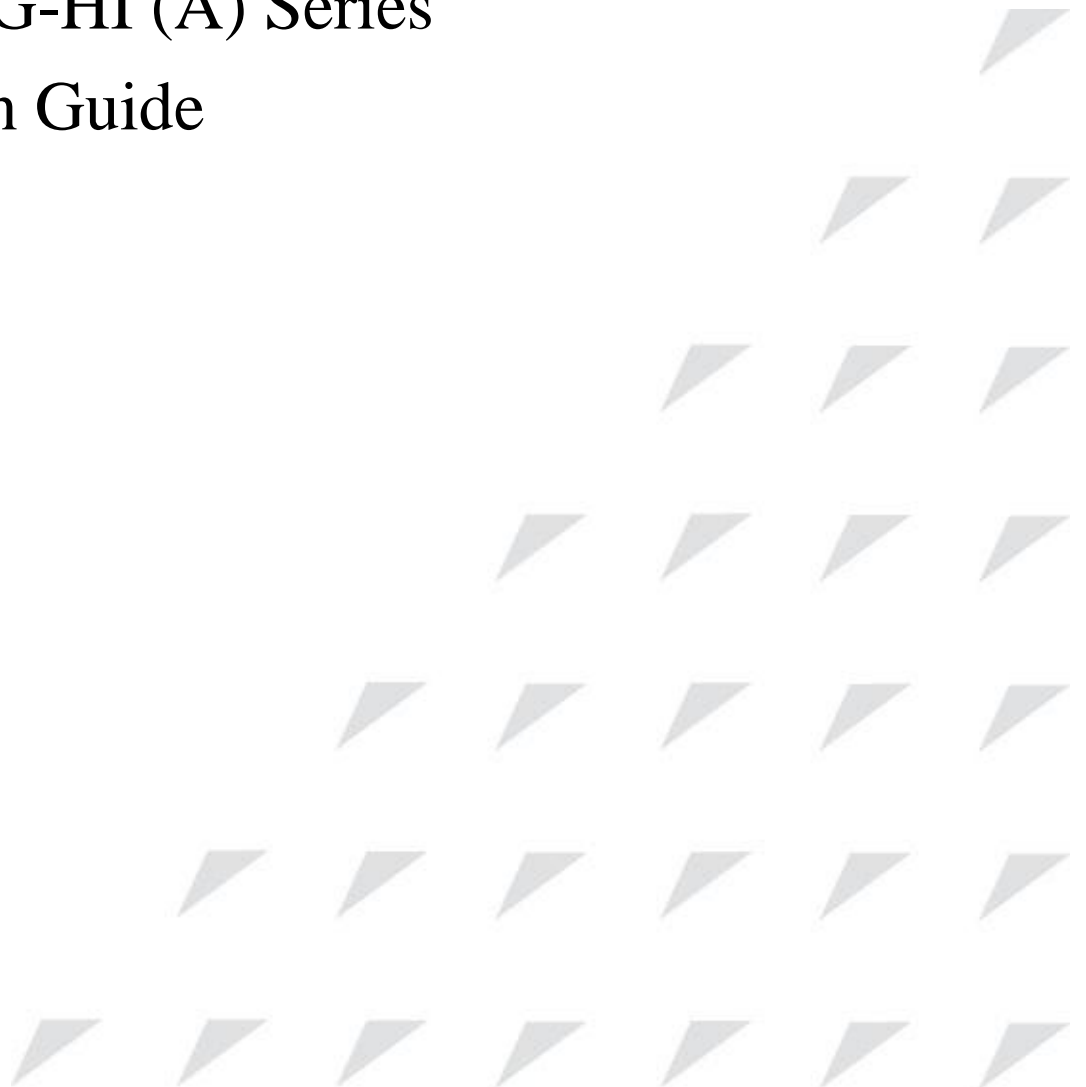


[www.raisecom.com](http://www.raisecom.com)

# ISCOM2600G-HI (A) Series Configuration Guide (Rel\_01)



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 ©2018

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 describes features supported by the ISCOM2600G-HI series switch, and related configurations, including basic configurations, basic principles and configuration procedures of Ethernet, ring network protection, reliability, security, and QoS, and related configuration examples.

The appendix lists terms, acronyms, and abbreviations involved in this document.

By reading this document, you can master principles and configurations of the ISCOM2600G-HI series switch, and how to network with the ISCOM2600G-HI series switch.

## Versions



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



Product name	Software version	Hardware version
ISCOM2600G-HI series switch	V3.50	A

## Conventions

### Symbol conventions

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

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.

Symbol	Description
 <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>	Buttons and navigation path are in <b>Boldface</b> .
<i>Italic</i>	Book titles are in <i>italics</i> .
<b>Lucida Console</b>	Terminal display is in <b>Lucida Console</b> .
Book Antiqua	Heading 1, Heading 2, Heading 3, and Block are in Book Antiqua.

## 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. 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   ... ] *	The parameter before the & sign can be repeated 1 to n times.

## Change history

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

### Issue 01 (2018-05-14)

Initial commercial release

---

# Contents

---

<b>1 Basic configurations .....</b>	<b>1</b>
1.1 CLI .....	1
1.1.1 Introduction.....	1
1.1.2 Privileges .....	2
1.1.3 Modes.....	2
1.1.4 Shortcut keys.....	4
1.1.5 Acquiring help.....	6
1.1.6 Display information .....	8
1.1.7 Command history .....	9
1.1.8 Restoring default value of command line .....	9
1.1.9 Logging commands.....	10
1.2 Accessing device .....	10
1.2.1 Introduction.....	10
1.2.2 Accessing through Console interface .....	11
1.2.3 Accessing through Telnet .....	12
1.2.4 Accessing through SSH.....	14
1.2.5 Managing users .....	16
1.2.6 Configuring HTTP Server.....	18
1.2.7 Checking configurations .....	18
1.2.8 Example for configuring user management .....	18
1.3 File management .....	20
1.3.1 Managing BootROM files.....	20
1.3.2 Managing system files .....	21
1.3.3 Managing configuration files .....	21
1.3.4 Checking configurations .....	23
1.3.5 Maintenance.....	23
1.4 Loading and upgrade.....	24
1.4.1 Introduction.....	24
1.4.2 Upgrading system software through BootROM.....	24
1.4.3 Upgrading system software through CLI.....	26
1.4.4 Checking configurations .....	27
1.5 Automatically updating version and configurations .....	27

1.5.1 Introduction.....	27
1.5.2 Preparing for configurations .....	27
1.5.3 Automatically updating version and configurations.....	28
1.5.4 Checking configurations .....	28
1.5.5 Maintenance .....	29
1.6 Time management .....	29
1.6.1 Introduction.....	29
1.6.2 Preparing for configurations .....	32
1.6.3 Default configurations of time management .....	32
1.6.4 Configuring time and time zone.....	34
1.6.5 Configuring DST .....	34
1.6.6 Configuring NTP .....	34
1.6.7 Configuring SNTP .....	36
1.6.8 Checking configurations .....	36
1.6.9 Example for configuring NTP.....	36
1.7 Interface management .....	39
1.7.1 Introduction.....	39
1.7.2 Default configurations of interface management .....	40
1.7.3 Configuring basic attributes of interfaces .....	40
1.7.4 Configuring interface rate statistics .....	41
1.7.5 Configuring flow control on interfaces .....	42
1.7.6 Shutting down/Restarting interface .....	42
1.7.7 Configuring Console interface .....	42
1.7.8 Configuring SNMP interface .....	43
1.7.9 Checking configurations .....	44
1.8 Configuring basic information .....	44
1.9 Task scheduling .....	45
1.9.1 Introduction.....	45
1.9.2 Configuring task scheduling .....	45
1.9.3 Checking configurations .....	46
1.10 Watchdog.....	46
1.10.1 Introduction.....	46
1.10.2 Preparing for configurations .....	47
1.10.3 Default configurations of Watchdog .....	47
1.10.4 Configuring Watchdog .....	47
1.10.5 Checking configurations .....	47
1.11 Configuring Banner.....	47
1.11.1 Preparing for configurations.....	47
1.11.2 Configuring Banner.....	48
1.11.3 Enabling Banner display .....	48
1.11.4 Checking configurations .....	49

<b>2 Ethernet .....</b>	<b>50</b>
2.1 MAC address table .....	50
2.1.1 Introduction .....	50
2.1.2 Preparing for configurations .....	52
2.1.3 Default configurations of MAC address table .....	53
2.1.4 Configuring static MAC address .....	53
2.1.5 Configuring blackhole MAC address .....	53
2.1.6 Filtering unknown multicast packets .....	54
2.1.7 Configuring MAC address learning .....	54
2.1.8 Configuring MAC address limit .....	54
2.1.9 Configuring aging time of MAC addresses .....	54
2.1.10 Enabling suppression of MAC address flapping .....	55
2.1.11 Checking configurations .....	55
2.1.12 Maintenance .....	55
2.1.13 Example for configuring MAC address table .....	56
2.2 VLAN .....	57
2.2.1 Introduction .....	57
2.2.2 Preparing for configurations .....	60
2.2.3 Default configurations of VLAN .....	60
2.2.4 Configuring VLAN attributes .....	61
2.2.5 Configuring interface mode .....	61
2.2.6 Configuring VLAN on Access interface .....	61
2.2.7 Configuring VLAN on Trunk interface .....	62
2.2.8 Configuring VLAN based on MAC address .....	63
2.2.9 Configuring VLAN based on IP subnet .....	63
2.2.10 Configuring VLAN based on IP subnet .....	64
2.2.11 Checking configurations .....	64
2.2.12 Example for configuring VLAN .....	65
2.3 PVLAN .....	68
2.3.1 Introduction .....	68
2.3.2 Preparing for configuration .....	68
2.3.3 Default configurations of PVLAN .....	68
2.3.4 Configuring PVLAN type .....	69
2.3.5 Configuring PVLAN association .....	69
2.3.6 Configuring PVLAN mode on interface .....	70
2.3.7 Checking configuration .....	71
2.3.8 Example for configuring PVLAN .....	71
2.4 QinQ .....	75
2.4.1 Introduction .....	75
2.4.2 Preparing for configurations .....	76
2.4.3 Default configurations of QinQ .....	76
2.4.4 Configuring basic QinQ .....	76



2.4.5 Configuring selective QinQ .....	77
2.4.6 Configuring network-side interface to Trunk mode .....	78
2.4.7 Configuring TPID .....	78
2.4.8 Checking configurations .....	79
2.4.9 Example for configuring basic QinQ .....	79
2.4.10 Example for configuring selective QinQ .....	81
2.5 VLAN mapping .....	83
2.5.1 Introduction .....	83
2.5.2 Preparing for configurations .....	83
2.5.3 Default configurations of VLAN mapping .....	84
2.5.4 Configuring VLAN mapping .....	84
2.5.5 Checking configurations .....	84
2.5.6 Example for configuring VLAN mapping .....	85
2.6 STP/RSTP .....	87
2.6.1 Introduction .....	87
2.6.2 Preparation for configuration .....	90
2.6.3 Default configurations of STP .....	90
2.6.4 Enabling STP .....	91
2.6.5 Configuring STP parameters .....	91
2.6.6 Configuring edge interface .....	92
2.6.7 Configuring link type .....	92
2.6.8 Configuring BPDU filtering .....	93
2.6.9 Configuring BPDU Guard .....	93
2.6.10 Configuring MRSTP .....	94
2.6.11 Checking configurations .....	94
2.6.12 Example for configuring STP .....	95
2.7 MSTP .....	97
2.7.1 Introduction .....	97
2.7.2 Preparation for configuration .....	100
2.7.3 Default configurations of MSTP .....	100
2.7.4 Enabling MSTP .....	101
2.7.5 Configuring MST region and its maximum number of hops .....	101
2.7.6 Configuring root/backup bridge .....	102
2.7.7 Configuring interface priority and system priority .....	103
2.7.8 Configuring network diameter for switch network .....	104
2.7.9 Configuring internal path cost of interface .....	104
2.7.10 Configuring external path cost of interface .....	105
2.7.11 Configuring maximum transmission rate on interface .....	105
2.7.12 Configuring MSTP timer .....	106
2.7.13 Configuring edge interface .....	106
2.7.14 Configuring BPDU filtering .....	107
2.7.15 Configuring BPDU Guard .....	107

2.7.16 Configuring STP/RSTP/MSTP mode switching .....	108
2.7.17 Configuring link type .....	109
2.7.18 Configuring root interface protection.....	109
2.7.19 Configuring interface loopguard .....	110
2.7.20 Configuring TC packet suppression.....	110
2.7.21 Checking configurations .....	111
2.7.22 Maintenance .....	111
2.7.23 Example for configuring MSTP .....	111
2.8 MRSTP.....	116
2.8.1 Introduction.....	116
2.8.2 Preparing for configurations .....	116
2.8.3 Default configurations of MRSTP .....	117
2.8.4 Enabling MRSTP .....	117
2.8.5 Configuring MRSTP parameters.....	117
2.8.6 Checking configurations .....	118
2.9 Loop detection.....	118
2.9.1 Introduction.....	118
2.9.2 Preparing for configurations .....	120
2.9.3 Default configurations of loop detection.....	120
2.9.4 Configuring loop detection .....	121
2.9.5 Checking configurations .....	122
2.9.6 Maintenance .....	122
2.9.7 Example for configuring inner loop detection .....	122
2.10 Interface protection .....	124
2.10.1 Introduction.....	124
2.10.2 Preparing for configurations .....	124
2.10.3 Default configurations of interface protection .....	124
2.10.4 Configuring interface protection .....	125
2.10.5 Configuring interface isolation .....	125
2.10.6 Checking configurations .....	125
2.10.7 Example for configuring interface protection .....	126
2.11 Port mirroring .....	127
2.11.1 Introduction.....	127
2.11.2 Preparing for configurations.....	128
2.11.3 Default configurations of port mirroring .....	128
2.11.4 Configuring port mirroring on local port .....	128
2.11.5 Checking configurations .....	129
2.11.6 Example for configuring port mirroring.....	129
2.12 L2CP .....	131
2.12.1 Introduction.....	131
2.12.2 Preparing for configurations .....	131
2.12.3 Default configurations of L2CP .....	131

2.12.4 Configuring global L2CP .....	131
2.12.5 Configuring L2CP profile .....	132
2.12.6 Configuring L2CP profile on interface .....	132
2.12.7 Checking configurations .....	133
2.12.8 Maintenance .....	133
2.12.9 Example for configuring L2CP .....	133
2.13 Voice VLAN .....	136
2.13.1 Introduction .....	136
2.13.2 Preparing for configurations .....	138
2.13.3 Default configurations of voice VLAN .....	138
2.13.4 Configuring QoS of voice VLAN .....	139
2.13.5 Enabling voice VLAN .....	139
2.13.6 Configuring OUI address .....	140
2.13.7 Checking configurations .....	140
2.13.8 Example for adding interface to voice VLAN and configuring it to work in manual mode .....	141
2.13.9 Example for configuring IP phone to access voice VLAN packets through LLDP .....	142
2.14 GARP .....	144
2.14.1 Introduction .....	144
2.14.2 Preparing for configurations .....	146
2.14.3 Default configurations of GARP .....	147
2.14.4 Configuring basic functions of GARP .....	147
2.14.5 Configuring GVRP .....	148
2.14.6 Checking configurations .....	148
2.14.7 Example for configuring GVRP .....	149
<b>3 ISF .....</b>	<b>152</b>
3.1 Introduction .....	152
3.1.1 ISF advantages .....	152
3.1.2 ISF application .....	153
3.2 ISF concepts .....	153
3.2.2 Principles of ISF .....	156
3.2.3 ISF merge and split .....	159
3.2.4 ISF management and maintenance .....	160
3.2.5 MAD .....	161
3.3 Establishing ISF environment .....	161
3.3.1 Establishment flow .....	161
3.3.2 Planning number of ISF members .....	162
3.3.3 Planning roles and IDs of ISF members .....	163
3.3.4 Planning ISF topology .....	163
3.3.5 Planning ISF physical interfaces .....	163
3.3.6 Installing ISF members .....	163
3.3.7 Connecting ISF cables .....	163

3.3.8 Configuring ISF system software.....	163
3.4 Configuring ISF .....	164
3.4.1 Preparing for configurations .....	164
3.4.2 Default configurations of ISF.....	164
3.4.3 Preconfiguration mode .....	164
3.4.4 Non-preconfiguration mode .....	165
3.5 Preconfiguring ISF in standalone mode .....	165
3.5.1 Configuring ISF interface .....	166
3.5.2 Configuring member priority .....	166
3.5.3 Configuring ISF mode .....	167
3.6 Configuring ISF in ISF mode .....	167
3.6.1 Configuring ISF mode .....	167
3.6.2 Configuring ISF domain ID .....	167
3.6.3 Configuring ISF interface .....	168
3.6.4 Configuring member ID.....	169
3.6.5 Configuring member priority .....	170
3.6.6 Configuring reservation time for ISF bridge MAC address .....	170
3.6.7 Configuring MAC address synchronization.....	171
3.6.8 Enabling automatic device restart upon ISF merge.....	171
3.6.9 Configuring MAD.....	172
3.7 Checking configurations .....	177
3.8 Configuration examples .....	178
3.8.1 Example for configuring ISF in preconfiguration mode with BFD MAD .....	178
3.8.2 Example for configuring ISF in non-preconfiguration mode with BFD MAD.....	181
3.8.3 Example for switching member device from ISF mode to standalone mode .....	184
3.8.4 Example for configuring four devices to form ISF .....	186
<b>4 Ring network protection.....</b>	<b>192</b>
4.1 G.8032.....	192
4.1.1 Introduction.....	192
4.1.2 Preparing for configurations .....	192
4.1.3 Default configurations of G.8032 .....	193
4.1.4 Creating G.8032 ring.....	193
4.1.5 Configuring ERPS fault detection mode.....	195
4.1.6 (Optional) creating G.8032 tributary ring .....	196
4.1.7 (Optional) configuring G.8032 switching control .....	198
4.1.8 Checking configurations .....	198
4.1.9 Maintenance .....	199
4.2 ELPS (G.8031).....	199
4.2.1 Introduction.....	199
4.2.2 Preparing for configurations .....	199
4.2.3 Default configurations of ELPS .....	200

4.2.4 Creating ELPS pair .....	200
4.2.5 Configuring ELPS fault detection mode .....	202
4.2.6 (Optional) configuring ELPS control .....	202
4.2.7 Checking configurations .....	203
4.2.8 Maintenance .....	203
4.2.9 Example for configuring 1:1 ELPS protection .....	204
<b>5 IP services .....</b>	<b>207</b>
5.1 IP basis .....	207
5.1.1 Introduction .....	207
5.1.2 Preparing for configurations .....	207
5.1.3 Default configurations of Layer 3 interface .....	207
5.1.4 Configuring IPv4 address of VLAN interface .....	208
5.1.5 Configuring IPv6 address of VLAN interface .....	208
5.1.6 Configuring attributes of management VLAN .....	208
5.1.7 Checking configurations .....	209
5.1.8 Example for configuring VLAN interface to interconnect with host .....	209
5.2 Loopback interface .....	211
5.2.1 Introduction .....	211
5.2.2 Preparing for configurations .....	211
5.2.3 Default configurations of loopback interface .....	211
5.2.4 Configuring IP address of loopback interface .....	211
5.2.5 Configuring interface loopback .....	212
5.2.6 Checking configurations .....	212
5.3 ARP .....	212
5.3.1 Introduction .....	212
5.3.2 Preparing for configurations .....	213
5.3.3 Default configurations of ARP .....	213
5.3.4 Configuring static ARP entries .....	214
5.3.5 Configuring dynamic ARP entries .....	214
5.3.1 Configuring proxy ARP .....	214
5.3.2 Checking configurations .....	215
5.3.3 Maintenance .....	215
5.3.4 Example for configuring ARP .....	215
5.4 NDP .....	217
5.4.1 Introduction .....	217
5.4.2 Preparing for configurations .....	217
5.4.3 Default configurations of NDP .....	218
5.4.4 Configuring static neighbor entries .....	218
5.4.5 Configuring times of sending NS messages for detecting duplicated addresses .....	218
5.4.6 Configuring maximum number of NDPs allowed to be learnt on Layer 3 interface .....	219
5.4.7 Checking configurations .....	219

5.4.8 Maintenance .....	219
5.5 Static route .....	220
5.5.1 Introduction.....	220
5.5.2 Preparing for configurations .....	220
5.5.3 Configuring static route .....	220
5.5.4 Configuring route mangement .....	221
5.5.5 Checking configurations .....	221
5.5.6 Example for configuring static route.....	222
5.6 RIP .....	224
5.6.1 Introduction.....	224
5.6.2 Configuring basic RIP functions .....	226
5.6.3 Configuring RIP version .....	226
5.6.4 Redistributing external routes .....	227
5.6.5 Configuring RIP timer.....	228
5.6.6 Configuring loop suppression .....	228
5.6.7 Configuring authentication .....	229
5.6.8 Configuring routing policy.....	229
5.6.9 Configuring route calculation .....	230
5.6.10 Checking configurations .....	230
5.6.11 Maintenance .....	231
5.7 OSPFv2 .....	231
5.7.1 Introduction.....	231
5.7.2 Configuring basic functions of OSPF .....	236
5.7.3 Configuring OSPF route attributes.....	237
5.7.4 Configuring load balancing.....	239
5.7.5 Configuring OSPF network .....	239
5.7.6 Optimizing OSPF network.....	240
5.7.7 Configuring OSPF authentication mode .....	243
5.7.8 Configuring Stub area .....	244
5.7.9 Controlling OSPF routing information .....	244
5.7.10 Configuring OSPF routing policy .....	246
5.7.11 Checking configurations .....	249
5.7.12 Maintenance .....	250
<b>6 DHCP.....</b>	<b>251</b>
6.1 DHCP Client .....	251
6.1.1 Introduction.....	251
6.1.2 Preparing for configurations .....	254
6.1.3 Default configurations of DHCP Client .....	254
6.1.4 Configuring DHCP Client.....	255
6.1.5 Configuring DHCPv6 Client.....	255
6.1.6 Checking configurations .....	256

6.1.7 Example for configuring DHCP Client .....	256
6.2 Zero-configuration .....	258
6.2.1 Introduction.....	258
6.2.2 Default configurations of zero-configuration.....	259
6.2.3 Preparing for configuration.....	259
6.2.4 Configuring DHCP Client.....	260
6.2.5 (Optional) configuring zero-configuration polling.....	260
6.2.6 Checking configurations .....	260
6.2.7 Example for IPv6 zero-configuration.....	261
6.3 DHCP Snooping .....	265
6.3.1 Introduction.....	265
6.3.2 Preparing for configurations .....	266
6.3.3 Default configurations of DHCP Snooping.....	266
6.3.4 Configuring DHCP Snooping .....	266
6.3.5 Configure DHCP Snooping to support Option 82.....	267
6.3.6 Configuring DHCPv6 Snooping .....	268
6.3.7 Checking configurations .....	268
6.3.8 Example for configuring DHCP Snooping.....	269
6.4 DHCP Options.....	270
6.4.1 Introduction.....	270
6.4.2 Preparing for configurations .....	272
6.4.3 Default configurations of DHCP Option.....	272
6.4.4 Configuring DHCP Option fields.....	272
6.4.5 Configuring DHCP Option 18 over IPv6.....	273
6.4.6 Configuring DHCP Option 37 over IPv6.....	274
6.4.7 Configuring user-defined DHCP Option over IPv6 .....	274
6.4.8 Checking configurations .....	275
6.5 DHCP Server.....	275
6.5.1 Introduction.....	275
6.5.2 Preparing for configurations .....	278
6.5.3 Creating and configuring IPv4 address pool .....	278
6.5.4 Enabling DHCPv4 Server on VLAN interface .....	279
6.5.5 Enabling DHCP Server on VLAN interface .....	279
6.5.6 Configuring DHCP Server to support Option 82 .....	279
6.5.7 Checking configurations .....	279
6.5.8 Example for configuring DHCPv4 Server .....	280
6.6 DHCP Relay .....	281
6.6.1 Introduction.....	281
6.6.2 Preparing for configurations .....	282
6.6.3 Default configurations of DHCP Relay.....	282
6.6.4 Configuring global DHCP Relay .....	283
6.6.5 Configuring DHCP Relay on VLAN interface .....	283

6.6.6 Configuring global DHCPv6 Relay .....	283
6.6.7 Configuring DHCPv6 Relay on VLAN interface .....	284
6.6.8 (Optional) configuring DHCP Relay to support Option 82 .....	284
6.6.9 Checking configurations .....	284
6.6.10 Example for configuring DHCPv4 Relay .....	285
<b>7 QoS.....</b>	<b>287</b>
7.1 Introduction .....	287
7.1.1 Service model.....	287
7.1.2 Priority trust .....	288
7.1.3 Traffic classification.....	288
7.1.4 Traffic policy.....	290
7.1.5 Priority mapping .....	291
7.1.6 Queue scheduling.....	291
7.1.7 Congestion avoidance .....	293
7.1.8 Rate limiting based on interface and VLAN .....	294
7.1.9 QoS enhancement .....	294
7.2 Configuring priority .....	295
7.2.1 Preparing for configurations .....	295
7.2.2 Default configurations of basic QoS .....	295
7.2.3 Configuring types of priorities trusted by interface .....	296
7.2.4 Configuring mapping from CoS to local priority .....	296
7.2.5 Configuring mapping from DSCP to local priority and color .....	297
7.2.6 Configuring DSCP mutation .....	297
7.2.7 Configuring CoS remarking .....	298
7.2.8 Checking configurations .....	298
7.3 Configuring congestion management.....	299
7.3.1 Preparing for configurations .....	299
7.3.2 Default configurations of congestion management.....	299
7.3.3 Configuring SP queue scheduling .....	299
7.3.4 Configuring WRR or SP+WRR queue scheduling .....	300
7.3.5 Configuring DRR or SP+DRR queue scheduling .....	300
7.3.6 Configuring queue bandwidth guarantee .....	300
7.3.7 Checking configurations .....	301
7.4 Configuring congestion avoidance.....	301
7.4.1 Preparing for configurations .....	301
7.4.2 Default configurations of congestion avoidance .....	301
7.4.3 Configuring SRED .....	302
7.4.4 Checking configurations .....	302
7.5 Configuring traffic classification and traffic policy .....	302
7.5.1 Preparing for configurations .....	302
7.5.2 Default configurations of traffic classification and traffic policy .....	303



7.5.3 Creating traffic class .....	303
7.5.4 Configuring traffic classification rules .....	303
7.5.5 Creating rate limiting rule and shapping rule .....	304
7.5.6 Creating traffic policy .....	305
7.5.7 Defining traffic policy mapping .....	305
7.5.8 Defining traffic policy operation .....	306
7.5.9 Applying traffic policy to interfaces .....	307
7.5.10 Checking configurations .....	307
7.5.11 Maintenance .....	308
7.6 Configuring rate limiting .....	308
7.6.1 Preparing for configurations .....	308
7.6.2 Configuring rate limiting based on interface .....	308
7.6.3 Checking configurations .....	309
7.7 Bandwidth rate limiting .....	309
7.7.1 Introduction .....	309
7.7.2 Preparing for configurations .....	310
7.7.3 Default configurations of bandwidth rate limiting .....	310
7.7.4 Configuring bandwidth guarantee .....	311
7.7.5 Configuring hierarchical bandwidth guarantee .....	312
7.7.6 Checking configurations .....	313
7.8 Configuration examples .....	314
7.8.1 Example for configuring congestion management .....	314
7.8.2 Example for configuring rate limiting based on traffic policy .....	316
7.8.3 Example for configuring rate limiting based on interface .....	319
<b>8 Multicast .....</b>	<b>321</b>
8.1 Multicast .....	321
8.2 Basic functions of Layer 2 multicast .....	326
8.2.1 Introduction .....	326
8.2.2 Preparing for configurations .....	328
8.2.3 Default configurations of Layer 2 multicast basic functions .....	328
8.2.4 Configuring basic functions of Layer 2 multicast .....	328
8.2.5 Checking configurations .....	329
8.2.6 Maintenance .....	329
8.3 IGMP Snooping .....	330
8.3.1 Introduction .....	330
8.3.2 Preparing for configurations .....	330
8.3.3 Default configurations of IGMP Snooping .....	331
8.3.4 Configuring IGMP Snooping .....	331
8.3.5 Checking configurations .....	331
8.3.6 Example for applying multicast on ring network .....	332
8.4 IGMP Querier .....	335

8.4.1 Introduction.....	335
8.4.2 Preparing for configurations .....	336
8.4.3 Default configurations of IGMP Querier .....	336
8.4.4 Configuring IGMP Querier .....	337
8.4.5 Checking configurations .....	338
8.4.6 Example for configuring IGMP Snooping and IGMP Querier.....	338
8.5 IGMP MVR.....	340
8.5.1 Introduction.....	340
8.5.2 Preparing for configurations .....	340
8.5.3 Default configurations of IGMP MVR .....	341
8.5.4 Configuring IGMP MVR .....	341
8.5.5 Checking configurations .....	342
8.5.6 Example for configuring IGMP MVR .....	343
8.6 IGMP filtering .....	345
8.6.1 Introduction.....	345
8.6.2 Preparing for configurations .....	345
8.6.3 Default configurations of IGMP filtering.....	346
8.6.4 Enabling global IGMP filtering.....	346
8.6.5 Configuring IGMP filtering profile.....	346
8.6.6 Configuring maximum number of multicast groups .....	347
8.6.7 Checking configurations .....	348
8.6.8 Example for applying IGMP filtering on interface .....	348
8.7 Multicast VLAN copy .....	350
8.7.1 Introduction.....	350
8.7.2 Preparing for configurations .....	352
8.7.3 Default configurations of multicast VLAN copy .....	353
8.7.4 Configuring multicast VLAN copy .....	353
8.7.5 Configuring static multicast members of VLAN copy.....	354
8.7.6 Configuring customer VLAN of VLAN copy.....	354
8.7.7 Checking configurations .....	355
8.8 MLD.....	355
8.8.1 Introduction.....	355
8.8.2 Preparing for configurations .....	356
8.8.3 Default configurations of MLD .....	356
8.8.4 Configuring basic functions of MLD .....	356
8.8.5 Configuring MLD Snooping .....	357
8.8.6 Configuring MLD Querier .....	358
8.8.7 Configuring MLD filtering .....	359
8.8.8 Checking configurations .....	360
8.8.9 Maintenance .....	361
<b>9 OAM .....</b>	<b>362</b>

