring DAI static binding

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#arp-inspection static</b>	Enable DAI static binding. You can use the <b>no ip verify source static</b> command to disable this function.
3	<b>Raisecom(config)#interface { epon-olt   gigabitethernet } slot-id/port-id</b>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config-if-*-*:*)#arp-inspection binding ip-address [ mac-address ] vlan vlan id</b>	(Optional) configure DAI static binding. You can use the <b>no arp-inspection binding ip-address [ mac-address ] vlan vlan id</b> command to delete static binding relation.
5	<b>Raisecom(config-if-*-*:*)#arp-inspection trust</b>	(Optional) enable interface trust. You can use the <b>no arp-inspection trust</b> command to disable this function.

## Configuring DAI dynamic binding

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#arp-inspection dynamic</b>	Enable DAI dynamic binding.
3	<b>Raisecom(config)#interface { epon-olt   gigabitethernet } slot-id/port-id</b>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config-if-**-*)#arp-inspection trust</b>	(Optional) enable interface trust. You can use the <b>no arp-inspection trust</b> command to disable this function.

## 13.9.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show arp-inspection</b>	Show the enabled status of static and dynamic binding tables.
2	<b>Raisecom#show arp-inspection binding</b>	Show IPv4 DAI binding on all interfaces.
3	<b>Raisecom#show interface arp-inspection</b>	Show interface trusted status.

## 13.10 Maintenance

Command	Description
<b>Raisecom(config)#clear filter [ filter-number ] statistics</b>	Clear ACL filter statistics.
<b>Raisecom(config)#clear tacacs statistics</b>	Clear TACACS+ statistics.

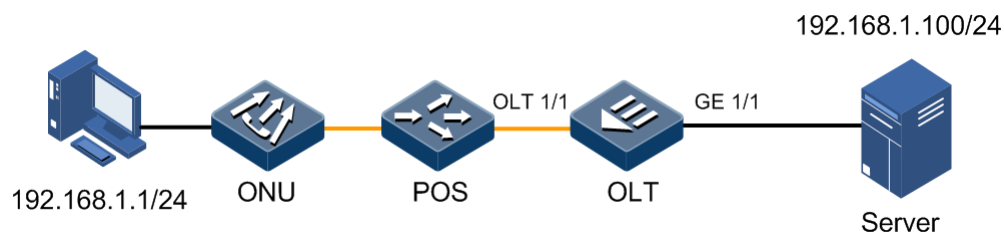
## 13.11 Configuration examples

### 13.11.1 Example for configuring ACL

#### Networking requirements

As shown in Figure 13-1, to control users to access the server, you can configure ACL forbidding 192.168.1.1 to access the server 192.168.1.100.

Figure 13-1 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
```

### Step 2 Apply ACL on the interface OLT 1/1.

```
Raisecom(config)#filter ip-access-list 1001 ingress interface epon-olt
1/1
```

## 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** to show filter configurations.

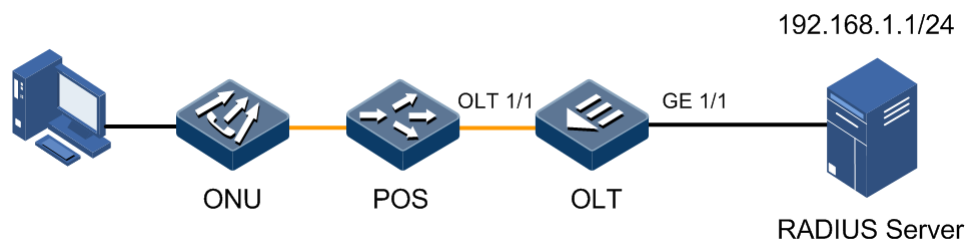
```
Raisecom#show filter
Filter ID : 1001
ACL ID    : 1
Hardware   : Yes
Egress Port : epon-olt 1/1
Ingress Port : epon-olt 1/1
Statistics  : Disable
```

## 13.11.2 Example for configuring RADIUS

### Networking requirements

As shown in Figure 13-2, to control users to access the device, you need to deploy RADIUS authentication and accounting on the OLT to authenticate login users and record their operations. It is required that the interval to send update packets is 2min and the user is logged off when accounting fails.

Figure 13-2 RADIUS networking



### Configuration steps

Step 1 Configure RADIUS authenticating login users.

```
Raisecom#radius 192.168.1.1
Raisecom#radius-key raisecom
Raisecom#user login radius-user
```

Step 2 Configure RADIUS accounting 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** to show RADIUS configurations.

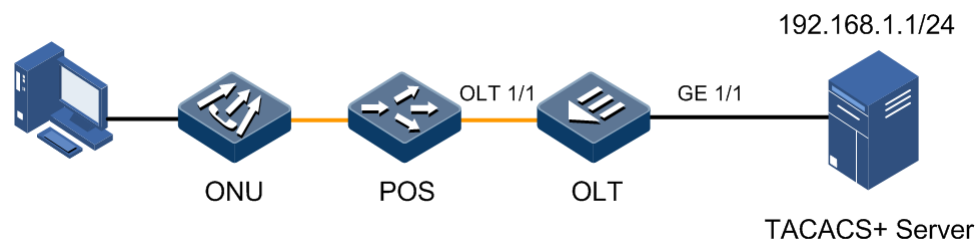
```
Raisecom#show radius-server
Authentication server IP:      192.168.1.1 port:1812
Backup authentication server IP: 0.0.0.0 port:1812
Authentication server key:    raisecom
Accounting server IP:         192.168.1.1 port:1813
Backup accounting server IP:  0.0.0.0 port:1813
Accounting server key:        raisecom
```

## 13.11.3 Example for configuring TACACS+

### Networking requirements

As shown in Figure 13-3, to control users to access the device, you need to deploy TACACS+ authentication on the OLT to authenticate login users.

Figure 13-3 TACACS+ networking



### Configuration steps

Configure TACACS+ authenticating 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** to show TACACS+ configurations.

```
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
```

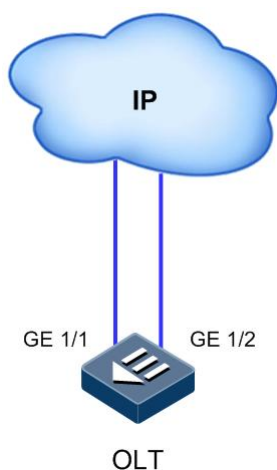
```
Total Packet Recv:          0
Num of Error Packets:       0
Accounting server Address:   0.0.0.0
Backup Accounting server Address: 0.0.0.0
```

## 13.11.4 Example for configuring storm control

### Networking requirements

As shown in Figure 13-4, 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 length is 1024 KBytes.

Figure 13-4 Storm control networking



### Configuration steps

Configure storm control on the OLT.

```
Raisecom#config
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1/1)#storm-control broadcast
Raisecom(config-if-gigabitethernet-1/1)#storm-control dlf
Raisecom(config-if-gigabitethernet-1/1)#storm-control bps 2000 burst 1024
Raisecom(config-if-gigabitethernet-1/1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1/2)#storm-control broadcast
Raisecom(config-if-gigabitethernet-1/2)#storm-control dlf
Raisecom(config-if-gigabitethernet-1/2)#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
gigabitethernet1/1	enable	disable	enable	2000kb/s Burst 1024 KB
gigabitethernet1/2	enable	disable	enable	2000kb/s Burst 1024 KB

# 14 Configuring link security

---

This chapter introduces the link security feature and configuration process of the ISCOM5508, and provides related configuration examples, including the following sections:

- Overview of link security
- Configuring OLT backbone fiber protection (Type B)
- Configuring PON full protection (Type C)
- Configuring PON full protection (Type D)
- Configuring OLT hand-in-hand uplink interface protection
- Configuring cross-OLT PON interface dual-homed protection (Type B)
- Configuring link aggregation
- Configuring link-state tracking
- Configuring RRPS
- Configuring loopback detection
- Configuring interface backup
- Maintenance
- Configuration examples

## 14.1 Overview of link security

### 14.1.1 Link protection on PON interface

The ISCOM5508 supports PON interface protection (Type B, Type C, and Type D) and cross-OLT PON interface dual-homed protection (Type B):

- OLT backbone fiber protection (Type B): provide redundancy protection for backbone fiber and OLT PON interface.
- PON full protection (Type C): provide redundancy protection for OLT dual-PON interface, ONU dual-optical module, backbone fiber, POS, and branch fiber.
- PON full protection (Type D): provide redundancy protection for OLT dual-PON interface, ONU dual-PON interface, backbone fiber, POS, and branch fiber.
- Cross-OLT PON interface dual-homed protection (Type B): be extended based on standard Type B protection and provide redundancy protection for backbone fiber, OLT, PON interface, and uplink interface.

## OLT backbone fiber protection (Type B)

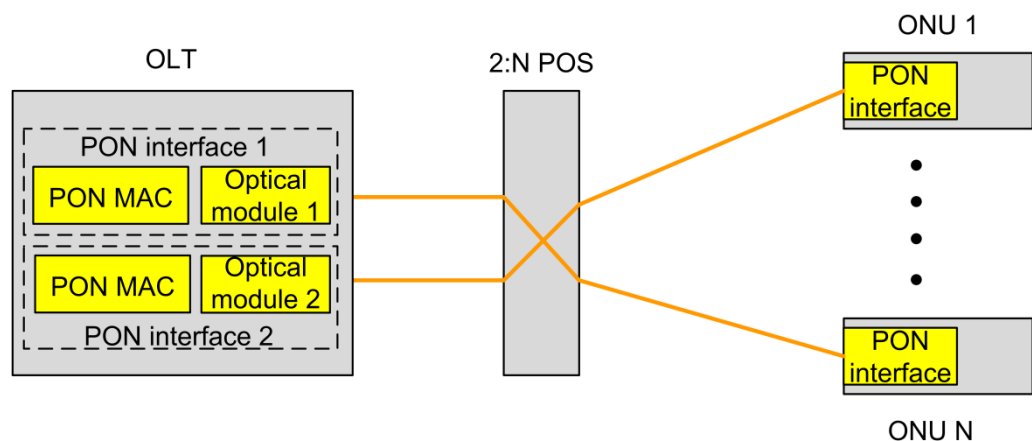
OLT backbone fiber protection (Type B) provides redundancy protection for backbone fiber and OLT PON interface. Two PON interfaces on the OLT adopt the independent PON MAC chip and optical module to realize protection between the two PON interfaces.

Type B protection can protect PON interfaces on the same OLT. The requirements are as below:

- OLT: the secondary OLT PON interface is in cold backup status. The OLT detects the link status and PON interface status, and performs switching. The OLT should ensure that services on the primary PON interface can be backed up to the secondary PON interface synchronously. In this case, the secondary PON interface can keep the service properties of the ONU unchanged in the protection process.
- POS: one 2:N POS
- ONU: no requirement

Figure 14-1 shows the principle of OLT backbone fiber protection (Type B)

Figure 14-1 Principle of OLT backbone fiber protection (Type B)



## PON full protection (Type C)

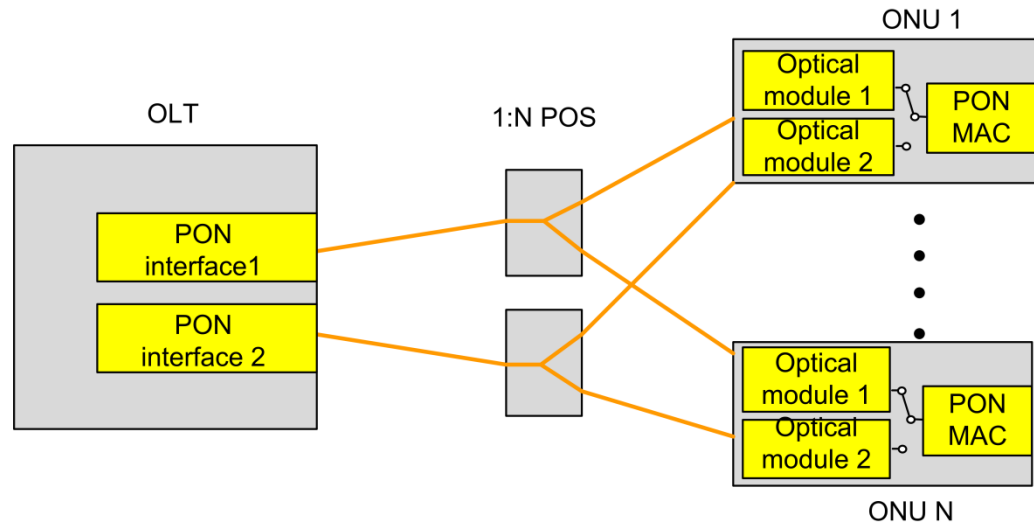
PON full protection (Type C) provides redundancy protection for OLT dual-PON interface, ONU dual-optical module, backbone fiber, POS, and branch fiber.

PON full protection (Type C) can protect PON interfaces on the same OLT. The requirements are as below:

- OLT: the secondary OLT PON interface is in cold backup status. The OLT detects the link status and PON interface status, and performs switching. The OLT should ensure that services on the primary PON interface can be backed up to the secondary PON interface synchronously. In this case, the secondary PON interface can keep the service properties of the ONU unchanged in the protection process.
- POS: two 1:N POSs
- ONU: the ONU adopts one PON MAC chip and different optical modules. The secondary optical module is in cold backup status. Both OLT and ONU detect the link status, and decide whether to perform switching based on the link status.

Figure 14-2 shows the principle of PON full protection (Type C)

Figure 14-2 Principle of PON full protection (Type C)



## PON full protection (Type D)

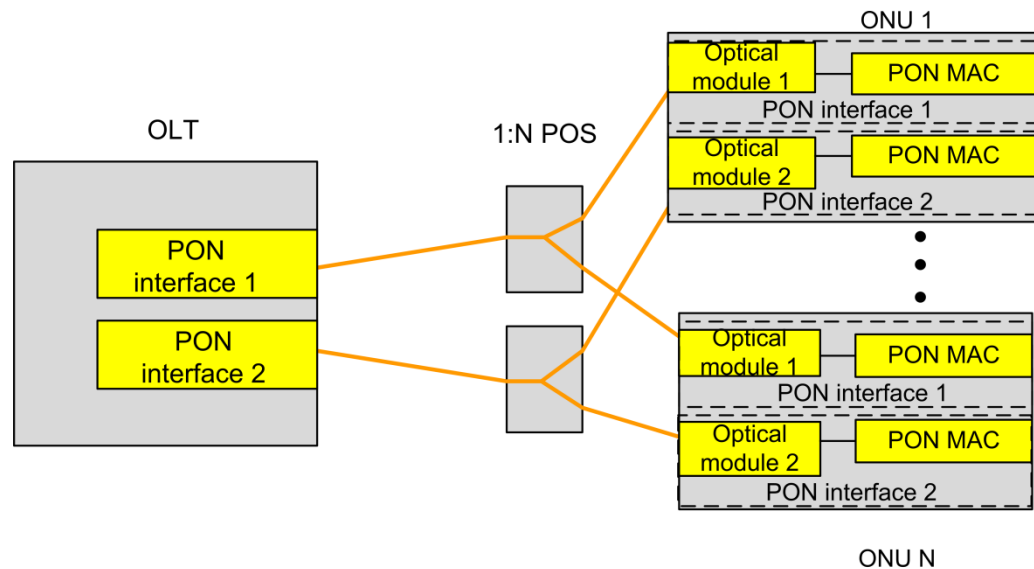
PON full protection (Type D) provides redundancy protection for OLT dual-PON interface, ONU dual-PON interface, backbone fiber, POS, and branch fiber.

PON full protection (Type D) can protect PON interfaces on the same OLT. The requirements are as below:

- OLT: the secondary OLT PON interface is in cold backup status. The OLT and ONU detect the link status and PON interface status bidirectionally, and perform switching independently. The OLT should ensure that services on the primary PON interface can be backed up to the secondary PON interface synchronously. In this case, the secondary PON interface can keep the service properties of the ONU unchanged in the protection process.
- POS: two 1:N POSs
- ONU: the ONU adopts different PON MAC chips and different optical modules. The ONU should ensure that services on the primary PON interface can be backed up to the secondary PON interface synchronously. In this case, the secondary PON interface can keep the service properties of the ONU unchanged in the protection process.

Figure 14-3 shows the principle of PON full protection (Type D).

Figure 14-3 Principle of PON full protection (Type D)



## Cross-OLT PON interface dual-homed protection (Type B)

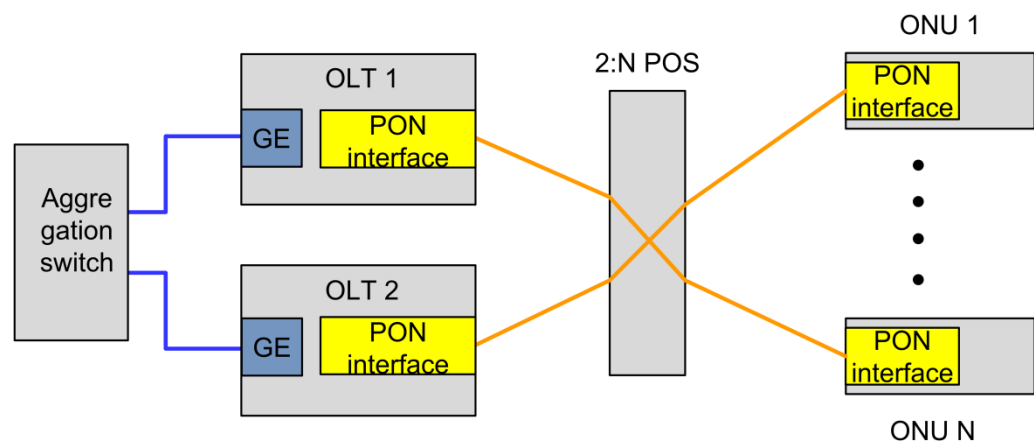
Cross-OLT PON interface dual-homed protection (Type B), extended based on standard Type B protection, provides redundancy protection for backbone fiber, OLT, PON interface, and uplink interface.

Cross-OLT PON interface dual-homed protection (Type B) can protect PON interfaces on different OLTs. The requirements are as below:

- OLT: the secondary OLT optical module is in cold backup status. The OLT detects the link status and PON interface status, and performs switching.
- POS: one 2:N POS
- ONU: no requirement

Figure 14-4 shows the principle of cross-OLT PON interface dual-homed protection (Type B).

Figure 14-4 Principle of cross-OLT PON interface dual-homed protection (Type B)





## 14.1.2 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. In addition to effectively improving reliability on links between devices, link aggregation helps gain higher bandwidth without upgrading hardware.

### 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.

### Static LACP link aggregation

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 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.

## 14.1.3 Link-state tracking

Link-state tracking provides an interface linkage scheme to extend the range of link backup. By monitoring uplinks and synchronizing downlinks, the downlink devices can be informed of faults of uplink devices immediately to trigger switching, thus preventing traffic loss because downlink devices are not informed of uplink failures.