9.1 Introduction .....	362
9.2 EFM .....	364
9.2.1 Introduction.....	364
9.2.2 Preparing for configurations .....	364
9.2.3 Default configurations of EFM .....	364
9.2.4 Configuring basic functions of EFM.....	365
9.2.5 Configuring active functions of EFM .....	366
9.2.6 Configuring EFM passive function.....	367
9.2.7 Checking configurations .....	369
9.2.8 Maintenance .....	370
9.3 CFM (IEEE 802.1ag/ITU-Y.1731).....	370
9.3.1 Introduction.....	370
9.3.2 Preparing for configurations .....	373
9.3.3 Enabling CFM.....	373
9.3.4 Configuring basic functions of CFM .....	374
9.3.5 Configuring CFM fault detection.....	375
9.3.6 Configuring fault acknowledgement.....	377
9.3.7 Configuring CFM fault location.....	378
9.3.8 Configuring alarm indication signal.....	379
9.3.9 Configuring Ethernet locked signal .....	380
9.3.10 Configuring Ethernet CSF .....	381
9.3.11 Configuring performance monitoring .....	381
9.3.12 Checking configurations .....	381
9.3.13 Example for configuring CFM.....	382
9.4 SLA .....	385
9.4.1 Introduction.....	385
9.4.2 Preparing for configurations .....	387
9.4.3 Limits on SLA configuration .....	387
9.4.4 Default configurations of SLA.....	388
9.4.5 Creating SLA operation .....	388
9.4.6 Configuring SLA scheduling .....	389
9.4.7 Configuring SLA threshold.....	389
9.4.8 Configuring maintenance window .....	390
9.4.9 Configuring availability test.....	390
9.4.10 Enabling alarms .....	391
9.4.11 Checking configurations .....	391
9.4.12 Example for configuring SLA.....	392
9.5 BFD.....	393
9.5.1 Introduction.....	393
9.5.2 Preparing for configurations .....	394
9.5.3 Configuring BFD session binding.....	394
9.5.4 Configuring BFD session parameters .....	395

9.5.5 Checking configurations .....	396
<b>10 Security.....</b>	<b>397</b>
10.1 ACL.....	397
10.1.1 Introduction.....	397
10.1.2 Preparing for configurations .....	398
10.1.3 Configuring MAC ACL .....	398
10.1.4 Configuring ACL period .....	401
10.1.5 Configuring filter .....	402
10.1.6 Checking configurations .....	402
10.1.7 Maintenance .....	403
10.2 Port security MAC .....	403
10.2.1 Introduction.....	403
10.2.2 Preparing for configurations .....	404
10.2.3 Default configurations of port security MAC .....	404
10.2.4 Configuring basic functions of port security MAC.....	405
10.2.5 Configuring static secure MAC address.....	406
10.2.6 Configuring dynamic secure MAC address .....	406
10.2.7 Configuring sticky secure MAC address .....	407
10.2.8 Checking configurations .....	408
10.2.9 Maintenance .....	408
10.2.10 Example for configuring port security MAC .....	408
10.3 Dynamic ARP inspection .....	410
10.3.1 Introduction.....	410
10.3.2 Preparing for configurations .....	412
10.3.3 Default configurations of dynamic ARP inspection .....	412
10.3.4 Configuring trusted interfaces of dynamic ARP inspection .....	412
10.3.5 Configuring static binding of dynamic ARP inspection .....	413
10.3.6 Configuring dynamic binding of dynamic ARP inspection.....	413
10.3.7 Configuring protection VLAN of dynamic ARP inspection .....	413
10.3.8 Configuring rate limiting on ARP packets on interface .....	414
10.3.9 Checking configurations .....	414
10.3.10 Example for configuring dynamic ARP inspection.....	414
10.4 RADIUS.....	417
10.4.1 Introduction.....	417
10.4.2 Preparing for configurations .....	418
10.4.3 Default configurations of RADIUS .....	418
10.4.4 Configuring RADIUS authentication.....	418
10.4.5 Configuring RADIUS accounting.....	419
10.4.6 Checking configurations .....	420
10.4.7 Example for configuring RADIUS .....	420
10.5 TACACS+ .....	422

10.5.1 Introduction.....	422
10.5.2 Preparing for configurations .....	422
10.5.3 Default configurations of TACACS+ .....	423
10.5.4 Configuring TACACS+ authorization.....	423
10.5.5 Configuring TACACS+ authentication .....	423
10.5.6 Configuring TACACS+ accounting .....	424
10.5.7 Configuring TACACS+ authorization.....	424
10.5.8 Checking configurations .....	424
10.5.9 Maintenance .....	425
10.5.10 Example for configuring TACACS+.....	425
10.6 Storm control.....	426
10.6.1 Introduction.....	426
10.6.2 Preparing for configurations .....	427
10.6.3 Default configurations of storm control .....	427
10.6.4 Configuring storm control.....	428
10.6.5 Configuring DLF packet forwarding.....	429
10.6.6 Checking configurations .....	429
10.6.7 Example for configuring storm control.....	429
10.7 802.1x.....	431
10.7.1 Introduction.....	431
10.7.2 Preparing for configurations .....	433
10.7.3 Default configurations of 802.1x .....	433
10.7.4 Configuring basic functions of 802.1x.....	434
10.7.5 Configuring 802.1x re-authentication .....	435
10.7.6 Configuring 802.1x timers .....	435
10.7.7 Checking configurations .....	436
10.7.8 Maintenance .....	436
10.7.9 Example for configuring 802.1x .....	437
10.8 IP Source Guard .....	438
10.8.1 Introduction.....	438
10.8.2 Preparing for configurations .....	440
10.8.3 Default configurations of IP Source Guard .....	440
10.8.4 Configuring interface trust status of IP Source Guard .....	440
10.8.5 Configuring IP Source Guard binding.....	441
10.8.6 Configuring priority and rate limit of IP source guard .....	442
10.8.7 Checking configurations .....	442
10.8.8 Example for configuring IP Source Guard .....	442
10.9 PPPoE+ .....	444
10.9.1 Introduction.....	444
10.9.2 Preparing for configurations .....	445
10.9.3 Default configurations of PPPoE+ .....	446
10.9.4 Configuring basic functions of PPPoE+ .....	446

10.9.5 Configuring PPPoE+ packet information.....	447
10.9.6 Checking configurations .....	449
10.9.7 Maintenance .....	449
10.9.8 Example for configuring PPPoE+ .....	450
10.10 Configuring CPU protection .....	452
10.10.1 Preparing for configurations .....	452
10.10.2 Configuring global CPU CAR .....	452
10.10.3 Checking configurations .....	452
10.10.4 Maintenance .....	453
10.11 Configuring anti-ARP attack .....	453
10.11.1 Preparing for configurations.....	453
10.11.2 Configuring ARP.....	453
10.11.3 Checking configurations .....	454
<b>11 Reliability .....</b>	<b>455</b>
11.1 Link aggregation.....	455
11.1.1 Introduction .....	455
11.1.2 Preparing for configurations.....	457
11.1.3 Configuring manual link aggregation.....	457
11.1.4 Configuring static LACP link aggregation .....	458
11.1.5 Configuring manual master/slave link aggregation .....	459
11.1.6 Checking configurations .....	460
11.1.7 Example for configuring static LACP link aggregation .....	461
11.2 Interface backup .....	463
11.2.1 Introduction .....	463
11.2.2 Preparing for configurations.....	465
11.2.3 Default configurations of interface backup .....	465
11.2.4 Configuring basic functions of interface backup.....	465
11.2.5 (Optional) configuring FS on interfaces.....	466
11.2.6 Checking configurations .....	467
11.2.7 Example for configuring interface backup .....	467
11.3 Link-state tracking.....	470
11.3.1 Introduction .....	470
11.3.2 Preparing for configurations.....	470
11.3.3 Default configurations of link-state tracking.....	470
11.3.4 Configuring link-state tracking .....	470
11.3.5 Checking configurations .....	471
11.3.6 Example for configuring link-state tracking.....	472
11.4 UDLD.....	474
11.4.1 Introduction .....	474
11.4.2 Preparing for configurations.....	474
11.4.3 Default configurations of UDLD .....	474

11.4.4 Configuring UDLD .....	474
11.4.5 Checking configurations .....	474
11.5 mLACP.....	475
11.5.1 Introduction.....	475
11.5.2 Preparing for configurations.....	476
11.5.3 Configuring ICCP channel .....	476
11.5.4 Configuring mLACP link aggregation .....	477
11.5.5 Checking configurations .....	477
11.5.6 Maintenance .....	478
11.5.7 Example for configuring mLACP .....	478
<b>12 System management.....</b>	<b>483</b>
12.1 SNMP.....	483
12.1.1 Introduction.....	483
12.1.2 Preparing for configurations .....	485
12.1.3 Default configurations of SNMP .....	485
12.1.4 Configuring basic functions of SNMPv1/SNMPv2c .....	486
12.1.5 Configuring basic functions of SNMPv3 .....	487
12.1.6 Configuring IP address authentication by SNMP server .....	488
12.1.7 Configuring other information about SNMP .....	488
12.1.8 Configuring Trap.....	489
12.1.9 Checking configurations .....	490
12.1.10 Example for configuring SNMPv1/SNMPv2c and Trap.....	490
12.1.11 Example for configuring SNMPv3 and Trap.....	492
12.2 RMON.....	494
12.2.1 Introduction.....	494
12.2.2 Preparing for configurations .....	496
12.2.3 Default configurations of RMON .....	496
12.2.4 Configuring RMON statistics .....	496
12.2.5 Configuring RMON historical statistics.....	497
12.2.6 Configuring RMON alarm group.....	497
12.2.7 Configuring RMON event group .....	498
12.2.8 Checking configurations .....	498
12.2.9 Maintenance .....	498
12.2.10 Example for configuring RMON alarm group.....	499
12.3 LLDP.....	500
12.3.1 Introduction.....	500
12.3.2 Preparing for configurations .....	503
12.3.3 Default configurations of LLDP .....	503
12.3.4 Enabling global LLDP .....	503
12.3.5 Enabling interface LLDP .....	504
12.3.6 Configuring basic functions of LLDP .....	504

12.3.7 Configuring LLDP alarm .....	505
12.3.8 Configuring TLV .....	505
12.3.9 Checking configurations .....	505
12.3.10 Maintenance .....	506
12.3.11 Example for configuring LLDP .....	506
12.4 Optical module DDM .....	509
12.4.1 Introduction .....	509
12.4.2 Preparing for configurations .....	510
12.4.3 Default configurations of optical module DDM .....	510
12.4.4 Enabling optical module DDM .....	510
12.4.5 Enabling optical module DDM Trap .....	511
12.4.6 Checking configurations .....	511
12.5 System log .....	512
12.5.1 Introduction .....	512
12.5.2 Preparing for configurations .....	513
12.5.3 Default configurations of system log .....	513
12.5.4 Configuring basic information of system log .....	514
12.5.5 Configuring system log output .....	514
12.5.6 Checking configurations .....	516
12.5.7 Maintenance .....	516
12.5.8 Example for configuring outputting system logs to log host .....	516
12.6 Alarm management .....	518
12.6.1 Introduction .....	518
12.6.2 Preparing for configurations .....	522
12.6.3 Configuring basic functions of alarm management .....	522
12.6.4 Checking configurations .....	524
12.7 Hardware environment monitoring .....	524
12.7.1 Introduction .....	524
12.7.2 Preparing for configurations .....	527
12.7.3 Default configurations of hardware environment monitoring .....	527
12.7.4 Enabling global hardware environment monitoring .....	527
12.7.5 Configuring temperature monitoring alarm .....	528
12.7.6 Configuring power supply alarm .....	528
12.7.7 Clearing all hardware environment monitoring alarms manually .....	528
12.7.8 Checking configurations .....	529
12.8 CPU monitoring .....	529
12.8.1 Introduction .....	529
12.8.2 Preparing for configurations .....	530
12.8.3 Default configurations of CPU monitoring .....	530
12.8.4 Showing CPU monitoring information .....	530
12.8.5 Configuring CPU monitoring alarm .....	531
12.8.6 Checking configurations .....	531



12.9 Cable diagnosis .....	531
12.9.1 Introduction.....	531
12.9.2 Preparing for configurations .....	532
12.9.3 Configuring cable diagnosis.....	532
12.9.4 Checking configurations .....	532
12.10 Memory monitoring .....	533
12.10.1 Preparing for configurations .....	533
12.10.2 Configuring memory monitoring .....	533
12.10.3 Checking configurations .....	533
12.11 Ping .....	534
12.11.1 Introduction .....	534
12.11.2 Configuring Ping .....	534
12.12 Traceroute.....	535
12.12.1 Introduction.....	535
12.12.2 Configuring Traceroute .....	535
12.13 Performance statistics.....	536
12.13.1 Introduction.....	536
12.13.2 Preparing for configurations .....	536
12.13.3 Default configurations of performance statistics.....	536
12.13.4 Configuring performance statistics .....	536
12.13.5 Checking configurations .....	537
12.13.6 Maintenance .....	537
<b>13 Appendix .....</b>	<b>538</b>
13.1 Terms .....	538
13.2 Acronyms and abbreviations .....	543

# Figures

Figure 1-1 Accessing device through PC connected with RJ45 Console interface .....	11
Figure 1-2 Configuring communication parameters in Hyper Terminal .....	12
Figure 1-3 Networking with device as Telnet server .....	13
Figure 1-4 Networking with device as Telnet client .....	14
Figure 1-5 User management networking .....	19
Figure 1-6 Basic principles of NTP .....	31
Figure 1-7 NTP networking .....	37
Figure 2-1 Forwarding packets according to the MAC address table .....	51
Figure 2-2 MAC networking .....	56
Figure 2-3 VLAN partitions .....	58
Figure 2-4 VLAN and interface protection networking .....	65
Figure 2-5 Networking with PVLAN .....	72
Figure 2-6 Principles of basic QinQ .....	75
Figure 2-7 Basic QinQ networking .....	80
Figure 2-8 Selective QinQ networking .....	81
Figure 2-9 Principles of VLAN mapping .....	83
Figure 2-10 VLAN mapping networking .....	85
Figure 2-11 Network storm due to loopback .....	88
Figure 2-12 Loop networking with STP .....	89
Figure 2-13 Failure in forwarding VLAN packets due to RSTP .....	90
Figure 2-14 STP networking .....	95
Figure 2-15 Basic concepts of the MSTI network .....	98
Figure 2-16 MSTI concepts .....	99
Figure 2-17 Networking with multiple spanning trees instances in MST region .....	100
Figure 2-18 MSTP networking .....	112
Figure 2-19 Configuring MRSTP for specifying root bridge .....	116

Figure 2-20 Loop detection networking .....	119
Figure 2-21 Loop detection networking .....	123
Figure 2-22 Interface protection networking.....	126
Figure 2-23 Principles of port mirroring .....	127
Figure 2-24 Port mirroring networking .....	130
Figure 2-25 L2CP networking.....	134
Figure 2-26 Networking for IP phone to connect to switch .....	137
Figure 2-27 Networking for IP phone to connect PC to the switch.....	138
Figure 2-28 Networking with adding interface to voice VLAN and configuring it to work in manual mode ...	141
Figure 2-29 Configuring IP phone to access voice VLAN packets through LLDP.....	143
Figure 2-30 Principles of GVRP .....	146
Figure 2-31 GVRP networking .....	149
Figure 3-1 ISF networking .....	153
Figure 3-2 ISF visualization .....	154
Figure 3-3 ISF merge .....	155
Figure 3-4 ISF split .....	156
Figure 3-5 Chain networking .....	157
Figure 3-6 Ring networking .....	157
Figure 3-7 ISF relay networking .....	158
Figure 3-8 Flow for establishing the ISF environment.....	162
Figure 3-9 Multi-ISF-domain networking.....	168
Figure 3-10 BFD MAD networking (without intermediate device) .....	173
Figure 3-11 BFD MAD networking (with intermediate device) .....	174
Figure 3-12 Clearing MAD fault (clearing ISF link fault) .....	176
Figure 3-13 Clearing MAD fault (ISF link fault and Active ISF fault) .....	177
Figure 3-14 ISF networking (BFD MAD mode).....	179
Figure 3-15 ISF networking with member device changing from ISF mode to standalone mode .....	182
Figure 3-16 ISF networking (BFD MAD mode).....	185
Figure 3-17 Networking topology before configuring ISF .....	187
Figure 3-18 Networking topology after adding Switch A to ISF.....	188
Figure 4-1 1:1 ELPS networking.....	204
Figure 5-1 VLAN interface networking .....	209
Figure 5-2 Configuring ARP networking .....	216

Figure 5-3 Principles of NDP address resolution .....	217
Figure 5-4 Configuring static route .....	222
Figure 5-5 Roles of broadcast interface .....	233
Figure 5-6 OSPF area and router type .....	235
Figure 6-1 DHCP typical networking .....	252
Figure 6-2 Structure of DHCP packet .....	252
Figure 6-3 DHCP Client networking .....	254
Figure 6-4 DHCP Client networking .....	257
Figure 6-5 Zero-configuration server networking .....	259
Figure 6-6 Zero-configuration networking .....	261
Figure 6-7 Configuring DHCPv6 address pool and prefix .....	263
Figure 6-8 Automatically obtaining files through zero-configuration .....	264
Figure 6-9 DHCP Snooping .....	265
Figure 6-10 DHCP Snooping networking .....	269
Figure 6-11 DHCP Server and Client networking .....	276
Figure 6-12 Structure of a DHCP packet .....	276
Figure 6-13 DHCP Server networking .....	280
Figure 6-14 Typical application of DHCP Relay .....	282
Figure 6-15 DHCP Relay networking .....	285
Figure 7-1 Traffic classification .....	289
Figure 7-2 Structure of an IP packet header .....	289
Figure 7-3 Structures of the ToS priority and DSCP .....	289
Figure 7-4 Structure of a VLAN packet .....	289
Figure 7-5 Structure of CoS .....	290
Figure 7-6 SP scheduling .....	292
Figure 7-7 WRR scheduling .....	292
Figure 7-8 DRR scheduling .....	293
Figure 7-9 Queue scheduling networking .....	314
Figure 7-10 Rate limiting based on traffic policy .....	316
Figure 7-11 Rate limiting based on interface .....	319
Figure 8-1 Multicast transmission networking .....	322
Figure 8-2 Basic concepts in multicast .....	324
Figure 8-3 Mapping between IPv4 multicast address and multicast MAC address .....	325

Figure 8-4 Operating of IGMP and Layer 2 multicast features .....	325
Figure 8-5 IGMP Snooping networking.....	330
Figure 8-6 Ring network multicast networking.....	333
Figure 8-7 IGMP Snooping networking.....	338
Figure 8-8 IGMP MVR networking .....	341
Figure 8-9 MVR networking.....	343
Figure 8-10 Applying IGMP filtering on interface.....	349
Figure 8-11 Data transmission of IGMP MVR .....	351
Figure 8-12 Data transmission of multicast VLAN copy .....	352
Figure 8-13 Multicast VLAN copy networking .....	353
Figure 9-1 OAM loopback .....	364
Figure 9-2 MDs at different levels .....	371
Figure 9-3 MEP and MIP .....	372
Figure 9-4 CFM networking .....	383
Figure 9-5 SLA test networking .....	386
Figure 9-6 SLA test networking .....	392
Figure 10-1 Port security MAC networking.....	409
Figure 10-2 Principles of dynamic ARP inspection .....	411
Figure 10-3 Configuring dynamic ARP inspection .....	415
Figure 10-4 RADIUS networking .....	421
Figure 10-5 TACACS+ networking .....	425
Figure 10-6 Storm control networking.....	430
Figure 10-7 802.1x structure .....	431
Figure 10-8 Dot1x networking.....	437
Figure 10-9 Principles of IP Source Guard .....	439
Figure 10-10 Configuring IP Source Guard .....	443
Figure 10-11 Accessing the network through PPPoE authentication .....	445
Figure 10-12 PPPoE+ networking.....	450
Figure 11-1 Dual-homed application based on LACP .....	456
Figure 11-2 Static LACP mode Link aggregation networking .....	461
Figure 11-3 Principles of interface backup.....	464
Figure 11-4 Networking with interface backup in different VLANs.....	465
Figure 11-5 Interface backup networking .....	468

Figure 11-6 Link-state tracking networking .....	472
Figure 11-7 Dual-homed application based on LACP .....	475
Figure 11-8 mLACP networking .....	479
Figure 12-1 Principles of SNMP .....	484
Figure 12-2 SNMPv3 authentication mechanism.....	487
Figure 12-3 SNMPv1/SNMPv2c networking .....	490
Figure 12-4 SNMPv3 and Trap networking .....	492
Figure 12-5 RMON networking .....	495
Figure 12-6 RMON networking .....	499
Figure 12-7 Structure of a LLDPDU .....	501
Figure 12-8 Structure of a TLV packet.....	501
Figure 12-9 LLDP networking .....	507
Figure 12-10 Networking of outputting system log to log host .....	517
Figure 12-11 Principles of Ping.....	534
Figure 12-12 Principles of Traceroute .....	535

# Tables

Table 1-1 Shortcut keys for display features .....	8
Table 2-1 Interface mode and packet processing.....	58
Table 6-1 Fields of a DHCP packet.....	252
Table 6-2 Planned data .....	261
Table 6-3 Common DHCP options.....	270
Table 6-4 Fields of a DHCP packet.....	277
Table 7-1 Mapping from DSCP or CoS to local priority .....	291
Table 7-2 Mapping between local priority and queue .....	291
Table 7-3 Default mapping from CoS to local priority .....	295
Table 7-4 Default mapping from DSCP to local priority.....	296
Table 7-5 Default mapping from ToS to local priority and color .....	296
Table 12-1 TLV types .....	501
Table 12-2 IEEE 802.1 organization-defined TLVs .....	502
Table 12-3 IEEE 802.3 organization-defined TLVs .....	502
Table 12-4 Log levels.....	512
Table 12-5 Alarm fields .....	519
Table 12-6 Alarm levels.....	519
Table 12-7 Trap information .....	526
Table 12-8 Syslog information .....	526

# 1 Basic configurations

---

This chapter describes basic configurations and configuration procedures of the ISCOM2600G-HI series switch, and provides related configuration examples, including the following sections:

- CLI
- Accessing device
- File management
- Loading and upgrade
- Automatically updating version and configurations
- Time management
- Interface management
- Configuring basic information
- Task scheduling
- Watchdog
- Configuring Banner

## 1.1 CLI

### 1.1.1 Introduction

The Command-line Interface (CLI) is a medium for you to communicate with the ISCOM2600G-HI series switch. You can configure, monitor, and manage the ISCOM2600G-HI series switch through the CLI.

You can log in to the ISCOM2600G-HI series switch through the terminal equipment or through a computer that runs the terminal emulation program. Enter commands at the system prompt.

The CLI supports the following features:

- Configure the ISCOM2600G-HI series switch locally through the Console interface.
- Configure the ISCOM2600G-HI series switch locally or remotely through Telnet/Secure Shell v2 (SSHv2).



- Commands are classified into different levels. You can execute the commands that correspond to your level only.
- The commands available to you depend on which mode you are currently in.
- Shortcut keys can be used to execute commands.
- Check or execute a history command by checking command history. The last 20 history commands can be saved on the ISCOM2600G-HI series switch.
- Enter a question mark (?) at the system prompt to obtain online help.
- The ISCOM2600G-HI series switch supports multiple intelligent analysis methods, such as fuzzy match and context association.

## 1.1.2 Privileges

The ISCOM2600G-HI series switch uses hierarchical protection methods to divide commands into 16 privileges in an ascending order.

- Privileges 0–4: viewing privilege. Users can execute viewing commands, such as the **ping**, **clear**, and **history** commands.
- Privileges 5–10: monitoring privilege. Users can execute monitoring commands, such as the **show** command.
- Privileges 11–14: configuring privilege. Users can execute commands for configuring different services, such as Virtual Local Area Network (VLAN) and Internet Protocol (IP).
- Privilege 15: administering privilege. Users can execute basic commands for administering the system.

## 1.1.3 Modes

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

Establish a connection with the ISCOM2600G-HI series switch. If the ISCOM2600G-HI series switch is in default configuration, it will enter user EXEC mode, and the screen will display:

```
Raisecom#
```

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

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



### Note

- The CLI prompts that Raisecom is a default host name. You can modify it by using the **hostname** *name* command in privileged EXEC mode.
- Commands executed in global configuration mode can also be executed in other modes. The functions vary on command modes.

- You can use the **exit** or **quit** command to return to the upper command mode.
- You can execute the **end** command to return to privileged EXEC mode from any modes but user EXEC mode and privileged EXEC mode.

The ISCOM2600G-HI series switch supports the following command line modes:

Mode	Enter method	Description
Privileged EXEC	In user EXEC mode, enter the <b>enable</b> command and correct password.	Raisecom#
Global configuration	In privileged EXEC mode, enter the <b>config terminal</b> command.	Raisecom(config)#
Physical layer interface configuration	In global configuration mode, enter the <b>interface { gigabitEthernet   tengigabitEthernet } unit/slot/interface</b> command.	Raisecom(config-gigabitEthernet1/1/interface)# Raisecom(config-tengigabitEthernet1/1/interface)#
SNMP interface configuration	In global configuration mode, enter the <b>interface fastEthernet 1/0/1</b> command.	Raisecom(config-fastEthernet1/0/1)#
Loopback interface configuration	In global configuration mode, enter the <b>interface loopback lb-number</b> command.	Raisecom(config-loopback)#
VLAN configuration	In global configuration mode, enter the <b>vlan vlan-id</b> command.	Raisecom(config-vlan)#
Aggregation group configuration	In global configuration mode, enter the <b>interface port-channel channel-number</b> command.	Raisecom(config-port-channel)#
Traffic classification configuration	In global configuration mode, enter the <b>class-map class-map-name</b> command.	Raisecom(config-cmap)#
Traffic policy configuration	In global configuration mode, enter the <b>policy-map policy-map-name</b> command.	Raisecom(config-pmap)#
Traffic policy configuration binding with traffic classification	In policy configuration mode, enter the <b>class-map class-map-name</b> command.	Raisecom(config-pmap-c)#
Basic IP ACL configuration	In global configuration mode, enter the <b>access-list acl-number</b> command. In this command, <i>acl-number</i> ranges from 1000 to 1999.	Raisecom(config-acl-ipv4-std)#
Extended IP ACL configuration	In global configuration mode, enter the <b>access-list acl-number</b> command. In this command, <i>acl-number</i> ranges from 2000 to 2999.	Raisecom(config-acl-ipv4-ext)#

Mode	Enter method	Description
MAC ACL configuration	In global configuration mode, enter the <b>access-list <i>acl-number</i></b> command. In this command, <i>acl-number</i> ranges from 3000 to 3999.	Raisecom(config-acl-mac)#
User ACL configuration	In global configuration mode, enter the <b>access-list <i>acl-number</i></b> command. In this command, <i>acl-number</i> ranges from 5000 to 5999.	Raisecom(config-acl-udf)#
MST region configuration	In global configuration mode, enter the <b>spanning-tree region-configuration</b> command.	Raisecom(config-region)#
Profile configuration	In global configuration mode, enter the <b>igmp filter profile <i>profile-number</i></b> command.	Raisecom(config-igmp-profile)#
cos-remark configuration	In global configuration mode, enter the <b>mls qos mapping cos-remark <i>profile-id</i></b> command.	Raisecom(cos-remark)#
cos-to-pri configuration	In global configuration mode, enter the <b>mls qos mapping cos-to-local-priority <i>profile-id</i></b> command.	Raisecom(cos-to-pri)#
dscp-mutation configuration	In global configuration mode, enter the <b>mls qos mapping dscp-mutation <i>profile-id</i></b> command.	Raisecom(dscp-mutation)#
dscp-to-pri configuration	In global configuration mode, enter the <b>mls qos mapping dscp-to-local-priority <i>profile-id</i></b> command.	Raisecom(dscp-to-pri)#
SRED profile configuration	In global configuration mode, enter the <b>mls qos sred profile <i>profile-id</i></b> command.	Raisecom(sred)#
Traffic monitoring profile configuration	In global configuration mode, enter the <b>mls qos policer-profile <i>policer-name</i> [ single ]</b> command.	Raisecom(traffic-policer)#
Chinese prompt	In any configuration mode, enter the <b>language chinese</b> command.	Raisecom#
English prompt	In any configuration mode, enter the <b>language english</b> command.	Raisecom#

## 1.1.4 Shortcut keys

The ISCOM2600G-HI series switch supports the following shortcut keys.

Shortcut key	Description
<b>Up Arrow</b> (↑)	Show the previous command if there is any command entered earlier; the displayed command does not change if the current command is the earliest one in history records.
<b>Down Arrow</b> (↓)	Show the next command if there is any newer command. The displayed command does not change if the current command is the newest one in history records.
<b>Left Arrow</b> (←)	Move the cursor leftward by one character. The displayed command does not change if the cursor is already at the beginning of the command.
<b>Right Arrow</b> (→)	Move the cursor rightward by one character. The displayed command does not change if the cursor is already at the end of the command.
<b>Backspace</b>	Delete the character before the cursor. The displayed command does not change if the cursor is already at the beginning of the command.
<b>Tab</b>	<p>Press <b>Tab</b> after entering a complete keyword, and the cursor will automatically appear a space to the end. Press <b>Tab</b> again, and the system will show the follow-up available keywords.</p> <p>Press <b>Tab</b> after entering an incomplete keyword, and the system automatically executes partial helps:</p> <ul style="list-style-type: none"> <li>• When only one keyword matches the entered incomplete keyword, the system takes the complete keyword to replace the entered incomplete keyword and leaves one space between the cursor and end of the keyword.</li> <li>• When no keyword or multiple keywords match the entered incomplete keyword, the system displays the prefix, and you can press <b>Tab</b> to check words circularly. In this case, there is no space from the cursor to the end of the keyword. Press <b>Space bar</b> to enter the next word.</li> <li>• If you enter an incorrect keyword, pressing <b>Tab</b> will move the cursor to the next line and the system will prompt an error. In this case, the entered keyword does not change.</li> </ul>
<b>Ctrl+A</b>	Move the cursor to the beginning of the command.
<b>Ctrl+B</b>	Identical to the <b>Left Arrow</b> key.
<b>Ctrl+C</b>	Interrupt the ongoing command, such as <b>ping</b> and <b>traceroute</b> .
<b>Ctrl+D</b> or <b>Delete</b>	Delete the character at the cursor.
<b>Ctrl+E</b>	Move the cursor to the end of the command.
<b>Ctrl+F</b>	Identical to the Right Arrow key
<b>Ctrl+K</b>	Delete all characters from the cursor to the end of the command.
<b>Ctrl+L</b>	Clear screen information.
<b>Ctrl+S</b>	Identical to the <b>Down Arrow</b> key
<b>Ctrl+W</b>	Identical to the <b>Up Arrow</b> key

Shortcut key	Description
<b>Ctrl+X</b>	Delete all characters before the cursor (except the cursor location).
<b>Ctrl+Y</b>	Show history commands.
<b>Ctrl+Z</b>	Return to privileged EXEC mode from the current mode (except user EXEC mode).
<b>Space bar</b> or <b>Y</b>	Scroll down one screen.
<b>Enter</b>	Scroll down one line.

## 1.1.5 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 available for each command mode.

Raisecom#?

The command output is as below.

```

aaa          Authentication, Authorization, Accounting
boot         system boot
bootrom      Bootrom
clear        Reset functions
clock        System time and date
config       Configuration from terminal interface
console      Console
copy         load configuration information
debug        Debugging functions (see also 'undebug')
delete       Delete flash file
.....

```

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

Raisecom(config)#ntp ?

The command output is as below.

peer                    Configure NTP peer  
refclock-master      Set local clock as reference clock  
server                Configure NTP server

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

Raisecom(config)#**interface vlan ?**

The command output is as below.

<1-4094>    vlan number

## Incomplete help

You can acquire incomplete help under following three conditions:

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

Raisecom(config)#**c?**

The command output is as below.

class-map    Set class map  
clear        Clear buffer content  
command-log   Log the command to the file  
console      console  
cpu           Configure cpu parameters  
cpu-protect   Config cpu protect information  
create        Create static VLAN

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

Raisecom(config)#**show ?**

The command output is as below.

```
link-state-tracking  Fault tracking
link-trace           Link trace
```

- 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 messages

The ISCOM2600G-HI series switch prints out the following error messages according to error type when you enter incorrect commands:

Error message	Description
% Incomplete command.	The user has entered an incomplete command.
Error input in the position marked by '^'.	The keyword marked "^" is invalid.
Ambiguous input in the position marked by '^'	The keyword marked "^" is not clear.



### Note

If there is an error message mentioned above, use CLI help information to solve the problem.

## 1.1.6 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 1-1.

Table 1-1 Shortcut keys for display features

Shortcut key	Description
Press <b>Space bar</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 displayed information

The ISCOM2600G-HI series switch 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 you need to add filtering rules to filter out unnecessary information.

The **show** command on the ISCOM2600G-HI series switch supports three kinds of filter modes:

- | **begin** *string*: show all lines starting from the assigned string, in case-sensitive mode.
- | **exclude** *string*: show all lines mismatching the assigned string, in case-sensitive mode.
- | **include** *string*: show all lines only matching the assigned string, in case-sensitive mode.

## 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 1-1. If page-break is disabled, all messages are displayed when they are displayed at more than one screen.

By default, page-break is enabled.

Configure terminal page-break for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>terminal page-break enable</b>	Enable terminal page-break.

## 1.1.7 Command history

The history commands can be automatically saved at the CLI. You can use the up arrow (↑) or down arrow (↓) to schedule a history command. By default, the last 20 history commands are saved. You can configure the number of commands to be saved at the CLI.

Configure the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>terminal history number</b>	(Optional) configure the number of history commands saved in the system.
2	Raisecom# <b>terminal time-out period</b>	(Optional) configure the Console terminal timeout period.
3	Raisecom# <b>history</b>	Show history commands entered by the user.
4	Raisecom# <b>show terminal</b>	Show terminal configurations of the user.

## 1.1.8 Restoring default value of command line

The default value of command line can be restored by **no** form or **enable | disable** form.

- **no** form: be provided in front of a command and used to restore the default value, disable some feature, or delete a configuration. It is used to perform an operation that is opposite to the command. Therefore, the command with a **no** form is also called a reverse command.



- **enable | disable** form: be provided behind a command or in the middle of a command. The **enable** parameter is used to enable some feature or function while the **disable** parameter is used to disable some feature or function.

For example:

- In physical layer interface configuration mode, the **description string** command is used to modify descriptions about an interface while the **no description** command is used to delete descriptions about the interface and restore to the default values.
- In physical layer interface configuration mode, the **shutdown** command is used to disable an interface while the **no shutdown** command is used to enable an interface.
- In global configuration mode, the **terminal page-break enable** command is used to enable page-break while the **terminal page-break disable** command is used to disable terminal page-break.



### Note

Most configuration commands have default values, which often are restored by the **no** form.

## 1.1.9 Logging commands

Configure command logging for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>command-log enable</b>	Enable command logging.

## 1.2 Accessing device

### 1.2.1 Introduction

The ISCOM2600G-HI series switch can be configured and managed in Command Line Interface (CLI) mode or NView NNM network management mode.

The ISCOM2600G-HI series switch CLI mode has a variety of configuration modes:

- Console mode: it must use Console mode in the first configuration.
- Telnet mode: log on through the Console mode, open Telnet service on the Switch, configure the IP address of the VLAN interface, configure the user name and password, and then take remote Telnet configuration.
- SSH mode: before accessing the ISCOM2600G-HI series switch through SSH, you need to log in to the ISCOM2600G-HI series switch and start SSH services through the Console interface.

When configuring the ISCOM2600G-HI series switch in network management mode, you must first configure the IP address of the VLAN interface on CLI, and then configure the ISCOM2600G-HI series switch through NView NNM network management platform.

## 1.2.2 Accessing through Console interface

### Introduction

The Console interface is an interface which is commonly used to connect the network device with a PC running terminal emulation programs. You can use this interface to configure and manage local devices. This management method can communicate directly without a network, so it is called out-of-band management. You can also perform configuration and management on the ISCOM2600G-HI series switch through the Console interface when the network fails.

In the following two conditions, you can only log in to the ISCOM2600G-HI series switch and configure it through the Console interface:

- The ISCOM2600G-HI series switch is powered on to start for the first time.
- Accessing the ISCOM2600G-HI series switch through Telnet fails.

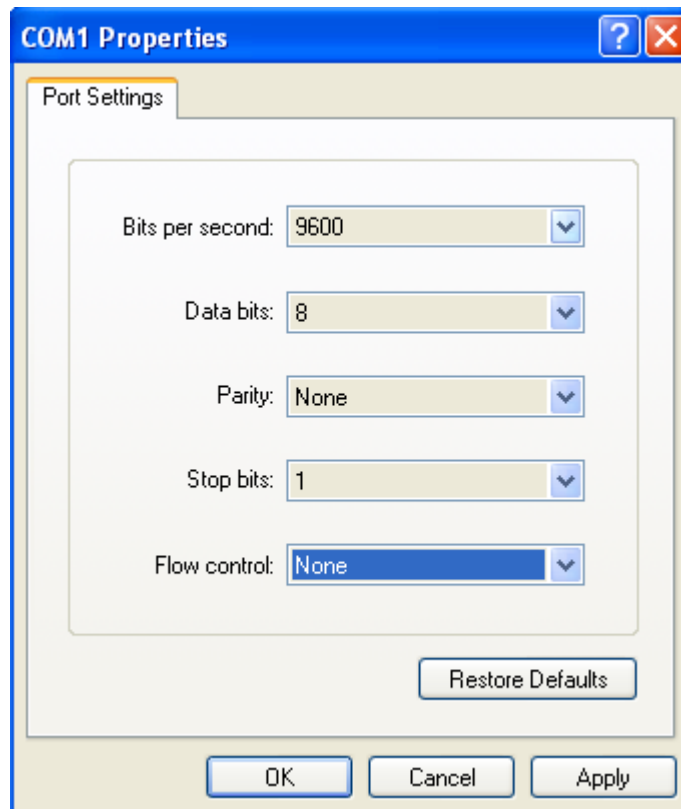
### Accessing device through RJ45 Console interface

If you want to access the ISCOM2600G-HI series switch through PC through RJ45 Console interface, connect Console interface and PC RS-232 serial port, as shown in Figure 1-1; then run the terminal emulation program such as Windows XP Hyper Terminal program in PC to configure communication parameters as shown in Figure 1-2, and then log in to the ISCOM2600G-HI series switch.

Figure 1-1 Accessing device through PC connected with RJ45 Console interface



Figure 1-2 Configuring communication parameters in Hyper Terminal



### Note

By default, the baud rate of the serial interface is 9600.

Configure the baud rate of the serial interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>config</b> Raisecom(config)# <b>console baud-rate 9600</b>	Modify the baud rate of the serial interface to 115200, 19200, 38400, or 9600.

## 1.2.3 Accessing through Telnet

### Note

By default, the default management IP address of the out-of-band management interface (SNMP interface: fastethernet 1/0/1), and the subnet mask is 255.255.255.0. To modify the IP address, log in to the ISCOM2600G-HI series switch and configure it. Both the default user name and password are raisecom. In Telnet connection status, if you enter the password incorrectly for three 3 times, the Telnet connection will be automatically disconnected.

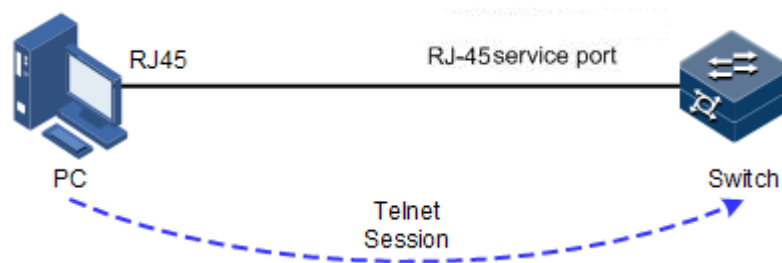
You can use a PC to log in to the ISCOM2600G-HI series switch remotely through Telnet. You can log in to an ISCOM2600G-HI series switch from PC at first, then Telnet another

ISCOM2600G-HI series switch on the network. You do not need to connect a PC to each ISCOM2600G-HI series switch.

Telnet services provided by the ISCOM2600G-HI series switch are as below:

- Telnet Server: run the Telnet client program on a PC to log in to the ISCOM2600G-HI series switch, and take configuration and management. As shown in Figure 1-3, ISCOM2600G-HI series switch is providing Telnet Server service at this time.

Figure 1-3 Networking with device as Telnet server

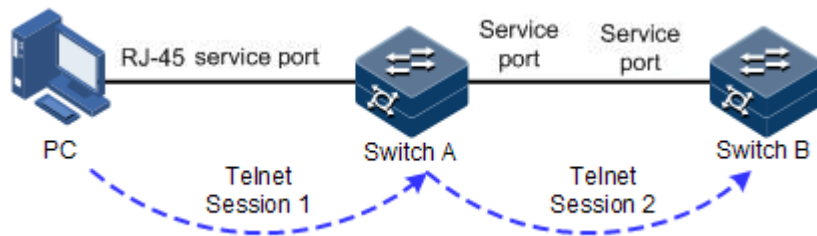


Before accessing the ISCOM2600G-HI series switch through Telnet, you need to log in to the ISCOM2600G-HI series switch through the Console interface and start the Telnet service. Take the following configurations on the ISCOM2600G-HI series switch that needs to start Telnet service.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface fastethernet 1/0/1</b>	Enter out-of-band network management interface configuration mode
3	<b>Raisecom(config-fastethernet 1/0/1)#ip address ip-address [ ip-mask ]</b>	Configure the IP address of the out-of-band network management interface. By default, it is 192.168.0.1/24. Both the default user name and password are raisecom.
4	<b>Raisecom(config)#telnet-server accept interface-type interface-list</b>	(Optional) configure the interface in support of Telnet function.
5	<b>Raisecom(config)#telnet-server close terminal-telnet session-number</b>	(Optional) release the specified Telnet connection.
6	<b>Raisecom(config)#telnet-server max-session session-number</b>	(Optional) configure the maximum number of Telnet sessions supported by the ISCOM2600G-HI series switch. By default, it is 10.
7	<b>Raisecom(config)# telnet-server access-list { ip access-list number   ipv6 access-list number }</b>	(Optional) configure the ACL number of the Telnet.
8	<b>Raisecom(config)#telnet-server disable</b>	(Optional) disable Telnet Server. At the same time, the corresponding port number will be disabled.

- Telnet Client: when you connect to the ISCOM2600G-HI series switch through the PC terminal emulation program or Telnet client program on a PC, then telnet other ISCOM2600G-HI series switch and configure/manage them. As shown in Figure 1-4, Switch A not only acts as Telnet server but also provides Telnet client service.

Figure 1-4 Networking with device as Telnet client



Configure Telnet Client device as below.

Step	Command	Description
1	<pre>Raisecom#telnet { ip-address   ipv6-address } [ port port-id ] Raisecom#telnet ipv4-address [ port port-id ] [ sourceip source-ip-address ]</pre>	Log in to another device through Telnet.

## 1.2.4 Accessing through SSH

Telnet is lack of security authentication and it transports messages through Transmission Control Protocol (TCP) which exists with big potential security hazard. Telnet service may cause hostile attacks, such as Deny of Service (DoS), host IP spoofing, and routing spoofing.

The traditional Telnet and File Transfer Protocol (FTP) transmit password and data in plain text, which cannot satisfy users' security demands. SSHv2 is a network security protocol, which can effectively prevent the disclosure of information in remote management through data encryption, and provides greater security for remote login and other network services in network environment.

SSHv2 allows data to be exchanged through TCP and it establishes a secure channel over TCP. Besides, SSHv2 supports other service ports besides standard port 22, avoiding illegal attacks from the network.

Before accessing the ISCOM2600G-HI series switch through SSHv2, you must log in to the ISCOM2600G-HI series switch through the Console interface and start SSH service.


Default configurations for accessing the ISCOM2600G-HI series switch through SSHv2 are as below.

Function	Default value
SSH server status	Disable
Local SSH key pair length	512 bits
Key renegotiation period	0h
SSH authentication method	password

Function	Default value
SSH authentication timeout	600s
Allowable failure times for SSH authentication	20
SSH snooping port ID	22
SSH session status	Disable
SSH version	v2

Configure SSH services for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#generate ssh-key length</b>	Generate local SSHv2 key pair and designate its length. By default, the length is 512 bits.
3	<b>Raisecom(config)#ssh2 server</b>	Start the SSH server. By default, it is not started. Use the <b>no ssh2 server</b> command to shut down the SSH server. (Optional) configure SSH key renegotiation period.
4	<b>Raisecom(config)#ssh2 server authentication { password   rsa-key }</b>	(Optional) configure SSHv2 authentication mode. By default, it is password.
5	<b>Raisecom(config)#ssh2 server authentication public-key public key</b>	(Optional) record the public key of the client on the ISCOM2600G-HI series switch in rsa-key authentication mode.
6	<b>Raisecom(config)#ssh2 server authentication-timeout period</b>	(Optional) configure the SSHv2 authentication timeout. The Gazelle S3028 refuses to authenticate the client and then closes the connection when the client authentication time exceeds this upper limit. By default, it is 600s.
7	<b>Raisecom(config)#ssh2 server authentication-retries times</b>	(Optional) configure the allowable failure times for SSHv2 authentication. The ISCOM2600G-HI series switch refuses to authenticate the client and then closes the connection when the number of client authentication failure times exceeds the upper limit. By default, it is 20.

Step	Command	Description
8	<code>Raisecom(config)#ssh2 server port port- number</code>	(Optional) configure SSHv2 snooping port number. By default, it is 22.  <b>Note</b> When configuring SSHv2 snooping port number, the entered parameter cannot take effect until SSH is restarted.
9	<code>Raisecom(config)#ssh2 server max-session session-number</code>	(Optional) configure the maximum number of SSHv2 sessions.
10	<code>Raisecom(config)#ssh2 access-list { ip access-list number   ipv6 access-list number }</code>	(Optional) configure the ACL number.
11	<code>Raisecom(config)#ssh2 server rekey-interval value</code>	(Optional) configure the SSH renegotiation time.
12	<code>Raisecom(config)# ssh2 server close session session- number</code>	(Optional) close the specified SSHv2 session.

## 1.2.5 Managing users

When you start the ISCOM2600G-HI series switch for the first time, connect the PC through Console interface to the ISCOM2600G-HI series switch, enter the initial user name and password in HyperTerminal to log in and configure the ISCOM2600G-HI series switch.



### Note

By default, both the user name and password are raisecom.

If there is no privilege restriction, any remote user can log in to the ISCOM2600G-HI series switch through Telnet or access network by establishing a PPP (Point to Point Protocol) connection when service interfaces are configured with IP address. This is unsafe to the ISCOM2600G-HI series switch and network. Creating user for the ISCOM2600G-HI series switch and configuring password and privilege help manage login users and ensures network and device security.

Default configurations of user management are as below.

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

Function	Default value
New user activation status	Activate
New user service type	N/A
Enable password	raisecom
User login authentication mode	local-user
Enable login authentication mode	local-user

Configure login user management for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#user name</b> <i>user-name</i> <b>password</b> [ <b>cipher</b>   <b>simple</b> ] <i>password</i>	Create or modify the user name and password.
2	<b>Raisecom#user name</b> <i>user-name</i> <b>privilege</b> <i>privilege-level</i>	Configure the login user privilege.
3	<b>Raisecom#user</b> <i>user-name</i> { <b>allow-exec</b>   <b>disallow-exec</b> } <i>first-keyword</i> [ <i>second-keyword</i> ]	(Optional) configure the priority rule for login user to perform the command line.
4	<b>Raisecom#user</b> <i>user-name</i> <b>service-type</b> { <b>lan-access</b>   <b>ssh</b>   <b>telnet</b>   <b>web</b>   <b>console</b>   <b>all</b> }	(Optional) configure the service type supported by the user.
5	<b>Raisecom#user login</b> { <b>console</b>   <b>telnet</b>   <b>ssh</b>   <b>web</b> } { <b>local-radius</b>   <b>local-user</b>   <b>radius-local</b>   <b>radius-user</b>   <b>local-tacacs</b>   <b>tacacs-local</b>   <b>tacacs-user</b> }	(Optional) configure the authentication mode for different user login modes.
6	<b>Raisecom#enable password</b> [ <b>cipher</b> <i>password</i> ]	(Optional) modify the password for entering privileged EXEC mode. Users with the level lower than 11 do not need the password for entering privileged EXEC mode.
7	<b>Raisecom#password check</b> { <b>complex</b>   <b>simple</b> }	(Optional) configure authentication mode of privileged users.
8	<b>Raisecom#logout</b>	Exit the system.



## Note

- Besides the default user raisecom, you can create up to 9 local user accounts.
- The login password is 8–16 characters, mandatorily including digits, lower-case letters, and upper-case letters.
- A local user with a level lower than 15, unless allowed to execute the command to modify the login password, is not allowed to modify the login password.



## 1.2.6 Configuring HTTP Server

Enable SSH Server for the ISCOM2600G-HI series switch as below.

You can log in to the ISCOM2600G-HI series switch through the Web interface.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>ip http server enable</b>	Enable HTTP Server.

## 1.2.7 Checking configurations

Use the following commands to check the configuration results.

No.	Command	Description
1	Raisecom# <b>show user table</b>	Show login user information.
2	Raisecom# <b>show user active</b>	Show information about users logged in to the ISCOM2600G-HI series switch.
3	Raisecom# <b>show telnet-server</b>	Show configurations of the Telnet server.
4	Raisecom# <b>show ssh public-key [ authentication ]</b>	Show the public key used for SSH authentication on the ISCOM2600G-HI series switch and client.
5	Raisecom# <b>show ssh2 { server   session }</b>	Show SSHv2 server or session information.

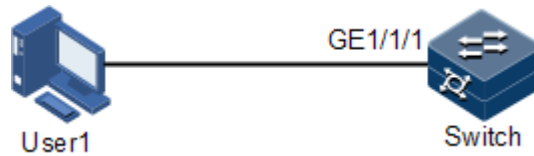
## 1.2.8 Example for configuring user management

### Networking requirements

As shown in Figure 1-5, to prevent malicious users from logging in to the ISCOM2600G-HI series switch and to eliminate risks on the ISCOM2600G-HI series switch, configure user management as below:

- Configure the user login mode to local-user.
- Create a local user user1 with plain password of aaAA123@.
- Configure the user1 privilege to privilege 10.
- Configure the user1 service type to Telnet.

Figure 1-5 User management networking



## Configuration steps

Step 1 Configure the user login authentication mode.

```
Raisecom#user login local-user
```

Step 2 Create a local user user1.

```
Raisecom#user name user1 password simple aaAA123@
```

Step 3 Configure the user privilege.

```
Raisecom#user user1 privilege 10
```

Step 4 Configure the service type of the user.

```
Raisecom#user user1 service-type telnet
```

## Checking results

Use the **show user table detail** command to show configurations of local users.

```
Raisecom#show user table detail
User Login :local-user
Enable Login:local-user

Username:raisecom
Priority:15
Server:Local
Login :console
Status :online
Service type:console telnet ssh web lan-access
User State :active

Username:user1
```

```
Priority:10
Server:Local
Login :--
Status :offline
Service type:console telnet ssh web lan-access
User State :active
User command control config:
-----
Type:allow
First keyword :minrror
```

Use the newly-created user name user1 and password aaAA123@ to log in to the ISCOM2600G-HI series switch, and check whether the user privilege is correctly configured.

```
Login:user1
Password:
Raisecom>enable
Raisecom#config
Raisecom(config)#arp 192.168.0.2 000E.5E12.3456
Set successfully.
```

## 1.3 File management

### 1.3.1 Managing BootROM files

In Boot mode, you can do the following operations.

Operation	Description
t	Update system software to the ISCOM2600G-HI series switch.
m	Update the boot file to the ISCOM2600G-HI series switch.
b	Read system software from the ISCOM2600G-HI series switch, and load it.
s	Specify the sequence of system software to be loaded upon startup.
e	Clear environment variables.
r	Restart the ISCOM2600G-HI series switch.
p	Configure the BootROM password.
?/h	Show information about system files and help.

Configure the ISCOM2600G-HI series switch as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	<code>Raisecom#upload bootstrap { ftp ip-address user-name password file-name   tftp ip-address file-name   sftp ip-address user-name password file-name } [ dir ]</code>	(Optional) download the BootROM file through FTP or TFTP.
2	<code>Raisecom#erase [ file-name ]</code>	(Optional) delete files saved in the Flash.

## 1.3.2 Managing system files

System files are the files needed for system operation (such as system startup software and configuration file). These files are usually saved in the memory. The ISCOM2600G-HI series switch manages them through a file system to facilitate managing the memory. The file system can create, delete, and modify the file and directory.

In addition, the ISCOM2600G-HI series switch supports dual-system. There are 2 independent sets of system software saved at the memory. When the ISCOM2600G-HI series switch fails to work due to upgrade failure, you can use the other set to boot the ISCOM2600G-HI series switch.

Manage system files for the ISCOM2600G-HI series switch as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	<code>Raisecom#download system-boot { ftp { ipv4-address   ipv6-address } user-name password file-name   tftp { ipv4-address   ipv6-address } file-name   sftp { ipv4-address   ipv6-address } user-name password file-name } [ system1.z   system2.z ]</code>	(Optional) download the system boot file through FTP or TFTP to the device.
2	<code>Raisecom#erase [ file-name ]</code>	(Optional) delete files saved in the Flash.
3	<code>Raisecom#upload system-boot { ftp { ipv4-address   ipv6-address } user-name password file-name   tftp { ipv4-address   ipv6-address } file-name   sftp { ipv4-address   ipv6-address } user-name password file-name } { system1.z   system2.z }</code>	(Optional) upload the system boot file through FTP or TFTP to the local device.

## 1.3.3 Managing configuration files

Configuration files are loaded after starting the system; different files are used in different scenarios to achieve different service functions. After starting the system, you can configure the ISCOM2600G-HI series switch and save the configuration files. New configurations will take effect in next boot.

The configuration file has a suffix ".cfg", and can be opened by the text book program in Windows system. The contents are in the following format:

- Be saved in the mode+command format.
- Just keep the non-default parameters to save space (see the command reference manual for default values of configuration parameters).
- Use the command mode for basic frame to organize commands. Put parameters of one mode together to form a section, and the sections are separated by the exclamation mark (!).

The ISCOM2600G-HI series switch starts initialization by reading configuration files from the memory after being powered on. Thus, the configurations in configuration files are called the default configurations. If there is no configuration file in the memory, the ISCOM2600G-HI series switch uses the default parameters for initialization.

The configuration that is currently used by the ISCOM2600G-HI series switch is called the running configuration.

You can modify the running configuration of ISCOM2600G-HI series switch through CLI. The running configuration can be used as initial configuration upon next power-on. You must use the **write** command to save running configurations in the memory and form a configuration file.

Manage configuration files for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>download startup-config</b> { ftp { ipv4-address /ipv6-address } user-name password file-name   tftp { ipv4-address /ipv6-address } file-name   sftp { ipv4-address /ipv6-address } user-name password file-name } } [ dir ]	(Optional) download the startup configuration file through FTP or TFTP.
2	Raisecom# <b>download backup-config</b> { ftp { ipv4-address /ipv6-address } user-name password file-name   tftp { ipv4-address /ipv6-address } file-name   sftp { ipv4-address /ipv6-address } user-name password file-name } } [ dir ]	(Optional) download the backup configuration file through FTP or TFTP.
3	Raisecom# <b>erase</b> [ file-name ]	(Optional) delete files saved in the Flash.
4	Raisecom# <b>upload startup-config</b> { ftp { ipv4-address /ipv6-address } user-name password file-name   tftp { ipv4-address /ipv6-address } file-name   sftp { ipv4-address /ipv6-address } user-name password file-name } } [ dir ]	(Optional) upload the startup configuration file through FTP or TFTP.
5	Raisecom# <b>upload backup-config</b> { ftp { ipv4-address /ipv6-address } user-name password file-name   tftp { ipv4-address /ipv6-address } file-name   sftp ip-address user-name password file-name } } [ dir ]	(Optional) upload the backup configuration file through FTP or TFTP.

Step	Command	Description
6	Raisecom# <b>upload command-log</b> { ftp { ipv4-address /ipv6-address } user-name password file-name   tftp { ipv4-address /ipv6-address } file-name   sftp { ipv4-address /ipv6-address } user-name password file-name } [ dir ]	(Optional) upload the command line logging file and system logs through FTP or TFTP.
7	Raisecom# <b>upload logging-file</b> { ftp { ipv4-address /ipv6-address } user-name password file-name   tftp { ipv4-address /ipv6-address } file-name   sftp { ipv4-address /ipv6-address } user-name password file-name } [ dir ]	(Optional) upload the system log file through FTP or TFTP.
8	Raisecom# <b>write</b>	(Optional) save the running configuration file in the Flash.


### 1.3.4 Checking configurations


Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# <b>show startup-config</b>	Show configurations loaded upon device startup.
2	Raisecom# <b>show running-config</b>	Show running configurations.

### 1.3.5 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>write</b> [ backup-config ]	Save running configurations as a startup configuration file which can take effect upon next startup.   <b>Caution</b> When you save running configurations as a startup configuration file, the file will overwrite the original startup configuration file; therefore back up the original one in advance.
2	Raisecom# <b>dir</b>	Show names of system files. You can view the remaining size of the Flash.

Step	Command	Description
3	<b>Raisecom#erase</b> [ <i>file-name</i>   <b>backup-</b> <b>config</b> ]	Delete a specified system file. If the file-name parameter is not configured, this configuration will delete the startup configuration file.   <b>Caution</b> After a file is deleted through this command, it cannot be restored. Use this command with caution.
4	<b>Raisecom#syslog</b> <b>save</b>	Save log files.

## 1.4 Loading and upgrade

### 1.4.1 Introduction

#### Loading

Traditionally, configuration files are loaded through the serial interface, which takes a long time due to low rate and unavailable remote loading. FTP and TFTP loading modes can solve those problems and make operation more convenient.

The ISCOM2600G-HI series switch supports TFTP auto-loading mode.

TFTP auto-loading refers that you can obtain the configuration files from a server and then configure the ISCOM2600G-HI series switch. Auto-loading allows configuration files to contain loading related commands for multiple configurations loading to meet file auto-loading requirements in complex network environment.

The ISCOM2600G-HI series switch provides several methods to confirm configuration file name on the TFTP server, such as manually entering, obtaining through DHCP, and using default name of the configuration file. Besides, you can assign certain naming conventions for configuration files, and then the ISCOM2600G-HI series switch confirms the name according to naming conventions and its attributes (device type, MAC address, software version, and so on).

#### Upgrade

The ISCOM2600G-HI series switch needs to be upgraded if you want to add new features, optimize functions, or fix bugs in the current software version.

The ISCOM2600G-HI series switch supports the following two upgrade modes:

- Upgrade through BootROM
- Upgrade through CLI

### 1.4.2 Upgrading system software through BootROM

You need to upgrade system software through BootROM under the following conditions:

- The device is started for the first time.
- A system file is damaged.
- The card is started improperly.

Before upgrading system software through BootROM, you should establish a TFTP environment, and use the PC as the TFTP server and the ISCOM2600G-HI series switch as the client. Basic requirements are as below.

- Configure the TFTP server. Ensure that the TFTP server is available.
- Configure the IP address of the TFTP server; keep it in the same network segment with that of the ISCOM2600G-HI series switch.
- Connect the Ethernet interface on the TFTP server to the SNMP interface on the ISCOM2600G-HI series switch. The default IP address of the SNMP interface is 192.168.0.1 by default.

Upgrade system software through BootROM for the ISCOM2600G-HI series switch as below.

Step	Operation
1	<p>Log in to the ISCOM2600G-HI series switch through serial interface as the administrator, enter Privileged EXEC mode, and restart the ISCOM2600G-HI series switch with the <b>reboot</b> command.</p> <p><b>Raisecom#reboot</b></p>
2	<p>When the system successfully loads the big BootROM, and it displays "Press space to enter big boot menu", press <b>Space bar</b> to enter the interface starting with [raisecom]. The command list is displayed as below:</p> <pre>                                 BOOT ***** t: Update system from tftp. m: Update boot from tftp. b: Boot system from flash. e: Erase bootline para. s: Select system image to boot. p: Password setting. r: Reboot. ?/h: Help menu. [Raisecom]: </pre>



Step	Operation
3	<p>Type "t" to upgrade system software to the ISCOM2600G-HI series switch.</p> <pre>[Raisecom]:t ipaddr: 192.168.5.100 serverip: 192.168.5.1 filename: uImage  Current system partiton info: Partition number   Name                Size ----- 1                  iscom2600_image    16320072 2                  None                0</pre> <p>Please input system partition number for upgrading(1-2):1</p>
4	<p>Type "m" to upgrade the Boot software to the ISCOM2600G-HI series switch.</p> <pre>[Raisecom]:m ipaddr: 192.168.5.100 serverip: 192.168.5.1 filename: uImage mboot.bin  press y to confirm: y</pre>
5	<p>Type "r" to rapidly execute the big BootROM file. The ISCOM2600G-HI series switch is restarted and will load the downloaded startup file.</p>

### 1.4.3 Upgrading system software through CLI

Before upgrading system software through CLI, you should establish a TFTP environment, and use a PC as the TFTP server and the ISCOM2600G-HI series switch as the client. Basic requirements are as below.