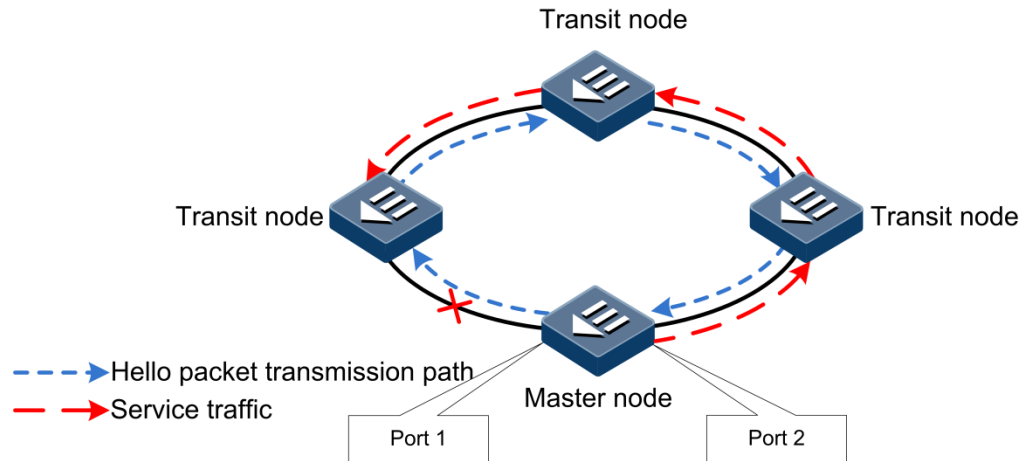
## 14.1.4 RRPS

With the development of Ethernet to the MAN, voice and video multicast service has come up with higher requirements on the Ethernet redundancy protection and fault recovery time. The fault recovery convergence time of the original STP mechanism is at the second level, which is far from meeting requirements on the fault recovery time in the MAN.

Raisecom Ring Protection Switching (RRPS) technology is RAISECOM independent research and development protocol, which can ensure that there is no data loop in the Ethernet ring through blocking some interface on the ring. RRPS solves the problems of weak protection and taking too long to recover faults of the traditional data network. RRPS, in theory, can provide 50ms rapid protection features.

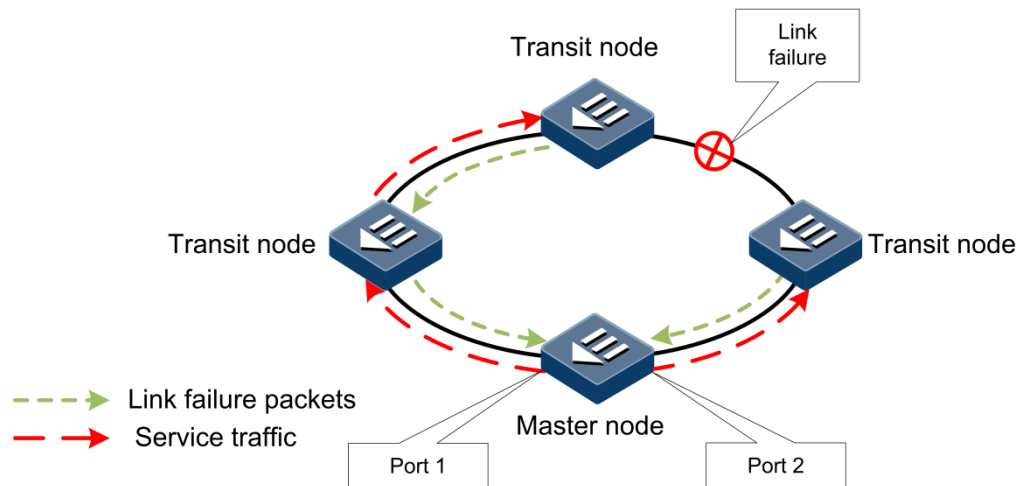
As shown in Figure 14-5, the network consists of a master node, multiple transit nodes, and control VLAN. Configure Port 1 and Port 2 on the master node. Generally, the master node sends Hello packets periodically through Port 1. If the master node receives the Hello packet from Port 2, the Ethernet ring is in normal status and you should logically block Port 1 immediately.

Figure 14-5 Ethernet ring in normal status



Once the link fails (such as, link interruption), the failure adjacent node or interface will check the fault immediately and send link failure packets to the master node. If the master node receives the link failure packet, the Ethernet ring is in fault status and you should unblock Port 1 immediately. At the same time, the master node sends packets to inform other transit nodes of link failure to make them change transmission direction. Data traffic will be switched to normal link after transit nodes update the forwarding table. As shown in Figure 14-6.

Figure 14-6 Ethernet ring in switching status



### 14.1.5 Loopback detection

Loopback detection aims to solve problems caused by loops on the network, and improve the self-checking ability, fault tolerance, and robustness of the network.

The process of loopback detection is as below:

- Each interface of the device sends the loopback-detection packet periodically (the interval is configurable and by default it is 4s).
- The device checks the source MAC address of the received loopback detection packet, if the source MAC address is identical to the MAC address of the device, it is believed that a loop is generated on some interface of the device.

- If the Tx interface ID is identical to Rx interface ID, shut down the interface.
- If the Tx interface ID is not identical to Rx interface ID, shut down the interface with a bigger ID, and leave the interface with a smaller ID in Up status.

## 14.1.6 Interface backup

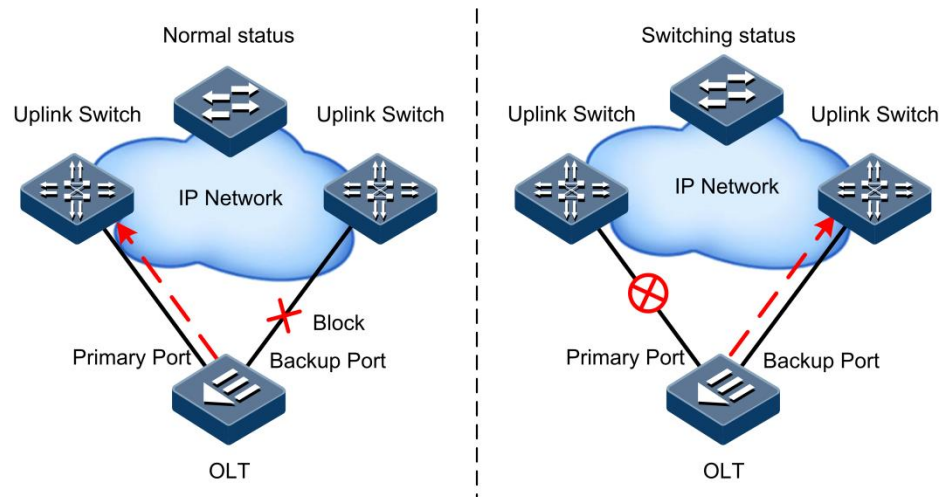
Interface backup is another solution of STP. When STP is disabled, you can realize basic link redundancy by manually configuring interface backup.

Interface backup is realized by configuring the interface backup group. Each interface backup group contains a primary interface and a backup interface. The principle of interface backup is as below:

- When the device is in normal status, all services are forwarded through the primary interface.
- When the link on the primary interface fails, services are switched to the backup interface for forwarding automatically.

Figure 14-7 shows the principle of interface backup.

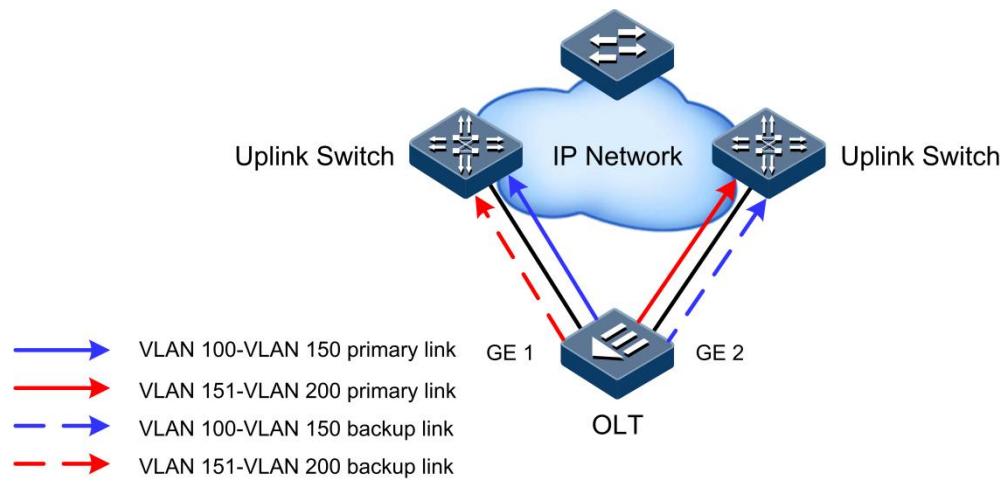
Figure 14-7 Principle of interface backup



## VLAN-based interface backup

Through applying interface backup on the VLAN, you can make two interfaces forward data simultaneously in different VLANs. As shown in Figure 14-8, through creating VLANs and adding interfaces to the VLAN, you can realize VLAN-based interface backup.

Figure 14-8 Principle of VLAN-based interface backup



In different VLANs, the interface forwarding status is shown as below:

- Under normal conditions, configure the ISCOM5508 in VLANs 100–150. GE 1 is the primary interface and GE 2 is the backup interface. In VLANs 151–200, GE 2 is the primary interface and GE 1 is the backup interface. Therefore, GE 1 forwards traffic of VLANs 1–100, and GE 2 forwards traffic of VLANs 101–200.
- When GE 1 fails, GE 2 forwards traffic of VLANs 100–150.
- When GE 1 restores normally and keeps Up for a period (restore-delay), GE 1 forwards traffic of VLANs 100–150, and GE 2 forwards traffic of VLANs 151–200.

VLAN-based interface backup can be used for load balancing. Moreover, it does not depend on configurations of uplink devices, thus facilitating users' operation.

## 14.2 Configuring OLT backbone fiber protection (Type B)

### 14.2.1 Preparing for configurations

#### Scenario

- Protection between PON interfaces on the same PON card of the OLT
- Protection between PON interfaces on different PON cards of the OLT

#### Prerequisite

There should not be created ONU on the secondary PON interface.

### 14.2.2 Default configurations

N/A

### 14.2.3 Configuring OLT backbone fiber protection (Type B)




#### Caution

- To ensure services to be switched properly, enable interface isolation on PON interfaces in the protection group of OLT backbone fiber protection (Type B).
- PON interfaces in the protection group of OLT backbone fiber protection (Type B) should not be shut down.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#protect-group group-id primary slot-id/olt-id secondary slot-id/olt-id type backbone-pon-protect</b>	Create the OLT backbone fiber protection group. You can use the <b>no protect-group group-id</b> command to delete the protection group.
3	<b>Raisecom(config)#protect-group group-id { enable   disable }</b>	Enable/Disable the protection group.
4	<b>Raisecom(config)#sync-data protect-group { group-id   all }</b>	Configure synchronizing data on the primary PON interface and primary ONU link to the secondary PON interface and secondary ONU link respectively.
5	<b>Raisecom(config)#protect-group group-id auto-recover-time second</b>	(Optional) configure the auto-recovery time. You can use the <b>no protect-group group-id auto-recover-time</b> command to restore default configurations.
6	<b>Raisecom(config)#protect-group group-id force-switch</b>	(Optional) configure FS.
7	<b>Raisecom(config)#protect-group group-id lock { primary   secondary   null }</b>	(Optional) configure locking the working link in the protection group.

### 14.2.4 Configuring ONU holdover

To ensure that services on the ONU are not interrupted due to deregistration when the OLT performs backbone fiber switching, you need to configure holdover on the ONU.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*/*:*)#protect-group holdover activated time period</b>	Configure the ONU holdover time. You can use the <b>no protect-group holdover time</b> command to restore default configurations.
		 <b>Note</b> We recommend that the holdover time does not exceed 200ms.

Step	Command	Description
4	Raisecom(config-epon-onu- */*:*)# <b>protect-group holdover</b> { <b>activated</b>   <b>deactivated</b> } [ <b>time period</b> ]	Enable/Disable holdover.

## 14.2.5 Checking configurations

No.	Command	Description
1	Raisecom# <b>show protect-group group-id</b>	Show configurations and operation status of the protection group.
2	Raisecom# <b>show epon-onu slot-id/olt-id/onu-id holdover</b>	Show configurations of ONU holdover.

## 14.3 Configuring PON full protection (Type C)

### 14.3.1 Preparing for configurations

#### Scenario

PON full protection (Type C) provides redundancy protection for OLT dual-PON interface, ONU dual-optical module, backbone fiber, POS, and branch fiber.

#### Prerequisite

- There is no online ONU on the primary link.
- There is no created ONU on the secondary link.

### 14.3.2 Default configurations

N/A

### 14.3.3 Configuring OLT PON full protection (Type C)




#### Caution

- To ensure services to be switched properly, enable interface isolation on PON interfaces in the PON full protection group.
- PON interfaces in the PON full protection group should not be shut down.

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

Step	Command	Description
2	<b>Raisecom(config)#protect-group</b> <i>group-id</i> <b>primary</b> <i>slot-id/olt-id</i> <b>secondary</b> <i>slot-id/olt-id</i> <b>type full-pon-protect</b>	Create the OLT PON full protection group. You can use the <b>no protect-group</b> <i>group-id</i> command to delete the protection group.
3	<b>Raisecom(config)#protect-group</b> <i>group-id</i> <b>{ enable   disable }</b>	Enable/Disable the protection group.
4	<b>Raisecom(config)#sync-data protect-group</b> <b>{ group-id   all }</b>	Configure synchronizing data on the primary PON interface and primary ONU link to the secondary PON interface and secondary ONU link respectively.

### 14.3.4 Configuring ONU PON full protection (Type C)

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu</b> <i>slot-id/olt-id/onu-id</i>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*//*:*)#protect-group</b> <b>holdover</b> <i>time period</i>	Configure the ONU holdover time. You can use the <b>no protect-group holdover time</b> command to restore default configurations.  <b>Note</b> We recommend that the holdover time does not exceed 200ms.
4	<b>Raisecom(config-epon-onu-*//*:*)#protect-group</b> <b>holdover</b> <b>{ activated   deactivated }</b> <b>[ time period ]</b>	Enable/Disable holdover.
5	<b>Raisecom(config-epon-onu-*//*:*)#protect-group</b> <b>primary</b> <i>pon-port-id</i>	(Optional) configure the primary interface in the ONU full protection group. You can use the <b>no protect-group primary</b> command to restore default configurations.
6	<b>Raisecom(config-epon-onu-*//*:*)#protect-group</b> <b>auto-recover-time</b> <i>second</i>	(Optional) configure the auto-recovery time. You can use the <b>no protect-group auto-recover-time</b> command to restore default configurations.
7	<b>Raisecom(config-epon-onu-*//*:*)#protect-group</b> <b>forced-switch</b>	(Optional) configure FS.
8	<b>Raisecom(config-epon-onu-*//*:*)#protect-group</b> <b>lock</b> <b>{ primary   secondary }</b>	(Optional) configure locking the working link in the protection group. You can use the <b>no protect-group lock</b> command to unlock the working link.

## 14.3.5 Checking configurations

No.	Command	Description
1	<code>Raisecom#show protect-group group-id</code>	Show configurations and operation status of the OLT protection group.
2	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id protect-group</code>	Show configurations and operation status of ONU Type C protection group.
3	<code>Raisecom#show epon-onu { primary   secondary   switched } protect-group</code>	Show configurations and current status of the protection group working on the ONU which is performing primary/secondary link switching.
4	<code>Raisecom#show epon-onu slot-id/olt-id/onu-list holdover</code>	Show configurations of ONU holdover.

## 14.4 Configuring PON full protection (Type D)

### 14.4.1 Preparing for configurations

#### Scenario

PON full protection (Type D) provides redundancy protection for OLT dual-PON interface, ONU dual-PON interface, backbone fiber, POS, and branch fiber.

#### Prerequisite

N/A

### 14.4.2 Default configurations

N/A

### 14.4.3 Configuring OLT PON full protection (Type D)



#### Caution

- To ensure services to be switched properly, enable interface isolation on PON interfaces in the PON full protection group.
- PON interfaces in the PON full protection group should not be shut down.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#protect-onu-group group-id primary slot-id/olt-id/onu-id secondary slot-id/olt-id/onu-id</code>	Configure the OLT PON full protection group. You can use the <b>no protect-onu-group group-id</b> command to delete the protection group.



Step	Command	Description
3	<b>Raisecom(config)#sync-data protect-group</b> <b>{ group-id   all }</b>	Configure synchronizing data on the primary PON interface and primary ONU link to the secondary PON interface and secondary ONU link respectively.

#### 14.4.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show protect-group group-id</b>	Show configurations and operation status of the OLT protection group.
2	<b>Raisecom#show protect-onu-group group-id</b>	Show configurations and operation status of ONU Type D protection group.

### 14.5 Configuring OLT hand-in-hand uplink interface protection

#### 14.5.1 Preparing for configurations

##### Scenario

OLT hand-in-hand uplink interface protection is mainly used between the OLT uplink interface and the upper layer device to provide two links (primary and secondary) for the OLT uplink services and enhance the service security.

##### Prerequisite

N/A

#### 14.5.2 Default configurations

N/A

#### 14.5.3 Configuring OLT hand-in-hand uplink interface protection

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#extend-uplink-protect type { ge port slot-id/port-id   trunk group group-id }</b>	Configure the protection interface.

Step	Command	Description
3	<code>Raisecom(config)#extend-uplink-protect cycle <i>period</i></code>	Configure the polling cycle of OLT hand-in-hand uplink interface protection.
4	<code>Raisecom(config)#extend-uplink-protect { enable   disable }</code>	Enable/Disable OLT hand-in-hand uplink interface protection.

## 14.5.4 Checking configurations

No.	Command	Description
1	<code>Raisecom#show extend-uplink-protect</code>	Show information about hand-in-hand uplink interface protection.

## 14.6 Configuring cross-OLT PON interface dual-homed protection (Type B)

### 14.6.1 Preparing for configurations

#### Scenario

Cross-OLT PON interface dual-homed protection (Type B) can be used to protect PON interfaces on different OLTs.

#### Prerequisite

- Both the primary and secondary interfaces should not be shut down.
- Two OLTs can communicate on Layer 3.
- There should not be created ONU on the secondary link.

### 14.6.2 Default configurations

N/A

### 14.6.3 Configuring cross-OLT PON interface dual-homed protection (Type B)



#### Caution

Configurations parameters (enabling status, recovery time, and locking status) and alarm status of the protection groups on the two OLTs should be consistent. Otherwise, protection switching between the two OLTs will fail.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#protect-group</b> <i>group-id</i> <b>primary</b> <i>slot-id/olt-id</i> <b>secondary</b> <i>slot-id/olt-id</i> <b>type</b> <b>backbone-pon-protect-extend</b> <b>local-port-role</b> { <b>primary</b>   <b>secondary</b> } <b>peer-device-description</b> <i>device-description</i> <b>peer-device-ip-address</b> <i>ip-address</i>	Configure the cross-OLT PON interface protection group. You can use the <b>no protect-group</b> <i>group-id</i> command to delete the protection group.
3	<b>Raisecom(config)#protect-group</b> <i>group-id</i> { <b>enable</b>   <b>disable</b> }	Enable/Disable the protection group.
4	<b>Raisecom(config)#protect-group</b> <i>group-id</i> <b>auto-recover-time</b> <i>second</i>	(Optional) configure the auto-recovery time. You can use the <b>no protect-group</b> <i>group-id</i> <b>auto-recover-time</b> command to restore default configurations.
5	<b>Raisecom(config)#protect-group</b> <i>group-id</i> <b>force-switch</b>	(Optional) configure FS.
6	<b>Raisecom(config)#protect-group</b> <i>group-id</i> <b>lock</b> { <b>primary</b>   <b>secondary</b>   <b>null</b> }	(Optional) configure locking the working link in the protection group.



### Note

Configurations of the primary and secondary OLTs cannot be synchronized automatically. So you should synchronize configurations of all member interfaces and ONUs on the two OLTs manually.