- Connect the Ethernet interface on the TFTP server to the SNMP interface on the ISCOM2600G-HI series switch. The default IP address of the SNMP interface is 192.168.0.1 by default.
- Configure the TFTP server, and ensure that the server is available.
- Configure the IP address of the TFTP server; keep it in the same network segment with that of the ISCOM2600G-HI series switch so that the ISCOM2600G-HI series switch can access the TFTP server.

Upgrade system software through CLI for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#download system-boot { ftp { ipv4-address / ipv6-address } user-name password file-name   tftp { ipv4-address / ipv6-address } file-name / sftp { ipv4-address / ipv6-address } user-name password file-name } [ system1.z   system2.z ]</code>	Download the system boot file through FTP, SFTP, or TFTP. This command supports the IPv6 address.
2	<code>Raisecom#boot sequence</code>	(Optional) configure the sequence for loading system software.
3	<code>Raisecom#reboot [ now ]</code>	Restart the ISCOM2600G-HI series switch, and it will automatically load the downloaded system boot file.

## 1.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show startup-config</code>	Show information about the startup configuration file.
2	<code>Raisecom#show running-config</code>	Show information about the running configuration file.
3	<code>Raisecom#show version</code>	Show system version.

## 1.5 Automatically updating version and configurations

### 1.5.1 Introduction

After being powered on, the ISCOM2600G-HI series switch can automatically obtain the new version and configurations. After obtaining an IP address as a DHCP client, it will automatically download configuration files and system files from the TFTP server to update version and configurations.

### 1.5.2 Preparing for configurations

#### Scenario

To use the ISCOM2600G-HI series switch as a DHCP client, you must enable DHCP Client. The DHCP client actively sends a Discover broadcast packet. After receiving the packet, the DHCP server pads information, such as the assigned IP address to the Offer packet, and sends the packet to the DHCP client. Meanwhile, it pads the IP address of the TFTP server to Option 150 and pads the name of the configuration file or system file to Option 67. After receiving

these packets, the DHCP client resolves Option 150 for the IP address of the TFTP server and resolves Option 67 for the name of the configuration file or system file according to naming conversions, resolves Option 17 for the file path.

## Prerequisite

- Configure the address pool on the DHCP server and configure Option 67 and Option 150 in the address pool.
- Configure DHCP Client.

## 1.5.3 Automatically updating version and configurations

Configure automatic update of version and configurations for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlan <i>vlan-id</i></b>	Enter Layer 3 interface configuration mode.
3	<b>Raisecom(config-vlan1)#ip address dhcp [ server-ip <i>ip-address</i> ]</b>	Configure the DHCP client to apply for the IP address through DHCP.
4	<b>Raisecom(config-vlan1)#auto-config enable</b> <b>Raisecom(config-vlan1)#exit</b>	Enable automatic update of version and configurations.
5	<b>Raisecom(config)#auto-save enable</b>	(Optional) enable automatic saving of configurations.
6	<b>Raisecom(config)#auto-load time <i>hour minute second</i></b>	(Optional) configure the time for saving configuration after successfully loading the configuration file.



### Note

- After configuring the ISCOM2600G-HI series switch, save configurations and restart it. Then, it will automatically apply for the IP address and conduct update operations.
- Connect the DHCP client to the DHCP server properly. Connect the DHCP client to the TFTP server properly.

## 1.5.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show auto-config</b>	Show configurations of automatic update of version and configurations.

No.	Command	Description
2	Raisecom# <b>show buffer-config</b>	Show information about the configuration file in the buffer.

## 1.5.5 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
Raisecom(config)# <b>clear buffer_config</b>	Clear the configuration file in the buffer.

## 1.6 Time management

### 1.6.1 Introduction

With development and extension of Internet in all aspects, multiple applications involved in time need accurate and reliable time, such as online realtime transaction, distributed network calculation and processing, transport and flight management, and data management.

To ensure precise system time, the ISCOM2600G-HI series switch provides complete time management functions, including manually configuring system time and time zone, manually configuring Daylight Saving Time (DST), Network Time Protocol (NTP), and Simple Network Time Protocol (SNTP).

#### Time and time zone

The device time is usually configured to the local time of the device while the time zone is configured to the local time zone based on Greenwich Mean Time (GMT) (for example, China Beijing is in the eastern eight zone based on GMT, so its time zone is configured to +08:00).

The ISCOM2600G-HI series switch supports displaying time in the format of "year-month-day hour:minute:second" and offset of the time zone. You can manually configure the time and time zone of the ISCOM2600G-HI series switch.

#### DST

DST is a kind of artificially regulated local time system for saving energy. Time is usually advanced one hour in summer to make people sleep early and rise early to save energy, but different countries have different stipulations for DST. In this case, you should consider local conditions when configuring DST.

The ISCOM2600G-HI series switch supports configuring the start time, end time, offset of the DST.

## NTP

Network Time Protocol (NTP) is a standard Internet protocol for time synchronization, used to synchronize time between the distributed time servers and clients. NTP transmits data based on UDP, using UDP port 123 and guaranteeing high precision (error around 10ms).

Figure 1-6 shows basic principles of NTP. Clock synchronization works as below:

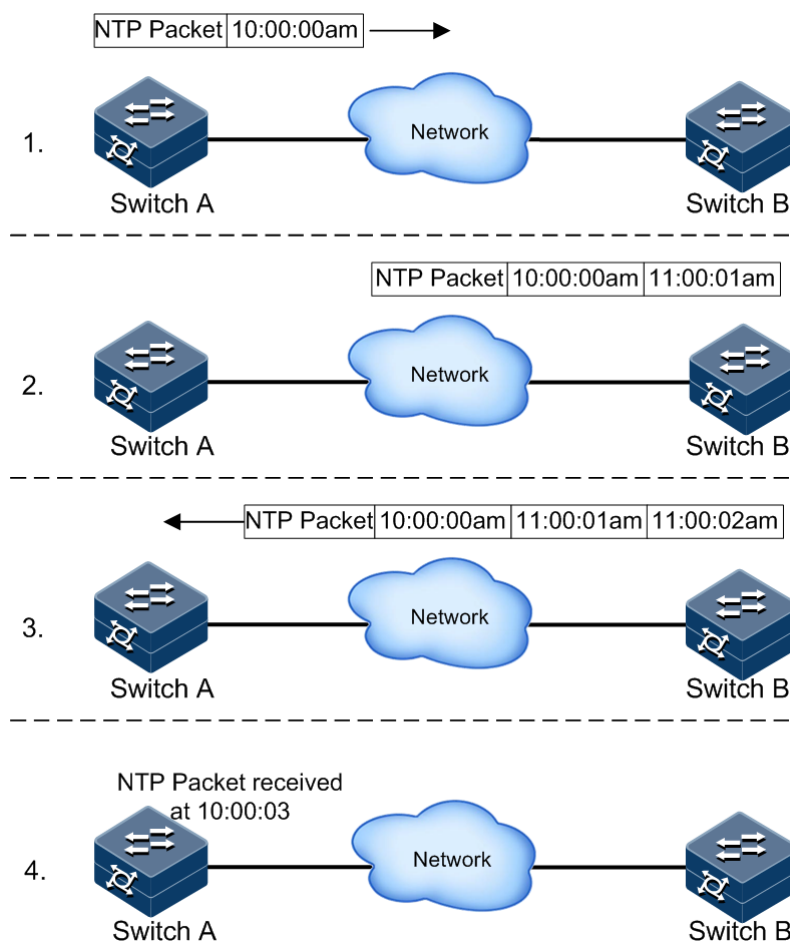
- Step 1 Switch A sends Switch B a NTP message which carries the timestamp of leaving Switch A. The timestamp is 10:00:00am and recorded as t1.
- Step 2 When the message reaches Switch B, it is added with the timestamp of reaching Switch B, which is 11:00:01am and recorded as t2.
- Step 3 When the message leaves Switch B, it is added with the timestamp of leaving Switch B, which is 11:00:02am and recorded as t3.
- Step 4 When switch A receives the response message, it adds a new timestamp, which is 11:00:03am and recorded as t4.

At present, Switch A has enough information to calculate two important parameters:

- Round-trip delay of the NTP message:  $\text{delay} = (t4 - t1) - (t3 - t2)$
- Time offset between Switch A and Switch B:  $\text{offset} = ((t2 - t1) + (t3 - t4))/2$

Switch A configures its clock based on previous two parameters to synchronize clock with Switch B.

Figure 1-6 Basic principles of NTP



The ISCOM2600G-HI series switch adopts multiple NTP working modes for time synchronization:

- Client/Server mode

In this mode, the client sends clock synchronization messages to different servers. The servers work in server mode automatically after receiving the synchronization message and sending response messages. The client receives response messages, performs clock filtering and selection, and is synchronized to the preferred server.

In this mode, the client can be synchronized to the server but the server cannot be synchronized to the client. The ISCOM2600G-HI series switch can work as a client or server.

- Symmetric mode

In this mode, you can configure the passive peer on the active peer. The active peer sends a clock synchronization message to the passive peer. The passive peer works in passive mode automatically after receiving the message and sends the answering message back. By exchanging messages, the two peers establish the symmetric peer mode. The peer with fewer stratum synchronizes time with the one with more stratum. The active and passive peers in this mode can synchronize each other.

## SNTP

Simple Network Time Protocol (SNTP) is used to synchronize the system time of the ISCOM2600G-HI series switch to the GMT and transmit the GMT to local time according to the system settings of time zone. When the SNTP client and server are in different time zones, the SNTP client will be synchronized to the GMT and then translated into the local time according to system settings of time zone.

The SNTP client obtains time in two modes: actively sending a request packet or passively monitoring the packet. They are implemented as below:

- Unicast mode: the SNTP client actively sends a request packet. After being configured with the IP address of the SNTP unicast server, the device tries to obtain clock signals every 10s from the SNTP server. The maximum timeout for obtaining clock signals from the SNTP server is 60s.
- Multicast or broadcast mode: SNTP client passively monitors the packet.
  - After being configured to multicast mode, the device monitors the multicast IP address of 224.0.1.1 in real time and obtain clock signals from the SNTP multicast server. The maximum timeout for obtaining clock signals from the SNTP server is 60s.
  - After being configured to broadcast mode, the device monitors the broadcast IP address of 255.255.255.255 in real time and obtain clock signals from the SNTP broadcast server. The maximum timeout for obtaining clock signals from the SNTP server is 60s.

## 1.6.2 Preparing for configurations

### Scenario

Configure the system time of the ISCOM2600G-HI series switch, and guarantee precision of the system time.

- The time and time zone that is manually configured take effect immediately.
- After NTP or SNTP is enabled, the synchronized time will override the current system time after a synchronization period.
- NTP and SNTP are mutually exclusive, so they cannot be concurrently configured.

### Prerequisites

N/A

## 1.6.3 Default configurations of time management

### Time and time zone

Default configurations of time and time zone are as below.

Function	Default value
Time zone offset	+08:00-CCT
Display mode of the system clock	Default



## Note

China Coast Time (CCT) is the standard time code. Several countries define their local time by reference to GMT by advancing or adjusting backward several hours on the basis of GMT and their longitudes or time zones. To be convenient, establish a series of standard time codes, including:

- China Coast Time (CCT): GMT +8:00
- Eastern Daylight Time (EDT): GMT +4:00
- Eastern Standard Time (EST): GMT +5:00
- Central Daylight Time (CDT): GMT -5:00
- Central Standard Time (CST): GMT -6:00
- Mountain Daylight Time (MDT): GMT -6:00
- Mountain Standard Time (MST): GMT -7:00
- Pacific Daylight Time (PDT): GMT -7:00
- Pacific Standard Time (PST): GMT -8:00

## DST

Default configurations of DST are as below.

Function	Default value
DST status	Disable

## NTP

Default configurations of NTP are as below.

Function	Default value
Whether the device is NTP master clock	No
Global NTP server	Inexistent
Global NTP equity	Inexistent
Reference clock source	0.0.0.0
Identity authentication	Disable
Identity authentication key ID	N/A
Trusted key	N/A

## SNTP

Default configurations of SNTP are as below.

Function	Default value
IP address of the SNTP server	N/A




## 1.6.4 Configuring time and time zone

Configure the time and time zone for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>clock set</b> <i>hour minute second year month day</i>	Configure system time.
2	Raisecom# <b>clock timezone</b> { +   - } <i>hour minute timezone-name</i>	Configure the local time zone.
3	Raisecom# <b>clock display</b> { <b>default</b>   <b>utc</b> }	Configure system clock display mode.

## 1.6.5 Configuring DST

Configure DST for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>clock summer-time enable</b>	Enable DST.
2	Raisecom# <b>clock summer-time recurring</b> { <i>week</i>   <i>last</i> } { <i>fri</i>   <i>mon</i>   <i>sat</i>   <i>sun</i>   <i>thu</i>   <i>tue</i>   <i>wed</i> } <i>month hour minute</i> { <i>week</i>   <i>last</i> } { <i>fri</i>   <i>mon</i>   <i>sat</i>   <i>sun</i>   <i>thu</i>   <i>tue</i>   <i>wed</i> } <i>month hour minute offset-mm</i>	Configure calculation period for system DST.  <b>Note</b> Underlined command lines indicate the termination DST.



### Note

- When you configure system time manually, if the system uses DST, such as DST from 2 A.M. on the second Sunday, April to 2 A.M. on the second Sunday, September every year, you have to adjust the clock one hour forward during this period, configure time offset as 60 minutes, and the period from 2 A.M. to 3 A.M. on the second Sunday, April each year is inexistent. The time setting by manual operation during this period shows failure.
- The summer time in southern hemisphere is opposite to the northern hemisphere, which is from September to April of next year. If you configure the start time later than the end time, the system will suppose that it is in the Southern Hemisphere. In other words, the summer time is from the start time this year to the ending time of next year.

## 1.6.6 Configuring NTP

Configure NTP for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	Raisecom(config)#ntp server { ipv4-address   ipv6-address } [ version version-number ] [ keyid key-id ]	(Optional) configure the IP address of the NTP server for the client working in server/client mode.
3	Raisecom(config)#ntp peer { ipv4-address   ipv6-address } [ version version-number ] [ keyid key-id ]	(Optional) configure the IP address of the NTP peer for the ISCOM2600G-HI series switch working in symmetric peer mode.
4	Raisecom(config)#ntp refclock-master [ ip-address ] [ stratum ]	Configure the clock of the ISCOM2600G-HI series switch as the NTP reference clock source for the ISCOM2600G-HI series switch.



### Note

If the ISCOM2600G-HI series switch is configured as the NTP reference clock source, it cannot be configured as the NTP server or NTP symmetric peer; vice versa.

## Configuring NTP identity authentication

A network with high requirements for security requires identity authentication when NTP is used. After enabled with identity authentication, a NTP client synchronizes with the NTP server that passes identity authentication, thus guaranteeing network security. Only after the NTP client is enabled with identity authentication can it authenticate the NTP server. If it is disabled with identity authentication, it will directly synchronize time with the NTP server without authentication regardless of that the NTP server carries key information.

Configure NTP identity authentication for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ntp authenticate enable	Enable identity authentication on the NTP server/client.
3	Raisecom(config)#ntp authentication-keyid key-id md5 password	Configure the key ID and key password for identity authentication on the NTP server/client.
4	Raisecom(config)#ntp trusted-keyid key-id	Configure the key ID for identity authentication on the NTP server/client as a trusted ID.  <div data-bbox="852 1659 948 1747" data-label="Image"></div> <div data-bbox="943 1695 1045 1736" data-label="Section-Header"><h3>Note</h3></div> <p>Only after the NTP client is enabled with identity authentication can it authenticate the NTP server, and can it synchronize time with the NTP server that provides a trusted key.</p>

## 1.6.7 Configuring SNTP

### Configuring unicast feature of SNTP client

Configure unicast feature of SNTP client for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#sntp server</b> { <i>ipv4-address</i>   <i>ipv6-address</i> }	Configure the IP address of the SNTP unicast server. After the SNTP server is configured with an IP address, the ISCOM2600G-HI series switch tries to get the clock information from the SNTP server every 10s. In addition, the maximum timeout is 60s.

## 1.6.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show clock</b> [ <b>summer-time-recurring</b> ]	Show configurations of the time zone and DST.
2	<b>Raisecom#show sntp</b>	Show SNTP configurations.
3	<b>Raisecom#show ntp status</b>	Show NTP configurations.
4	<b>Raisecom#show ntp associations</b> [ <b>detail</b> ]	Show information about NTP connection.
5	<b>Raisecom#show ntp authentication</b>	Show information about NTP identity authentication.

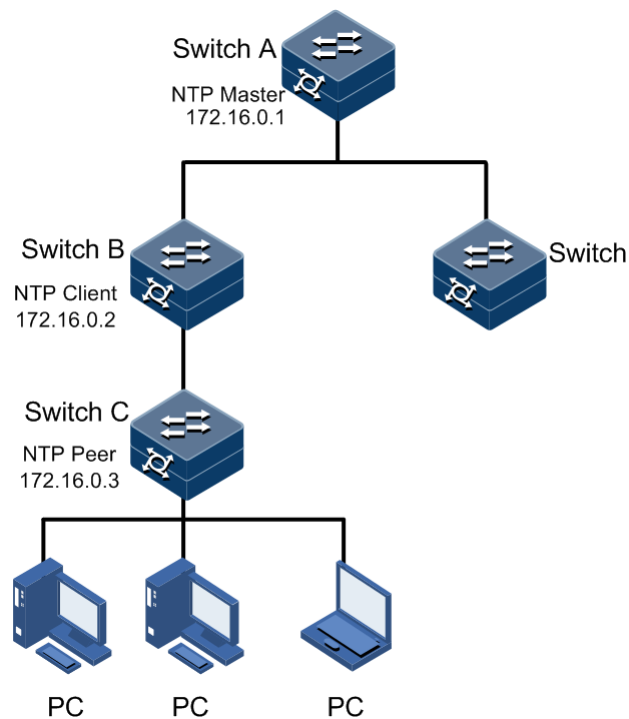
## 1.6.9 Example for configuring NTP

### Networking requirements

Establish a clock synchronization system in a company to keep consistency and precision of the system time. Basic planning is as below:

- Configure Switch A as the master clock source of the clock synchronization system.
- Configure Switch B as the client of the clock synchronization system. Configure the upper-layer Switch A as the NTP server.
- Configure Switch C as the NTP entity of Switch B so that Switch C receives downlink synchronization data from Switch B.

Figure 1-7 NTP networking



## Configuration steps

Step 1 Configure Switch A.

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

Step 2 Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#ntp server 172.16.0.1
SwitchB(config)#ntp peer 172.16.0.3
```

## Checking results

- Check Switch A.

Use the **show ntp status** command to view configurations of Switch A.

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

```

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

```

- Check Switch B.

Use the **show ntp status** command to view configurations of Switch B.

```

SwitchB#show ntp status
Clock status   :synchronized
NTP peer      :172.16.0.1
NTP version   :3
NTP mode      :ntpSlave
Leap          :0
Poll          :6
Stratum       :9
Precision     :2**-16
Reference clock :172.16.0.1
Reference time :5333d671.383980f6(Thu 2014-03-27,15:44:58.466)
Current time   :5333d697.0a917f54(Thu 2014-03-27,15:45:58.765)
Root delay     :0.000000
Root dispersion :0.010004

```

Use the **show ntp associations** command to view information about NTP sessions of Switch B.

```

SwitchB#show ntp associations
Server(ip)      refid      stratum poll when      delay
offset          dispersion  mode reach
-----
(s)172.16.0.1   127.127.1.0    8      6    55      0.000000    -
1.965874       14.875517     4      255
Peer(ip)        refid      stratum poll when      delay
offset          dispersion  mode reach
-----
(u)172.16.0.3   0.0.0.0        16      6    125     0.000000
0.000000       16.000000     0      0

```

- Check Switch C.

Use the **show ntp status** command to view configurations of Switch C.

```
Raisecom#show ntp status
Clock status :    synchronized
NTP peer :       172.16.0.2
NTP version :    3
NTP mode :       ntpSlave
Leap :          0
Poll :          6
Stratum :        10
Precision :      2**-22
Reference clock : 172.16.0.2
Reference time :  4d62a905.00000000(Mon 2011-02-22,02:03:49)
Current time :    5333dd97.00000000(Thu 2014-03-27,16:13:11)
Root delay :      4.154726
Root dispersion : 14.034068
```

Use the **show ntp associations** command to view information about NTP sessions of Switch C.

```
Raisecom#show ntp associations
Active(IP)      refid      stratum poll when      delay      offset
dispersion     mode reach
-----
(s)172.16.0.2   172.16.0.1      9        6      97596571    4.154726
13447.112484   0.000930        1        6
```

## 1.7 Interface management

### 1.7.1 Introduction

Ethernet is a very important LAN networking technology which is flexible, simple, and easy to implement. The Ethernet interface includes the Ethernet electrical interface and Ethernet optical interface.

The ISCOM2600G-HI series switch supports both Ethernet electrical and optical interfaces.

#### Auto-negotiation

Auto-negotiation is used to make the devices at both ends of a physical link automatically choose the same working parameters by exchanging information. The auto-negotiation parameters include duplex mode, interface rate, and flow control. Once successful in negotiation, the devices at both ends of the link can work in the same duplex mode and interface rate.

## Cable connection

Generally, the Ethernet cable can be categorized as the Medium Dependent Interface (MDI) cable and Medium Dependent Interface crossover (MDI-X) cable. MDI provides physical and electrical connection from terminal to network relay device while MDI-X provides connection between devices of the same type (terminal to terminal). Hosts and routers use MDI cables while hubs and switches use MDI-X interfaces. Usually, the connection of different devices should use the MDI cable while devices of the same type should use the MDI-X cable. Devices in auto-negotiation mode can be connected by the MDI or MDI-X cable.

The Ethernet cable of the ISCOM2600G-HI series switch supports auto-MDI/MDIX.

## 1.7.2 Default configurations of interface management

Default configurations of interface management are as below.

Function	Default value
Maximum forwarding frame length of interface	2000 bytes
Duplex mode of interface	Auto-negotiation
Interface rate	Auto-negotiation
Interval for monitoring the interface rate	5s
Interface rate statistics status	Disable
Interval of interface dynamic statistics	5s
Interface flow control status	Disable
Interface status	Enable
L2protocol peer stp status	Disable

## 1.7.3 Configuring basic attributes of interfaces

The interconnected devices cannot communicate normally if their interface attributes (such as MTU, duplex mode, and rate) are inconsistent, and then you have to adjust the interface attributes to make the devices at both ends match each other.

The Ethernet physical layer works in three modes as below:

- Half duplex: devices can receive or send messages at a time.
- Full duplex: devices can receive and send messages concurrently.
- Auto-negotiation: devices can automatically choose duplex mode by exchanging information. Once successful in negotiation, the devices at both ends of the link can work in the same duplex mode, interface rate, and flow control mode.

Configure the basic attributes of interface for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter physical layer interface configuration mode.
4	<code>Raisecom(config- gigaethernet1/1/port)#duplex { full   half   auto }</code>	Configure the duplex mode of the interface.
5	<code>Raisecom(config- gigaethernet1/1/port)#speed { auto   10   100   1000   10000 }</code>	Configure the interface rate. It depends on specifications of the optical module for the optical interface. When there is no 10 Gbit/s interface on the device, it does not support configuring the 10 Gbit/s rate.
6	<code>Raisecom(config- gigaethernet1/1/port)#tpid { 8100   9100   88a8 }</code>	(Optional) configure the interface TPID. By default, it is 0x8100.
7	<code>Raisecom(config- gigaethernet1/1/port)#jumbo frame frame-size</code>	(Optional) configure the MTU on the interface. The device supports configuring MTU on interfaces in batches.
8	<code>Raisecom(config- gigaethernet1/1/port)#mdi { xover   auto   normal }</code>	(Optional) configure the MDI/MDIX mode of the electrical interface.
9	<code>Raisecom(config- gigaethernet1/1/port)#vibration-suppress peroid second</code>	(Optional) configure the period for suppressing vibration on the interface.
10	<code>Raisecom(config)#interface tunnel interface-number</code>	Create a Tunnel interface.
11	<code>Raisecom(config- tunnel1/1/1)#tunnel source ip-address</code>	Configure the source IP address of the Tunnel interface.
12	<code>Raisecom(config- tunnel1/1/1)#tunnel destination ip-address</code>	Configure the destination IP address of the Tunnel interface.
13	<code>Raisecom(config- tunnel1/1/1)#tunnel mode ipv6ip</code>	Configure the encryption type of the Tunnel interface to IPv6 over IPv4.

## 1.7.4 Configuring interface rate statistics

Configure interface rate statistics for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.



Step	Command	Description
3	<code>Raisecom(config-gigaethernet1/1/port)#clear interface statistics</code>	Clear statistics about the interface rate.

## 1.7.5 Configuring flow control on interfaces

IEEE 802.3x is a flow control method for full duplex on the Ethernet data layer. When the client sends a request to the server, it will send the PAUSE frame to the server if there is system or network jam. Then, it delays data transmission from the server to the client.

Configure flow control on interfaces for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/port)#flowcontrol { receive   send } { off   on }</code>	Enable/Disable interface flow control over 802.3x packets. By default, it is disabled.

## 1.7.6 Shutting down/Restarting interface


Shut down/Restart an interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/port)#shutdown</code>	Shut down the current interface. Use the <b>no shutdown</b> command to re-enable the disabled interface.

## 1.7.7 Configuring Console interface

Configure the Console interface for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<b>Raisecom(config)#console open</b>	(Optional) enable the Console interface. Use this command in non-Console command lines only.   <b>Caution</b>  If you use the <b>console close</b> command to disable the Console interface, this will cause the ISCOM2600G-HI series switch to be out of control. Use it with caution.
3	<b>Raisecom(config)#login-trap enable</b>	(Optional) enable Trap sending upon user login or exit.

## 1.7.8 Configuring SNMP interface



### Note

By default, the IP address of the SNMP interface is 192.168.0.1 and the subnet mask is 255.255.255.0.

Configure the SNMP interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface fastethernet 1/0/1</b>	Enter SNMP interface configuration mode. The device supports shutdown.
3	<b>Raisecom(config-fastethernet1/0/1)#ip address ip-address [ ip-mask ]</b>	Configure the IPv4 address of the SNMP interface.
4	<b>Raisecom(config-fastethernet1/0/1)#ipv6 address ipv6-address/prefix-length [ eui-64 ]</b> <b>Raisecom(config-fastethernet1/0/1)#ipv6 address ipv6-address link-local</b>	Configure the IPv6 address of the SNMP interface.
5	<b>Raisecom(config-fastethernet1/0/1)#ip dhcp server</b>	(Optional) enable DHCP Server on the SNMP interface.
6	<b>Raisecom(config-fastethernet1/0/1)#ip dhcp client { class-id class-id   client-id client-id   hostname hostname }</b>	(Optional) configure information about the DHCP client on the SNMP interface, including the class ID, client ID, and host name.
7	<b>Raisecom(config-fastethernet1/0/1)#ip dhcp client renew</b>	(Optional) configure the IP address to be renewed for the SNMP interface.

## 1.7.9 Checking configurations


Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# <b>show interface</b> [ <b>range</b> ] [ <i>interface-type interface-number</i> ]	Show the interface status. The device supports showing blocked VLANs.
2	Raisecom# <b>show l2protocol peer stp</b> [ <i>interface-type interface-number</i> ]	Show status of L2protocol Peer STP on the interface.
3	Raisecom# <b>show interface</b> <i>interface-type interface-number</i> <b>statistics</b> [ <b>dynamic</b> ] [ <b>detail</b> ] Raisecom# <b>show interface statistics</b> <b>dynamic</b> [ <b>detail</b> ]	Show interface statistics.
4	Raisecom# <b>show interface brief</b>	Show the interface list.
5	Raisecom# <b>show interface</b> [ <i>interface-type interface-number</i> ] <b>description</b>	Show the interface description.

## 1.8 Configuring basic information

Configure basic information for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>host</b> <b>name</b> <i>name</i>	(Optional) configure the device name. The device name is within 64 characters in length, and supports special characters, such as " ", "\", "'", "<", ">", and "&". By default, the device name is Raisecom. The system supports changing device name to make users distinguish different devices on the network. Once the device name changes, it can be seen in terminal prompt.
2	Raisecom# <b>lang</b> <b>uage</b> { <b>chinese</b>   <b>english</b> }	(Optional) configure language mode. By default, the language is English.

Step	Command	Description
3	<code>Raisecom#write</code>	<p>Save configurations.</p> <p>Save configurations to the ISCOM2600G-HI series switch after configurations, and the new configurations will overwrite the original configurations.</p> <p>If new configurations are not saved, they will be lost after restarting, and the ISCOM2600G-HI series switch will continue to working with the original configurations.</p> <div>  <b>Caution</b> </div> <p>Use the <b>erase file-name</b> command to delete the configuration file. This operation cannot be rolled back, so use this command with caution.</p>
4	<code>Raisecom#reboot [ now ]</code>	<p>(Optional) configure restart options.</p> <p>When the ISCOM2600G-HI series switch fails, restart it to try to solve the problem according to actual condition.</p>
5	<code>Raisecom#show exception [ last [ count ] ]</code>	Show information about exceptional restart.
6	<code>Raisecom#clear exception</code>	Clear information about exceptional restart.
7	<code>Raisecom#show tech-support</code>	Show common system information, such as the CPU, memory, terminal connection status, and DDM.

## Caution

- Restarting the ISCOM2600G-HI series switch interrupts services, so use the command with caution.
- Save configurations before restarting to avoid loss of configurations.

## 1.9 Task scheduling

### 1.9.1 Introduction

To use some commands periodically or at a specified time, configure task scheduling.

The ISCOM2600G-HI series switch supports scheduling tasks by combining the program list with command lines. You just need to specify the start time of the task, period, and end time in the program list, and then bind the program list to command lines to implement the periodic execution of command lines.

### 1.9.2 Configuring task scheduling

Configure task scheduling for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#schedule-list list-number start date-time { mm-dd-yyyy hh:mm:ss [ every { day   week } stop mm-dd-yyyy hh:mm:ss ]   every days-interval time-interval [ stop mm-dd-yyyy hh:mm:ss ] }</b> <b>Raisecom(config)#schedule-list list-number start date-time mm-dd-yyyy hh:mm:ss every weekday-list { fri   mon   off-day   sta   sun   thu   tue   wed   working-day   weekday-list }</b> <b>Raisecom(config)#schedule-list list-number start up-time days-after-startup hh:mm:ss [ every days-interval time-interval [ stop days-after-startup hh:mm:ss ] ]</b>	Create a scheduling list, and configure it.
3	<b>Raisecom(config)#command-string schedule-list list-number</b>	Bind the command line which needs periodical execution and supports the scheduling list to the scheduling list.

## 1.9.3 Checking configurations

Use the following command to check configuration results.

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

## 1.10 Watchdog

### 1.10.1 Introduction

The external electromagnetic field interferes with the working of the Microcontroller Unit (MCU), and causes program elapsing and endless loop; consequently the system fails to work normally. To monitor the realtime running status of the MCU, a program is specially used, which is commonly known as Watchdog.

The ISCOM2600G-HI series switch will be restarted when it fails to work due to task suspension or endless loop, and it neither sends signals to restart the watchdog timer.

Watchdog can prevent the system program from endless loop due to uncertain fault, thus improving system stability.

## 1.10.2 Preparing for configurations

### Scenario

By configuring Watchdog, you can prevent the system program from endless loop due to uncertain fault, thus improving system stability.

### Prerequisite

N/A

## 1.10.3 Default configurations of Watchdog

Default configurations of Watchdog are as below.

Function	Default value
Watchdog status	Enable

## 1.10.4 Configuring Watchdog

Configure Watchdog for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#watchdog enable</b>	Enable Watchdog.

## 1.10.5 Checking configurations

Use the following command to check configuration results.

Step	Command	Description
1	<b>Raisecom#show watchdog</b>	Show Watchdog status.

## 1.11 Configuring Banner

### 1.11.1 Preparing for configurations

#### Scenario

Banner is a message to display when you log in to or exit the ISCOM2600G-HI series switch, such as the precautions or disclaimer.

You can configure the Banner of the ISCOM2600G-HI series switch as required. In addition, the ISCOM2600G-HI series switch provides the Banner switch. After Banner display is enabled, the configured Banner information appears when you log in to or exit the ISCOM2600G-HI series switch.


After configuring Banner, use the **write** command to save configurations. Otherwise, Banner information will be lost when the ISCOM2600G-HI series switch is restarted.

## Prerequisite

N/A

## 1.11.2 Configuring Banner

Configure Banner for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#banner login</b> <i>w</i> Press Enter. <i>message w</i>	Configure the Banner contents. Enter the <b>banner login</b> and <i>w</i> , press <b>Enter</b> , enter the Banner contents, and then end with the <i>w</i> character.   <b>Note</b> The <i>w</i> parameter is a character with the length of 1. It is the beginning and end marker of the Banner contents. These 2 marks must be the identical character. We recommend selecting the specified character that will not occur at the <i>message</i> . The message parameter is the Banner contents. Up to 2560 characters are supported.
3	<b>Raisecom(config)#clear banner login</b>	(Optional) clear contents of the Banner.

## 1.11.3 Enabling Banner display

Enable Banner display for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#banner enable</b>	Enable Banner display. By default, Banner display is disabled. Use the <b>banner disable</b> command to disable Banner display.

## 1.11.4 Checking configurations

Use the following commands to check configurations.

No.	Command	Description
1	<code>Raisecom#show banner login</code>	Show Banner status and contents of the configured Banner.



# 2 Ethernet

---

This chapter describes basic principles and configuration procedures for Ethernet, and provides related configuration examples, including the following sections:

- MAC address table
- VLAN
- PVLAN
- QinQ
- VLAN mapping
- STP/RSTP
- MSTP
- MRSTP
- Loop detection
- Interface protection
- Port mirroring
- L2CP
- Voice VLAN
- GARP

## 2.1 MAC address table

### 2.1.1 Introduction

The MAC address table records mappings between MAC addresses and interfaces. It is the basis for an Ethernet device to forward packets. When the Ethernet device forwards packets on Layer 2, it searches the MAC address table for the forwarding interface, implements expedited forwarding of packets, and reduces broadcast traffic.

The MAC address table contains the following information:

- Destination MAC address
- Destination MAC address related interface number
- Interface VLAN ID
- Flag bits

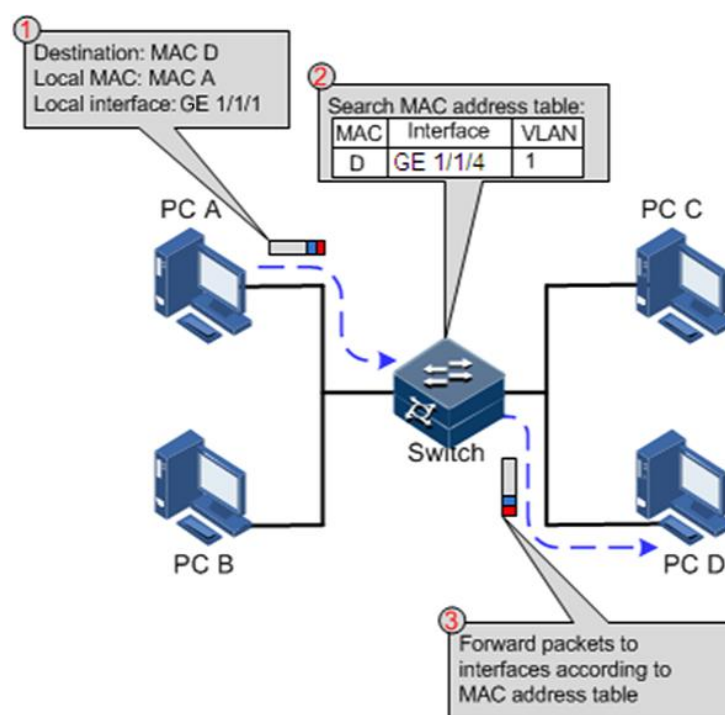
The ISCOM2600G-HI series switch supports showing MAC address information by device, interface, or VLAN.

## Forwarding modes of MAC addresses

When forwarding packets, based on the information about MAC addresses, the ISCOM2600G-HI series switch adopts the following modes:

- **Unicast:** when a MAC address entry, related to the destination MAC address of a packet, is listed in the MAC address table, the ISCOM2600G-HI series switch will directly forward the packet to the receiving interface through the egress interface of the MAC address entry. If the entry is not listed, the ISCOM2600G-HI series switch broadcasts the packet to all interfaces except the receiving interface, as shown in Figure 2-1.

Figure 2-1 Forwarding packets according to the MAC address table



- **Multicast:** when the ISCOM2600G-HI series switch receives a packet of which the destination MAC address is a multicast address, it will broadcast the packet. If multicast is enabled and storm control over unknown packets is also enabled, the packet will be sent to the specified Report interface. If no Report interface is specified, the packet will be discarded.
- **Broadcast:** when the ISCOM2600G-HI series switch receives an all-F packet, or the MAC address is not listed in the MAC address table, the ISCOM2600G-HI series switch forwards the packet to all interfaces except the interface that receives this packet. Broadcast addresses are special multicast addresses.

## Classification of MAC addresses

MAC address table is divided into static address entry and dynamic address entry.

- **Static MAC address entry:** also called permanent address, added and removed by the user manually, not aged with time. For a network with small changes of devices, adding

static address entry manually can reduce the network broadcast flow, improve the security of the interface, and prevent entries from being lost after the system is reset.

- Dynamic MAC address entry: the ISCOM2600G-HI series switch can add dynamic MAC address entries through MAC address learning. The entries are aged according to the configured aging time, and will be empty after the system is reset.

## Aging time of MAC addresses

There is limit on the capacity of the MAC address table on the ISCOM2600G-HI series switch. To maximize the use of the MAC address table, the ISCOM2600G-HI series switch uses the aging mechanism to update the MAC address table. For example, when the ISCOM2600G-HI series switch creates a dynamic entry, it starts the aging timer. If it does not receive packets from the MAC address in the entry during the aging time, the ISCOM2600G-HI series switch will delete the entry.

The ISCOM2600G-HI series switch supports automatic aging of MAC addresses. The aging time ranges from 10s to 1000000s and can be 0. The value 0 indicates no aging.



### Note

The aging mechanism takes effect on dynamic MAC addresses.

## Forwarding policies of MAC addresses

The MAC address table has two forwarding policies:

When receiving packets on an interface, the ISCOM2600G-HI series switch searches the MAC address table for the interface related to the destination MAC address of packets.

- If successful, it forwards packets on the related interface, records the source MAC addresses of packets, interface number of ingress packets, and VLAN ID in the MAC address table. If packets from other interface are sent to the MAC address, the ISCOM2600G-HI series switch can send them to the related interface.
- If failed, it broadcasts packets to all interfaces except the source interface, and records the source MAC address in the MAC address table.

## MAC address limit

The MAC address limit is used to limit the number of MAC addresses, avoid extending the searching time of forwarding entry caused by a too large MAC address table and degrading the forwarding performance of the Ethernet switch, and it is effective to manage the MAC address table.

The MAC address limit improves the speed of forwarding packets.

## 2.1.2 Preparing for configurations

### Scenario

Configure the static MAC address table in the following situations:

- The static MAC address can be configured for a fixed server, special persons (manager, financial staff), fixed and important hosts to ensure that all data flow forwarding to these MAC addresses are forwarded from static MAC address related interface in priority.

- For the interface with fixed static MAC address, you can disable MAC address learning to avoid other hosts visiting LAN data from the interface.

Configure the aging time of dynamic MAC addresses to avoid saving excessive MAC address entries in the MAC address table and running out of MAC address table resources, and to achieve aging of dynamic MAC addresses.

## Prerequisite

N/A

## 2.1.3 Default configurations of MAC address table

Default configurations of the MAC address table are as below.

Function	Default value
MAC address learning status	Enable
MAC address aging time	300s
MAC address limit	Unlimited

## 2.1.4 Configuring static MAC address

Configure static MAC address as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mac-address static unicast</b> <i>mac-address vlan vlan-id interface-type interface-number</i>	Configure static unicast MAC addresses.



### Note

The MAC address of the source device, multicast MAC address, FFFF.FFFF.FFFF, and 0000.0000.0000 cannot be configured as static unicast MAC address.

## 2.1.5 Configuring blackhole MAC address

Configure blackhole MAC addresses as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mac-address blackhole</b> <i>mac-address vlan vlan-id</i>	Configure blackhole MAC addresses.

## 2.1.6 Filtering unknown multicast packets

Filter unknown multicast packets for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mac-address multicast drop-unknown { reserved- address   vlan vlan-list }</b>	(Optional) filter unknown multicast packets.

## 2.1.7 Configuring MAC address learning

Configure MAC address learning for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config- gigaethernet1/1/port)#mac-address learning enable { interface-type interface-number   vlanlist vlan- list }</b>	Enable MAC address learning.

## 2.1.8 Configuring MAC address limit

Configure the MAC address limit for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config- gigaethernet1/1/port)#mac-address threshold threshold-value</b>	Configure interface-based MAC address limit.

## 2.1.9 Configuring aging time of MAC addresses

Configure the aging time of MAC addresses for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<b>Raisecom(config)#mac-address aging-time { 0   period }</b>	Configure the aging time of MAC addresses.

## 2.1.10 Enabling suppression of MAC address flapping

Enable suppression of MAC address flapping for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mac-address mac-move enable</b>	Enabling global suppression of MAC address flapping.

## 2.1.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show mac-address static</b> [ <i>interface-type interface-number</i>   <i>vlan vlan-id</i> ]	Show static unicast MAC addresses.
2	<b>Raisecom#show mac-address multicast</b> [ <i>vlan vlan-id</i> ] [ <i>count</i> ]	Show Layer 2 multicast addresses or the number of existing multicast MAC address.
3	<b>Raisecom#show mac-address blackhole</b>	Show the blackhole MAC address.
4	<b>Raisecom#show mac-address threshold</b> [ <i>interface-type interface-number</i>   <i>vlan vlan-list</i> ]	Show the dynamic MAC address limit.
5	<b>Raisecom#show mac-address aging-time</b>	Show the aging time of dynamic MAC addresses.
6	<b>Raisecom#show mac-address learning</b> [ <i>interface-type interface-list</i> ] [ <i>vlan</i> ]	Show status of MAC address learning.
7	<b>Raisecom#show mac-address count</b> [ <i>vlan vlan-id</i> ] [ <i>interface-type interface-number</i> ]	Show the number of MAC address entries.

## 2.1.12 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
<code>Raisecom(config)#clear mac-address [ mac-address ] { all   dynamic   blackhole   static }</code>	Clear MAC addresses.
<code>Raisecom(config)#clear mac-address { all   dynamic   static } [ vlan vlan-id ] interface-type interface-number</code>	Clear MAC addresses of a specified interface.
<code>Raisecom(config)#clear mac-address blackhole vlan vlan-id</code>	Clear blackhole MAC address entries in a specified VLAN.
<code>Raisecom(config)#search mac-address mac-address { all   dynamic   static } [ interface-type interface-number ] [ vlan vlan-id ]</code>	Search for a MAC address.

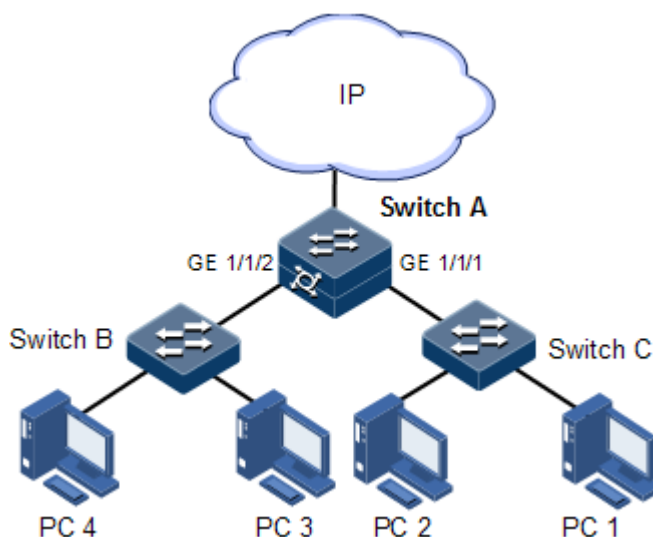
## 2.1.13 Example for configuring MAC address table

### Networking requirements

As shown in Figure 2-2, configure Switch A as below:

- Configure a static unicast MAC address 0001.0203.0405 on GE 1/1/2 and configure its VLAN to VLAN 10.
- Configure the aging time to 500s.

Figure 2-2 MAC networking



### Configuration steps

Step 1 Create VLAN 10, and activate it, and add GE 1/1/2 to VLAN 10.

```

Raisecom#config
Raisecom(config)#create vlan 10 active
  
```

```
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#switchport mode access
Raisecom(config-gigabitEthernet1/1/2)#switchport access vlan 10
Raisecom(config-gigabitEthernet1/1/2)#exit
```

- Step 2 Configure a static unicast MAC address 0001.0203.0405 on GE 1/1/2, which belongs to VLAN 10.

```
Raisecom(config)#mac-address static unicast 0001.0203.0405 vlan 10
gigabitEthernet 1/1/2
```

- Step 3 Configure the aging time to 500s.

```
Raisecom(config)#mac-address aging-time 500
```

## Checking results

Use the **show mac-address** to show configurations of MAC addresses.

```
Raisecom#show mac-address all gigabitEthernet 1/1/2
Aging time: 500 seconds
Mac Address      Port                      Vlan    Flags
-----
0001.0203.0405   gigabitEthernet1/1/2      10      Static
```

## 2.2 VLAN

### 2.2.1 Introduction

#### Overview

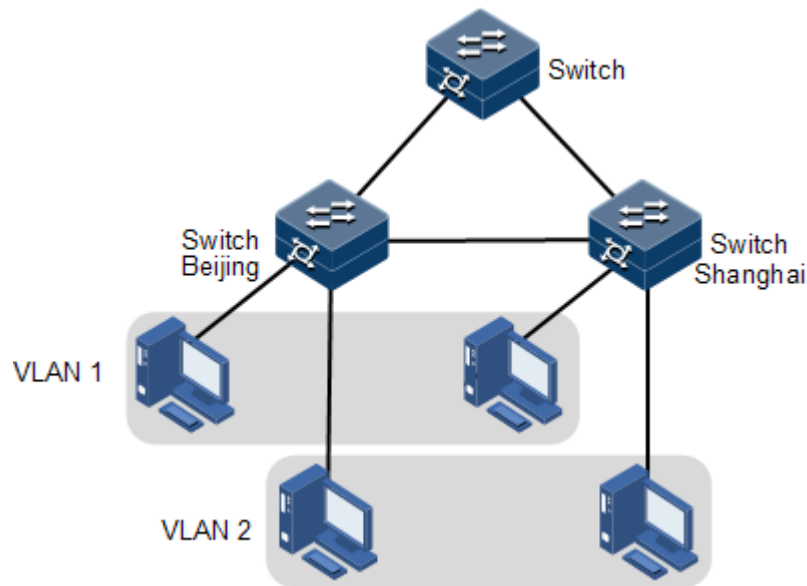
Virtual Local Area Network (VLAN) is a protocol to solve Ethernet broadcast and security problem. It is a Layer 2 isolation technique that partitions a LAN into different broadcast domains logically rather than physically, and then the different broadcast domains can work as virtual groups without any influence from one another. In terms of functions, VLAN has the same features as LAN, but members in one VLAN can access one another without restriction by physical location.

#### VLAN partitions

There are multiple ways of VLAN partitions, such as by interface, by MAC address, by IP subnet, and by protocol, as shown in Figure 2-3.



Figure 2-3 VLAN partitions



VLAN technique can partition a physical LAN into different broadcast domains logically. Hosts without intercommunication requirements can be isolated by VLAN, so VLAN partitions improve network security, and reduce broadcast flow and broadcast storm.

The ISCOM2600G-HI series switch complies with IEEE 802.1Q standard VLAN and supports 4094 concurrent VLANs.

- VLAN partitions by interface

The ISCOM2600G-HI series switch supports VLAN partitions by interface. The ISCOM2600G-HI series switch has two interface modes: Access mode and Trunk mode. The method for processing packets for the two modes is shown as below.

Table 2-1 Interface mode and packet processing

Interface type	Processing ingress packets		Processing egress packets
	Untagged packets	Tagged packets	
Access	Add the Access VLAN Tag to the packet.	<ul style="list-style-type: none"> <li>• If the VLAN ID of the packet is equal to the Access VLAN ID, the interface will receive the packet.</li> <li>• If the VLAN ID of the packet is not equal to the Access VLAN ID, the interface will discard the packet.</li> </ul>	<ul style="list-style-type: none"> <li>• If the VLAN ID of the packet is equal to the Access VLAN ID, the interface will remove the Tag and send the packet.</li> <li>• If the VLAN ID of the packet is excluded from the list of VLANs of which packets are allowed to pass by the interface, the interface will discard the packet.</li> </ul>

Interface type	Processing ingress packets		Processing egress packets
	Untagged packets	Tagged packets	
Trunk	Add the Native VLAN Tag to the packet.	<ul style="list-style-type: none"> <li>• If the VLAN ID of the packet is included in the list of VLANs of which packets are allowed to pass by the interface, the interface will receive the packet.</li> <li>• If the VLAN ID of the packet is excluded from the list of VLANs of which packets are allowed to pass by the interface, the interface will discard the packet.</li> </ul>	<ul style="list-style-type: none"> <li>• If the VLAN ID of the packet of the packet is equal to the Native VLAN ID, the interface will remove the Tag and send the packet.</li> <li>• If the VLAN ID of the packet is not equal to the Native VLAN ID and the interface allows packets of the VLAN to pass, the interface will keep the original Tag and send the packet.</li> </ul>

- VLAN partitions by MAC address

This refers to VLAN partitions by the source MAC address of the packet.

- When an interface receives an untagged packet, it matches the source MAC address of the packet with the VLAN MAC addresses. If they are the same, the match is successful. In this case, the interface adds the VLAN ID specified by VLAN MAC addresses, and forwards the packet. If they are different, the interface continues to match the packet with the IP address-based VLAN and interface-based VLAN in descending order.
- When a tagged packet reaches an interface, if its VLAN ID is in the VLAN ID list allowed to pass by the interface, the interface receives it. Otherwise, the interface discards it.

- VLAN partitions by IP subnet

This refers to VLAN partitions by the source IP subnet of the packet.

- When an interface receives an untagged packet, it determines the VLAN of the packet by the source IP subnet of the packet, and then transmits the packet in the specified VLAN.
- When a tagged packet reaches an interface, if its VLAN ID is in the VLAN ID list allowed to pass by the interface, the interface receives it. Otherwise, the interface discards it.

- VLAN partitions by protocol

This refers to VLAN partitions by the protocol type carried in the packet received by the interface and assigning different VLAN IDs for packets. The protocol VLAN is defined by the protocol profile. One interface can be associated with multiple protocol profiles. After an interface is associated with protocol VLANs, it will process packets as below:

- After receiving an untagged packet from an interface, the device adds the VLAN Tag of the protocol VLAN defined by the protocol profile if the packet matches the protocol profile, or adds the default VLAN Tag if the packet does not match the protocol profile.
- When receiving a tagged packet from an interface, the device receives the packet if the VLAN ID is in the list of VLANs of which packets are allowed to pass by the interface,

or discards the packet if the VLAN ID is not in the list of VLANs of which packets are allowed to pass by the interface.

## 2.2.2 Preparing for configurations

### Scenario

The main function of VLAN is to partition logic network segments. There are 2 typical application modes:

- One kind is that in a small LAN several VLANs are created on a device, the hosts that connect to the device are divided by VLAN. So hosts in the same VLAN can communicate, but hosts between different VLANs cannot communicate. For example, the financial department needs to be separated from other departments and they cannot access each other. Generally, the interface to connect host is in Access mode.
- The other kind is that in bigger LAN or enterprise network multiple devices connect to multiple hosts and the devices are cascaded, and data packets carry VLAN Tag for forwarding. The interfaces in the same VLAN on multiple devices can communicate, but the interfaces in different VLANs cannot communicate. This mode is used in enterprise that has many employees and needs a large number of hosts, in the same department but different position, the hosts in one department can access one another, so users have to partition VLANs on multiple devices. Layer 3 devices, such as routers, are required if users want to communicate among different VLANs. The cascaded interfaces among devices are configured in Trunk mode.

When configuring the IP address for VLAN, you can associate a Layer 3 interface for it. Each Layer 3 interface corresponds to one IP address and one VLAN.

### Prerequisite

N/A

## 2.2.3 Default configurations of VLAN

Default configurations of VLAN are as below.

Function	Default value
Create VLAN	VLAN 1 and VLAN 4093
Active status of static VLAN	Active
Interface mode	Access
Access VLAN	VLAN 1
Native VLAN of Trunk interface	VLAN 1
Allowable VLAN in Trunk mode	VLAN 1
Allowable untagged VLAN in Trunk mode	VLAN 1
VLAN mapping table ID	VLAN ID

## 2.2.4 Configuring VLAN attributes

Configure VLAN attributes for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#create vlan <i>vlan-list</i> active</b>	Create a VLAN. The command can also be used to create VLANs in batches.
3	<b>Raisecom(config)#vlan vlan-id</b>	Enter VLAN configuration mode.
4	<b>Raisecom(config- vlan)#name <i>vlan-name</i></b>	(Optional) configure the VLAN name.



### Note

- The VLAN created by the **vlan *vlan-id*** command is in active status.
- All configurations of VLAN do not take until the VLAN is activated.

## 2.2.5 Configuring interface mode

Configure the interface mode for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config- gigaetherent1/1/port)#switchport mode { access   trunk }</b>	Configure the interface to Access or Trunk mode.

## 2.2.6 Configuring VLAN on Access interface

Configure the VLAN on the Access interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config- gigaetherent1/1/port)#switchport mode access</b> <b>Raisecom(config- gigaetherent1/1/port)#switchport access vlan <i>vlan-id</i></b>	Configure the interface to Access mode, and add the Access interface to the VLAN.

Step	Command	Description
4	Raisecom(config-gigaetherne1/1/port)# <b>switchport access egress-allowed vlan</b> { all   [ add   remove ] <i>vlan-list</i> }	(Optional) configure the VLAN allowed to pass by the Access interface.



## Note

- The interface allows Access VLAN packets to pass regardless of configuration for VLAN allowed by the Access interface. The forwarded packets do not carry the VLAN Tag.
- When configuring the Access VLAN, the system creates and activates a VLAN automatically if you have not created and activated a VLAN in advance.
- If you delete the Access VLAN manually, the system will automatically configure the interface Access VLAN as the default VLAN.
- When you configure the interface Access VLAN as the non-default Access VLAN, the default Access VLAN 1 is the VLAN allowed by the Access the egress interface, you can delete Access VLAN 1 from the allowed VLAN list of the egress Access interface.
- If the configured Access VLAN is not the default VLAN and there is no default VLAN in the allowed VLAN list of the Access interface, the interface does not allow packets of the default VLAN to pass.
- The allowed VLAN list of the Access interface is effective to static VLANs only, and ineffective to cluster VLAN, GVRP dynamic VLAN, and so on.

## 2.2.7 Configuring VLAN on Trunk interface

Configure the VLAN on the Trunk interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaetherne1/1/port)# <b>switchport mode trunk</b>	Configure the interface to Trunk mode.
4	Raisecom(config-gigaetherne1/1/port)# <b>switchport trunk native vlan</b> <i>vlan-id</i>	Configure the Native VLAN of the interface.
5	Raisecom(config-gigaetherne1/1/port)# <b>switchport trunk allowed vlan</b> { all   [ add   remove ] <i>vlan-list</i> }	(Optional) configure VLANs allowed to pass by the Trunk interface.
6	Raisecom(config-gigaetherne1/1/port)# <b>switchport trunk untagged vlan</b> { all   [ add   remove ] <i>vlan-list</i> }	(Optional) configure VLANs from which the Trunk interface can remove Tag.



## Note

- The system will create and activate the VLAN if no VLAN is created and activated in advance when configuring the Native VLAN.
- The system configures the interface Trunk Native VLAN as default VLAN if you have deleted or blocked Native VLAN manually.
- The interface allows incoming and outgoing VLAN packet allowed by the Trunk interface. If the VLAN is Trunk untagged VLAN, the VLAN Tag is removed from the packets at the egress interface. Otherwise the packets are not modified.
- When configuring Trunk untagged VLAN list, the system automatically adds all untagged VLAN to the VLAN allowed by the Trunk interface.
- The VLAN list and untagged VLAN list allowed by the Trunk interface are only effective to static VLAN, and ineffective for cluster VLAN, GVRP dynamic VLAN.

## 2.2.8 Configuring VLAN based on MAC address

Configure the VLAN based on MAC address for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mac-vlan</b> <i>mac-address</i> [ <b>mask</b> <i>mac-address-mask</i> ] <b>vlan</b> <i>vlan-id</i> [ <b>priority</b> <i>value</i> ]	Associate a MAC address with a VLAN.
3	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config-gigaethernet1/1/port)#mac-vlan enable</b>	Enable MAC-VLAN.
5	<b>Raisecom(config-gigaethernet1/1/port)#vlan precedence</b> { <b>mac-vlan</b>   <b>ip-subnet-vlan</b> }	(Optional) configure priorities of MAC-VLAN and IP subnet VLAN.



## Caution

- If the IP address or subnet mask is invalid, the configuration will fail.
- If you associate a created IP subnet to a VLAN but this association conflict with an existing association (for example, the IP subnet or VLAN is already associated), the association will fail.

## 2.2.9 Configuring VLAN based on IP subnet

Configure the VLAN based on IP subnet for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip-subnet-vlan</b> <i>ip-address</i> [ <i>ip-mask</i> ] <b>vlan</b> <i>vlan-id</i> [ <b>priority</b> <i>value</i> ]	Associate a MAC address with an IP subnet.

Step	Command	Description
3	Raisecom(config)# <b>interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	Raisecom(config-gigaetherne <sup>t</sup> 1/1/port)# <b>ip-subnet-vlan enable</b>	Enable VLAN partitions based on IP subnet.
5	Raisecom(config-gigaetherne <sup>t</sup> 1/1/port)# <b>vlan precedence { mac-vlan   ip-subnet-vlan }</b>	(Optional) configure priorities of MAC-VLAN and IP subnet VLAN.



### Caution

- If the IP address or subnet mask is invalid, the configuration will fail.
- If you associate a created IP subnet to a VLAN but this association conflict with an existing association (for example, the IP subnet is associated with different VLANs), the association will fail.

## 2.2.10 Configuring VLAN based on IP subnet

Configure the VLAN based on IP subnet for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>protocol-vlan</b> <i>protocol-index { ipv4   ipv6   ether<sup>t</sup>type protocol-id }</i>	Configure the rule for associating the protocol VLAN with Ethernet packets.
3	Raisecom(config)# <b>interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	Raisecom(config-gigaetherne <sup>t</sup> 1/1/port)# <b>switchport protocol-vlan</b> <i>protocol-index vlan-id</i>	Configure the rule for associating the interface with the protocol VLAN.

## 2.2.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# <b>show vlan</b> [ <i>vlan-list</i>   <b>static</b>   <b>dynamic</b> ] [ <b>detail</b> ]	Show VLAN configurations.
2	Raisecom# <b>show mac-vlan</b> [ <b>mask</b>   <b>efficient</b> ] { <b>all</b>   <b>vlan</b> <i>vlan-id</i> }	Show MAC VLAN configurations.

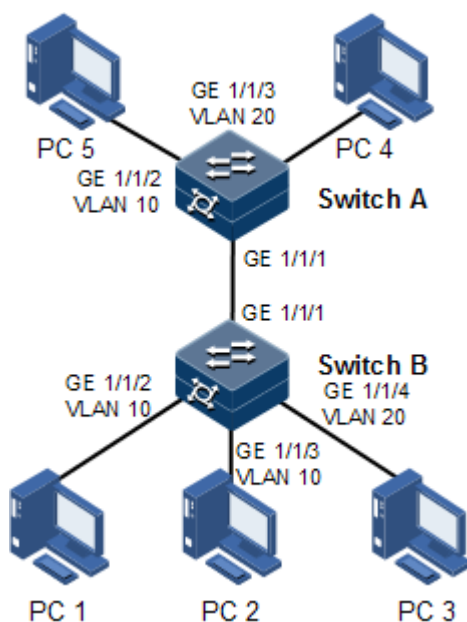
No.	Command	Description
3	<b>Raisecom#show mac-vlan aging-time</b>	Show the aging time of MAC VLANs.
4	<b>Raisecom#show switchport</b> <i>interface-type interface-number</i>	Show VLAN configurations on the interface.
5	<b>Raisecom#show protocol-vlan all</b>	Show configurations of all protocol VLANs.
6	<b>Raisecom#show protocol-vlan</b> <b>interface</b> <i>interface-type</i> <i>interface-number</i>	Show configurations of the protocol VLAN on the interface.

## 2.2.12 Example for configuring VLAN

### Networking requirements

As shown in Figure 2-4, PC 1, PC 2, and PC 5 belong to VLAN 10, PC 3 and PC 4 belong to VLAN 20; Switch A and Switch B are connected by the Trunk interface; PC 3 and PC 4 cannot communicate because VLAN 20 is not allowed to pass in the link; PC 1 and PC 2 under the same Switch B are enabled with interface protection function so that they cannot communicate with each other, but can respectively communicate with PC 5.

Figure 2-4 VLAN and interface protection networking



### Configuration steps

- Step 1 Create VLAN 10 and VLAN 20 on the two switches respectively, and activate them.  
Configure Switch A.