## 14.6.4 Checking configurations

No.	Command	Description
1	<b>Raisecom(config)#show protect-group</b> <i>group-id</i>	Show configurations and operation status of the protection group.

## 14.7 Configuring link aggregation

### Scenario

When needing to provide higher bandwidth and reliability for a link between two devices, you can configure the 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.

### 14.7.2 Default configurations

Default configurations of link aggregation on the ISCOM5508 are as below.

Function	Default value
Link aggregation	Enable
LACP link aggregation	Enable
LAG	N/A
Load balancing mode	sxordmac
LACP system priority	32768

### 14.7.3 Configuring manual link aggregation

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface port-channel group-id</b>	Create a LAG and enter LAG configuration mode.
3	<b>Raisecom(config-port-channel-*)#port-channel mode manual</b>	Configure manual link aggregation.
4	<b>Raisecom(config-port-channel-*)#port-channel loading-sharing mode { dip   sip   dmac   smac   sxordip   sxordmac }</b>	Configure the load balancing mode of the LAG.
5	<b>Raisecom(config-port-channel-*)#interface gigabitethernet slot-id/port-list</b>	Add interfaces to the LAG in batch. You can use the <b>no interface gigabitethernet slot-id/port-list</b> command to delete the interface from the LAG.
	<b>Raisecom(config-port-channel-*)#exit</b> <b>Raisecom(config)#interface gigabitethernet slot-id/port-id</b> <b>Raisecom(config-if-gigabitethernet-*)#port-channel group-id</b>	Add an interface to the LAG. You can use the <b>no port-channel group-id</b> command to delete the interface from the LAG.




#### Note

In the same LAG, member interfaces that share loads must be identically configured to avoid improper forwarding of packets. These configurations include STP, QoS, QinQ, VLAN, interface properties, and MAC address learning.

- STP: STP enabling/disabling status on the interface, link attributes connected to the port (point-to-point or not), port path cost, STP priority, packet Tx rate limiting, loopback protection, root protection, edge port or not.
- QoS: traffic monitoring, traffic shaping, rate limiting, SP queue, WRR queue scheduling, interface priority, and interface trust mode.
- 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.

## 14.7.4 Configuring static LACP link aggregation

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#lACP system-priority</b> <i>system-priority</i>	<p>(Optional) configure the LACP system priority.</p> <p>You can use the <b>no lACP system-priority</b> command to restore default configurations.</p> <div>  <b>Note</b> </div> <p>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.</p>
3	<b>Raisecom(config)#interface port-channel</b> <i>port-channel-number</i>	Enter LAG configuration mode.
4	<b>Raisecom(config-port-channel-*)#port-channel mode lACP-static</b>	Configure the static LACP LAG.
5	<b>Raisecom(config-port-channel-*)#port-channel loading-sharing mode</b> { <b>dip</b>   <b>sip</b>   <b>dmac</b>   <b>smac</b>   <b>sxordip</b>   <b>sxordmac</b> }	Configure the load balancing mode of the LAG.
6	<b>Raisecom(config-port-channel-*)#interface gigabitEthernet</b> <i>slot-id/port-list</i>	<p>Add interfaces to the LAG in batch.</p> <p>You can use the <b>no interface gigabitEthernet slot-id/port-list</b> command to delete the interface from the LAG.</p>
	<b>Raisecom(config-port-channel-*)#exit</b> <b>Raisecom(config)#interface</b> <b>gigabitEthernet</b> <i>slot-id/port-id</i> <b>Raisecom(config-if-*:*)#port-channel</b> <i>group-id</i>	<p>Add an interface to the LAG.</p> <p>You can use the <b>no port-channel group-id</b> command to delete the interface from the LAG.</p>



## 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.

### 14.7.5 Checking configurations

No.	Command	Description
1	<code>Raisecom#show lacp system</code>	Show system LACP configurations.
2	<code>Raisecom#show lacp neighbor</code>	Show neighbor LACP information, including flag, interface priority, device ID, Age, operation key, interface ID, and status of the interface state machine.
3	<code>Raisecom#show lacp internal</code>	Show local LACP interface configurations.
4	<code>Raisecom#show lacp statistics</code>	Show interface LACP statistics, including total number of received/sent LACP packets, the number of received/sent Marker packets, the number of received/sent Marker Response packets, the number of errored packets.
5	<code>Raisecom#show port-channel [ group-id ]</code>	Show LAG configurations.

## 14.8 Configuring link-state tracking

### Scenario

When the uplink fails, if downlink devices are not informed of the link failure, traffic will be interrupted because it cannot be switched to the backup link.

Through link-state tracking, uplink and downlink interfaces of the transit device are added to a link-state group, and the uplink interface is monitored in real time. Once all uplink interfaces fail, all downlink interfaces are set to Down status. When at least one uplink interface recovers, all downlink interfaces recover to Up status. Therefore, faults of uplink devices can be transmitted to the downlink devices immediately. Uplink interfaces are not influenced when downlink interfaces fail.


### Prerequisite

Connect the interface, configure its physical parameters, and make it Up at the physical layer.

## 14.8.2 Default configurations

N/A

## 14.8.3 Configuring link-state tracking

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#link-state-tracking group group-number</b>	Create a link-state group. You can use the <b>no link-state-tracking group group-number</b> command to delete the link-state group.
3	<b>Raisecom(config)#link-state-tracking group group-number { enable   disable }</b>	Enable/Disable the link-state group.
4	<b>Raisecom(config)#interface { gigabitethernet slot-id/port-id   epon-olt slot-id/port-id   port-channel group-id }</b>	Enter interface configuration mode.
5	<b>Raisecom(config-if-**-*)#link-state-tracking group group-number { downstream   upstream }</b>	Configure the link-state group to which the interface belongs and the interface type.   <b>Note</b> An interface can belong to one link-state group only and the interface can only be an uplink or downlink interface.



### Note

One link-state group can contain several uplink interfaces. Link-state tracking will not be performed when at least one uplink interface is Up. Only when all uplink interfaces are Down, link-state tracking occurs.

## 14.8.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show link-state-tracking group [ group-number ]</b>	Show link-state group configurations and status. Using this command does not display information about the link-state group which has been created but is not enabled and has no member interface.

## 14.9 Configuring RRPS

### Scenario

As a metro Ethernet technology, RRPS solves the problems of weak protection and taking too long to recover faults of the traditional data network. RRPS, in theory, can provide 50ms rapid protection features and is compatible with traditional Ethernet protocol, and is an important technology option and solution for metro broadband access network optimization and transformation.

RRPS technology is Raisecom independent research and development protocol, which achieves the elimination of ring network loopback, fault protection switching, and automatic fault recovery function through simple configuration, and makes the fault protection switching time less than 50ms.

### Prerequisite

N/A

### 14.9.2 Default configurations

Default configurations of RRPS on the ISCOM5508 are as below.

Function	Default value
RRPS status	Disable
Interval to send Hello packets	1s
Fault recovery delay	5s
Bridge priority	1
Ring interface aging time	15s
Ring protocol packet VLAN	2
Ring description	Ethernet ring <i>ring-id</i>



### Caution

For all devices on a ring, we recommend that configurations of the fault recovery time, interval to send Hello packets, ring protocol packet VLAN, and aging time of the ring interface are consistent with those of master node.

### 14.9.3 Creating Ethernet ring

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



Step	Command	Description
2	<code>Raisecom(config)#create ethernet ring ring-id</code>	Create an Ethernet ring. Use the <b>no ethernet ring ring-id</b> command to delete the Ethernet ring.
3	<code>Raisecom(config)#interface gigabitethernet slot-id/port-id</code>	Enter physical interface configuration mode.
4	<code>Raisecom(config-if-gigabitethernet- *:*)#ethernet ring ring-id { primary   secondary }</code>	Create the primary/secondary interface for the Ethernet ring.
5	<code>Raisecom(config-if-gigabitethernet- *:*)#exit</code> <code>Raisecom(config)#ethernet ring ring-id { enable   disable }</code>	Enable/Disable the Ethernet ring.


## 14.9.4 Configuring basic functions of Ethernet ring



### Note

Master node selection: at the beginning, all nodes consider themselves as the master node, one of two interfaces is blocked, so no data loop on the ring; when two interfaces on the ring node receive the same Hello packet for many times, the node considers that the ring topology is stable and can be selected as the master node. Other nodes will enable the blocked interface. Generally, there is only one master node, which ensures that only one interface is blocked, and connectivity of nodes on the ring is proper.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ethernet ring ring-id hello-time hello-time</code>	(Optional) configure the interval to send Hello packets on the Ethernet ring. Use the <b>no ethernet ring ring-id hello-time hello-time</b> command to restore default configurations.  <div data-bbox="748 1438 831 1520" data-label="Image"></div> <div data-bbox="834 1471 940 1512" data-label="Section-Header"><h3>Note</h3></div> <p>The interval to send Hello packets on the Ethernet ring should be less than half of the aging time of the ring interface.</p>
3	<code>Raisecom(config)#ethernet ring ring-id restore-delay delay- time</code>	(Optional) configure the fault recovery delay on the Ethernet ring. When the fault recovers, the original working link restores to work after the delay expires. You can use the <b>no ethernet ring ring-id restore-delay delay-time</b> command to restore default configurations.
4	<code>Raisecom(config)#ethernet ring ring-id priority priority</code>	(Optional) configure the bridge priority on the Ethernet ring. You can use the <b>no ethernet ring ring-id priority priority</b> command to restore default configurations.

Step	Command	Description
5	<code>Raisecom(config)#<b>ethernet ring</b> <i>ring-id</i> <b>description</b> <i>string</i></code>	(Optional) configure ring descriptions. You can use the <b>no ethernet ring ring-id description</b> command to restore default configurations.
6	<code>Raisecom(config)#<b>ethernet ring</b> <i>ring-id</i> <b>hold-time</b> <i>hold-time</i></code>	(Optional) configure the aging time of the Ethernet ring interface. You can use the <b>no ethernet ring ring-id hold-time</b> command to restore default configurations.   <b>Note</b> If the Ethernet ring interface has not received a Hello packet in the aging time, age this interface. If the interface on a node is in blocked status, it will enable the temporarily blocked interface to ensure the normal communication of all nodes on the Ethernet ring.
7	<code>Raisecom(config)#<b>ethernet ring</b> <i>ring-id</i> <b>protocol-vlan</b> <i>vlan-id</i></code>	(Optional) configure the Ethernet ring protocol VLAN. You can use the <b>no ethernet ring ring-id protocol-vlan</b> command to restore default configurations.
8	<code>Raisecom(config)#<b>ethernet ring</b> <b>upstream-group</b> { <i>group-list</i> }</code>	(Optional) configure the uplink interface group on the Ethernet ring. You can use the <b>no ethernet ring upstream-group</b> command to restore default configurations.



### Note

- The uplink interface group works with link-state tracking, and supports dual homming topology applications.
- The uplink interface group ID is corresponding to the link-state group ID.

## 14.9.5 Checking configurations

No.	Command	Description
1	<code>Raisecom#<b>show ethernet ring</b> [ <i>ring-id</i> ]</code>	Show information about the Ethernet ring.
2	<code>Raisecom#<b>show ethernet ring port</b></code>	Show information about the Ethernet ring interface.
3	<code>Raisecom#<b>show ethernet ring port</b> <b>statistic</b></code>	Show Ethernet ring interface statistics.

## 14.9.6 Maintenance

Command	Description
<code>Raisecom(config)#clear ethernet ring <i>ring-id</i> statistics</code>	Clear Ethernet ring interface statistics.

## 14.10 Configuring loopback detection

### 14.10.1 Preparing for configurations

#### Scenario

On the network, hosts or Layer 2 devices connected downlink to all access devices may form loopback intentionally or involuntarily. Enabling loopback detection on the downlink interface of the access device can avoid the network congestion formed by unlimited data traffic caused by loopback on the downlink interface. Once the loopback is detected, Trap will be reported or the interface will be blocked.

#### Prerequisite

Configure physical parameters of the interface and make the interface Up at the physical layer.

### 14.10.2 Default configurations

Default configurations of loopback detection on the ISCOM5508 are as below.

Function	Default value
Global loopback detection status	Disable
loopback detection status on interface	Disable
Loopback detection VLAN	VLAN 1
MAC address of loopback detection packet	FFFF.FFFF.FFFF
Loopback detection period	4s
Loopback detection recovery time	300s
Action upon receiving link detection packets on the current bridge	Discarding (send Trap and block the interface)
Action upon receiving link detection packets on other bridges	Trap-only (send Trap only without blocking the interface)

Default configurations of loopback detection on the ONU are as below.

Function	Default value
loopback detection status on interface	Enable
Loopback detection period	4s
Loopback detection VLAN	N/A
Shutdown time of loopback interface	infinite

### 14.10.3 Configuring loopback detection on OLT



#### Note

- Loopback detection and STP are exclusive, only one can be enabled at one time.
- Loopback detection cannot be enabled on both ends of the directly-connected device simultaneously; otherwise, interfaces at both ends will be blocked.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#loopback-detection</b>	Enable global loopback detection. You can use the <b>no loopback-detection</b> command to disable this function.
3	<b>Raisecom(config)#loopback-detection destination-address mac-address</b>	(Optional) configure the destination MAC address of the loopback detection packet. You can use the <b>no loopback-detection destination-address</b> command to restore default configurations.
4	<b>Raisecom(config)#loopback-detection down-time { second   infinite }</b>	(Optional) configure the shutdown time of the loopback interface. You can use the <b>no loopback-detection down-time</b> command to restore default configurations.
5	<b>Raisecom(config)#loopback-detection hello-time second</b>	(Optional) configure the loopback detection period. You can use the <b>no loopback-detection hello-time</b> command to restore default configurations.
6	<b>Raisecom(config)#loopback-detection vlan vlan-id</b>	(Optional) configure the loopback detection VLAN. You can use the <b>no loopback-detection vlan</b> command to restore default configurations.
7	<b>Raisecom(config)#interface { gigabitethernet   epon-olt } slot-id/port-id</b>	Enter physical interface configuration mode.
8	<b>Raisecom(config-if-*:*:*)#loopback-detection</b>	Enable loopback detection on the interface. You can use the <b>no loopback-detection</b> command to disable this function.
9	<b>Raisecom(config-if-*:*:*)#loopback-detection { exloop   loop } { discarding   trap-only }</b>	Configure the action of the interface upon receiving the loopback detection packet.

Step	Command	Description
10	<code>Raisecom(config-if-*:*:*)#no loopback-detection discarding</code>	(Optional) enable the blocked interface manually.



### Note

When you need to perform loopback detection on the ONU under the OLT, adopt the following methods:

- Enable loopback detection on the OLT PON interface when detecting the link between ONUs under different PON interfaces.
- Enable loopback detection on the ONU when detecting the link between ONUs under the same PON interface.

## 14.10.4 Configuring loopback detection on ONU



### Note

- Loopback detection and STP are exclusive, only one can be enabled at one time.
- Loopback detection cannot be enabled on both ends of the directly-connected device simultaneously; otherwise, interfaces at both ends will be blocked.

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 remote management configuration mode.
3	<code>Raisecom(config-epon-onu-*/*:*)#loopback-detection vlan vlan-id</code>	(Optional) configure the loopback detection VLAN. You can use the <b>no loopback-detection vlan</b> command to restore default configurations.
4	<code>Raisecom(config-epon-onu-*/*:*)#loopback-detection hello-time second</code>	(Optional) configure the loopback detection period. You can use the <b>no loopback-detection hello-time</b> command to restore default configurations.
5	<code>Raisecom(config-epon-onu-*/*:*)#exit</code> <code>Raisecom(config)#epon-onu uni ethernet slot-id/olt-id/onu-id/uni-id</code>	Enter EPON ONU UNI configuration mode.
6	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)#loopback-detection { enable   disable }</code>	Enable/Disable loopback detection on the interface.
7	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)#loopback-detection auto-shutdown { enable   disable }</code>	Enable/Disable auto-shutdown on the loopback interface.
8	<code>Raisecom(config-epon-onu-ethernet-*/*/*:*)#loopback-detection down-time { second   infinite }</code>	(Optional) configure the shutdown time of the loopback interface. You can use the <b>no loopback-detection down-time</b> command to restore default configurations.

## 14.10.5 Checking configurations

### Checking configurations on OLT

No.	Command	Description
1	<code>Raisecom#show [interface { gigabitethernet   epon-olt } slot-id/port-id ] loopback-detection [ statistics ]</code>	Show loopback detection configurations and statistics.

### Checking configurations on ONU

No.	Command	Description
1	<code>Raisecom#show epon-onu slot-id/olt-id/onu-id loopback-detection</code>	Show loopback detection configurations on the ONU.
2	<code>Raisecom#show epon-onu loopback-port</code>	Show loopback information about all ONU interfaces to locate and troubleshoot faults.

## 14.11 Configuring interface backup

### 14.11.1 Preparing for configurations

#### Scenario

Interface backup is another solution of STP. When STP is disabled, you can realize basic link redundancy by manually configuring interface backup.

#### Prerequisite


Loopback detection and STP are exclusive, only one can be enabled at one time. So disable STP before configuring interface backup.

### 14.11.2 Default configurations

Default configurations of interface backup on the ISCOM5508 are as below.

Function	Default value
Interface backup group	N/A
Interface recovery	Enable
Interface recovery delay	15s
Interface backup group VLAN	1–4094

### 14.11.3 Creating interface backup group


Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#create port-backup group <i>group-id</i></b>	Create an interface backup group. You can use the <b>no create backup-port group <i>group-id</i></b> command to delete the configuration.
3	<b>Raisecom(config)#port-backup group <i>group-id</i> { enable   disable }</b>	Enable/disable the interface backup group.   <b>Note</b> The following two reasons may lead to enabling interface backup group failure: <ul style="list-style-type: none"> <li>• The interface backup group does not exist.</li> <li>• The primary/backup interface is not configured in the interface backup group.</li> </ul>

### 14.11.4 Configuring interface backup group

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#port-backup group <i>group-id</i> vlanlist <i>vlan-list</i></b>	Configure interface backup group VLAN. You can use the <b>no port-backup group <i>group-id</i> vlanlist</b> command to restore default configurations.
3	<b>Raisecom(config)#interface { gigabitethernet   epon-olt } <i>slot-id/port-id</i></b>	Enter physical interface configuration mode.
4	<b>Raisecom(config-if-<i>*:*</i>)#port-backup group <i>group-id</i> { primary-port   backup-port }</b>	Configure the primary interface and backup interface. You can use the <b>no port-backup group <i>group-id</i> { primary-port   backup-port }</b> command to delete the configuration.
5	<b>Raisecom(config-if-<i>*:*</i>)#port-backup group <i>group-id</i> restore-mode { enable   disable }</b>	Enable/Disable interface recovery.
6	<b>Raisecom(config-if-<i>*:*</i>)#port-backup group <i>group-id</i> restore-delay <i>time</i></b>	Configure the interface recovery delay. You can use the <b>no port-backup group <i>group-id</i> restore-delay</b> command to restore default configurations.

### 14.11.5 Configuring Force Switch

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

Step	Command	Description
2	<b>Raisecom(config)#port-backup group <i>group-id</i> force-switch</b>	<p>Configure FS on the interface backup group.</p> <div>  <b>Note</b> </div> <ul style="list-style-type: none"> <li>• When FS 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.</li> <li>• When FS 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.</li> </ul>

### 14.11.6 Checking configurations

No.	Command	Description
1	<b>Raisecom#show port-backup group [ <i>group-id</i> ]</b>	Show interface backup configurations.

## 14.12 Maintenance

Command	Description
<b>Raisecom(config)#clear ethernet ring <i>ring-id</i> statistics</b>	Clear protection ring statistics.