```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#create vlan 10,20 active
```

Configure Switch B.

```
Raisecom#name SwitchB
SwitchB#config
SwitchB(config)#create vlan 10,20 active
```

- Step 2 Add GE 1/1/2 and GE 1/1/3 in Access mode on Switch B to VLAN 10, add GE 1/1/4 as Access mode to VLAN 20, configure GE 1/1/1 to Trunk mode, and allow VLAN 10 to pass.

```
SwitchB(config)#interface gigabitEthernet 1/1/2
SwitchB(config-gigabitEthernet1/1/2)#switchport mode access
SwitchB(config-gigabitEthernet1/1/2)#switchport access vlan 10
SwitchB(config-gigabitEthernet1/1/2)#exit
SwitchB(config)#interface gigabitEthernet 1/1/3
SwitchB(config-gigabitEthernet1/1/3)#switchport mode access
SwitchB(config-gigabitEthernet1/1/3)#switchport access vlan 10
SwitchB(config-gigabitEthernet1/1/3)#exit
SwitchB(config)#interface gigabitEthernet 1/1/4
SwitchB(config-gigabitEthernet1/1/4)#switchport mode access
SwitchB(config-gigabitEthernet1/1/4)#switchport access vlan 20
SwitchB(config-gigabitEthernet1/1/4)#exit
SwitchB(config)#interface gigabitEthernet 1/1/1
SwitchB(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchB(config-gigabitEthernet1/1/1)#switchport trunk allowed vlan 10
confirm
SwitchB(config-gigabitEthernet1/1/1)#exit
```

- Step 3 Add GE 1/1/2 as Access mode on Switch A to VLAN 10, add GE 1/1/3 as Access mode to VLAN 20, configure GE 1/1/1 to Trunk mode, and allow VLAN 10 to pass.

```
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#switchport mode access
SwitchA(config-gigabitEthernet1/1/2)#switchport access vlan 10
SwitchA(config-gigabitEthernet1/1/2)#exit
SwitchA(config)#interface gigabitEthernet 1/1/3
SwitchA(config-gigabitEthernet1/1/3)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/3)#switchport trunk native vlan 20
SwitchA(config-gigabitEthernet1/1/3)#exit
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/1)#switchport trunk allowed vlan 10
confirm
```

## Checking results

Use the **show vlan** command to show VLAN configurations.

Take Switch B for example.

```
SwitchB#show vlan
```

```
Switch Mode: --
```

VLAN	Name	State	Status	Priority	Member-Ports
------	------	-------	--------	----------	--------------

1	Default	active	static	--	P 1-6
2	VLAN0002	active	other	--	P 1-28
10	VLAN0010	active	static	--	gigaethernet1/1/2
					gigaethernet1/1/3
20	VLAN0020	active	static	--	gigaethernet1/1/4

Use the **show switchport interface** *interface-type interface-number* command to show configurations of the interface VLAN.

Take Switch B for example.

```
SwitchB#show switchport interface gigaethernet 1/1/2
```

```
Interface: gigaethernet1/1/2
```

```
Switch Mode: switch
```

```
Reject frame type: none
```

```
Administrative Mode: access
```

```
Operational Mode: access
```

```
Access Mode VLAN: 10
```

```
Administrative Access Egress VLANs:
```

```
Operational Access Egress VLANs: 10
```

```
Trunk Native Mode VLAN: 1
```

```
Trunk Native VLAN: untagged
```

```
Administrative Trunk Allowed VLANs:
```

```
Operational Trunk Allowed VLANs: 1
```

```
Administrative Trunk Untagged VLANs:
```

```
Operational Trunk Untagged VLANs: 1
```

```
Administrative private-vlan host-association: 1
```

```
Administrative private-vlan mapping: 1
```

```
Operational private-vlan: --
```

Check whether the Trunk interface permitting VLAN passing is correct by making PC 1 ping PC 5, PC 2 ping PC 5, and PC 3 ping PC 4.

- PC 1 can ping through PC 5, so VLAN 10 communication is normal.
- PC 2 can ping through PC 5, so VLAN 10 communication is normal.
- PC 3 fails to ping through PC 4, so VLAN 20 communication is abnormal.

## 2.3 PVLAN

### 2.3.1 Introduction

Private VLAN (PVLAN) provides Layer 2 isolation between interfaces in a VLAN, and it is effective to distribute VLAN resources.

#### PVLAN type

VLANs are divided into two types: primary VLAN and secondary VLAN. The primary VLAN and secondary VLAN form a PVLAN domain. The primary VLAN can communicate both in and out of PVLANs, but the secondary VLAN can communicate in the PVLAN only.

- Primary VLAN: each PVLAN can be configured with only one primary VLAN. Interface of all types in PVLAN are members of primary VLAN.
- Secondary VLAN: it can be divided into isolated VLAN and community VLAN according to the different forwarding and isolation rules.
  - Isolated VLAN: each PVLAN can be configured with only one isolated VLAN.
  - Community VLAN: each PVLAN can be configured with multiple community VLANs.

#### Interface modes of PVLAN

The interface to be able to communicate with the external network is called the Promiscuous interface. The interface in the secondary VLAN is the Host interface.

- Promiscuous interface: it belongs to all PVLANs in the PVLAN domain. It can communicate with all interfaces.
- Isolated interface: isolated interfaces cannot communicate with each other, but they can communicate with the Promiscuous interface and Trunk interface.
- Community interface: community interfaces in a community can communicate with each other, but community interfaces in different communities cannot communicate with each other. All community interfaces can communicate with the Promiscuous interface and Trunk interface.

### 2.3.2 Preparing for configuration

#### Scenario

PVLAN, used on an enterprise Intranet, allows devices inside the VPLAN to communicate with the default gateway only rather than the Intranet.

#### Prerequisite

Create a static VLAN and activate it.

### 2.3.3 Default configurations of PVLAN

Default configurations of PVLAN are as below.

Function	Default value
PVLAN mode on the interface	Access mode

## 2.3.4 Configuring PVLAN type

Configure the PVLAN type for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#private-vlan</b> <b>{ primary vlan <i>vlan-id</i>   isolated</b> <b>vlan <i>vlan-id</i>   community</b> <b>vlan <i>vlan-list</i> }</b>	Configure the PVLAN type.



### Caution

- Up to 32 primary VLANs and 2048 secondary VLANs are allowed.
- If the VLAN is associated, its PVLAN type cannot be modified nor deleted.

## 2.3.5 Configuring PVLAN association

Configure PVLAN association for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#private-vlan</b> <b>{ primary vlan <i>vlan-id</i>   isolated</b> <b>vlan <i>vlan-id</i>   community</b> <b>vlan <i>vlan-list</i> }</b>	Configure the PVLAN type.
3	<b>Raisecom(config)#private-vlan</b> <b>association <i>primary-vlan-id</i> [ add  </b> <b>remove ] <i>secondary-vlan-list</i></b>	Configuration association of the primary VLAN and secondary VLANs.



### Caution

- Before configuring VLAN association, create a VLAN and activate it, configure PVLAN type, configure the primary VLAN and secondary VLANs, and choose the correct association type. Otherwise, VLAN association cannot be configured.
- The primary VLAN and secondary VLANs cannot be configured to the default VLAN 1. If VLAN 2 is the cluster VLAN, it cannot be configured as the PVLAN.
- A secondary VLAN can be added to only one PVLAN.
- A primary VLAN can be associated with only one isolated VLAN, or up to 64 secondary VLANs.

## 2.3.6 Configuring PVLAN mode on interface

The VLAN of the ISCOM2600G-HI series switch supports Access and Trunk interface modes, and the PVLAN supports promiscuous interface mode and host interface mode.



### Caution

- The promiscuous interface mode and host interface mode can be configured with association or mapping which already exists. Otherwise, the configuration will fail.
- When an interface is configured to the host interface mode or promiscuous interface mode without being associated with or mapped to a primary VLAN or secondary VLAN, the interface allows untagged packets to enter.
- IGMP runs on the primary VLAN only. The VLANs to data flow to pass in uplink and downlink of PVLAN are different, so you cannot configure IGMP Snooping to implement multicast; instead, you need to configure IGMP MVR.

Configure the PVLAN mode on the interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#switchport mode private-vlan { host  promiscuous }</code>	Configure the PVLAN mode on the interface.
4	<code>Raisecom(config- gigaethernet1/1/1)#exit</code>	Return to global configuration mode.
5	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter physical layer interface configuration mode.
6	<code>Raisecom(config- gigaethernet1/1/1)#switchport private-vlan host-association primary-vlan-id secondary- vlan-id</code>	Associate the primary VLAN of the host interface with the secondary VLAN.  Use the <b>no switchport private-vlan host-association</b> command to delete the association between the primary VLAN of the host interface with the secondary VLAN.
7	<code>Raisecom(config- port)#switchport private-vlan trunk host-association secondary-vlan-id</code>	Configure the host interface associated with the secondary VLAN to be able to forward tagged packets.  Use the <b>no switchport private-vlan trunk host-association</b> command to delete this configuration.

Step	Command	Description
8	<code>Raisecom(config-gigaethernet1/1/1)#switchport private-vlan mapping primary-vlan-id [ add   remove ] secondary-vlan-list</code>	Configure the mapping of the primary VLAN and secondary VLANs on the promiscuous interface.  Use the <b>no switchport private-vlan mapping</b> command to delete the association between the primary VLAN of the promiscuous interface with the secondary VLAN.
9	<code>Raisecom(config-port)#switchport private-vlan trunk mapping primary-vlan-id</code>	Configure the interface mapped with the primary VLAN to be able to forward tagged packets.  Use the <b>no switchport private-vlan trunk mapping</b> command to delete this configuration.

## 2.3.7 Checking configuration

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show vlan private-vlan</code>	Show PVLAN configuration.
2	<code>Raisecom#show switchport interface interface-type interface-number</code>	Show configuration of interface VLAN attributes.
3	<code>Raisecom#show vlan [ vlan-list   static   dynamic ] [ detail ]</code>	Show configuration of VLAN attributes.

## 2.3.8 Example for configuring PVLAN

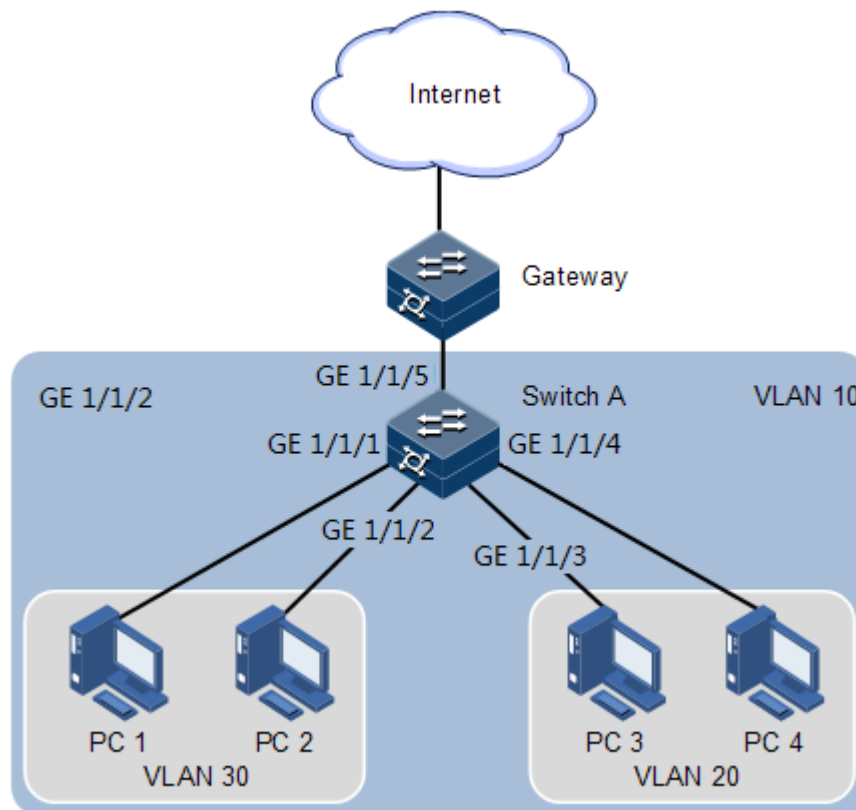
### Networking requirements

To effectively distribute VLAN resources, you need to properly partition and configure VLANs. As shown in Figure 2-5, on Switch A, configure VLAN 10 as the primary VLAN, VLAN 20 as the isolated VLAN, and VLAN 30 as the community VLAN. The detailed configurations are as below:

- Configure GE 1/1/1 and GE 1/1/2 as community interfaces. Associate primary VLAN 10 with secondary VLAN 30.
- Configure GE 1/1/3 and GE 1/1/4 as isolated interfaces. Associate primary VLAN 10 with secondary VLAN 20.
- Configure GE 1/1/5 as the promiscuous interface. Map PVLAN with VLAN 10, VLAN 20, and VLAN 30.
- Connect PC 1 and PC 2 to community interfaces GE 1/1/1 and GE 1/1/2 respectively, and they can communicate with these two interfaces and the promiscuous interface GE 1/1/5.

- Connect PC 3 and PC 4 to isolated interfaces GE 1/1/1 and GE 1/1/2 respectively, and they can communicate with the promiscuous interface GE 1/1/1 only.

Figure 2-5 Networking with PVLAN



## Configuration steps

Step 1 Configure the PVLAN type.

```
Raisecom#config
Raisecom(config)#create vlan 10,20,30 active
Raisecom(config)#private-vlan primary vlan 10
Raisecom(config)#private-vlan community vlan 30
Raisecom(config)#private-vlan isolated vlan 20
Raisecom(config)#private-vlan association 10 20,30
```

Step 2 Configure the promiscuous interface mode and mapping of the primary VLAN and secondary VLAN on the promiscuous interface.

```
Raisecom(config)#interface gigabitEthernet 1/1/5
Raisecom(config-gigabitEthernet1/1/5)#switchport mode private-vlan
promiscuous
Raisecom(config-gigabitEthernet1/1/5)#switchport private-vlan mapping 10
20,30
```

```
Raisecom(config-gigaethernet1/1/5)#exit
```

- Step 3 Configure the host interface mode and association of the primary VLAN with the secondary VLAN on the host interface.

Configuration on GE 1/1/1 and GE 1/1/2, GE 1/1/3 and GE 1/1/4 are identical. Take GE 1/1/1 and GE 1/1/3 for example.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode private-vlan host
Raisecom(config-gigaethernet1/1/1)#switchport private-vlan host-
association 10 30
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#switchport mode private-vlan host
Raisecom(config-gigaethernet1/1/3)#switchport private-vlan host-
association 10 20
```

## Checking results

Use the **show vlan private-vlan** command to show PVLAN configurations on the ISCOM2600G-HI series switch.

```
Raisecom#show vlan private-vlan
VLAN ID: 10
Pvlan type: primary
Port-list: GE1/1/5,1/1/1-2
Associated-vlans: 20,30

VLAN ID: 20
Pvlan type: isolate
Port-list: GE1/1/5
Associated-vlans: 10

VLAN ID: 30
Pvlan type: community
Port-list: GE1/1/5,1/1/1
Associated-vlans: 10
```

Use the **show interface interface-type interface-number switchport** command to show configurations of VLAN attributes on the promiscuous interface GE 1/1/5, community interface GE 1/1/1, and isolated interface GE 1/1/3.

```
Raisecom#show interface gigaethernet 1/1/5 switchport
Interface: gigaethernet1/1/5
Reject frame type: none
Administrative Mode: promiscuous
```



```
Operational Mode: promiscuous
Access Mode VLAN: 1
Administrative Access Egress VLANs:
Operational Access Egress VLANs: 1
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: N/A
Administrative Trunk Untagged VLANs:
Operational Trunk Untagged VLANs: N/A
Administrative private-vlan host-association: 1
Administrative private-vlan mapping: 10 20,30
Operational private-vlan: 10 20,30
```

```
Raisecom#show interface gigabitEthernet 1/1/1 switchport
Interface: gigabitEthernet1/1/1
Reject frame type: none
Administrative Mode: host
Operational Mode: host
Access Mode VLAN: 1
Administrative Access Egress VLANs:
Operational Access Egress VLANs: 1
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: N/A
Administrative Trunk Untagged VLANs:
Operational Trunk Untagged VLANs: N/A
Administrative private-vlan host-association: 10 30
Administrative private-vlan mapping: 1
Operational private-vlan: 10 30
```

```
Raisecom#show interface gigabitEthernet 1/1/3 switchport
Interface: gigabitEthernet 1/1/3
Reject frame type: none
Administrative Mode: host
Operational Mode: host
Access Mode VLAN: 1
Administrative Access Egress VLANs:
Operational Access Egress VLANs: 1
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: N/A
Administrative Trunk Untagged VLANs: N/A
Operational Trunk Untagged VLANs: N/A
Administrative private-vlan host-association: 10 20
Administrative private-vlan mapping: 1
Operational private-vlan: 10 20
```

## 2.4 QinQ

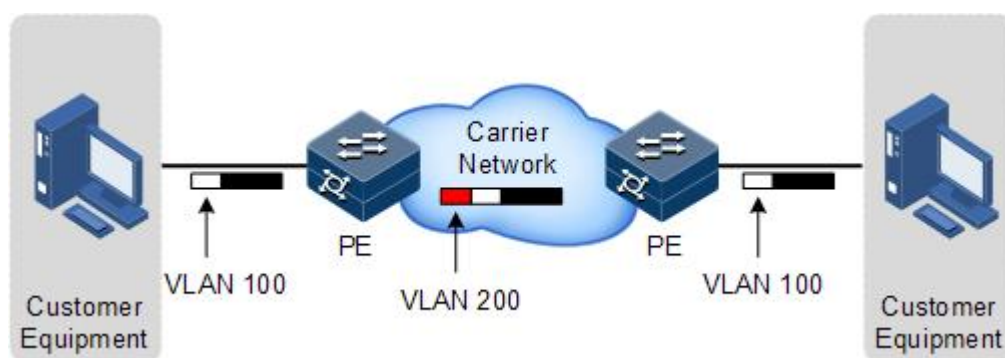
### 2.4.1 Introduction

QinQ (also known as Stacked VLAN or Double VLAN) technique is an extension to 802.1Q defined in IEEE 802.1ad standard.

#### Basic QinQ

Basic QinQ is a simple Layer 2 VPN tunnel technique, which encapsulates outer VLAN Tag for user private network packets at carrier access end, then the packet with double VLAN Tag traverse backbone network (public network) of the carrier. On the public network, packets are transmitted according to outer VLAN Tag (namely, the public network VLAN Tag), the user private network VALN Tag is transmitted as data in packets.

Figure 2-6 Principles of basic QinQ



Typical networking of basic QinQ is shown as Figure 2-6; the ISCOM2600G-HI series switch is the PE.

Packets are transmitted from the user device to the PE, and the VLAN ID of packet tag is 100. Packet will be added with outer tag with VLAN 1000 when traversing from the PE device at the network side interface to the carrier network.

Packets with the VLAN 1000 outer Tag are transmitted to PE device on the other side by the carrier, and then the PE will remove the outer tag VLAN 1000 and send packets to the user device. Now the packets return to carrying only one tag VLAN 100.

This technique can save public network VLAN ID resources. You can plan private network VLAN ID to avoid conflict with public network VLAN ID.

#### Selective QinQ

Selective QinQ is an enhancement to basic QinQ, which classifies flow according to user data features, then encapsulates different types flow into different outer VLAN Tags. This technique is implemented through combination of interface and VLAN. Selective QinQ can perform different actions on different VLAN Tags received by one interface and add different outer VLAN IDs for different inner VLAN IDs. According to configured mapping rules for inner and outer Tags, you can encapsulate different outer Tags for different inner tagged packets.

Selective QinQ makes structure of the carrier network more flexible. You can classify different terminal users on the access device interface by VLAN Tag and then, encapsulate

different outer Tags for users in different classes. On the public network, you can configure QoS policy according to outer Tag and configure data transmission priority flexibly to make users in different classes receive corresponding services.

## 2.4.2 Preparing for configurations

### Scenario

Basic QinQ configuration and selective QinQ configuration for the ISCOM2600G-HI series switch are based on different service requirements.

- Basic QinQ

With application of basic QinQ, you can add outer VLAN Tag to plan the private VLAN ID freely to make the user device data at both ends of carrier network transparently transmitted without conflicting with VLAN ID on the service provider network.

- Selective QinQ

Different from basic QinQ, outer VLAN Tag of selective QinQ can be selectable according to different services. There are multiple services and different private VLAN ID on the user network which are divided by adding different outer VLAN Tag for voice, video, and data services, then implementing different distributaries and inner and outer VLAN mapping for forwarding different services.

### Prerequisite

- Connect the interface.
- Configure its physical parameters to make it Up.
- Create VLANs.



#### Note

Double-tagged VLAN mapping cannot be concurrently configured with basic QinQ or tagged CVLAN/Priority-tagged VLAN mapping on the same interface.

## 2.4.3 Default configurations of QinQ

Default configurations of QinQ are as below.

Function	Default value
Outer VLAN Tag TPID	0x8100
Basic QinQ status	Disable
Selective QinQ status	Disable

## 2.4.4 Configuring basic QinQ

Configure basic QinQ on the ingress interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaetherne</b> 1/1/port) <b>#dot1q-tunnel</b> 1	Enable basic QinQ on the interface. The device supports this configuration on the LAG interface or in ISF mode.
4	<b>Raisecom(config-</b> <b>gigaetherne</b> 1/1/port) <b>#switchport</b> <b>qinq default-cvlan</b> <i>vlan-id</i>	Configure basic QinQ, add double Tags, and specify the PVID used by the CVLAN and SVLAN.
5	<b>Raisecom(config-</b> <b>gigaetherne</b> 1/1/port) <b>#switchport</b> <b>reject-frame { tagged   untagged }</b>	Configure the types of packets disallowed to be forwarded.



## Note

- To use basic QinQ functions on an interface, configure its attributes first by configuring it to the Access or Trunk interface and configuring the default VLAN.
- When basic QinQ is enabled on the interface, all packets are processed as untagged packets. If you configure the untagged packets to be discarded, tagged packets are also discarded.
- VLAN mapping based on VLAN+CoS and VLAN mapping based on VLAN cannot be concurrently configured.

## 2.4.5 Configuring selective QinQ

Configure selective QinQ on the ingress interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaetherne</b> 1/1/port) <b>#switchport vlan-</b> <b>mapping-miss discard</b>	Configure the interface to discard tagged packets that fail to match selective QinQ or VLAN mapping rules.
4	<b>Raisecom(config-</b> <b>gigaetherne</b> 1/1/port) <b>#switchport vlan-</b> <b>mapping ethertype { arp   eapol  </b> <b>flowcontrol   ip   ipv6 / loopback  </b> <b>mpls   mpls-mcast   pppoe   pppoe disc  </b> <b>user-define protocol id   x25  </b> <b>x75 }add-outer</b> <i>outer-vlan-id</i>	Configure EtherType selective QinQ, and add mapping rules for Tag VLAN.

Step	Command	Description
5	<pre> Raisecom(config- gigaetherne1/1/port)#switchport vlan- mapping both priority-tagged [ cos cos- value ] add-outer outer-vlan-id [ cos cos-value ] [ remove   translate vlan- id ] Raisecom(config- gigaetherne1/1/port)#switchport vlan- mapping both cvlan custom-vlan-list [ cos cos-value ] add-outer outer-vlan- id [ cos cos-value ] { remove   translate vlan-id } Raisecom(config- gigaetherne1/1/port)#switchport vlan- mapping both { untag   inner inner- vlan-id } add-outer outer-vlan-id [ cos cos-value ] </pre>	(Optional) configure bidirectional selective QinQ, and add outer VLAN rules. The device supports this configuration on the LAG or in ISF mode.



## Note

Double-tagged VLAN mapping cannot be concurrently configured with basic QinQ or tagged CVLAN/Priority-tagged VLAN mapping on the same interface. Before configuring selective QinQ and specifying CoS of the outer VLAN, configure basic QinQ.

## 2.4.6 Configuring network-side interface to Trunk mode

Configure the network-side interface to Trunk mode for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaetherne1/1/port)#switchport</b> <b>mode trunk</b>	Configure interface trunk mode, permit double-tagged packet to pass.

## 2.4.7 Configuring TPID

Configure the TPID on the network side interface for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<code>Raisecom(config)#<b>interface</b> <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/port)#<b>tpid</b> <i>tpid</i></code>	Configure the TPID of the outer VLAN Tag on the interface.

## 2.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#<b>show dot1q-tunnel</b></code>	Show configurations of basic QinQ.
2	<code>Raisecom#<b>show vlan-mapping both</b> <b>interface</b> <i>interface-type</i> <i>interface-number</i></code>	Show configurations of selective QinQ.
3	<code>Raisecom#<b>show vlan-mapping</b> <b>interface</b> <i>interface-type</i> <i>interface-number</i></code>	Show configurations of selective QinQ of EtherType on the interface.

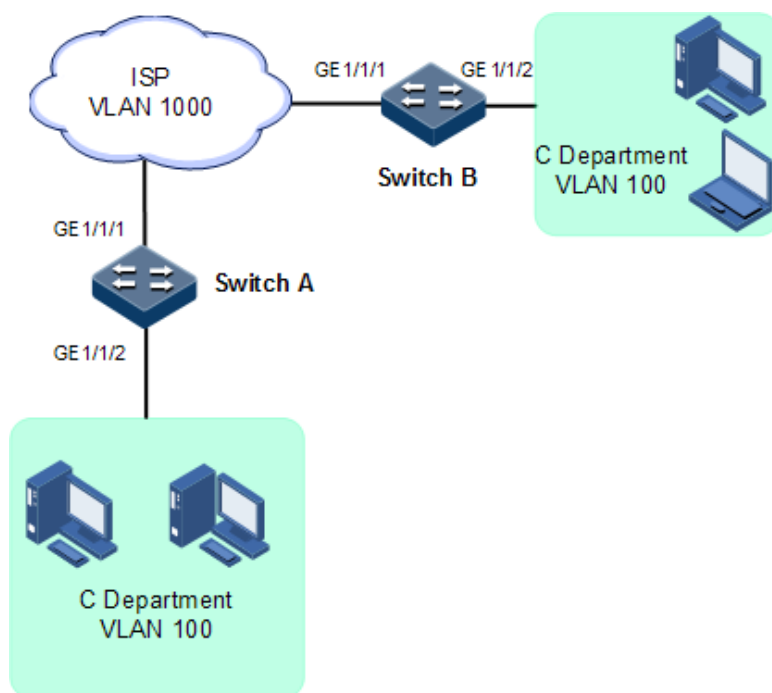
## 2.4.9 Example for configuring basic QinQ

### Networking requirements

As shown in Figure 2-7, Switch A and Switch B are connected to two branches of Department C, which are in different locations. Department C uses VLAN 100, and needs to communicate through VLAN 1000 of the carrier network. The carrier TPID is 9100.

Configure basic QinQ on Switch A and Switch B to enable normal communication inside a department through the carrier's network.

Figure 2-7 Basic QinQ networking



## Configuration steps

Configure Switch A and Switch B.

Configurations of Switch A are the same with those of Switch B. Take Switch A for example.

Step 1 Create VLAN 100 and VLAN 1000, and activate them. TPID is 9100.

```
Raisecom#config
Raisecom(config)#create vlan 100,1000 active
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#switchport mode trunk
Raisecom(config-gigabitEthernet1/1/1)#switchport trunk allowed vlan 1000
Raisecom(config-gigabitEthernet1/1/1)#tpid 9100
Raisecom(config-gigabitEthernet1/1/1)#exit
```

Step 2 Configure basic QinQ on the interface.

```
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#switchport mode trunk
Raisecom(config-gigabitEthernet1/1/2)#switchport trunk native vlan 1000
Raisecom(config-gigabitEthernet1/1/2)#dot1q-tunnel
Raisecom(config-gigabitEthernet1/1/2)#switchport qinq 100
Raisecom(config-gigabitEthernet1/1/2)#exit
```

## Checking results

Use the **show dot1q-tunnel** command to show QinQ configurations.

```
Raisecom#show dot1q-tunnel
Interface          QinQ Status  Outer TPID on port  Cos override  vlan-
map-miss
-----
gigaethernet1/1/1  -           0x9100             -             disable
gigaethernet1/1/2  dot1q-tunnel 0x8100             -             disable
```

## 2.4.10 Example for configuring selective QinQ

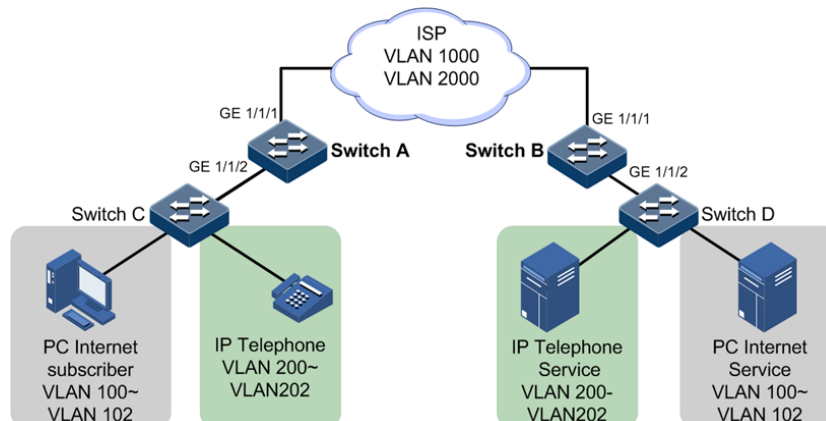
### Networking requirements

As shown in Figure 2-8, the carrier network contains common PC Internet access services and IP phone services. PC Internet access services are assigned to VLAN 1000, and IP phone services are assigned to VLAN 2000.