## 14.13 Configuration examples

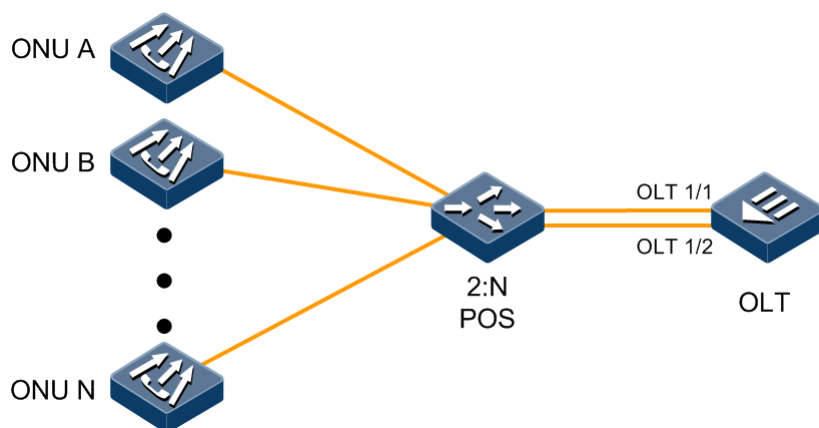
### 14.13.1 Example for configuring OLT backbone fiber protection (Type B)

#### Networking requirements

As shown in Figure 14-9, to enhance reliability of the link between the OLT and ONU, you need to configure OLT backbone fiber protection (Type B) on the OLT. Add OLT 1/1 and OLT 1/2 into the protection group, of which the former is the primary link while the latter is the secondary link. Configure the auto-recovery time to 10min and the holdover time of ONU 1/1/1 to 500ms.



Figure 14-9 Configuring OLT backbone fiber protection (Type B)



## Configuration steps

Step 1 Create the OLT backbone fiber protection group.

```
Raisecom#config
Raisecom(config)#protect-group 1 primary 1/1 secondary 1/2 type backbone-pon-protect
```

Step 2 Configure synchronizing data on the primary PON interface and primary ONU link to the secondary PON interface and secondary ONU link respectively.

```
Raisecom(config)#sync-data protect-group 1
```

Step 3 Configure the auto-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 500
Raisecom(config-epon-onu-1/1/1)#protect-group holdover activated time 500
Raisecom(config-epon-onu-1/1/1)#end
```

## Checking results

Use the **show protect-group** command on the OLT to show configurations and operation status of the protection group.

```
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

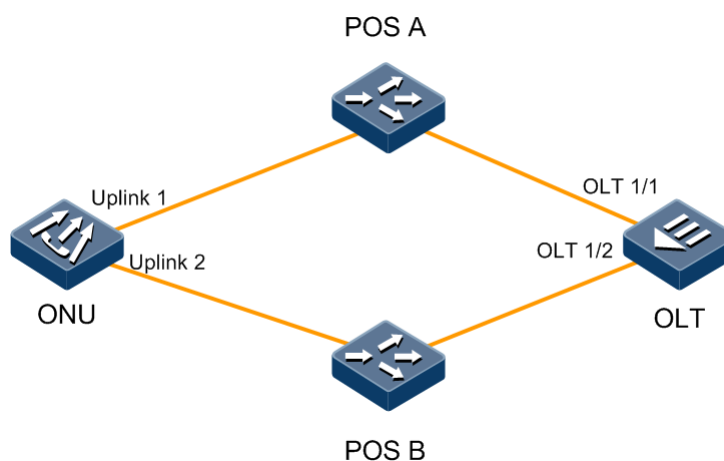
```

## 14.13.2 Example for configuring PON full protection (Type C)

### Networking requirements

As shown in Figure 14-10, to enhance reliability of the link between the OLT and ONU, you need to configure PON full protection (Type C) on the OLT and ONU. Add OLT 1/1 and OLT 1/2 into the protection group, of which the former is the primary link while the latter is the secondary link. Configure the ONU holdover time to 500ms.

Figure 14-10 Configuring PON full protection (Type C)



### Configuration steps

Step 1 Create the OLT full protection group.

```
Raisecom#config
```

```
Raisecom(config)#protect-group 1 primary 1/1 secondary 1/2 type full-pon-protect
```

- Step 2 Configure synchronizing data on the primary PON interface and primary ONU link to the secondary PON interface and secondary ONU link respectively.

```
Raisecom(config)#sync-data protect-group 1
```

- Step 3 Enable the protection group.

```
Raisecom(config)#protect-group 1 enable
```

- Step 4 Configure the ONU holdover time.

```
Raisecom(config)#epon-onu 1/1/1  
Raisecom(config-epon-onu-1/1:1)#protect-group holdover time 500  
Raisecom(config-epon-onu-1/1:1)#protect-group holdover activated time 500  
Raisecom(config)#end
```

## Checking results

Use the **show protect-group** command on the OLT to show configurations and operation status of the protection group.

```
Raisecom(config)#show protect-group 1  
Group ID: 1  
  Group type           : Full 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 : Hotbackup  
  Auto-recovery time   : 0 min  
  Successful switching count: 0  
  Last switching result : Succeeded
```

Use the **show epon-onu slot-id/olt-id/onu-id protect-group** command on the OLT to show configurations and operation status of the ONU protection group.

```
Raisecom#show epon-onu 1/1/1 protect-group
Group ID: 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
```

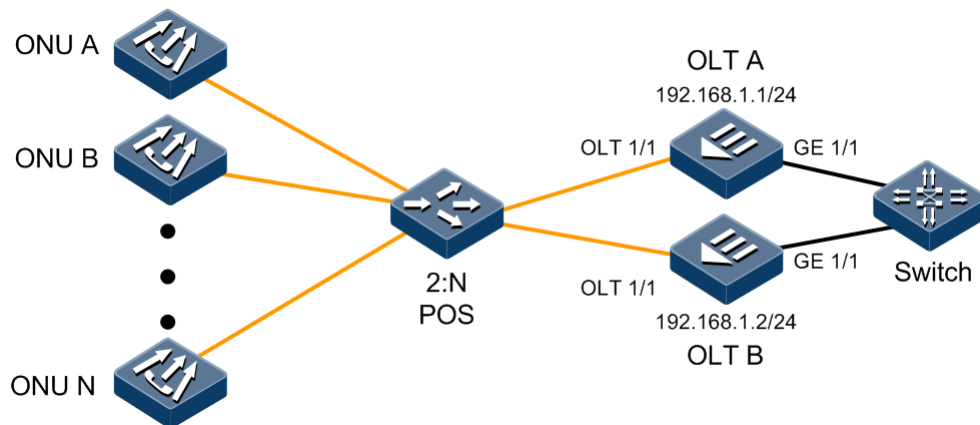
### 14.13.3 Example for configuring cross-OLT PON interface dual-homed protection (Type B)

#### Networking requirements

As shown in Figure 14-11, to enhance reliability of the entire link, you need to configure cross-OLT PON interface dual-homed protection on two OLTs.

- OLT A, the primary device, the IP address of which is 192.168.1.1, uses OLT 1/1 to connect downlink to the POS and GE 1/1 to connect uplink to the switch.
- OLT B, the secondary device, the IP address of which is 192.168.1.2, uses OLT 2/1 to connect downlink to POS and uses GE 1/1 to connect uplink to the switch.

Figure 14-11 Configuring cross-OLT PON interface dual-homed protection (Type B)



#### Configuration steps

- Configure OLT A.

Step 1 Configure the IP address of OLT A.

```
Raisecom#config
Raisecom(config)#interface vlanif 0
```

```
Raisecom(config-vlanif-0)#ip address 192.168.1.1 255.255.255.0 1
Raisecom(config-vlanif-0)#end
```

Step 2 Configure descriptions of OLT A.

```
Raisecom#config
Raisecom(config)#device description ISCOM5508a
```

Step 3 Create the cross-OLT PON interface 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
ISCOM5508b peer-divice-ip-address 192.168.1.2
```

Step 4 Enable the protection group.

```
Raisecom(config)#protect-group 1 enable
```

- Configure OLT B.

Step 5 Configure the IP address of OLT B.

```
Raisecom#config
Raisecom(config)#interface vlanif 0
Raisecom(config-vlanif-0)#ip address 192.168.1.2 255.255.255.0 1
Raisecom(config-vlanif-0)#end
```

Step 6 Configure descriptions of OLT B.

```
Raisecom#config
Raisecom(config)#device description ISCOM5508b
```

Step 7 Create the cross-OLT PON interface 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
ISCOM5508a peer-divice-ip-address 192.168.1.1
```

Step 8 Enable the protection group.

```
Raisecom(config)#protect-group 1 enable
```

## Checking results

Use the **show protect-group** command on OLT A to show configurations and operation status of the OLT protection group.

```
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 : ISCOM5508b
  Peer device IP address : 192.168.1.2
  Last alarm status     : Normal
```

Use the **show protect-group** command on OLT B to show configurations and operation status of the OLT protection group.

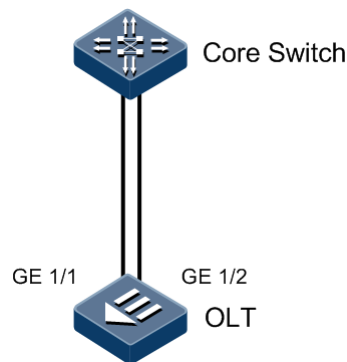
```
Raisecom#show protect-group 1
Group ID: 1
  Group type           : Backbone PON protection between OLTs
  Primary line         : 1/1
  Primary line state    : Normal
  Secondary line        : 2/1
  Secondary line state  : LOS
  Group admin status    : Enabled
  Group lock status     : Unlocked
  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 : ISCOM5508b
  Peer device IP address : 192.168.1.1
  Last alarm status     : Normal
```

## 14.13.4 Example for configuring manual link aggregation

### Networking requirements

As shown in Figure 14-12, to improve link reliability between the OLT and uplink aggregation switch, you can configure manual link aggregation on the OLT. Add GE 1/1 and GE 1/2 to the LAG to form a single logical interface. The LAG performs load balancing according to the source MAC address.

Figure 14-12 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 gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#port-channel 1
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#port-channel 1
Raisecom(config-if-gigabitethernet-1:2)#exit
```

## Checking results

Use the **show port-channel** command to show global configurations of manual link aggregation.

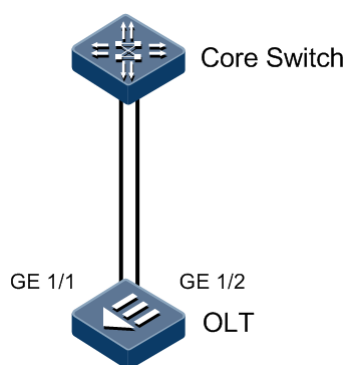
```
Raisecom#show port-channel 1
Port-channel ID : 1
Mode             : Manual
Load-sharing Mode : smac
Member ports      : gigabitethernet 1/1,2
Efficient ports   :
```

## 14.13.5 Example for configuring static LACP link aggregation

### Networking requirements

As shown in Figure 14-13, to improve link reliability between the OLT and uplink aggregation switch, you can configure static LACP link aggregation on the OLT. Add GE 1/1 and GE 1/2 to the LAG. GE 1/1 works as the primary link, and GE 1/2 works as the backup link.

Figure 14-13 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 gigabitethernet 1/1
```



```
Raisecom(config-if-gigabitethernet-1:1)#port-channel 1
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#port-channel 1
Raisecom(config-if-gigabitethernet-1:2)#exit
```

- Step 3 Configure the priority of GE 1/ to make the GE 1/1 as the primary link and GE 1/2 as the backup link.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigaethgigabitethernet-1:1)#lACP port-priority 10000
Raisecom(config-if-gigaethgigabitethernet-1:1)#exit
```

## Checking results

Use the **show port-channel** command on the OLT to show static LACP link aggregation global configurations.

```
Raisecom#show port-channel
Port-channel ID : 1
  Mode           : LACP-static
  Load-sharing Mode : smac
  Member ports    : gigabitethernet 1/1,2
  Efficient ports  :
```

Use the **show lacp internal** command on the OLT to show configurations of peer 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
```

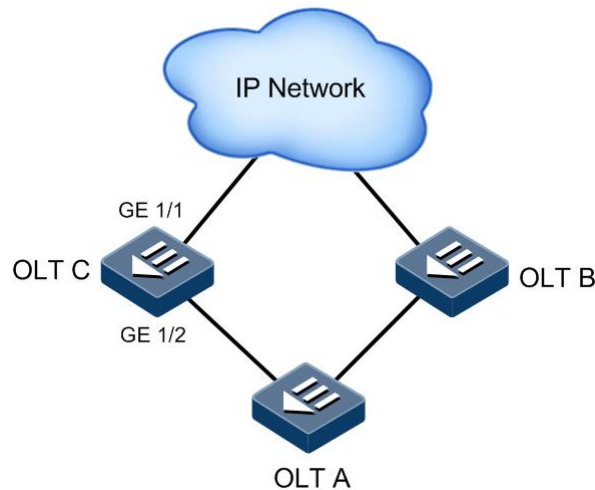
Port	State	Flags	Port-Pri	Admin-key	Oper-key	Port-State
1/1	down	FA	10000	0x1	0x1	0x4d
1/2	down	FA	32768	0x1	0x1	0x4d

## 14.13.6 Example for configuring link-state tracking

### Networking requirements

As shown in Figure 14-14, OLT C/OLT A is one of dual homing devices. Configure link-state tracking on OLT C to ensure that OLT A can detect the link failure quickly and switch to the backup link when the uplink of OLT C fails.

Figure 14-14 Link-state tracking networking



### Configuration steps

Step 1 Create and enable the link-state group.

```
Raisecom#config
Raisecom(config)#link-state-tracking group 1
```

Step 2 Configure the uplink interface of the link-state group.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#link-state-tracking group 1
upstream
Raisecom(config-if-gigabitethernet-1:1)#exit
```

Step 3 Configure the downlink interface of the link-state group.

```
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#link-state-tracking group 1
downstream
```

## Checking results

Use the **show link-state-tracking group** command to show link-state tracking configurations.

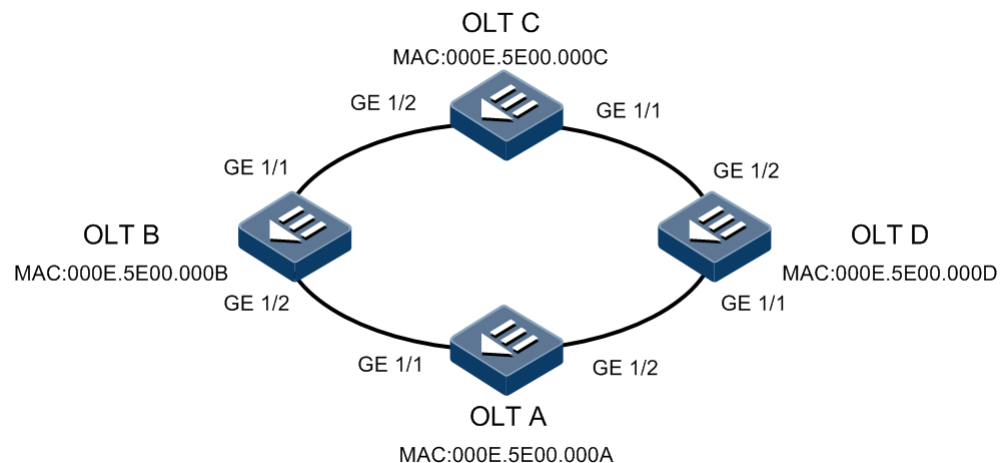
```
Raisecom#show link-state-tracking group 1
Link State Tracking Group: 1 (Enable)
Status: Failover
Upstream Interfaces:
gigabitethernet 1/1(Up)
Downstream Interfaces:
gigabitethernet1/2(Up)
```

## 14.13.7 Example for configuring Ethernet ring

### Networking requirements

As shown in Figure 14-15, four OLTs form a ring network. Configure the Ethernet ring feature to achieve elimination of ring network loopback, fault protection switching, and automatic fault recovery. OLT A is the master node.

Figure 14-15 Ethernet ring networking



### Configuration steps

Configurations on four OLTs are identical. Take OLT A for example.

Step 1 Configure the Ethernet ring on OLT A.

```
Raisecom#config
Raisecom(config)#create ethernet ring 1
Raisecom(config)#ethernet ring 1 enable
```

- Step 2 Configure the interface mode for OLT A and interface allowing the Ethernet ring protocol VLAN to pass.

```
Raisecom#config
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#ethernet ring 1 primary
Raisecom(config-if-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:1)#switchport trunk allowed vlan 2
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#ethernet ring 1 secondary
Raisecom(config-if-gigabitethernet-1:2)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:2)#switchport trunk allowed vlan 2
Raisecom(config-if-gigabitethernet-1:2)#exit
```

## Checking results

Use the **show ethernet ring** to show Ethernet ring configurations.

```
Raisecom#show ethernet ring
Ethernet Ring Upstream-Group:--
Ethernet Ring 1:
Ring Admin:          Enable
Ring State:          Unenclosed
Bridge State:        Block
Ring state duration: 0 days, 0 hours, 0 minutes, 55 seconds
Bridge Priority:      1
Bridge MAC:          000E.5E00.000A
Ring DB State:       Block
Ring DB Priority:     1
Ring DB:             000E.5E00.000A
Hello Time:          1
Restore delay:        5
Hold Time:           15
Protocol Vlan:        2
```

Use the **show ethernet ring port** to show Ethernet ring interface status.

```
Raisecom#show ethernet ring port
Ethernet Ring 1:
Primary Port:        1/1
Port Active State:   Active
State:               Block
Peer State:          None
Switch counts:       5
Current state duration: 0 days, 0 hours, 2 minutes, 28 seconds
Peer Ring Node:
1  --2:000E.5E00.000B:1--
```

```

2  --2:000E.5E00.000C:1--
3  --2:000E.5E00.000D:1-
Secondary Port:      1/2
Port Active State:   Active
State:               Forward
Peer State:          None
Switch counts:       6
Current state duration: 0 days, 0 hours, 2 minutes, 28 seconds
Peer Ring Node:
1  --1:000E.5E00.000D:2--
2  --1:000E.5E00.000C:2--
3  --1:000E.5E00.000B:2-

```



### Caution

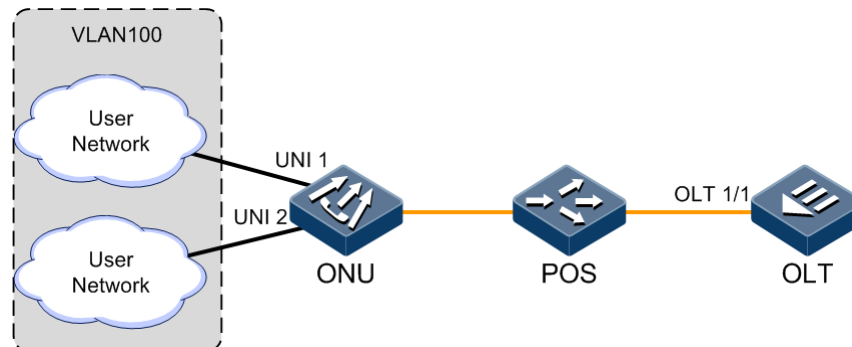
Before configuring Ethernet ring, you must configure the interface allowing the protocol VLAN to pass. By default, the protocol VLAN of the OLT is VLAN 2.

## 14.13.8 Example for configuring loopback detection

### Networking requirements

As shown in Figure 14-16, OLT 1/1 connects the ONU through a POS. The ONU connects to the user network through interfaces UNI1 and UNI 2. You can enable loopback detection on the ONU through OLT remote management to detect loopback in user VLAN 100.