Configure Switch A and Switch B as below to make the user and server communicate through the carrier network:

- Add outer Tag VLAN 1000 to VLANs 100–102 assigned to PC Internet access services.
- Add outer Tag 2000 to VLANs 200–202 for IP phone services.
- The carrier TPID is 9100.

Figure 2-8 Selective QinQ networking



### Configuration steps

Configure Switch A and Switch B.

Configurations of Switch A are the same with those of Switch B. Take Switch A for example.

- Step 1 Create and activate VLANs 100–102, VLANs 200–202, VLAN 1000, and VAN 2000. The TPID is 9100.



```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#create vlan 100,101,102,200,201,202,1000,2000 active
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/1)#switchport trunk allowed vlan 1000,2000
SwitchA(config-gigabitEthernet1/1/1)#tpid 9100
SwitchA(config-gigabitEthernet1/1/1)#exit
```

Step 2 Enable selective QinQ on GE 1/1/2.

```
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#switchport mode trunk
Raisecom(config-gigabitEthernet1/1/2)#switchport trunk allowed vlan
100,101,102,200,201,202,1000,2000
SwitchA(config-gigabitEthernet1/1/2)#switchport vlan-mapping both inner 100-
102 add-outer 1000
SwitchA(config-gigabitEthernet1/1/2)#switchport vlan-mapping both inner 200-
202 add-outer 2000
SwitchA(config-gigabitEthernet1/1/2)#exit
```

## Checking results

Use the following command to show configurations of selective QinQ.

Take Switch A for example.

```
SwitchA#show vlan-mapping both interface gigabitEthernet 1/1/2
Interface : GE1/1/2
Default cvlan: --
-----
Original Outer VLANs: --
Original Outer COS:  --
Original Inner VLANs: 200-202
Original Inner COS:  --
Vlan mapping Mode:   S-ADD
New Outer-VID:       2000
New Outer-COS:       --
New Inner-VID:       --
New Inner-COS:       --
-----
Original Outer VLANs: --
Original Outer COS:  --
Original Inner VLANs: 100-102
Original Inner COS:  --
Vlan mapping Mode:   S-ADD
New Outer-VID:       1000
New Outer-COS:       --
New Inner-VID:       --
New Inner-COS:       --
```

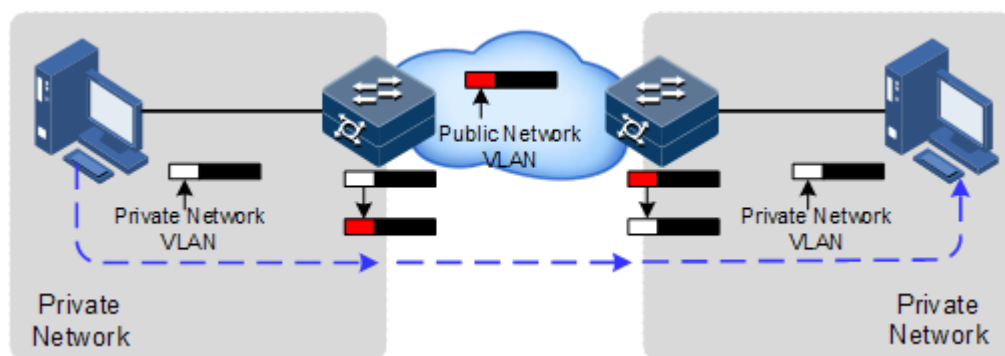
## 2.5 VLAN mapping

### 2.5.1 Introduction

VLAN mapping is used to replace the private VLAN Tag of Ethernet packets with carrier's VLAN Tag, making packets transmitted according to carrier's VLAN forwarding rules. When packets are sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Therefore packets are correctly sent to the destination.

Figure 2-9 shows principles of VLAN mapping.

Figure 2-9 Principles of VLAN mapping



After receiving a user private network packet with a VLAN Tag, the ISCOM2600G-HI series switch matches the packet according to configured VLAN mapping rules. If successful, it maps the packet according to configured VLAN mapping rules.

By supporting 1:1 VLAN mapping, the ISCOM2600G-HI series switch replaces the VLAN Tag carried by a packet from a specified VLAN to the new VLAN Tag.

Different from QinQ, VLAN mapping does not encapsulate packets with multiple layers of VLAN Tags, but needs to modify VLAN Tag so that packets are transmitted according to the carrier's VLAN forwarding rule.

### 2.5.2 Preparing for configurations

#### Scenario

Different from QinQ, VLAN mapping is used to change the VLAN Tag without encapsulating multilayer VLAN Tag so that packets are transmitted according to the carrier's VLAN mapping rules. VLAN mapping does not increase the frame length of the original packet. It can be used in the following scenarios:

- A user service needs to be mapped to a carrier's VLAN ID.
- Multiple user services need to be mapped to a carrier's VLAN ID.

## Prerequisite

- Connect the interface.
- Configure its physical parameters to make it Up.
- Create VLANs.

## 2.5.3 Default configurations of VLAN mapping

Default configurations of VLAN mapping are as below.

Function	Default value
VLAN mapping status	Disable

## 2.5.4 Configuring VLAN mapping

Configure VLAN mapping for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaetherne</b> t1/1/port) <b>#switchport</b> <b>vlan-mapping both outer</b> <i>vlan-id</i> <b>translate outer</b> <i>vlan-id</i> <b>Raisecom(config-</b> <b>gigaetherne</b> t1/1/port) <b>#switchport</b> <b>vlan-mapping both outer</b> <i>vlan-id</i> <b>inner</b> <i>inner -vlan-id</i> <b>translate</b> <b>outer</b> <i>vlan-id</i> <b>inner</b> <i>inner -vlan-id</i>	Configure the VLAN mapping rule based on outer and inner VLAN Tag in both the ingress and egress directions of the interface.
4	<b>Raisecom(config-</b> <b>gigaetherne</b> t1/1/1) <b>#switchport</b> <b>vlan-mapping both</b> <i>vlan-list</i> <b>translate</b> <i>vlan-id</i>	Configure the bidirectional N:1 VLAN mapping rule.



### Note

- Double-tagged VLAN mapping cannot be concurrently configured with basic QinQ or tagged CVLAN/Priority-tagged VLAN mapping on the same interface.
- To configure both N:1 VLAN mapping and VLAN Copy, you must configure the VLAN Copy and then configure N:1 VLAN mapping.

## 2.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show vlan-mapping both interface</b> <i>interface-type interface-number</i>	Show configurations of VLAN mapping.
2	<b>Raisecom#show vlan-mapping interface</b> <i>interface-type interface-number both</i> <b>translate</b>	Show configurations of N:1 VLAN mapping on the interface.

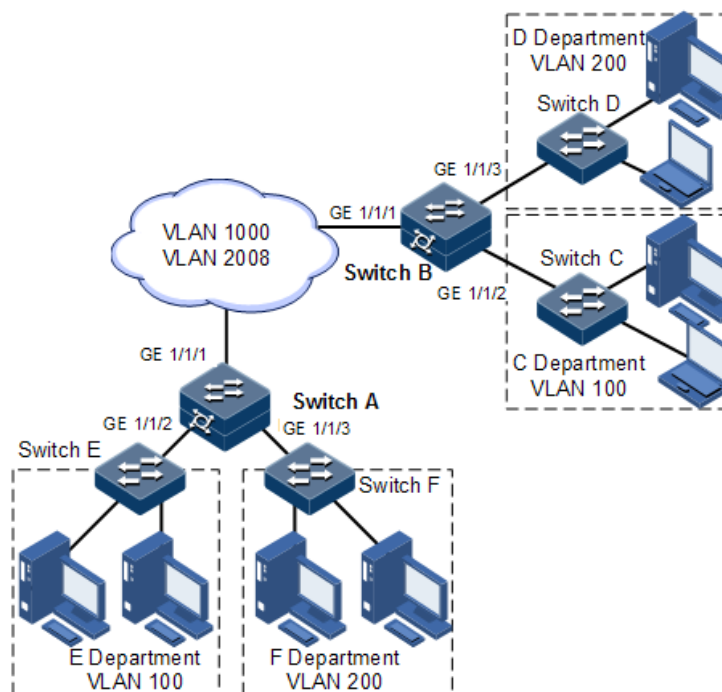
## 2.5.6 Example for configuring VLAN mapping

### Scenario

As shown in Figure 2-10, GE 1/1/2 and GE 1/1/3 on Switch A are connected to Department E using VLAN 100 and Department F using VLAN 200; GE 1/1/2 and GE 1/1/3 on Switch A are connected to Department C using VLAN 100 and Department D using VLAN 200. The carrier's network uses VLAN 1000 to transmit services between Department E and Department C and uses VLAN 2008 to transmit services between Department F and Department D.

Configure 1:1 VLAN mapping between Switch A and Switch B to implement normal communication inside each department.

Figure 2-10 VLAN mapping networking



### Configuration steps

Configure Switch A and Switch B.

Configuration steps for Switch A and Switch B are the same. Take Switch A for example.

Step 1 Create VLANs 100, 200, 1000, and 2008, and activate them.

```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#create vlan 100,200,1000,2008 active
```

Step 2 Configure GE 1/1/1 to Trunk mode, allowing packets of VLAN 1000 and VLAN 2008 to pass.

```
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/1)#switchport trunk allowed vlan 1000,2008
confirm
SwitchA(config-gigabitEthernet1/1/1)#exit
```

Step 3 Configure GE 1/1/2 to Trunk mode, allowing packets of VLAN 100 to pass. Configure VLAN mapping rules.

```
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/2)#switchport trunk allowed vlan 100
confirm
SwitchA(config-gigabitEthernet1/1/2)#switchport vlan-mapping both outer 100
translate 1000
SwitchA(config-gigabitEthernet1/1/2)#exit
```

Step 4 Configure GE 1/1/3 to Trunk mode, allowing packets of VLAN 200 to pass. Configure VLAN mapping rules.

```
SwitchA(config)#interface gigabitEthernet 1/1/3
SwitchA(config-gigabitEthernet1/1/3)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/3)#switchport trunk allowed vlan 200
confirm
SwitchA(config-gigabitEthernet1/1/3)#switchport vlan-mapping both outer
200 translate 2008
```

## Checking results

Use the **show vlan-mapping both interface gigabitEthernet 1/1/2** command to show configurations of 1:1 VLAN mapping.

```
SwitchA#show interface gigabitEthernet 1/1/2
Both Direction VLAN QinQ mapping rule:
Interface : GE 1/1/2
```

```
Default cvlan: --
-----
Original Outer VLANs: 100
Original Outer COS:  --
Original Inner VLANs: --
Original Inner COS:  --
Vlan mapping Mode:   S-TRANS
New Outer-VID:       1000
New Outer-COS:       --
New Inner-VID:       --
New Inner-COS:       --
-----

SwitchA#show vlan-mapping both interface gigaethernet 1/1/3
Both Direction VLAN QinQ mapping rule:
Interface : GE 1/1/3
Default cvlan: --
-----
Original Outer VLANs: 200
Original Outer COS:  --
Original Inner VLANs: --
Original Inner COS:  --
Vlan mapping Mode:   S-TRANS
New Outer-VID:       2008
New Outer-COS:       --
New Inner-VID:       --
New Inner-COS:       --
-----
```

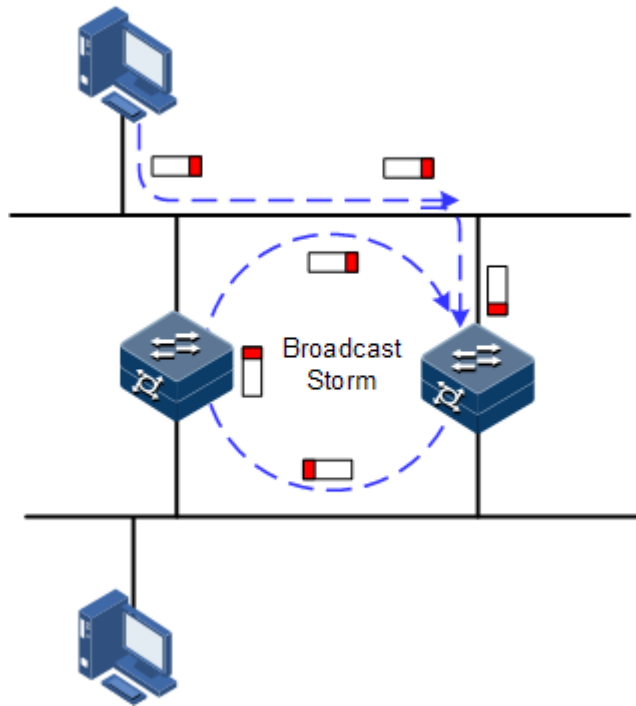
## 2.6 STP/RSTP

### 2.6.1 Introduction

#### STP

With the increasing complexity of network structure and growing number of switches on the network, the Ethernet network loops become the most prominent problem. Because of the packet broadcast mechanism, a loop causes the network to generate storms, exhaust network resources, and have serious impact to forwarding normal data. The network storm caused by the loop is shown in Figure 2-11.

Figure 2-11 Network storm due to loopback

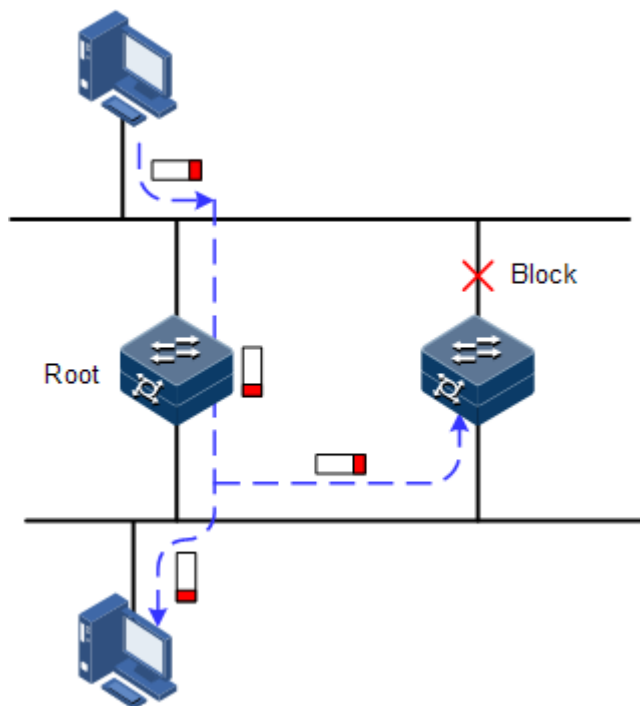


Spanning Tree Protocol (STP) is compliant to IEEE 802.1d standard and used to remove data physical loop in data link layer in the LAN.

The ISCOM2600G-HI series switch running STP can process Bridge Protocol Data Unit (BPDU) with each other for the election of root switch and selection of root port and designated port. It also can block loop interface on the ISCOM2600G-HI series switch logically according to the selection results, and finally trims the loop network structure to tree network structure without loop which takes an ISCOM2600G-HI series switch as root. This prevents the continuous proliferation and limitless circulation of packet on the loop network from causing broadcast storms and avoids declining packet processing capacity caused by receiving the same packets repeatedly.

Figure 2-12 shows loop networking with STP.

Figure 2-12 Loop networking with STP



Although STP can eliminate loop network and prevent broadcast storm well, its shortcomings are still gradually exposed with thorough application and development of network technology.

The major disadvantage of STP is the slow convergence speed.

## RSTP

For improving the slow convergent speed of STP, IEEE 802.1w establishes Rapid Spanning Tree Protocol (RSTP), which increases the mechanism to change interface blocking state to forwarding state, speed up the topology convergence rate.

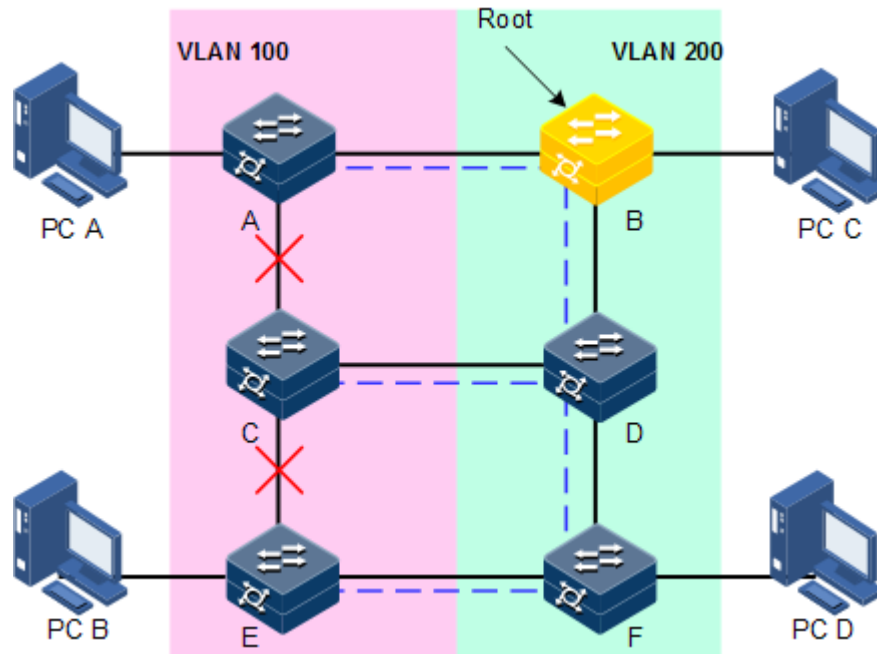
The purpose of STP/RSTP is to simplify a bridged LAN to a unitary spanning tree in logical topology and to avoid broadcast storm.

The disadvantages of STP/RSTP are exposed with the rapid development of VLAN technology. The unitary spanning tree simplified from STP/RSTP leads to the following problems:

- The whole switching network has only one spanning tree, which will lead to longer convergence time on a larger network.
- After a link is blocked, it does not carry traffic any more, causing waste of bandwidth.
- Packet of partial VLAN cannot be forwarded when network structure is unsymmetrical. As shown in Figure 2-13, Switch B is the root switch; RSTP blocks the link between Switch A and Switch C logically and makes that the VLAN 100 packet cannot be transmitted and Switch A and Switch C cannot communicate.



Figure 2-13 Failure in forwarding VLAN packets due to RSTP



## 2.6.2 Preparation for configuration

### Networking situation

In a big LAN, multiple devices are concatenated for accessing each other among hosts. They need to be enabled with STP to avoid loop among them, MAC address learning fault, and broadcast storm and network down caused by quick copy and transmission of data frame. STP calculation can block one interface in a broken loop and ensure that there is only one path from data flow to the destination host, which is also the best path.

### Preconditions

N/A

## 2.6.3 Default configurations of STP

Default configurations of STP are as below.

Function	Default value
Global STP status	Disable
Interface STP status	Enable
STP priority of device	32768
STP priority of interface	128
Path cost of interface	0
Max Age timer	20s
Hello Time timer	2s

Function	Default value
Forward Delay timer	15s

## 2.6.4 Enabling STP

Enable STP for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree enable</b>	Enable global STP.
3	<b>Raisecom(config)#spanning-tree mode { stp   rstp   mrstp }</b>	Configure spanning tree mode.
4	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical layer interface configuration mode.
5	<b>Raisecom(config-gigaetherne1/1/port)#spanning-tree enable</b>	Enable interface STP.

## 2.6.5 Configuring STP parameters

Configure STP parameters for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree priority priority-value</b>	(Optional) configure device priorities.
3	<b>Raisecom(config)#spanning-tree root { primary   secondary }</b>	(Optional) configure the device as the root or backup device.
4	<b>Raisecom(config)#interface interface-type interface-number</b> <b>Raisecom(config-gigaetherne1/1/port)#spanning-tree priority priority-value</b>	(Optional) configure interface priorities on the device.
5	<b>Raisecom(config-gigaetherne1/1/1)#spanning-tree extern-path-cost cost-value</b> <b>Raisecom(config-gigaetherne1/1/port)#exit</b>	(Optional) configure the path cost of the external interface on the device.
6	<b>Raisecom(config-gigaetherne1/1/port)#spanning-tree [ instance instance-id ] inter-path-cost cost</b>	(Optional) configure the path cost of the internal interface on the device.
7	<b>Raisecom(config)#spanning-tree hello-time value</b>	(Optional) configure the value of Hello Time.

Step	Command	Description
8	<b>Raisecom(config)#spanning-tree transit-limit</b> <i>value</i>	(Optional) configure the maximum transmission rate of the interface
9	<b>Raisecom(config)#spanning-tree forward-delay</b> <i>value</i>	(Optional) configure forward delay.
10	<b>Raisecom(config)#spanning-tree max-age</b> <i>value</i>	(Optional) configure the maximum age.

## 2.6.6 Configuring edge interface

The edge interface indicates that the interface neither directly connects to any devices nor indirectly connects to any device through the network.

The edge interface can change the interface status to forward quickly without any waiting time. You had better configure the Ethernet interface connected to user client as edge interface to make it quick to change to forward status.

The edge interface attribute depends on actual condition when it is in auto-detection mode; the real port will change to false edge interface after receiving BPDU when it is in force-true mode; when the interface is in force-false mode, whether it is true or false edge interface in real operation, it will maintain the force-false mode until the configuration is changed.

By default, all interfaces on the ISCOM2600G-HI series switch are configured in auto-detection attribute.

Configure the edge interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/port)#spanning-tree edged-port { auto   force-true   force-false }</b>	Configure attributes of the RSTP edge interface.

## 2.6.7 Configuring link type

Two interfaces connected by a point-to-point link can quickly transit to forward status by transmitting synchronization packets. By default, MSTP configures the link type of interfaces according to duplex mode. The full duplex interface is considered as the point-to-point link, and the half duplex interface is considered as the shared link.

You can manually configure the current Ethernet interface to connect to a point-to-point link, but the system will fail if the link is not point to point. Generally, we recommend configuring this item in auto status and the system will automatically detect whether the interface is connected to a point-to-point link.

Configure the link type for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#spanning-tree</b> <b>link-type { auto   point-to-point  </b> <b>shared }</b>	Configure the link type for interface.

## 2.6.8 Configuring BPDU filtering

After being enabled with BPDU filtering, the edge interface does not send BPDUs nor process received BPDUs.

Configure BPDU filtering for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#spanning-</b> <b>tree edged-port bpdu-filter enable</b> <i>interface-type interface-number</i>	Enable BPDU filtering on the edge interface.

## 2.6.9 Configuring BPDU Guard

Generally, on a switch, interfaces are directly connected with terminals (such as a PC) or file servers are configured to an edge interfaces. Therefore, these interfaces can be transferred quickly.

In normal status, these edge interfaces will not receive BPDUs. If somebody attacks the switch by forging the BPDU, the device will configure these edge interfaces to non-edge interfaces when these edge interfaces receive the forged BPDU and re-perform spanning tree calculation. This may cause network vibration.

BPDU Guard provided by MSTP can prevent this attack. After BPDU Guard is enabled, edge interfaces can avoid attack from forged BPDUs.

After BPDU Guard is enabled, the device will shut down the edge interfaces if they receive BPDUs and notify the NView NNM system of the case. The blocked edge interface is restored only by the administrator through the CLI.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree</b> <b>bpduguard enable</b>	Enable BPDU Guard.

Step	Command	Description
3	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#no spanning-</b> <b>tree bpduguard shutdown port</b>	Manually restore interfaces that are shut down by BPDU Guard.



### Note

When the edge interface is enabled with BPDU filtering and the device is enabled with BPDU Guard, BPDU Guard takes effect first. Therefore, an edge interface is shut down if it receives a BPDU.

## 2.6.10 Configuring MRSTP

Configure MRSTP for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree mrstp</b> <i>pro-id</i>	Create an MRSTP process.
3	<b>Raisecom(config)#spanning-tree mrstp</b> <i>pro-id priority priority</i>	Configure the priority of a specified process.
4	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#spanning-tree</b> <b>mrstp pro-id</b>	Bind the interface to the specified process.

## 2.6.11 Checking configurations

Use the following commands to check configuration results.

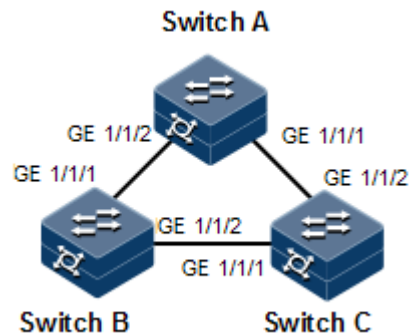
No.	Command	Description
1	<b>Raisecom#show spanning-tree</b>	Show basic configurations of STP.
2	<b>Raisecom#show spanning-tree</b> <i>interface-type interface-list</i> <b>[ detail ]</b>	Show STP configuration on the interface.
3	<b>Raisecom#show spanning-tree mrstp</b> <i>pro-id</i>	Show MRSTP configurations.

## 2.6.12 Example for configuring STP

### Networking requirements

As shown in Figure 2-14, Switch A, Switch B, and Switch C form a ring network, so the loop must be eliminated in the situation of a physical link forming a ring. Enable STP on them, configure the priority of Switch A to 0, and path cost from Switch B to Switch A to 10.

Figure 2-14 STP networking



### Configuration steps

Step 1 Enable STP on Switch A, Switch B, and Switch C.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree mode stp
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree mode stp
```

Configure Switch C.

```
Raisecom#hostname SwitchC
SwitchC#config
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree mode stp
```

Step 2 Configure interface modes on three switches.

Configure Switch A.

```
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/1)#exit
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/2)#exit
```

Configure Switch B.

```
SwitchB(config)#interface gigabitEthernet 1/1/1
SwitchB(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchB(config-gigabitEthernet1/1/1)#exit
SwitchB(config)#interface gigabitEthernet 1/1/2
SwitchB(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchB(config-gigabitEthernet1/1/2)#exit
```

Configure Switch C.

```
SwitchC(config)#interface gigabitEthernet 1/1/1
SwitchC(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchC(config-gigabitEthernet1/1/1)#exit
SwitchC(config)#interface gigabitEthernet 1/1/2
SwitchC(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchC(config-gigabitEthernet1/1/2)#exit
```

Step 3 Configure priority of spanning tree and interface path cost.

Configure Switch A.

```
SwitchA(config)#spanning-tree priority 0
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#spanning-tree extern-path-cost 10
```

Configure Switch B.

```
SwitchB(config)#interface gigabitEthernet 1/1/1
SwitchB(config-gigabitEthernet1/1/1)#spanning-tree extern-path-cost 10
```

## Checking results

Use the **show spanning-tree** command to show bridge status.

Take Switch A for example.

```
SwitchA#show spanning-tree
Spanning-tree admin state: enable
Spanning-tree 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
              MaxHops 20 Diameter 7
```

Use the **show spanning-tree port-list** *port-list* command to show interface status.

Take Switch A for example.