Figure 14-16 Loopback detection networking



### Configuration steps

Step 1 Configure the VLAN needing to enable loopback detection.

```

Raisecom#config
Raisecom(config)#epon-onu 1/1/1
Raisecom(config-epon-onu-1/1:1)#loopback-detection vlan 100
Raisecom(config-epon-onu-1/1:1)#exit

```

Step 2 Configure the UNI needing to enable loopback detection.

```
Raisecom(config)#epon-onu uni ethernet 1/1/1/1
Raisecom(config-epon-onu-ethernet-1/1/1:1)#loopback-detection enable
Raisecom(config-epon-onu-ethernet-1/1/1:1)#exit
Raisecom(config)#epon-onu uni ethernet 1/1/1/2
Raisecom(config-epon-onu-ethernet-1/1/1:2)#loopback-detection enable
```

## Checking results

Use the **show epon-onu slot-id/olt-id/onu-id loopback-detection** to show loopback detection configurations.

```
Raisecom#show epon-onu 1/1/1 loopback-detection
ONU ID: 1/1/1
Period: 4s
VLAN : 100
```

PORT ID	State	Loop Flag	State/Time	Source Port
1	enable	no	--/infinite	0
2	enable	no	--/infinite	0
3	disable	no	--/infinite	0
4	disable	no	--/infinite	0

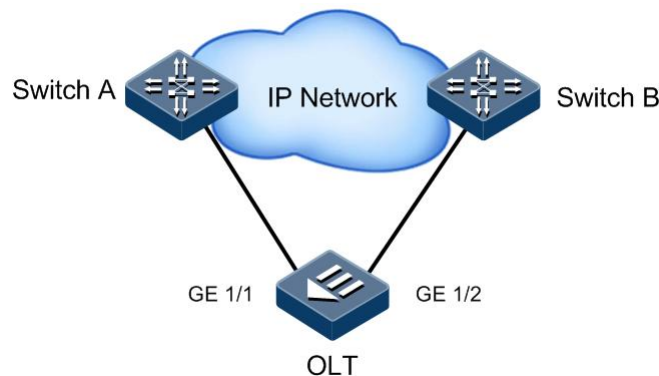
## 14.13.9 Example for configuring interface backup

### Networking requirements

As shown in Figure 14-17, 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:

- Create interface backup group 2, including interfaces GE 1/1 and GE 1/2. GE 1/1 is the primary interface of VLANs 100–150. GE 1/2 is the backup interface of VLANs 100–150.
- Create interface backup group 2, including GE 1/1 and GE 1/2. GE 1/2 is the primary interface of VLANs 151–200. GE 1/1 is the backup interface of VLANs 151–200.

Figure 14-17 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 gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#port-backup group 1 primary-port
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#port-backup group 1 backup-port
Raisecom(config-if-gigabitethernet-1:2)#exit
Raisecom(config)#create port-backup group 2
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#port-backup group 1 backup-port
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#port-backup group 1 primary-port
Raisecom(config-if-gigabitethernet-1:2)#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 interface backup** command to show interface backup configurations.

```
Raisecom#show interface backup
Group Id: 1
Primary Port(State): gigabitethernet1/1(Forwarding)
Backup Port(State) : gigabitethernet1/2(Discarding)
Vlanlist           : 100-150
Restore delay      : 15
Restore mode       : enable
switch state       : no force
switch count       : 0
-----
Group Id: 2
```

```
Primary Port(State): gigabitethernet1/2(Forwarding)
Backup Port(State) : gigabitethernet1/1(Discarding)
Vlanlist           : 151-200
Restore delay      : 15
Restore mode       : enable
switch state       : no force
switch count       : 0
-----
```



# 15 Configuring system management

---

This chapter introduces the basic principle and configuration process of the system management and maintenance feature of the ISCOM5508, and provides related configuration examples, including the following sections:

- Overview of system management
- Configuring SNMP
- Configuring RMON
- Configuring optical module DDM
- Configuring Layer 2 protocol transparent transmission
- Configuring PPPoE agent
- Configuring Watchdog
- Configuring system log
- Configuring port mirroring
- Configuring link detection
- Configuring LLDP
- Configuring system monitoring
- Configuring link monitoring
- Configuring alarm and event management
- BCMP
- Maintenance
- Configuration examples

## 15.1 Overview of system management

### 15.1.1 SNMP

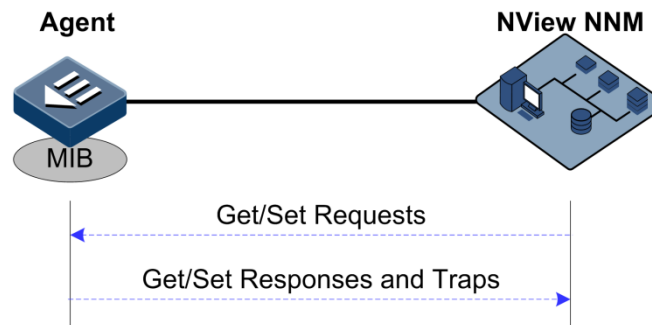
Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to resolve problems in managing network devices connected to the Internet. Through SNMP, a network management system can manage all network devices that support

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 15-1.

Figure 15-1 Working mechanism of SNMP



Raisecom NView NNM system can provide friendly Human Machine Interface (HMI) to facilitate network management. The below functions can be realized 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 trigger conditions according to protocol modules, enter/exit from system or reboot device when conditions are satisfied; reply module sends Trap packets to NView NNM system via 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.

- SNMP v1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a secret. 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 ISCOM5508, the message will be dropped.

- Compatible with SNMP v1, SNMP v2c also uses community name authentication mechanism. SNMP V2c supports more operation types, data types, and error codes, and thus better identifying errors.
- SNMP v3 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 store information in a tree structure, its root is on the top, without name. Nodes of the tree are the managed objects, which take a uniquely path starting from root (OID) for identification. SNMP packets can access network devices by checking the nodes in MIB tree directory.

### 15.1.2 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, as well as 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

### 15.1.3 System log

The system log refers 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 process. 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-22-2013 14:27:33 CONFIG-7-CONFIG:USER "raisecom" Run "logging on"
FEB-22-2013 06:46:20 CONFIG-6-LINK_D:port 2 Link Down
FEB-22-2013 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 is an example of system log sent to the host:

```
07-01-201311:31:28Local0.Debug20.0.0.6JAN 01 10:22:15 ISCOM5508: CONFIG-
7-CONFIG:USER " raisecom " Run " logging on "
07-01-200811:27:41Local0.Debug20.0.0.6JAN 01 10:18:30 ISCOM5508: 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 15-1.

Table 15-1 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



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. Such as, when the information is configured with the 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 ISCOM5508, 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 15-2 lists alarm fields.

Table 15-2 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 15-3.

Table 15-3 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)

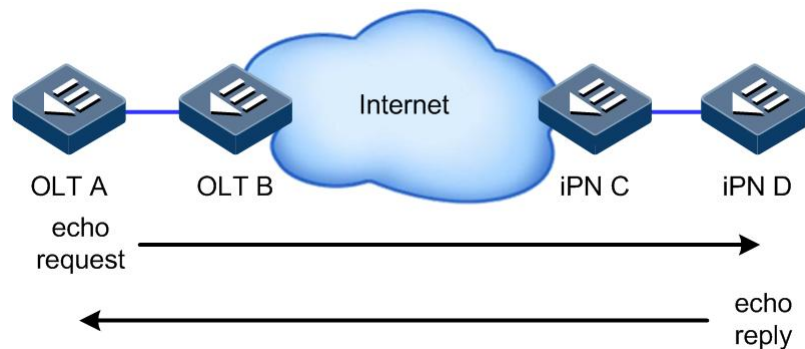
## 15.1.4 Ping

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 15-2 shows the working principle of Ping

Figure 15-2 Working principle of Ping



## 15.1.5 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.

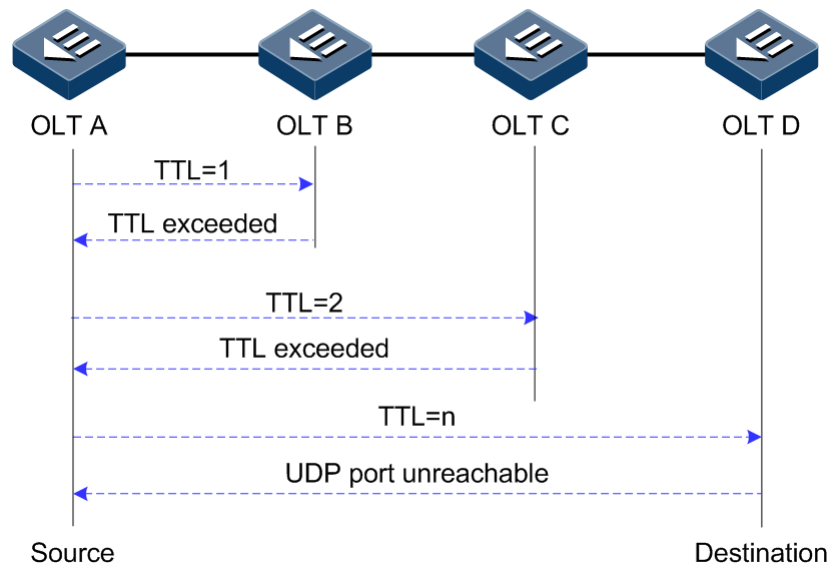
The following shows how Traceroute works:

- 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 be used, the destination host will send the 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 15-3 shows the working principle of Traceroute.

Figure 15-3 Working principle of Traceroute



## 15.1.6 LLDP

With the enlargement of network scale and increase of network devices, the network topology becomes more and more complex and network management becomes very important. A lot of network management software adopts "auto-detection" function to trace changes of network topology, but most of the software can only analyze to the 3<sup>rd</sup> layer and cannot make sure the interfaces connect to other devices.

Link Layer Discovery Protocol (LLDP) is based on IEEE 802.1ab standard. Network management system can fast grip the Layer 2 network topology and changes.

LLDP organizes the local device information in different Type Length Value (TLV) and encapsulates in Link Layer Discovery Protocol Data Unit (LLDPDU) to transmit to straight-connected neighbour. It also saves the information from neighbour as standard Management Information Base (MIB) for network management system querying and judging link communication.

### Basic concepts

The LLDP packet is the Ethernet packet encapsulated LLDPDU in the data unit.

LLDPDU is a data unit of LLDP packet. The device encapsulates local information in TLV before forming LLDPDU, and then several TLVs fit together into one LLDPDU, which will be encapsulated in Ethernet data for transmission.

As shown in Figure 15-4, a LLDPDU consists of multiple TLVs, of which four are mandatory and others are optional.

Figure 15-4 Structure of LLDPDU

Chassis ID TLV	Port ID TLV	Time To Live TLV	Optional TLV	...	Optional TLV	End Of LLDPDU TLV
M	M	M				M

M-mandatory TLV required for all LLDPDUs



TLV: the unit to make up a LLDPDU, which refers to the unit describing the type, length and information of the object.

As shown in Figure 15-5, each TLV indicates a piece of information about the local device, such as device ID, interface ID, related Chassis ID TLV, and Port ID TLV fixed TLV.

Figure 15-5 Structure of TLV

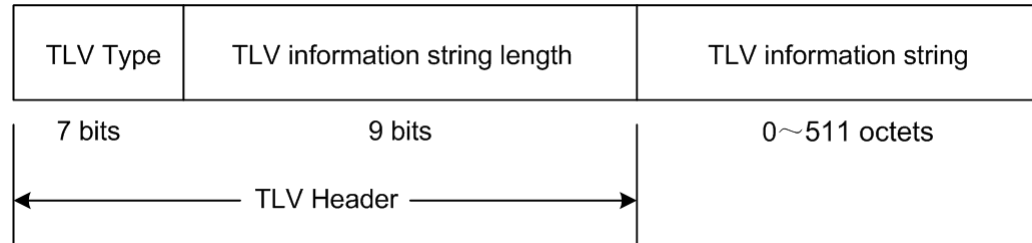


Table 15-4 lists the TLV types. At present, only types 0–8 are used.

Table 15-4 TLV type

TLV type	Description	Mandatory or optional
0	End Of LLDPDU, indicating end of the LLDP packet	Mandatory
1	Chassis Id, indicating the MAC address of the Tx device	Mandatory
2	Port Id, indicating the Tx port of the LLDP packet	Mandatory
3	Time To Live, indicating the aging time of the local information on the neighbor device	Mandatory
4	Port Description, indicating descriptions of the Ethernet interface	Optional
5	System Name, indicating the name of the device	Optional
6	System Description, indicating descriptions of the system	Optional
7	System Capabilities, indicating the main function of the system and used options	Optional
8	Management Address	Optional

## Working principle of LLDP

LLDP is a kind of point-to-point one-way issuance protocol, which notifies the peer device of link status of the local device by sending LLDPDU periodically (or sending LLDPDU when link status changes) from the local device to the peer.

The process of packet exchange is as below:

- When the local device sends the LLDPDU, it gets system information required by TLV from NView NNM system and gets configuration information from LLDP MIB to generate TLV and form LLDPDU to transmit to the peer.
- The peer receives LLDPDU and analyzes TLV information. If there is any change, the information will be updated in neighbor MIB table of LLDP and notifies the NView NNM system.

The Time To Live (TTL) of local device information in the neighbour node can be adjusted by modifying the parameter values of aging coefficient. Send LLDP packets to the neighbour node, the neighbour node will adjust the aging time of its neighbour node (Tx end) after receiving LLDP packets. The aging time formula,  $TTL = \text{Min} \{65535, (\text{interval} \times \text{hold-multiplier})\}$ :

- Interval refers to the time period to send LLDP packets from the device to the neighbor node.
- Hold-multiplier refers to the aging coefficient of the device information on the neighbor node.

## 15.1.7 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 high-efficiently.



### Note

The difference of 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-TI 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 not reported to the NMS nor recorded in the history event table. Event masking will not stop until you disable it manually.

## 15.2 Configuring SNMP

### 15.2.1 Default configurations

Default configurations of SNMP on the ISCOM5508 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			

### 15.2.2 Configuring basic functions of SNMP v1/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.

SNMP v1/v2c uses the community name authentication scheme. SNMP packets which are inconsistent with the community name will be discarded.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#snmp-server view <i>view-name</i> <i>oid-tree</i> [ <i>mask</i> ] { <i>included</i>   <i>excluded</i> }</b>	(Optional) create the SNMP view and configure the MIB variable range.
3	<b>Raisecom(config)#snmp-server community <i>com-name</i> [ <i>view view-name</i> ] { <i>ro</i>   <i>rw</i> }</b>	Create the community name and configure the corresponding view and access privilege.

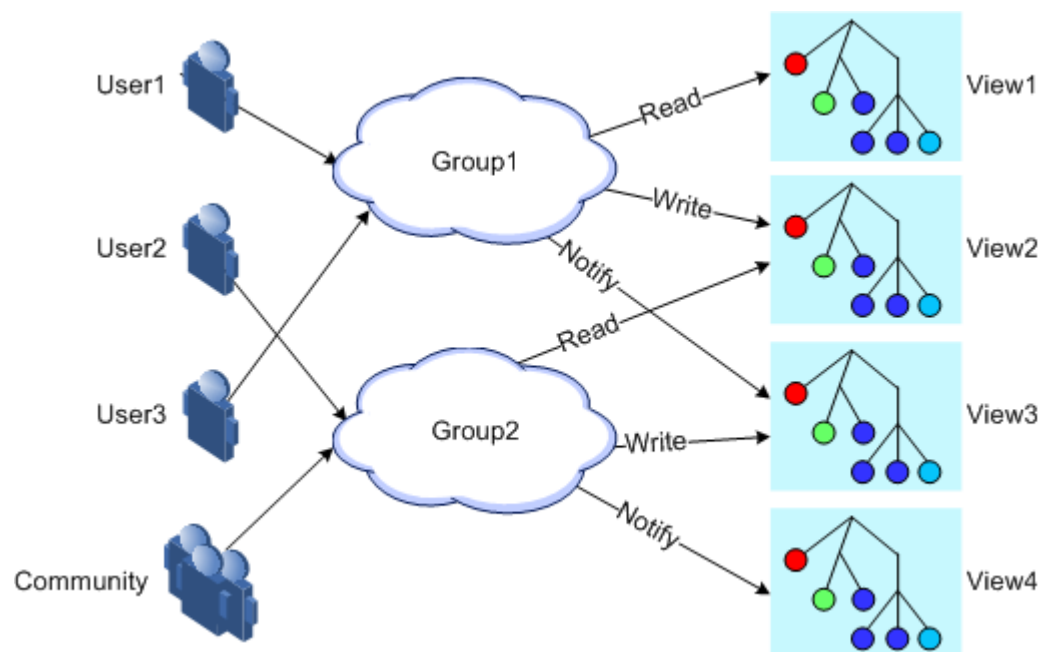
### 15.2.3 Configuring basic functions of SNMP v3

SNMP v3 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 15-6, the network management station uses SNMP v3 to access the ISCOM5508 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 15-6 Authentication mechanism of SNMP V3




Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#snmp-server view</b> <i>view-name</i> <i>oid-tree</i> [ <i>mask</i> ] { <i>included</i>   <i>excluded</i> }	Create the SNMP view and configure the MIB variable range.
3	<b>Raisecom(config)#snmp-server user</b> <i>username</i> [ <i>remote engineid</i> ] <b>authentication</b> { <i>md5</i>   <i>sha</i> } <i>authpassword</i>	Create the user and configure the authentication mode.
4	<b>Raisecom(config)#snmp-server user</b> <i>username</i> [ <i>remote engineid</i> ] <b>authkey</b> { <i>md5</i>   <i>sha</i> } <i>authkey</i>	Create the user and configure information about the authentication key.
5	<b>Raisecom(config)#snmp-server user</b> <i>username</i> [ <i>remote engineid</i> ]	Create the user and configure the remote SNMP engine ID.
6	<b>Raisecom(config)#snmp-server access</b> <i>group-name</i> [ <i>read view-name</i> ] [ <i>write view-name</i> ] [ <i>notify view-name</i> ] [ <i>context context-name</i> ] { <i>exact</i>   <i>prefix</i> } [ <i>usm</i> { <i>noauthnopriv</i>   <i>authnopriv</i> } ]	Create and configure the SNMP v3 access group.
7	<b>Raisecom(config)#snmp-server group</b> <i>group-name</i> <b>user</b> <i>username</i> { <i>v1sm</i>   <i>v2csm</i>   <i>usm</i> }	Configure mapping between the user and access group.

## 15.2.4 Configuring other information of SNMP

Configure other information of SNMP, including:

- Identification and contact of administrators
- Physical location of the ISCOM5508

SNMP v1, v2c, and v3 are in support of the above configurations.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#snmp-server contact</b> <i>contact</i>	(Optional) configure identification and contact of administrators.   <b>Note</b> For example, user the E-mail as the identification and contact of administrators.
3	<b>Raisecom(config)#snmp-server location</b> <i>location</i>	(Optional) specify the physical location of the device.

## 15.2.5 Configuring Trap



### Note

Except for the destination host configuration, Trap configurations of SNMP v1, 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 SNMP v1 and v2c, configure the community name; if using SNMP v3, configure the user name and SNMP view.
- Configure the routing protocol, and ensure that the route between the ISCOM5508 and NMS is reachable.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#snmp-server host ip-address version { 1   2c } name [ udpport value ]</code>	(Optional) configure the IPv4 Trap/Notification target host based on SNMP v1/v2.
3	<code>Raisecom(config)#snmp-server host ip-address version 3 { noauthnopriv   authnopriv } name [ udpport value ]</code>	(Optional) configure the IPv4 Trap/Notification target host based on SNMP v3.
4	<code>Raisecom(config)#snmp-server host ipv6 ipv6-address [ scopeid string ] version { 1   2c } name [ udpport value ]</code>	(Optional) configure the IPv6 Trap/Notification target host based on SNMP v1/v2.
5	<code>Raisecom(config)#snmp-server host ipv6 ipv6-address [ scopeid string ] version 3 { noauthnopriv   authnopriv } name [ udpport value ]</code>	(Optional) configure the IPv6 Trap/Notification target host based on SNMP v3.
6	<code>Raisecom(config)#snmp-server enable traps</code>	Enable the OLT to send Trap. You can use the <b>no snmp-server enable traps</b> command to disable this function.
7	<code>Raisecom(config)#snmp-server keepalive-trap { enable   disable   pause }</code>	Enable/Disable/Pause to send KeepAlive Trap.
8	<code>Raisecom(config)#snmp-server keepalive-trap interval period</code>	Configure the interval to send KeepAlive Trap from the device to the SNMP NMS. You can use the <b>no snmp-server keepalive-trap interval</b> command to restore default configurations.

## 15.2.6 Checking configurations

No.	Command	Description
1	<code>Raisecom#show snmp access</code>	Show privilege information about all access groups.

No.	Command	Description
2	<b>Raisecom#show snmp community</b>	Show configurations of the SNMP community.
3	<b>Raisecom#show snmp config</b>	Show SNMP basic configurations.
4	<b>Raisecom#show snmp group</b>	Show mapping between the SNMP user and access group.
5	<b>Raisecom#show snmp host</b>	Show information about the SNMP target host.
6	<b>Raisecom#show snmp statistics</b>	Show SNMP statistics.
7	<b>Raisecom#show snmp user</b>	Show SNMP user information.
8	<b>Raisecom#show snmp view</b>	Show SNMP view information.

## 15.3 Configuring RMON

### 15.3.1 Default configurations

Default configurations of RMON on the ISCOM5508 are as below.


Function	Default value
Statistics group	Enable
Historical statistics group	Disable
Alarm group	N/A
Event group	N/A

### 15.3.2 Configuring RMON statistics

RMON statistics is used to take statistics on an interface, including the number of Tx/Rx packets, undersized/oversized packets, collision, CRC and errors, discarded packets, length of Rx packets, fragments, broadcast packets, multicast packets, and unicast packets.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#rmon statistics { ip if-number   port-list port-list } [ owner owner-name ]</b>	Enable RMON statistics on an interface and configure related parameters.  You can use the <b>no rmon statistics { port-list port-list   ip if-num }</b> command to disable this function.

### 15.3.3 Configuring RMON historical statistics

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#rmon history { ip if-number   port-list port-list } [ shortinterval period ] [ longinterval period ] [ buckets number ] [ owner owner-name ]</b>	<p>Enable RMON historical statistics on an interface and configure related parameters.</p> <p>You can use the <b>no rmon history { ip if-number   port-list port-list }</b> command to disable the historical statistics group.</p> <div>  <b>Note</b> </div> <p>When the historical statistics group is disabled on the interface, the system will not take statistics on the interface and historical statistics will be cleared.</p>

### 15.3.4 Configuring RMON alarm group

You can monitor a MIB variable (mibvar) by setting a RMON alarm group instance (*alarm-id*). An alarm event is generated when the value of the monitored data exceeds the defined threshold. Related information is recorded in the log or Trap is sent to the NView NNM system according to the definition of alarm events.



#### Note

- The monitored MIB variable must be real, and the data type is correct. If the variable does not exist or the value type is incorrect, return ERROR. For the successfully configured alarm, if the variable cannot be collected later, close the alarm. Reset it if you need to monitor the variable again.
- Disabling the statistics feature on the interface refers to not taking statistics on the interface instead of not take statistics any more.

By default, the event ID to trigger an event is 0, which indicates no event is triggered. If the number is not set to 0 and there is no event configured in the event group, the event is not successfully triggered when the monitored variable is abnormal. The event cannot be successfully triggered unless the event is created.

The alarm will be triggered as long as the upper or lower threshold of the event in the event table is matched. The alarm is not generated even when alarm conditions are matched if the event related to the upper/lower threshold (*rising-event-id* or *falling-event-id*) is not configured in the event table.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#rmon alarm alarm-id mibvar [ interval period ] { delta   absolute } rising-threshold value [ event ] falling-threshold value [ event ] [ owner owner-name ]</b>	<p>Add alarm instances to the RMON alarm group and configure related parameters.</p> <p>You can use the <b>no rmon alarm alarm-id</b> command to delete the alarm group.</p>



## 15.3.5 Configuring RMON event group

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#rmon event <i>event-id</i></b> [ <b>log</b> ] [ <b>trap</b> ] [ <b>description</b> <i>string</i> ] [ <b>owner</b> <i>owner-name</i> ]	Add events to the RMON event group and configure processing modes of events. You can use the <b>no rmon event <i>event-id</i></b> command to delete the event group.

## 15.3.6 Checking configurations

No.	Command	Description
1	<b>Raisecom#show rmon alarms</b>	Show information about the RMON alarm group.
2	<b>Raisecom#show rmon events</b>	Show information about the RMON event group.
3	<b>Raisecom#show rmon statistics</b> [ <b>ip</b> <i>if-number</i>   <b>port</b> <i>port-id</i> ]	Show information about the RMON statistics group.
4	<b>Raisecom#show rmon history</b> [ <b>ip</b> <i>if-number</i>   <b>port</b> <i>port-id</i> ]	Show information about the RMON historical statistics group.

## 15.4 Configuring optical module DDM

### 15.4.1 Default configurations

Default configurations of optical module DDM on the ISCOM5508 are as below.

Function	Default value
Global optical module DDM	Enable (unconfigurable)
Global optical module alarm	Enable (unconfigurable)
Optical module DDM on the interface	Disable
Optical module alarm on the interface	Disable

### 15.4.2 Configuring optical module DDM

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface { epon-olt  </b> <b>gigabitethernet } <i>slot-id/port-id</i></b>	Enter physical interface configuration mode.

Step	Command	Description
3	<b>Raisecom(config-if-*:*:*)#transceiver ddm { enable   disable }</b>	Enable/Disable optical module DDM.
4	<b>Raisecom(config-if-*:*:*)#snmp trap transceiver { enable   disable }</b>	(Optional) enable/disable optical module DDM Trap on the interface.

### 15.4.3 Configuring optical module alarm

#### Configuring optical module alarm on OLT

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface epon-olt slot-id/olt-id</b>	Enter EPON interface configuration mode.
3	<b>Raisecom(config-if-epon-olt-*/*:*)#transceiver rx-onu-power onu onu-id monitor { enable   disable }</b>	Enable/Disable measurement and diagnosis of OLT optical module Rx power.
4	<b>Raisecom(config-if-epon-olt-*/*:*)#transceiver rx-onu-power onu onu-id { high-threshold   low-threshold } threshold-value</b>	Configure the threshold of ONU uplink optical power received by the OLT.

#### Configuring optical module alarm on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*/*:*)#snmp trap transceiver { voltage   bias   temp   tx-power   rx-power } { high-alarm   high-warning   low-warning   low-alarm } { enable   disable }</b>	Configure ONU optical module alarm.
4	<b>Raisecom(config-epon-onu-*/*:*)#transceiver { voltage   bias   temp   tx-power   rx-power } { high-alarm   high-warning   low-warning   low-alarm } threshold threshold-value</b>	Configure the threshold of ONU optical module alarm.

### 15.4.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show transceiver</b>	Show the global and interface status of the OLT optical module measurement and diagnosis.

No.	Command	Description
2	<b>Raisecom#show interface epon-olt slot-id/olt-id transceiver rx-onu-power [ violation ]</b>	Show information about the uplink average optical power of the ONU received by the optical module under the OLT PON interface.
3	<b>Raisecom#show interface { epon-olt   gigabitethernet } slot-id/port-id ddm [ detail ]</b>	Show the current performance, alarm status, and alarm threshold of the OLT optical module.
4	<b>Raisecom#show interface { epon-olt   gigabitethernet } slot-id/port-id ddm history [ 15m   24h ]</b>	Show historical performance parameters of the OLT optical module.
5	<b>Raisecom#show interface { epon-olt   gigabitethernet } slot-id/port-id ddm information</b>	Show the status of the OLT optical module.
6	<b>Raisecom#show interface { epon-olt   gigabitethernet } slot-id/port-id ddm threshold-violation</b>	Show the time from the last violation of the OLT optical module to the present and corresponding violation value.
7	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list transceiver information</b>	Show information about the ONU optical module.
8	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list transceiver detail</b>	Show parameters of the ONU optical module.
9	<b>Raisecom#show epon-onu slot-id/olt-id/onu-list snmp trap transceiver</b>	Show configurations of ONU optical module alarm.

## 15.5 Configuring Layer 2 protocol transparent transmission

### 15.5.1 Preparing for configurations

#### Scenario

In the ISP network, destination multicast addresses for some Layer 2 protocol packets cannot be forwarded. The Layer 2 protocol transparent transmission is configured to make the Layer 2 protocol packet of the user network traverse the ISP network and to realize the Layer 2 protocol to run in the same user network at different locations. With the Layer 2 protocol transparent transmission, you can modify the multicast addresses for Layer 2 protocol packets for forwarding them across the ISP. In addition, you can decapsulate the modified multicast address to the original one on the egress interface. Therefore, the same user network at different locations can run the same Layer 2 protocol.

#### Prerequisite

Configure physical parameters of the interface and make it Up at the physical layer.

### 15.5.2 Default configurations

Default configurations of Layer 2 protocol transparent transmission are as below.

Function	Default value
Layer 2 protocol transparent transmission	Disable
Destination MAC address of transparent transmission packets	010e.5e00.0003
CoS of transparent transmission packets	5
Specified VLAN of transparent transmission packets	N/A
Specified interface of transparent transmission packets	N/A
Interface disabling threshold of transparent transmission packets	N/A

### 15.5.3 Configuring Layer 2 protocol transparent transmission

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#relay</b>	Enable Layer 2 protocol transparent transmission. You can use the <b>no relay</b> command to disable this function.
3	<b>Raisecom(config)#relay destination-address mac-address</b>	(Optional) configure the destination MAC address of transparent transmission packets. You can use the <b>no relay destination-address</b> command to restore default configurations.
4	<b>Raisecom(config)#relay cos cos-value</b>	(Optional) configure the CoS value of transparent transmission packets. You can use the <b>no relay cos</b> command to restore default configurations.
5	<b>Raisecom(config)#interface { gigabitethernet   epon-olt } slot-id/port-id</b>	Enter physical interface configuration mode.
6	<b>Raisecom(config-if-*/*)#relay egress-port interface { gigabitethernet   epon-olt } slot-id/port-id</b>	Specify the egress interface of transparent transmission packets. You can use the <b>no relay egress interface</b> command to restore default configurations.
7	<b>Raisecom(config-if-*/*)#relay vlan vlan-id</b>	Configure the specified VLAN of transparent transmission packets. You can use the <b>no relay vlan</b> command to restore default configurations.

Step	Command	Description
8	<code>Raisecom(config-if-*-*:*)#<b>relay</b> { <b>all</b>   <b>stp</b> }</code>	Configure the type of transparent transmission packets on the interface.  You can use the <b>no relay { all   stp }</b> command to restore default configurations.

## 15.5.4 Checking configurations

No.	Command	Description
1	<code>Raisecom#<b>show relay</b></code>	Show configurations of Layer 2 protocol transparent transmission.
2	<code>Raisecom#<b>show interface { gigabitethernet   epon-olt } slot-id/port-id relay</b></code>	Show configurations of Layer 2 protocol transparent transmission on the interface.
3	<code>Raisecom#<b>show interface { gigabitethernet   epon-olt } slot-id/port-id relay statistics</b></code>	Show statistics of transparent transmission packets.

## 15.5.5 Maintenance


Command	Description
<code>Raisecom(config)#<b>clear interface { gigabitethernet   epon-olt } slot-id/port-id relay statistics</b></code>	Clear statistics of Layer 2 protocol transparent transmission.

## 15.6 Configuring PPPoE agent

### 15.6.1 Default configuration

Function	Default value
PPPoE agent global	Disabled
PPPoE agent interface	Disabled
Trust interface	N/A
Packet processing policies	Transparent transmission
Start position of overwriting	0
Overwriting length	24

## 15.6.2 Configuring PPPoE agent parameters

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <b>{ gigabitethernet   epon-olt }</b> <i>slot-id/port-id</i>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-*</b> <b>*/*:*)#pppoeagent trust</b>	(Optional) configure the interface as one trusted by PPPoE agent. You can use the <b>no pppoeagent trust</b> command to restore to default configurations.   <b>Note</b> When receiving PPPoE packets (such as PADI packets), the proxy will only forward these packets to the trusted interface. Therefore, you should configure the interface which is connected to the legal PPPoE server as a trusted interface.
4	<b>Raisecom(config-if-*</b> <b>*/*:*)#pppoeagent circuit-id</b> <i>circuit-id</i>	(Optional) configure the Circuit ID on the interface.  You can use the <b>no pppoeagent circuit-id</b> command to restore the default configurations.
5	<b>Raisecom(config-if-*</b> <b>*/*:*)#pppoeagent overwrite-</b> <b>policy { transparent   drop  </b> <b>replace }</b>	(Optional) configure the processing policies for PPPoE packets.
6	<b>raisecom(config-if-*</b> <b>*/*:*)#pppoeagent overwrite-</b> <b>policy replace offset</b> <i>value</i> <b>length</b> <i>value</i>	(Optional) configure the partial overwriting policies for PPPoE packets.

## 15.6.3 Enabling PPPoE agent

Step	Command	Description
1	<b>Raisecom#config</b>	Enable global configuration mode.
2	<b>Raisecom(config)#pppoeagent { enable</b> <b>  disable }</b>	Enable/Disable global PPPoE Agent.
3	<b>Raisecom(config)#interface</b> <b>{ gigabitethernet   epon-olt }</b> <i>slot-</i> <i>id/port-id</i>	Enter interface configuration mode.
4	<b>Raisecom(config-if-*</b> <b>*/*:*)#pppoeagent { enable  </b> <b>disable }</b>	Eable/Disable PPPoE Agent.

## 15.6.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show pppoeagent</b>	Show configurations of PPPoE Agent.
2	<b>Raisecom#show interface { gigabitethernet   ten-gigabitethernet   epon-olt   ten-giga-epon-olt   gpon-olt } slot-id/port-id pppoeagent statistics</b>	Show PPPoE Agent statistics on the interface.

## 15.7 Configuring Watchdog

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#watchdog { enable   disable }</b>	Enable/Disable Watchdog.

## 15.8 Configuring system log

### 15.8.1 Default configurations

Default configurations of system log on the ISCOM5508 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

### 15.8.2 Configuring basic information about system log

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

Step	Command	Description
2	Raisecom(config)# <b>logging on</b>	Enable system log. You can use the <b>no logging on</b> command to disable this function.
3	Raisecom(config)# <b>logging time-stamp { relative-start   none }</b>	Configure the type of timestamp.
4	Raisecom(config)# <b>logging rate rate</b>	Configure the Tx rate of system log.

### 15.8.3 Configuring output direction of system log

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>logging history</b>	(Optional) record system log in the buffer.
	Raisecom(config)# <b>logging console severity { severity-level   alerts   critical   debugging   emergencies   errors   informational   notifications   warnings }</b>	(Optional) output system log to the Console interface and configure parameter information.
	Raisecom(config)# <b>logging host host-id { ip   ipv6 } address ip-address facility { local0   local1   local2   local3   local4   local5   local6   local7 } severity [ log-level   alerts   critical   debugging   emergencies   errors   informational   notifications   warnings ]</b>	(Optional) output system log to the log host.
	Raisecom(config)# <b>logging monitor severity { severity-level   alerts   critical   debugging   emergencies   errors   informational   notifications   warnings }</b>	(Optional) output system log to the monitor terminal and configure the alarm level.

### 15.8.4 Checking configurations

No.	Command	Description
1	Raisecom# <b>show logging</b>	Show system log configurations.
2	Raisecom# <b>show logging host</b>	Show information about the system log host.
3	Raisecom# <b>show logging history</b>	Show information about system log buffer.
4	Raisecom# <b>show logging statistics</b>	Show statistics of system log.




## 15.9 Configuring port mirroring

### 15.9.1 Default configurations

N/A

### 15.9.2 Configuring port mirroring on OLT

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mirror { enable   disable }</b>	Enable/disable global port mirroring.
3	<b>Raisecom(config)#interface { gigabitethernet   epon-olt } slot-id/port-id</b>	Enter physical interface configuration mode.
4	<b>Raisecom(config-if-*/*)#mirror monitor-port uni-id</b>	<p>(Optional) configure the monitor port. You can use the <b>no mirror monitor-port</b> command to delete the monitor port.</p> <div>  <b>Note</b> </div> <p>The EPON interface cannot be configured as the monitor port, and it can only be configured as the source port. The Ethernet interface can be configured as the monitor port or mirroring source port.</p>
5	<b>Raisecom(config-if-*/*)#mirror source-port { both   egress   ingress }</b>	<p>(Optional) configure the mirroring source port. You can use <b>no mirror source-port</b> command to restore default configurations.</p>

### 15.9.3 Configuring port mirroring on ONU

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#epon-onu slot-id/olt-id/onu-id</b>	Enter EPON ONU remote management configuration mode.
3	<b>Raisecom(config-epon-onu-*/*:*)#mirror { enable   disable }</b>	Enable/Disable port mirroring on the UNI.
4	<b>Raisecom(config-epon-onu-*/*:*)#mirror monitor-port uni-id</b>	<p>Configure the monitor port. You can use the <b>no mirror monitor-port</b> command to delete the monitor port.</p>

Step	Command	Description
5	<b>Raisecom(config-epon-onu-*//*:*)#mirror source-port-list { both   egress   ingress } uni-list [ uplink ]</b>	Configure the source port and the monitor mode. You can use the <b>no mirror source-port-list { both   egress   ingress }</b> command to restore default configurations.

## 15.9.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show mirror</b>	Show configurations of port mirroring on the OLT.
2	<b>Raisecom#show epon-onu slot-id/olt-id/onu-id mirror</b>	Show configurations of port mirroring on the ONU.

## 15.10 Configuring link detection

### 15.10.1 Ping

Step	Command	Description
1	<b>Raisecom#ping ip-address [ count num ] [ size size ] [ waittime timeout ] [ source ip-address ]</b>	Test whether the IPv4 remote host is reachable.



#### Note

You cannot execute other operations on the device in the process of Ping. You can execute other operations after Ping is complete or press **Ctrl+C** to interrupt Ping.

### 15.10.2 Traceroute



#### Note

Configure the IP address and default gateway for the ISCOM5508 before using the Traceroute function.

Step	Command	Description
1	<b>Raisecom#traceroute ip-address [ firstttl fitst-ttl ] [ maxttl max-ttl ] [ port slot-id/port-id ] [ waittime period ] [ count count ]</b>	Test the IPv4 network connectivity using the <b>traceroute</b> command and show the network nodes passed through by the packet.
2	<b>Raisecom#traceroute ipv6 ipv6-address [ firstttl fitst-ttl ] [ maxttl max-ttl ] [ port slot-id/port-id ] [ waittime period ] [ count count ]</b>	Test the IPv6 network connectivity using the <b>traceroute</b> command and show the network nodes passed through by the packet.

## 15.11 Configuring LLDP

### 15.11.1 Default configurations

Default configurations of LLDP on the ISCOM5508 are as below.

Function	Default value
Global LLDP	Disable
LLDP on interface	Enable
Delay Tx timer	2s
Period Tx timer	30s
Aging coefficient	4
Restart timer	2s
LLDP alarm	Enable
Alarm notification timer	5s

### 15.11.2 Configuring global LLDP

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#lldp { enable   disable }</b>	Enable/Disable global LLDP.
3	<b>Raisecom(config)#lldp message-transmission interval <i>period</i></b>	(Optional) configure the period Tx timer of LLDP packets. You can use the <b>no lldp message-transmission</b> command to restore default configurations.
4	<b>Raisecom(config)#lldp message-transmission delay <i>period</i></b>	(Optional) configure delay Tx timer of LLDP packets. You can use the <b>no lldp message-transmission delay</b> command to restore default configurations.
5	<b>Raisecom(config)#lldp message-transmission hold-multiplier <i>hold-multiplier</i></b>	(Optional) configure the aging coefficient of LLDP packets. You can use the <b>no lldp message-transmission hold-multiplier</b> command to restore default configurations.
6	<b>Raisecom(config)#lldp restart-delay <i>period</i></b>	(Optional) configure the restart timer. When global LLDP is disabled, you can re-enable it only after the time configured by the restart timer. You can use the <b>no lldp restart-delay</b> command to restore default configurations.

## Caution

- After global LLDP is disabled, you cannot re-enable it immediately. Global LLDP cannot be enabled unless the restart timer times out. Because disabling or enabling operations will trigger logout and login of Tx and Rx packets, when disabling the LLDP function, the device will send the Shutdown packet, LLDP can be logged out after each interface completes sending the packet. That is, there is a delay after LLDP logout. If enabling LLDP again before the delayed logout, LLDP will be logged out in delayed logout, which will make the configuration different from the actual situation.
- When you configure the delay Tx timer and period Tx timer, the value of the delay Tx timer cannot exceed one quarter of that of the period Tx timer.

### 15.11.3 Configuring LLDP on interface

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <b>{ gigabitethernet   epon-olt } slot-</b> <b>id/port-id</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-if-*:*:*)#lldp { enable  </b> <b>disable }</b>	Enable/Disable LLDP on the interface.

### 15.11.4 Configuring LLDP alarm

Enable LLDP alarm notification to send the topology update alarm to the NView NNM system when the network changes.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#snmp trap lldp { enable  </b> <b>disable }</b>	Enable/Disable the LLDP alarm.
3	<b>Raisecom(config)#lldp trap-interval</b> <i>period</i>	(Optional) configure the period Tx time of LLDP Trap.

## Note

After enabling the LLDP alarm function, the device will send Trap when it detects neighbor aging, new neighbor, and neighbor information changing.

### 15.11.5 Checking configurations

No.	Command	Description
1	<b>Raisecom#show lldp local config</b>	Show LLDP local configurations.
2	<b>Raisecom#show lldp local system-data</b>	Show local LLDP status.

No.	Command	Description
3	<b>Raisecom#show interface { epon-olt   gigabitethernet } slot-id/port-id lldp local system-data</b>	Show configurations of the LLDP interface.
4	<b>Raisecom#show lldp remote [ detail ]</b>	Show LLDP local neighbor information.
5	<b>Raisecom#show interface { gigabitethernet   epon-olt } slot-id/port-id lldp remote [ detail ]</b>	Show LLDP interface neighbor information.
6	<b>Raisecom#show lldp statistic</b>	Show LLDP local packet statistics.
7	<b>Raisecom#show interface { gigabitethernet   epon-olt } slot-id/port-id lldp statistic</b>	Show LLDP interface packet statistics.

## 15.12 Configuring system monitoring

### 15.12.1 Default configurations

Default configurations of system monitoring on the ISCOM5508 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
Memory monitoring alarm threshold	1

### 15.12.2 Configuring temperature monitoring

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#shelf temperature-threshold threshold-value</b>	Configure the temperature alarm threshold. When the temperature of the device exceeds the threshold, the alarm is reported.

### 15.12.3 Configuring fan monitoring

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#fan speed mode</b> <b>{ auto   manual }</b>	Configure the fan control mode.
3	<b>Raisecom(config)#fan speed manual</b> <b>grade</b>	(Optional) configure the fan speed grade.



#### Note

You need to configure the fan control mode to manual mode before configuring the fan speed grade.

### 15.12.4 Configuring CPU monitoring

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#cpu threshold-</b> <b>trap</b>	Configure the CPU utilization threshold Trap feature.
3	<b>Raisecom(config)#cpu rising-</b> <b>threshold threshold</b>	Configure the CPU alarm rising threshold.
4	<b>Raisecom(config)#cpu falling-</b> <b>threshold threshold</b>	Configure the CPU alarm falling threshold.
5	<b>Raisecom(config)#cpu threshold-</b> <b>interval threshold</b>	Configure the CPU utilization monitoring period.

### 15.12.5 Configuring memory monitoring

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#memory avail-trap</b> <b>slot slot-list</b>	Configure the available memory utilization threshold Trap feature.
3	<b>Raisecom(config)#memory avail-</b> <b>threshold threshold slot slot-list</b>	Configure the memory monitoring alarm threshold.

### 15.12.6 Checking configurations

No.	Command	Description
1	<b>Raisecom#show fan</b>	Show the fan status and configurations.

No.	Command	Description
2	<b>Raisecom#show power</b>	Show power information, including power type, related threshold configurations, input and output voltage, related alarm status, and power version.
3	<b>Raisecom#show device</b>	Show information about the device, including temperature, temperature alarm threshold, power, and fan.
4	<b>Raisecom#show card-power</b> [ slot <i>slot-id</i> ]	Show voltage information of all cards in the slots (except for the power card and fan), including card voltage status and card voltage.
5	<b>Raisecom#show card-temperature</b> [ slot <i>slot-id</i> ]	Show temperature of all cards in the slots.
6	<b>Raisecom#show cpu-utilization</b> [ slot <i>slot-list</i> ] [ dynamic ]	Show CPU utilization of cards in the specified slot.
7	<b>Raisecom#show process sorted</b> { normal-priority   process-name }	Show the status of each task.
8	<b>Raisecom#show process cpu</b> [ sorted { 1min / 10min / 5sec / invoked } ]	Show the running status of each task.
9	<b>Raisecom#show process</b> <i>taskname</i>	Show detailed running status of a specified task.
10	<b>Raisecom#show process dead</b>	Show information about the dead task.
11	<b>Raisecom#show memory</b>	Show utilization of the system memory. This command is applicable to cartridge device only.
12	<b>Raisecom#show memory</b> [ slot <i>slot-list</i> ]	Show memory utilization of cards in the specified slot. This command is applicable to rack-mount device.
13	<b>Raisecom#show abnormal-reboot</b> [ slot <i>slot-list</i> ]	Show information about abnormal start.
14	<b>Raisecom#show abnormal-reboot last</b> [ slot <i>slot-list</i> ]	Show the status of the last abnormal start.
15	<b>Raisecom#show abnormal-reboot last wait-info</b> [slot <i>slot-list</i> ]	Show wait information about the last abnormal start.
16	<b>Raisecom#show epon-onu</b> <i>slot-id/olt-id/onu-list</i> <b>cpu-utilization</b>	Show CPU utilization of the ONU.
17	<b>Raisecom#show epon-onu</b> <i>slot-id/olt-id/onu-list</i> <b>memory</b>	Show information about the memory of the ONU.

## 15.13 Configuring link monitoring

Link monitoring refers to monitoring links between the OLT and ONU. The ISCOM5508 supports 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: <ul style="list-style-type: none"> <li>• The ONU is reset.</li> <li>• The backbone fiber or branch fiber connected to the ONU fails.</li> <li>• Severely errored code is generated.</li> </ul>
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 times out. 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 times out. Generally, this alarm is caused by poor-quality optical signals.

### 15.13.1 Default configurations

Default configurations of link monitoring on the ISCOM5508 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

### 15.13.2 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	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface epon-olt slot-id/olt-id</b>	Enter EPON interface configuration mode.
3	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap { enable   disable }</b>	(Optional) enable/disable alarm reporting.
4	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap encryption-key-update-failure { enable   disable }</b>	(Optional) enable/disable key update failure alarm.
5	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap ber-threshold-crossing downstream { enable   disable }</b>	(Optional) enable/disable downstream BER TCA.
6	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap ber-threshold-crossing upstream { enable   disable }</b>	(Optional) enable/disable upstream BER TCA.
7	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap fer-threshold-crossing downstream { enable   disable }</b>	(Optional) enable/disable downstream FER TCA.
8	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap fer-threshold-crossing upstream {enable   disable }</b>	(Optional) enable/disable upstream FER TCA.
9	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap llid-mismatch-threshold-crossing {enable   disable }</b>	(Optional) enable/disable LLID mismatch TCA.
10	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap llid-mismatch-threshold-crossing threshold rate</b>	(Optional) configure the threshold of LLID mismatch TCA.
11	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap onu-registration-unauthorized { enable   disable }</b>	(Optional) enable/disable illegal ONU registration alarm.
12	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap onu-registration-failure { enable   disable }</b>	(Optional) enable/disable ONU registration failure alarm.
13	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap onu-laser-always-on { enable   disable }</b>	(Optional) enable/disable ONU laser-always-on alarm.
14	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap onu-laser-always-on threshold power</b>	(Optional) configure the threshold of ONU laser-always-on alarm.
15	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap errored-frame { enable   disable }</b>	(Optional) enable/disable DOT3OAM errored-frame alarm.
16	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap errored-frame threshold value</b>	(Optional) configure the threshold of DOT3OAM errored-frame alarm.
17	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap errored-frame-period { enable   disable }</b>	(Optional) enable/disable DOT3OAM errored-frame-period alarm.
18	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap errored-frame-period threshold value</b>	(Optional) configure the threshold of DOT3OAM errored-frame-period alarm.
19	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap errored-frame-seconds-summary { enable   disable }</b>	(Optional) enable/disable DOT3OAM errored-frame-seconds-summary alarm.

Step	Command	Description
20	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap errored-symbol-period { enable   disable }</b>	(Optional) enable/disable DOT3OAM errored-symbol-period alarm.
21	<b>Raisecom(config-if-epon-olt-*:*)#snmp trap port-ber { enable   disable }</b>	(Optional) enable/disable BER alarm on the OLT interface.

### 15.13.3 Checking configurations

No.	Command	Description
1	<b>Raisecom#show interface epon-olt slot-id/olt-list snmp trap</b>	Show alarm management configurations on the OLT.
2	<b>Raisecom#show interface epon-onu slot-id/olt-id/onu-id snmp trap transceiver</b>	Show alarm management configurations on the ONU.

## 15.14 Configuring alarm and event management

### 15.14.1 Default configurations

Default configurations of alarm and event management on the ISCOM5508 are as below.

Function	Default value
Alarm Trap	Enable
Event Trap	Enable
Alarm delay	Disable
Alarm delay interval	10s
Timed alarm masking interval	3600s

### 15.14.2 Configuring alarm management

The alarm management feature on the ISCOM5508 includes alarm reporting, alarm masking, and alarm delay.

#### Configuring alarm reporting

Step	Command	Description
1	<b>Raisecom#config</b>	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>	(Optional) delete alarms in the current alarm table according to the serial number. The deleted alarms are recorded in the historical alarm table.

## 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>	Configure alarm masking on the alarm source of the whole device.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated on the whole device are masked.
	<code>Raisecom(config)#alarm inhibit [ range ] slot slot-list [ alarm-id alarm-id ]</code>	Configure alarm masking on the alarm source of the OLT slots.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated in the OLT slots are masked.
	<code>Raisecom(config)#alarm inhibit [ range ] interface { gigabitethernet   epon-olt } slot-id/port-id [ alarm-id alarm-id ]</code>	Configure alarm masking on the alarm source of the OLT interfaces.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated on the OLT interfaces are masked.
	<code>Raisecom(config)#alarm inhibit [ range ] interface epon-onu slot-id/olt-id/onu-id [ alarm-id alarm-id ]</code>	Configure alarm masking on the alarm source of the ONU.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated on the ONU are masked.
	<code>Raisecom(config)#alarm inhibit interface epon-onu slot-id/olt-id/onu-id [ range ] uni uni-id [ alarm-id alarm-id ]</code>	Configure alarm masking on the alarm source of the ONU UNI.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated on the ONU UNI are masked.

Step	Command	Description
3	<code>Raisecom(config)#alarm inhibit { dev   slot   port   onu   uni } alarm-id alarm-id</code>	Configure alarm masking based on the alarm ID.
4	<code>Raisecom(config)#alarm inhibit time dev [ alarm-id alarm-id ] [ interval interval ] [ start start-time every time stop end- time ]</code>	Configure timed alarm masking on the alarm source of the whole device.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated on the whole device are masked.
	<code>Raisecom(config)#alarm inhibit time [ range ] slot slot-list [ alarm-id alarm-id ] [ interval interval ] [ start start-time every time stop end-time ]</code>	Configure timed alarm masking on the alarm source of the OLT slots.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated in the OLT slots are masked.
	<code>Raisecom(config)#alarm inhibit time [ range ] interface { gigabitethernet   epon-olt } slot-id/port-id [ alarm-id alarm- id ] [ interval interval ] [ start start-time every time stop end- time ]</code>	Configure timed alarm masking on the alarm source of the OLT interfaces.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated on the OLT interfaces are masked.
	<code>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 ]</code>	Configure timed alarm masking on the alarm source of the ONU.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated on the ONU are masked.
	<code>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 ]</code>	Configure timed alarm masking on the alarm source the ONU UNI.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated on the ONU UNI are masked.
5	<code>Raisecom(config)#alarm inhibit time { dev   slot   port   onu   uni } alarm-id alarm-id [ interval interval ] [ start start-time every time stop end-time ]</code>	Configure timed alarm masking based on the alarm ID.
6	<code>Raisecom(config)#alarm inhibit interval time</code>	(Optional) configure the interval of timed alarm masking.

## Configuring alarm filtering

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#alarm filter dev</b> <b>[ alarm-id alarm-id ]</b>	Configure alarm filtering on the alarm source of the whole device.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated on the whole device are filtered.
3	<b>Raisecom(config)#alarm filter</b> <b>[ range ] slot slot-list [ alarm-</b> <b>id alarm-id ]</b>	Configure alarm filtering on the alarm source of the OLT slots.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated in the OLT slots are filtered.
4	<b>Raisecom(config)#alarm filter</b> <b>[ range ] interface</b> <b>{ gigabitethernet   epon-olt }</b> <b>slot-id/port-id [ alarm-id alarm-</b> <b>id ]</b>	Configure alarm filtering on the alarm source of the OLT interfaces.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated on the OLT interfaces are filtered.
5	<b>Raisecom(config)#alarm filter</b> <b>[ range ] interface epon-onu slot-</b> <b>id/olt-id/onu-id [ alarm-id alarm-</b> <b>id ]</b>	Configure alarm filtering on the alarm source of the ONU.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated on the ONU are filtered.
6	<b>Raisecom(config)#alarm filter</b> <b>interface epon-onu slot-id/olt-</b> <b>id/onu-id [ range ] uni uni-id</b> <b>[ alarm-id alarm-id ]</b>	Configure alarm filtering on the alarm source of the ONU UNI.  If you do not configure the <b>alarm-id alarm-id</b> parameter, it is believed that the alarm ID is not specified and all alarms generated on the ONU UNI are filtered.
7	<b>Raisecom(config)#alarm filter</b> <b>{ dev   slot   port   onu   uni }</b> <b>alarm-id alarm-id</b>	Configure alarm filtering based on the alarm ID.

## 15.14.3 Configuring event management

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

Step	Command	Description
2	<b>Raisecom(config)#event traps enable</b>	Enable/Disable the event Trap feature.
3	<b>Raisecom(config)#event inhibit dev [ event-id event-id ]</b>	Configure event masking on the event source of the whole device.  If you do not configure the <b>event-id event-id</b> parameter, it is believed that the event ID is not specified and all events generated on the whole device are masked.
4	<b>Raisecom(config)#event inhibit [ range ] slot slot-list [ event-id event-id ]</b>	Configure event masking on the event source of the OLT slots.  If you do not configure the <b>event-id event-id</b> parameter, it is believed that the event ID is not specified and all events generated in the OLT slots are masked.
5	<b>Raisecom(config)#event inhibit [ range ] interface { gigabitethernet   epon-olt } slot-id/port-id [ event-id event-id ]</b>	Configure event masking on the event source of the OLT interfaces.  If you do not configure the <b>event-id event-id</b> parameter, it is believed that the event ID is not specified and all events generated on the OLT interfaces are masked.
6	<b>Raisecom(config)#event inhibit [ range ] interface epon-onu slot-id/olt-id/onu-id [ event-id event-id ]</b>	Configure event masking on the event source of the ONU.  If you do not configure the <b>event-id event-id</b> parameter, it is believed that the event ID is not specified and all events generated on the ONU are masked.
7	<b>Raisecom(config)#event inhibit interface epon-onu slot-id/olt-id/onu-id [ range ] uni uni-id [ event-id event-id ]</b>	Configure event masking on the event source of the ONU UNI.  If you do not configure the <b>event-id event-id</b> parameter, it is believed that the event ID is not specified and all events generated on the ONU UNI are masked.
8	<b>Raisecom(config)#event inhibit { dev   slot   port   onu   uni } event-id event-id</b>	Configure event masking based on the event ID.

## 15.14.4 Checking configurations

No.	Command	Description
1	<b>Raisecom#show alarm inhibit</b>	Show alarm masking configurations.
2	<b>Raisecom#show alarm filter</b>	Show alarm filtering configurations.

No.	Command	Description
3	<b>Raisecom#show alarm active-table slot <i>slot-id</i> [ detail ]</b>	Show the alarm table in the current slot according to the alarm source, alarm type, or alarm generation time.
4	<b>Raisecom#show alarm alarm-id <i>alarm-id</i></b>	Show detailed information about alarms.
5	<b>Raisecom#show event inhibit</b>	Show event masking configurations.
6	<b>Raisecom#show event history-table [ slot <i>slot-id</i>   onu <i>slot-id/olt-id/onu-id</i>   port <i>solt-id/port-id</i>   dev   event-id <i>event-id</i>   start_time <i>start-time</i> end_time <i>end-time</i> ] [ detail ]</b>	Show the historical event table. The ISCOM5508 supports showing the historical event table according to the event source, event type, and generation time of the event.
7	<b>Raisecom#show event event-id <i>event-id</i></b>	Show detailed information about the alarm event.

## 15.15 BCMP

### 15.15.1 Default configurations

Default configurations of BCMP on the ISCOM5508 are as below.

Function	Default value
IP address of the BCMP server	0.0.0.0
UDP port of the BCMP server	5000
UDP port of the BCMP Proxy	5001

### 15.15.2 Configuring BCMP

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configurations.
2	<b>Raisecom(config)#bcmp server ip-address <i>ip-address</i></b>	Configure the IP address of the BCMP server.
3	<b>Raisecom(config)#bcmp server udp-port <i>port-id</i></b>	Configure the UDP port ID of the BCMP server.
4	<b>Raisecom(config)#bcmp proxy udp-port <i>port-id</i></b>	Configure the UDP port ID of the BCMP Proxy.

### 15.15.3 Checking configurations

No.	Command	Description
1	<code>Raisecom#show bcmp information</code>	Show BCMP configurations.

## 15.16 Maintenance

Command	Description
<code>Raisecom(config)#clear lldp statistic [ port-list slot-id/port-list ]</code>	Clear LLDP statistics.
<code>Raisecom(config)#clear lldp remote-table [ port-list slot-id/port-list ]</code>	Clear LLDP neighbor information.
<code>Raisecom(config)#clear logging history</code>	Clear log records in the buffer.

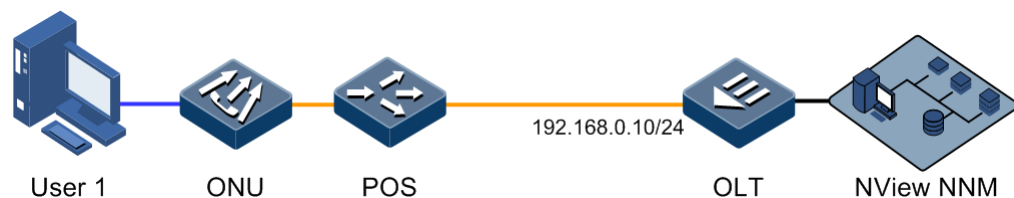
## 15.17 Configuration examples

### 15.17.1 Example for configuring SNMP

#### Networking requirements

As shown in Figure 15-7, 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 15-7 SNMP v3 networking



#### Configuration steps

Step 1 Configure the IP address.

```
Raisecom(config)#interface vlanif 0
Raisecom(config-vlanif-0)#ip address 192.168.0.10 10
```



```
Raisecom(config-vlanif-0)#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 the access group and its name.

Raisecom#**show snmp group**

Index	UserName	SecModel	GroupName
-----			
0	none	usm	initialnone
1	user1	usm	guestgroup
2	md5nopriv	usm	initial
3	shanopriv	usm	initial

## 15.17.2 Example for outputting system log to host

### Networking requirements

As shown in Figure 15-8, 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 15-8 Outputting system log to host



### Configuration steps

Step 1 Configure the IP address of the OLT.

```

Raisecom#config
Raisecom(config)#interface vlanif 0
Raisecom(config-vlanif-0)#ip address 192.168.0.6 255.255.255.0 1
Raisecom(config-vlanif-0)#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.

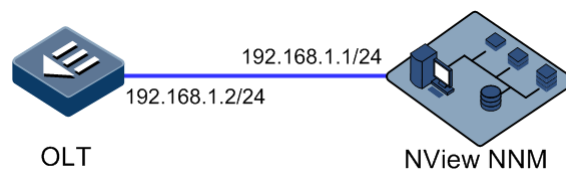
```
Raisecom#show logging
Syslog logging      : Enable
Rate-limited       : 10 messages per second
Logging time-stamp  : Relative time-stamp
Console logging     : Enable
Console severity    : Notifications
Monitor logging     : Disable
Monitor severity    : Informational
History logging     : Enable
History severity    : Debugging
File logging        : Disable
File severity       : Informational
```

## 15.17.3 Example for configuring KeepAlive Trap

### Networking requirements

As shown in Figure 15-9, the IP address of the OLT is 192.168.1.2. The IP address of the SNMP v2c Trap target host is 192.168.1.1. The read-write community name is public. And the SNMP version is v2c. Configure the interval to send KeepAlive Trap from the OLT to the SNMP NMS as 120s and enable KeepAlive Trap.

Figure 15-9 KeepAlive networking



### Configuration steps

Step 1 Configure the management IP address of the OLT.

```
Raisecom#config
Raisecom(config)#interface vlanif 0
Raisecom(config-vlanif-0)#ip address 192.168.1.2 255.255.255.0 1
Raisecom(config-vlanif-0)#exit
```

Step 2 Configure the IP address of the SNMP Trap target host.

```
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 show KeepAlive configurations.

```
Raisecom#show keepalive  
Keepalive Admin State:Enable  
Keepalive trap interval:120s  
Keepalive trap count:1
```

# 16 Appendix

---

This chapter lists terms, acronyms, and abbreviations involved in this document.

- Terms
- Acronyms and abbreviations

## 16.1 Terms

### A

Advanced  
Encryption  
Standard  
(AES)

It is a kind of block encryption standard adopted by the United States to replace the DES. At present, it has become the most widely used standard in the field of symmetric key cryptography.

### C

Connectivity  
Fault  
Management  
(CFM)

CFM is end-to-end service-level Ethernet OAM technology. This function is used to actively diagnose fault for Ethernet Virtual Connection (EVC) and provide cost-effective network maintenance solution via fault management function and improve network maintenance.

### D

Denial of  
Service (DoS)

A common network or computer attack, which aims to make the network or computer fail to provide normal services

Dynamic  
Bandwidth  
Allocation  
(DBA)

A mechanism to dynamically allocate uplink bandwidth in the interval of  $\mu$ s or ms. It can increase the uplink bandwidth utilization rate of the PON interface in the EPON and GPON system.

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 realize centralized management of IP addresses.
--	--

## E

Ethernet Linear Protection Switching (ELPS)	An APS protocol based on ITU-T G.8031 Recommendation to protect an Ethernet link. It is an end-to-end protection technology, including two line protection modes: linear 1:1 protection switching and linear 1+1 protection switching.
Ethernet Over Coaxial (EoC)	EoC enables transmitting Ethernet signals on the coaxial cable. EoC supports coupling CATV signals and Ethernet data signals, and transmitting the hybrid signals to the user side through the CATV coaxial cable, and then demodulating signals through the CNU. EoC is the key technology to realize tri-networks integration (data, voice, and CATV networks) and bidirectional reconstruction of HFC networks.
Ethernet Ring Protection Switching (ERPS)	An APS (Automatic Protection Switching) protocol based on ITU-T G.8032 Recommendation to provide backup link protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer.

## F

Link-state tracking	Provide a port association solution, extending link backup range. Transport fault of upper layer device quickly to downstream device by monitoring upstream link and synchronize downstream link, then trigger switching between master and standby device and avoid traffic loss.
Fiber to the Building (FTTB)	FTTB is based on perfection of broadband access method on the fiber network. Through FTTB and cable-to-household, broadband access can be realized.
Fiber to the Curb (FTTC)	The fiber is installed on the roadside within 1000 feet away from the Central Office to the households or offices.
Fiber to the Home (FTTH)	Namely, fiber is used to connect the household directly. FTTH not only helps gain greater bandwidth, but also increase transparency of data format, rate, wavelength, and protocol. Moreover, it is more adaptive to environment and power conditions, and simplifies the maintenance and installation.
Forward Error Correction (FEC)	It is a method to increase ODN power budget by adding Error Correcting Code (ECC). It supports longer transmission distance and larger splitting ratio.
Frequency Division Multiplexing (FDM)	It is a multiplexing technology which divides the carrier bandwidth into multiple sub-channels at different frequency bands. And each sub-channel can transmit one way of signals concurrently.

## 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 soft switch, or soft switch and H.248/MeGaCo terminal. It is also an important protocol supported by soft switch.

**HomePlug** HomePlug is a non-profit organization, which is established by 13 companies, such as, Panasonic, Intel, HP, and Sharp, in March, 2000. At present, HomePlug has developed into an enterprise alliance composed of 90 companies. The purpose of this organization is to unite leading enterprise in the field of applied electronics, consumer electronics, software, hardware, and retail, and so on to provide an open power-line Internet access specifications for various information appliances.

## I

**Institute of Electrical and Electronics Engineers (IEEE)** An international Institute of electrical and Electronics Engineers. It is one of the largest technical organizations. It has more than 360,000 members in 175 countries (up to 2005).

**Internet Assigned Numbers Authority (IANA)** It is mainly used to assign and maintain the unique code and value in Internet technology standard (protocol), such as the IP address or multicast address.

**Internet Engineering Task Force (IETF)** It is established in 1985. It is the most authoritative technology and standard organization, which develops and formulate specifications related to the Internet.

## 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.

**Link Aggregation Control Protocol (LACP)** A protocol used for realizing link dynamic aggregation. LACP communicates with the peer by exchanging LACPDU.

## M

Maintenance Association (MA)	MA, also called Service Instance, is part of a Maintenance Domain (MD). One MD can be divided into one MA or multiple MAs if required. One MA corresponds to one service and can be mapped to a VLAN. VLANs to which are mapped by different services cannot cross.
Maintenance associations End Point (MEP)	MEP is an edge node of a service instance. MEPs can be used to send and process CFM packets. The MA and the MD where MEP locates decide the VLAN and the level for packets received and sent by MEP.
Maintenance association Intermediate Point (MIP)	MIP is the internal node of a service instance, which is automatically created by the device. MIP cannot actively send CFM packets but can forward and respond to Link Trace Message (LTM) and LoopBack Message (LBM).
Maintenance Domain (MD)	MD is a network that runs the CFM function. It defines network range for OAM. MD can be identified with 8 levels (0–7). The bigger the number, the higher the level and the larger the MD range. Protocol packets in a lower-level MD will be discarded after entering into a higher-level MD. Protocol packets in a higher-level MD can transmit through a lower-level MD. In the same VLAN, Different MDs can be adjacent, embedded, but not crossed.
Maintenance Point (MP)	MEP and MIP are called as MP.
Mobile Backhaul	<p>Solve communication problem from BTS to BSC for 2G, NodeB to RNC for 3G.</p> <p>Mobile backhaul for 2G focuses on voice service, not request high bandwidth, implemented by TDM microwave or SDH/PDH device.</p> <p>In 3G times, lots of data service as HSPA, HSPA+, etc concerning to IP service, voice is changing to IP as well, namely IP RAN, to solve problem of IP RAN mobile backhaul is solving whole network backhaul, satisfying both data backhaul and voice transportation over IP (clock synchronization).</p>

## N

Network Time Protocol (NTP)	A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed timer server and clients. NTP is used to perform clock synchronization on all devices in the network that support clock. Therefore, devices can provide different applications based on some time. In addition, NTP can ensure very high accuracy (about 10ms).
-----------------------------	--

## O

Optical Distribution Frame (ODF)	A distribution connection device between the fiber and a communication device. It is an important part of the optical transmission system. It is mainly used for fiber splicing, optical connector installation, fiber adjustment, additional pigtail storage, and fiber protection.
----------------------------------	--



Optical Distribution Network (ODN)	The optical transmission channel between the OLT and ONU.
Open System Interconnection (OSI)	OSI, defined by the International Standard Organization (ISO), is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into seven abstraction layers. The seven layers are physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer.
Open Shortest Path First (OSPF)	An internal gateway dynamic routing protocol, which is used to decide the route in an Autonomous System (AS).
OLT backbone fiber protection (Type B)	Backbone fiber and OLT PON interface redundancy protection.
Orthogonal Frequency Division Multiplexing (OFDM)	OFDM is one kind of multi-carrier modulation. The purpose of OFDM is to divide the channel into multiple orthogonal sub-channels and transfer high-speed data signals into concurrent low-speed data flow, and then transmit these signals through each sub-channel after modulation.

## P

PON full protection (Type C)	Perform redundancy protection on OLT dual-PON interface, ONU dual-optical module, backbone fiber, POS, and branch fiber.
PON full protection (Type D)	Perform redundancy protection on OLT dual-PON interface, ONU dual-PON interface, backbone fiber, POS, and branch fiber.
Point-to-point Protocol over Ethernet (PPPoE)	With PPPoE, the remote device can control and account each access user.
Precision Time Protocol (PTP)	IEEE 1588 v2 protocol is also called PTP (Precision Time Protocol), a high-precision time protocol for synchronization used in measurement and control systems residing on a local area network. Accuracy in the sub-microsecond range may be achieved with low-cost implementations.

## Q

**QinQ** QinQ is (also called Stacked VLAN or Double VLAN) extended from 802.1Q, defined by IEEE 802.1ad recommendation. Basic QinQ is a simple Layer 2 VPN tunnel technology, encapsulating outer VLAN Tag for client private packets at carrier access end, the packets take double VLAN Tag passing through trunk network (public network). In public network, packets only transmit according to outer VLAN Tag, the private VLAN Tag are transmitted as data in packets.

**Quality of Service (QoS)** A commonly-used performance indicator of a telecommunication system or channel. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio. It functions to measure the quality of the transmission system and the effectiveness of the services, as well as the capability of a service provider to meet the demands of users.

## R

**Rapid Spanning Tree Protocol (RSTP)** RSTP is an extension of Spanning Tree Protocol, which realizes quick convergency of network topology.

**Remote Authentication Dial In User Service (RADIUS)** A protocol used to authenticate and account users in the network.

## S

**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.

**Simple Network Time Protocol (SNTP)** SNTP is mainly used for synchronizing time of devices in the network.

**Spanning Tree Protocol (STP)** STP can be used to eliminate network loops and back up link data. It blocks loops in logic to prevent broadcast storms. When the unblocked link fails, the blocked link is re-activated to act as the protection link.

**SyncE** A technology adopts Ethernet link codes recover clock, similar to SDH clock synchronization quality, SyncE provides frequency synchronization of high precision. Unlike traditional Ethernet just synchronize data packets at receiving node, SyncE implements real-time synchronization system for inner clock.

## T

Time Division Multiplexing (TDM)	TDM is a method to transmit multiple digital data, voice, and video signals on the same communication medium through different channels or cross pulse in timeslots.
Time Division Multiple Access (TDMA)	TDMA divides time into periodical frames and each frame are subdivided into multiple timeslots, each of which will send signals to the base station independently. On the condition of fixed time and synchronization, the base station can receive signals of each mobile terminal from each timeslot orderly. Meantime, signals sent by the base station to the mobile terminals are transmitted through the specified timeslots in sequence. Each mobile terminal can receive signals in the specified timeslot only, so signals will be received in order from the common channel.
TR069	It is a CPE WAN management protocol defined by DSL forum. It provides the general frame and protocol for management and configuration of home network devices on the next-generation network through remotely and concentratedly managing the gateway, router, and STB on the home network.

## 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 segment logically rather than physically, thus implementing virtual work groups which are based on Layer 2 isolation and do not affect each other.
Virtual Private Network (VPN)	It uses the Internet to establish a special data transmission channel to achieve secure, reliable, and remote data transmission.
Voice over Internet Protocol (VoIP)	VoIP can transfer analog voice signals into digital signals and transmit them through the IP network in packets. The biggest advantage of VoIP is that it can transmit voice, video, and data services at lower costs through the IP network.

## 16.2 Acronyms and abbreviations

### 3

3G	3rd-Generation
3GPP	The 3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2

### A

ACL	Access Control List
-----	---------------------

AES	Advanced Encryption Standard
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
AS	Autonomous System
<b>B</b>	
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
<b>C</b>	
CATV	Community Antenna Television
CBAT	Coax Broadcast Access Terminal
CC	Continuity Check
CCM	Continuity Check Message
CCS	Common Channel Signalling
CDMA2000	Code Division Multiple Access 2000
CDR	Calling Detail Records
CFM	Connectivity Fault Management
CE	Customer Edge
CESoPSN	Structure-Aware TDM Circuit Emulation Service over Packet Switched Network
CFI	Canonical Format Indicator
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common Internal Spanning Tree
CLI	Command Line Interface
CMCI	CNU Management Control Interface
CNU	Coax Network Unit
CoS	Class of Service
CO	Central Office
CPE	Customer Premises Equipment
CSMA	Carrier Sense Multiple Access
CST	Common Spanning Tree

CWDM                      Coarse Wavelength Division Multiplexing

## **D**

DBA                      Dynamic Bandwidth Allocation

DCN                      Data Communication Network

DHCP                     Dynamic Host Configuration Protocol

DoS                      Deny of Service

DRR                      Deficit Round Robin

DSCP                     Differentiated Services Code Point

DWDM                    Dense Wavelength Division Multiplexing

## **E**

EFM                      Ethernet in the First Mile

ELPS                     Ethernet Linear Protection Switching

EoC                      Ethernet over Coaxial

EPON                    Ethernet Passive Optical Network

ERPS                    Ethernet Ring Protection Switching

ESD                      Electro Static Discharge

EVC                      Ethernet Virtual Connection

## **F**

FDM                      Frequency-division multiplexing

FDQAM                   Frequency Diverse Quadrature Amplitude Modulation

FEC                      Forward Error Correction

FIB                      Forwarding Information Base

FIR                      Fixed Information Rate

FTTB                    Fiber to the Building

FTTC                    Fiber to the Curb

FTTH                    Fiber to the Home

FTP                      File Transfer Protocol

FR                        Frame Relay

## **G**

GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GPS	Global Positioning System
GPON	Gigabit-Capable PON
GUI	Graphic User Interface
GSM	Global System for Mobile Communications
GVRP	GARP VLAN Registration Protocol

## H

HDLC	High-Level Data Link Control
------	------------------------------

## I

IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
IP	Internet Protocol
IPDV	IP Packet Delay Variation
IST	Internal Spanning Tree
ITU-T	International Telecommunications Union-Telecommunication Standardization Sector
IWF	Inter-working Function

## L

LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LBM	LoopBack Message
LBR	LoopBack Reply
LLID	Logical Link Identifier
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit

LSA	Link-State Advertisement
LTM	LinkTrace Message
LTR	LinkTrace Reply
<b>M</b>	
MA	Maintenance Association
MAC	Medium Access Control
MD	Maintenance Domain
MEG	Maintenance Entity Group
MEP	Maintenance associations End Point
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MIP	Maintenance association Intermediate Point
MoCA	Multimedia over Coax Alliance
MP	Maintenance Point
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transferred Unit
MVR	Multicast VLAN Registration
MPCP	Multi-Point Control Protocol
<b>N</b>	
NAT	Network Address Translation
NMS	Network Management System
NNI	Network Node Interface
NView NNM	NView Network Node Management
NTP	Network Time Protocol
<b>O</b>	
OAM	Operation, Administration and Management
ODF	Optical Distribution Frame
ODN	Optical Distribution Network
OFDM	Orthogonal Frequency Division Multiplexing

OLT	Optical Line Terminal
ONU	Optical Network Unit
OSI	Open System Interconnect
OSPF	Open Shortest Path First

## **P**

P2P	Peer-to-Peer
P2MP	Point to Multipoint
PC	Personal Computer
PE	Provider Edge
PIB	Parameter Information Block
PIR	Peak Information Rate
PMD	Physical Medium Dependent
PoE	Power Over Ethernet
PPP	Point to Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PTP	Precision Time Protocol

## **Q**

QoS	Quality of Service
-----	--------------------

## **R**

RADIUS	Remote Authentication Dial In User Service
RED	Random Early Detection
RF	Radio Frequency
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
RMEP	Remote Maintenance association End Point
RNC	Radio Network Controller
RSTP	Rapid Spanning Tree Protocol

## **S**

SAToP	Structure-Agnostic Time Division Multiplexing (TDM) over Packet
-------	---



SFP	Small Form-factor Pluggables
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
SST	Single Spanning Tree
STP	Spanning Tree Protocol
<b>T</b>	
TACACS+	Terminal Access Controller Access Control System
TC	Transparent Clock
TCI	Tag Control Information
TCP	Transmission Control Protocol
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access
TDM	Time Division Multiplex
TDMA	Time Division Multiple Address
TDMoIP	Time Division Multiplexing over IP
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service
TPID	Tag Protocol Identifier
<b>U</b>	
URI	Uniform Resource Identifier
<b>V</b>	
VLAN	Virtual Local Area Network
VID	VLAN Identifier
VoIP	Voice over Internet Protocol
<b>W</b>	

WCDMA	Wideband Code Division Multiple Access
WDM	Wavelength Division Multiplexing
WiFi	Wireless Fidelity
WRED	Weighted Random Early Detection
WRR	Weight Round Robin