```
SwitchA#show spanning-tree gig Ethernet 1/1/1
GE1/1/1
PortProtocolEnable: admin: enable oper: enable Rootguard: disable
Loopguard: disable
Bpduguard: disable
ExternPathCost:200000
Partner STP Mode: stp
Bpdus send: 0 (TCN<0> Config<0> RST<0> MST<0>)
Bpdus received:0 (TCN<0> Config<0> RST<0> MST<0>)
State:blocking Role:non-designated Priority:128 Cost: 200000
Root: Mac 0000.0000.0000 Priority 0 RootCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0
```

## 2.7 MSTP

### 2.7.1 Introduction

Multiple Spanning Tree Protocol (MSTP) is defined by IEEE 802.1s. Recovering the disadvantages of STP and RSTP, the MSTP implements fast convergence and distributes different VLAN flow following its own path to provide an excellent load balancing mechanism.

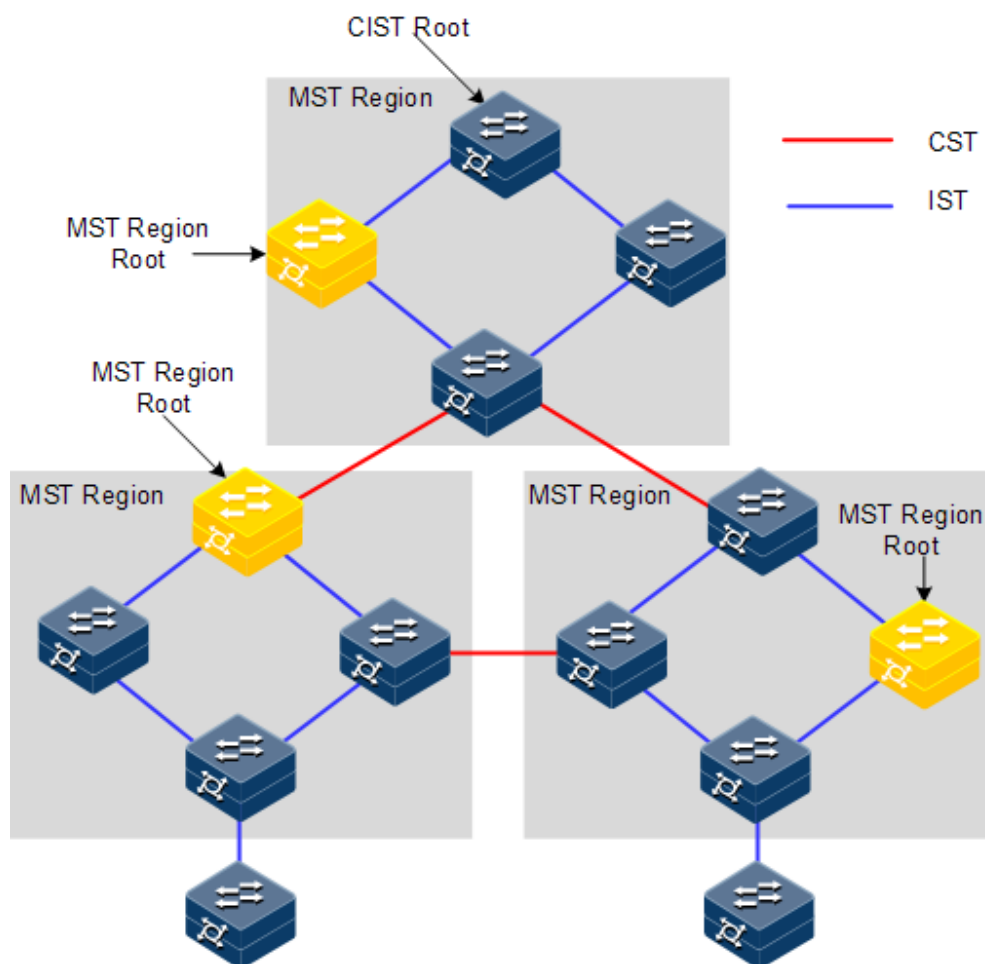
MSTP divides a switch network into multiple regions, called MST region. Each MST region contains several spanning trees but the trees are independent from each other. Each spanning tree is called a Multiple Spanning Tree Instance (MSTI).



MSTP protocol introduces Common Spanning Tree (CST) and Internal Spanning Tree (IST) concepts. CST refers to taking MST region as a whole to calculate and generating a spanning tree. IST refers to generating spanning tree in internal MST region.

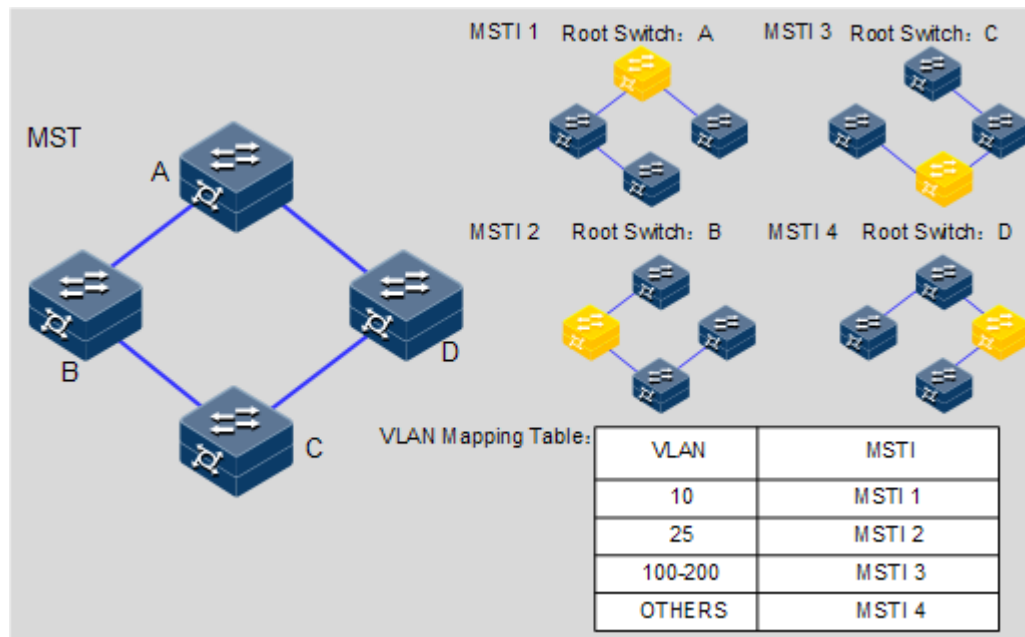
Compared with STP and RSTP, MSTP also introduces total root (CIST Root) and region root (MST Region Root) concepts. The total root is a global concept; all switches running STP/RSTP/MSTP can have only one total root, which is the CIST Root. The region root is a local concept, which is relative to an instance in a region. As shown in Figure 2-15, all connected devices only have one total root, and the number of region root contained in each region is associated with the number of instances.

Figure 2-15 Basic concepts of the MSTI network



There can be different MST instance in each MST region, which associates VLAN and MSTI by configuring the VLAN mapping table (relationship table of VLAN and MSTI). The concept sketch map of MSTI is shown in Figure 2-16.

Figure 2-16 MSTI concepts

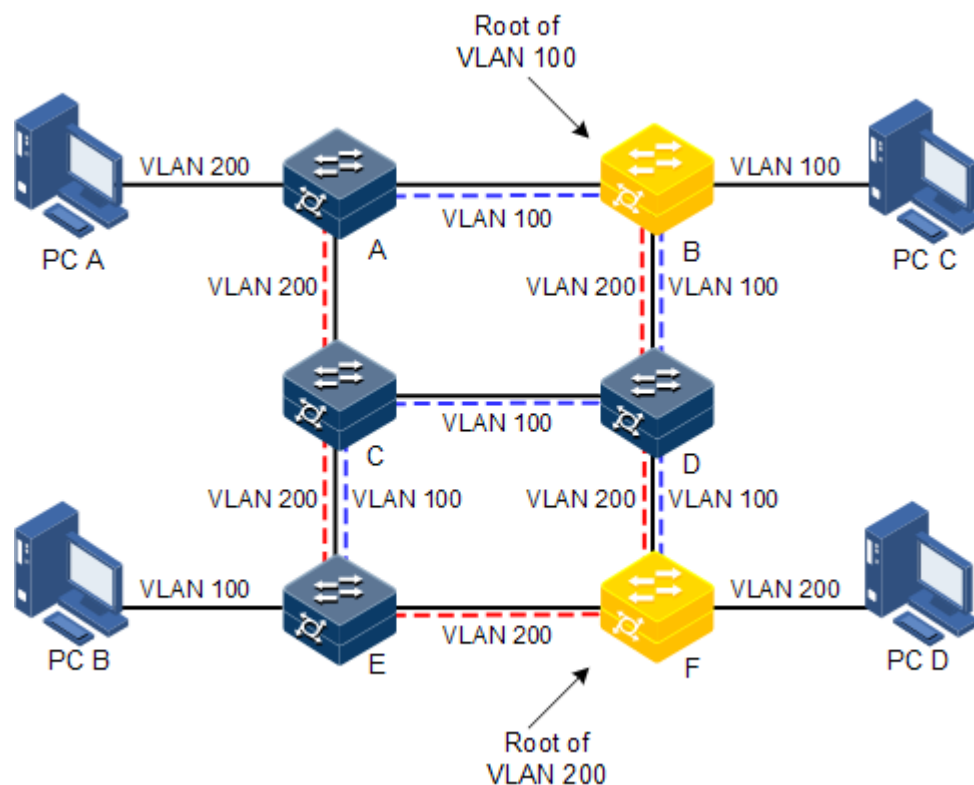


### Note

Each VLAN can map to one MSTI; in other words, data of one VLAN can only be transmitted in one MSTI but one MSTI may correspond to several VLANs.

Compared with STP and RSTP mentioned previously, MSTP has obvious advantages, including cognitive ability of VLAN, load balancing, similar RSTP interface status switching, and binding multiple VLAN to one MST instance, to reduce resource occupancy rate. In addition, devices running MSTP on the network are also compatible with the devices running STP and RSTP.

Figure 2-17 Networking with multiple spanning trees instances in MST region



Apply MSTP to the network as shown in Figure 2-17. After calculation, there are two spanning trees generated at last (two MST instances):

- MSTI 1 takes B as the root switch, forwarding packet of VLAN 100.
- MSTI 2 takes F as the root switch, forwarding packet of VLAN 200.

In this case, all VLANs can communicate internally, different VLAN packets are forwarded in different paths to share loading.

## 2.7.2 Preparation for configuration

### Scenario

In a big LAN or residential region aggregation, the aggregation devices make up a ring for link backup, avoiding loop and realizing load balancing. MSTP can select different and unique forwarding paths for each one or a group of VLANs.

### Prerequisite

N/A

## 2.7.3 Default configurations of MSTP

Default configurations of MSTP are as below.

Function	Default value
Global MSTP status	Disable
Interface MSTP status	Enable
Maximum number of hops in the MST region	20
MSTP priority of the device	32768
MSTP priority of the interface	128
Path cost of the interface	0
Maximum number of packets sent within each Hello time	3
Max Age timer	20s
Hello Time timer	2s
Forward Delay timer	15s
Revision level of the MST region	0

## 2.7.4 Enabling MSTP

Enable MSTP for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree mode mstp</b>	Configure spanning tree for MSTP.
3	<b>Raisecom(config)#spanning-tree enable</b>	Enable global STP.
4	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#spanning-tree</b> <b>enable</b>	Enable interface STP. The device supports this configuration on the LAG interface.

## 2.7.5 Configuring MST region and its maximum number of hops

You can configure region information about the ISCOM2600G-HI series switch when it is running in MSTP mode. The device MST region is determined by the region name, VLAN mapping table and configuration of MSTP revision level. You can configure current device in a specific MST region through following configuration.

The MST region scale is restricted by the maximum number of hops. Starting from the root bridge of spanning tree in the region, the number of forwarding hops decreases by 1 when the configuration message (BPDU) passes a device; the ISCOM2600G-HI series switch discards

the configuration message whose number of hops is 0. The device exceeding the maximum number of hops cannot join spanning tree calculation, so the MST region scale is restricted.

Configure MSTP region and its maximum number of hops for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree region-configuration</b>	Enter MST region configuration mode.
3	<b>Raisecom(config-region)#name</b> <i>name</i>	Configure the MST region name.
4	<b>Raisecom(config-region)#revision-level</b> <i>level-value</i>	Configure the revision level for the MST region.
5	<b>Raisecom(config-region)#instance</b> <i>instance-id</i> <b>vlan</b> <i>vlan-list</i> <b>Raisecom(config-region)#exit</b>	Configure mapping from MST region VLAN to instance.
6	<b>Raisecom(config)#spanning-tree max-hops</b> <i>hops-value</i>	Configure the maximum number of hops for MST region.



### Note

Only when the configured device is the region root can the configured maximum number of hops be used as the maximum number of hops for MST region; other non-region root cannot be configured this item.

## 2.7.6 Configuring root/backup bridge

Two methods for MSTP root selection are as below:

- To configure device priority and calculated by STP to confirm STP root bridge or backup bridge
- To assign MSTP root directly by a command

When the root bridge has a fault or is powered off, the backup bridge can replace the root bridge of related instance. In this case, if a new root bridge is assigned, the backup bridge will not become the root bridge. If several backup bridges for a spanning tree are configured, once the root bridge stops working, MSTP will choose the backup root with the lowest MAC address as the new root bridge.



### Note

We do not recommend modifying the priority of any device on the network if you directly assign the root bridge. Otherwise, the assigned root bridge or backup bridge may be invalid.

Configure the root bridge or backup bridge for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree</b> [ <b>instance</b> <i>instance-id</i> ] <b>root</b> { <b>primary</b>   <b>secondary</b> }	Configure the ISCOM2600G-HI series switch as the root bridge or backup bridge of a STP instance.



## Note

- You can confirm the effective instance of the root bridge or backup bridge through the **instance** *instance-id* parameter. The current device will be assigned as the root bridge or backup bridge of CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.
- The roots in device instances are mutually independent; in other words, they cannot only be the root bridge or backup bridge of one instance, but also the root bridge or backup bridge of other spanning tree instances. However, in a spanning tree instance, a device cannot be used as the root bridge and backup bridge concurrently.
- You cannot assign two or more root bridges for one spanning tree instance, but can assign several backup bridges for one spanning tree. Generally, you had better assign one root bridge and several backup bridges for a spanning tree.

## 2.7.7 Configuring interface priority and system priority

Whether the interface is elected as the root interface depends on interface priority. Under the identical condition, the interface with smaller priority will be elected as the root interface. An interface may have different priorities and play different roles in different instances.

The Bridge ID determines whether the ISCOM2600G-HI series switch can be elected as the root of the spanning tree. Configuring smaller priority helps obtain smaller Bridge ID and designate the ISCOM2600G-HI series switch as the root. If priorities of two ISCOM2600G-HI series switch devices are identical, the ISCOM2600G-HI series switch with lower MAC address will be elected as the root.

Similar to configuring root and backup root, priority is mutually independent in different instances. You can confirm priority instance through the **instance** *instance-id* parameter. Configure bridge priority for CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.

Configure the interface priority and system priority for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.

Step	Command	Description
3	Raisecom(config-gigaetherne1/1/port)# <b>spanning-tree</b> [ <b>instance</b> <i>instance-id</i> ] <b>priority</b> <i>priority-value</i> Raisecom(config-gigaetherne1/1/port)# <b>exit</b>	Configure the interface priority for a STP instance.
4	Raisecom(config)# <b>spanning-tree</b> [ <b>instance</b> <i>instance-id</i> ] <b>priority</b> <i>priority-value</i>	Configure the system priority for a STP instance.



### Note

The value of priorities must be multiples of 4096, such as 0, 4096, and 8192. It is 32768 by default.

## 2.7.8 Configuring network diameter for switch network

The network diameter indicates the number of nodes on the path that has the most devices on a switching network. In MSTP, the network diameter is valid only to CIST, and invalid to MSTI instance. No matter how many nodes in a path in one region, it is considered as just one node. Actually, network diameter should be defined as the region number in the path crossing the most regions. The network diameter is 1 if there is only one region on the entire network.

The maximum number of hops of the MST region is used to measure the region scale, while network diameter is a parameter to measure the whole network scale. The greater the network diameter is, the larger the network scale is.

Similar to the maximum number of hops of the MST region, only when the ISCOM2600G-HI series switch is configured as the CIST root device can this configuration take effect. MSTP will automatically configure the Hello Time, Forward Delay and Max Age parameters to a privileged value through calculation when configuring the network diameter.

Configure the network diameter for the switching network as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>spanning-tree</b> <b>bridge-diameter</b> <i>bridge-diameter-value</i>	Configure the network diameter for the switching network.

## 2.7.9 Configuring internal path cost of interface

When selecting the root interface and designated interface, the smaller the interface path cost is, the easier it is to be selected as the root interface or designated interface. Inner path costs of interface are independently mutually in different instances. You can configure internal path cost for instance through the **instance** *instance-id* parameter. Configure internal path cost of interface for CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.

By default, interface cost often depends on the physical features:

- 10 Mbit/s: 2000000
- 100 Mbit/s: 200000
- 1000 Mbit/s: 20000
- 10 Gbit/s: 2000

Configure the internal path cost for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/port)#spanning-tree</b> [ <b>instance</b> <i>instance-id</i> ] <b>inter-path-cost</b> <i>cost-value</i>	Configure the internal path cost of the interface.

## 2.7.10 Configuring external path cost of interface

The external path cost is the cost from the device to the CIST root, which is equal in the same region.

Configure the external path cost for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/port)#spanning-tree</b> <b>extern-path-cost</b> <i>cost-value</i>	Configure the external path cost of the interface.

## 2.7.11 Configuring maximum transmission rate on interface

The maximum transmission rate on an interface means the maximum number of transmitted BPDUs allowed by MSTP in each Hello Time. This parameter is a relative value and of no unit. The greater the parameter is configured, the more packets are allowed to be transmitted in a Hello Time, the more device resources it takes up. Similar with the time parameter, only the configurations on the root device can take effect.

Configure the maximum transmission rate on the interface for the ISCOM2600G-HI series switch as below.

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



Step	Command	Description
2	<b>Raisecom(config)#spanning-tree transit-limit <i>value</i></b>	Configure the maximum transmission rate on the interface.

## 2.7.12 Configuring MSTP timer

- **Hello Time:** the ISCOM2600G-HI series switch sends the interval of bridge configurations (BPDU) regularly to check whether there is failure in detection link of the ISCOM2600G-HI series switch. The ISCOM2600G-HI series switch sends Hello packets to other devices around in the Hello time to check if there is fault in the link. The default value is 2s. You can adjust the interval value according to network conditions. Reduce the interval when network link changes frequently to enhance the stability of STP. However, increasing the interval reduces CPU utilization rate for STP.
- **Forward Delay:** the time parameter to ensure the safe transit of device status. Link fault causes the network to recalculate spanning tree, but the new configuration message recalculated cannot be transmitted to the whole network immediately. There may be temporary loop if the new root interface and designated interface start transmitting data at once. This protocol adopts status remove system: before the root interface and designated interface starts forwarding data, it needs a medium status (learning status); after delay for the interval of Forward Delay, it enters forwarding status. The delay guarantees the new configuration message to be transmitted through whole network. You can adjust the delay according to actual condition; in other words, reduce it when network topology changes infrequently and increase it under opposite conditions.
- **Max Age:** the bridge configurations used by STP have a life time that is used to judge whether the configurations are outdated. The ISCOM2600G-HI series switch will discard outdated configurations and STP will recalculate spanning tree. The default value is 20s. Over short age may cause frequent recalculation of the spanning tree, while a too great age value will make STP not adapt to network topology change timely.

All devices in the whole switching network adopt the three time parameters on CIST root device, so only the root device configuration is valid.

Configure the MSTP timer for the ISCOM2600G-HI series switch as below.

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.
3	<b>Raisecom(config)#spanning-tree forward-delay <i>value</i></b>	Configure the Forward Delay.
4	<b>Raisecom(config)#spanning-tree max-age <i>value</i></b>	Configure the Max Age.

## 2.7.13 Configuring edge interface

The edge interface indicates the interface neither directly connecting to any devices nor indirectly connecting to any device through the network.

The edge interface can change the interface status to forward quickly without any waiting time. You had better configure the Ethernet interface connected to user client as edge interface to make it quick to change to forward status.

The edge interface attribute depends on actual condition when it is in auto-detection mode; the real port will change to false edge interface after receiving BPDU when it is in force-true mode; when the interface is in force-false mode, whether it is true or false edge interface in real operation, it will maintain the force-false mode until the configuration is changed.

By default, all interfaces on the ISCOM2600G-HI series switch are configured in auto-detection attribute.

Configure the edge interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#spanning-tree</b> <b>edged-port { auto   force-true  </b> <b>force-false }</b>	Configure attributes of the RSTP edge interface.

## 2.7.14 Configuring BPDU filtering

After being enabled with BPDU filtering, the edge interface does not send BPDU packets nor process received BPDU packets.

Configure BPDU filtering for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#spanning-tree</b> <b>edged-port bpdu-filter enable</b> <i>interface-type interface-number</i>	Enable BPDU filtering on the edge interface.

## 2.7.15 Configuring BPDU Guard

On a switch, interfaces directly connected with non-switch devices, such as terminals (such as a PC) or file servers, are configured as edge interfaces to implement fast transition of these interfaces.

In normal status, these edge interfaces do not receive BPDUs. If forged BPDU attacks the switch, the switch will configure these edge interfaces to non-edge interfaces when these edge interfaces receive forged BPDUs and re-perform spanning tree calculation. This may cause network vibration.

BPDU Guard provided by MSTP can prevent this type of attacks. After BPDU Guard is enabled, edge interfaces can avoid attacks from forged BPDU packets.

After BPDU Guard is enabled, the switch will shut down the edge interfaces if they receive BPDUs and notify the NView NNM system of the case. The blocked edge interface is restored only by the administrator through the CLI.

Configure BPDU Guard for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree bpduguard enable</b>	Enable BPDU Guard.
3	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config-gigaethernet1/1/port)#no spanning-tree bpduguard shutdown port</b>	Manually restore interfaces that are shut down by BPDU Guard.



## Note

When the edge interface is enabled with BPDU filtering and the device is enabled with BPDU Guard, BPDU Guard takes effect first. Therefore, an edge interface is shut down if it receives a BPDU.

## 2.7.16 Configuring STP/RSTP/MSTP mode switching

When STP is enabled, three spanning tree modes are supported as below:

- STP compatible mode: the ISCOM2600G-HI series switch does not implement fast switching from the replacement interface to the root interface and expedited forwarding by a specified interface; instead it sends STP configuration BPDU and STP Topology Change Notification (TCN) BPDU. After receiving MST BPDU, it discards unidentifiable part.
- RSTP mode: the ISCOM2600G-HI series switch implements fast switching from the replacement interface to the root interface and expedited forwarding by a specified interface. It sends RST BPDUs. After receiving MST BPDUs, it discards unidentifiable part. If the peer device runs STP, the local interface is switched to STP compatible mode. If the peer device runs MSTP, the local interface remains in RSTP mode.
- MSTP mode: the ISCOM2600G-HI series switch sends MST BPDU. If the peer device runs STP, the local interface is switched to STP compatible mode. If the peer device runs MSTP, the local interface remains in RSTP mode, and process packets as external information of region.

Configure the STP/RSTP/MSTP mode switching for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<code>Raisecom(config)#spanning-tree mode { stp   rstp   mstp }</code>	Configure the spanning tree mode.
3	<code>Raisecom(config-gigaethernet1/1/port)#spanning-tree mcheck</code>	(Optional) forcibly configure the interface to MSTP mode.

## 2.7.17 Configuring link type

Two interfaces connected by a point-to-point link can quickly transit to forward status by transmitting synchronization packets. By default, MSTP configures the link type of interfaces according to duplex mode. The full duplex interface is considered as the point-to-point link, and the half duplex interface is considered as the shared link.

You can manually configure the current Ethernet interface to connect to a point-to-point link, but the system will fail if the link is not point to point. Generally, we recommend configuring this item in auto status and the system will automatically detect whether the interface is connected to a point-to-point link.

Configure the link type for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/port)#spanning-tree link-type { auto   point-to-point   shared }</code>	Configure link type for interface.

## 2.7.18 Configuring root interface protection

The network will select a bridge again when it receives a packet with higher priority, which influences network connectivity and also consumes CPU resource. For the MSTP network, if someone sends BPDUs with higher priority, the network may become unstable due to continuous election.

Generally, priority of each bridge has already been configured in network planning phase. The nearer a bridge is to the edge, the lower the bridge priority is. So the downlink interface cannot receive the packets higher than bridge priority unless under someone attacks. For these interfaces, you can enable rootguard to refuse to process packets with priority higher than bridge priority and block the interface for a period to prevent other attacks from attacking sources and damaging the upper layer link.

Configure root interface protection for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<code>Raisecom(config)#<b>interface</b> <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/port)#<b>spanning-tree</b> <b>rootguard enable</b></code>	Enable/Disable root interface protection.

## 2.7.19 Configuring interface loopguard

The spanning tree has two functions: loopguard and link backup. Loopguard requires carving up the network topology into tree structure. There must be redundant links in the topology if link backup is required. Spanning tree can avoid loop by blocking the redundant link and enable link backup function by opening redundant link when the link breaks down.

The spanning tree module exchanges packets periodically, and the link has failed if it has not received packet in a period. Then select a new link and enable backup interface. In actual networking, the cause to failure in receiving packets may not link fault. In this case, enabling the backup interface may lead to loop.

Loopguard is used to keep the original interface status when it cannot receive packet in a period.



### Note

Loopguard and link backup are mutually exclusive; in other words, loopguard is implemented on the cost of disabling link backup.

Configure interface loop protection for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#<b>config</b></code>	Enter global configuration mode.
2	<code>Raisecom(config)#<b>interface</b> <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#<b>spanning-tree</b> <b>loopguard enable</b></code>	Configure interface loopguard attributes.

## 2.7.20 Configuring TC packet suppression

When the topology of the user access network changes, the forward address of the core network will be updated. When the topology becomes unstable, it will affect the core network. To avoid unstable topology, you can configure TC packet suppression on the interface. In this case, after the interface receives a TC packet, it will not forward the TC packet to other interfaces.

Configure TC packet suppression for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#spanning-tree</b> <b>tc-rejection { enable   disable }</b>	Configure TC packet suppression.

## 2.7.21 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show spanning-tree</b>	Show basic configurations of STP.
2	<b>Raisecom#show spanning-tree</b> <b>[ instance instance-id ] interface-</b> <b>type interface-list [ detail ]</b>	Show configurations of spanning tree on the interface.
3	<b>Raisecom#show spanning-tree region-</b> <b>operation</b>	Show operation information about the MST region.
4	<b>Raisecom(config-region)#show</b> <b>spanning-tree region-configuration</b>	Show configurations of the MST region.

## 2.7.22 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

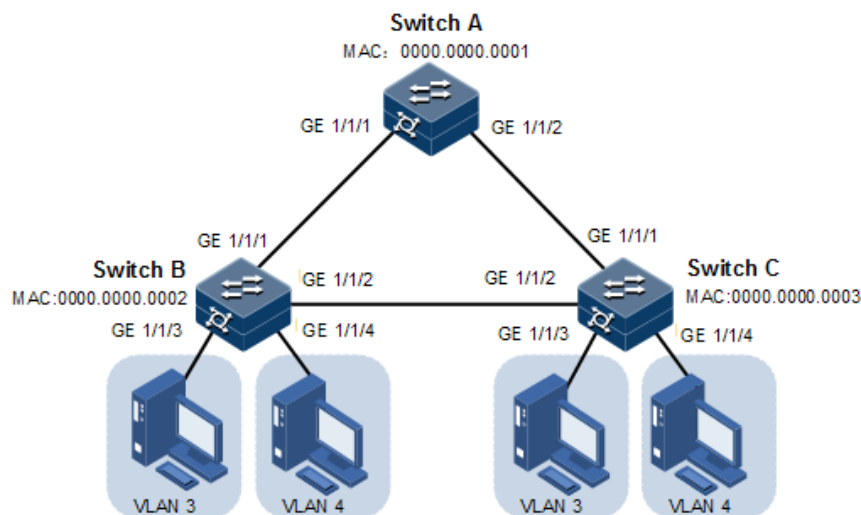
Command	Description
<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#spanning-tree clear</b> <b>statistics</b>	Clear statistics about spanning tree on the interface.

## 2.7.23 Example for configuring MSTP

### Networking requirements

As shown in Figure 2-18, three ISCOM2600G-HI series switch devices are connected to form a ring network through MSTP, with the region name aaa. Switch B, connected with a PC, belongs to VLAN 3. Switch C, connected with another PC, belongs to VLAN 4. Instant 3 is associated with VLAN 3. Instant 4 is associated with VLAN 4. Configure the path cost of instance 3 on Switch B so that packets of VLAN 3 and VLAN 4 are forwarded respectively in two paths, which eliminates loops and implements load balancing.

Figure 2-18 MSTP networking



## Configuration steps

- Step 1 Create VLAN 3 and VLAN 4 on Switch A, Switch B, and switch C respectively, and activate them.

Configure Switch A.

```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#create vlan 3,4 active
```

Configure Switch B.

```
Raisecom#name SwitchB
SwitchB#config
SwitchB(config)#create vlan 3,4 active
```

Configure Switch C.

```
Raisecom#name SwitchC
SwitchC#config
SwitchC(config)#create vlan 3,4 active
```

- Step 2 Configure GE 1/1/1 and GE 1/1/2 on Switch A to allow packets of all VLAN to pass in Trunk mode. Configure GE 1/1/1 and GE 1/1/2 on Switch B to allow packets of all VLANs to pass in Trunk mode. Configure GE 1/1/1 and GE 1/1/2 on Switch C to allow packets of all VLANs

to pass in Trunk mode. Configure GE 1/1/3 and GE 1/1/4 on Switch B and Switch C to allow packets of VLAN 3 and VLAN 4 to pass in Access mode.

Configure Switch A.

```
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/1)#exit
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/2)#exit
```

Configure Switch B.

```
SwitchB(config)#interface gigabitEthernet 1/1/1
SwitchB(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchB(config-gigabitEthernet1/1/1)#exit
SwitchB(config)#interface gigabitEthernet 1/1/2
SwitchB(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchB(config-gigabitEthernet1/1/2)#exit
SwitchB(config)#interface gigabitEthernet 1/1/3
SwitchB(config-gigabitEthernet1/1/3)#switchport access vlan 3
SwitchB(config-gigabitEthernet1/1/3)#exit
SwitchB(config)#interface gigabitEthernet 1/1/4
SwitchB(config-gigabitEthernet1/1/4)#switchport access vlan 4
SwitchB(config-gigabitEthernet1/1/4)#exit
```

Configure Switch C.

```
SwitchC(config)#interface gigabitEthernet 1/1/1
SwitchC(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchC(config-gigabitEthernet1/1/1)#exit
SwitchC(config)#interface gigabitEthernet 1/1/2
SwitchC(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchC(config-gigabitEthernet1/1/2)#exit
SwitchC(config)#interface gigabitEthernet 1/1/3
SwitchC(config-gigabitEthernet1/1/3)#switchport access vlan 3
SwitchC(config-gigabitEthernet1/1/3)#exit
SwitchC(config)#interface gigabitEthernet 1/1/4
SwitchC(config-gigabitEthernet1/1/4)#switchport access vlan 4
SwitchC(config-port)#exit
```

- Step 3 Configure spanning tree mode of Switch A, Switch B, and Switch C to MSTP, and enable STP. Enter MSTP configuration mode, and configure the region name to aaa and revision version to 0. Map instance 3 to VLAN 3, and instance 4 to VLAN 4. Exit from MST configuration mode.

Configure Switch A.



```
SwitchA(config)#spanning-tree mode mstp
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree region-configuration
SwitchA(config-region)#name aaa
SwitchA(config-region)#revision-level 0
SwitchA(config-region)#instance 3 vlan 3
SwitchA(config-region)#instance 4 vlan 4
```

Configure Switch B.

```
SwitchB(config)#spanning-tree mode mstp
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree region-configuration
SwitchB(config-region)#name aaa
SwitchB(config-region)#revision-level 0
SwitchB(config-region)#instance 3 vlan 3
SwitchB(config-region)#instance 4 vlan 4
SwitchB(config-region)#exit
```

Configure Switch C.

```
SwitchC(config)#spanning-tree mode mstp
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree region-configuration
SwitchC(config-region)#name aaa
SwitchC(config-region)#revision-level 0
SwitchC(config-region)#instance 3 vlan 3
SwitchC(config-region)#instance 4 vlan 4
```

- Step 4 Configure the internal path cost of GE 1/1/3 of spanning tree instance 3 to 500000 on Switch B.

```
SwitchB(config)#interface gigabitEthernet 1/1/3
SwitchB(config-port)#spanning-tree instance 3 inter-path-cost 500000
```

## Checking results

Use the **show spanning-tree region-operation** command to show configurations of the MST region.

Take Switch A for example.

```
SwitchA#show spanning-tree region-operation
Operational Information:
```

```
-----
Name: aaa
Revision level: 0
Instances running: 3
Digest: 0x024E1CF7E14D5DBBD9F8E059D2C683AA
Instance  Vlan Mapped
-----
1-2,5-4094
3
4
```

Use the **show spanning-tree instance 3** command to show basic information about spanning tree instance 3.

Take Switch A for example.

```
SwitchA#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP

MST ID: 3
-----
BridgeId:    Mac 000E.5E11.2233  Priority 32768
RegionalRoot: Mac 000E.5E11.2233  Priority 32768  InternalRootCost 0
Port      PortState  PortRole  PathCost  PortPriority  LinkType
-----
```

Use the **show spanning-tree instance 4** command to show basic information about spanning tree instance 4.

Take Switch A for example.

```
SwitchA#show spanning-tree instance 4
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP

MST ID: 4
-----
BridgeId:    Mac 000E.5E11.2233  Priority 32768
RegionalRoot: Mac 000E.5E11.2233  Priority 32768  InternalRootCost 0
Port      PortState  PortRole  PathCost  PortPriority  LinkType
-----
```

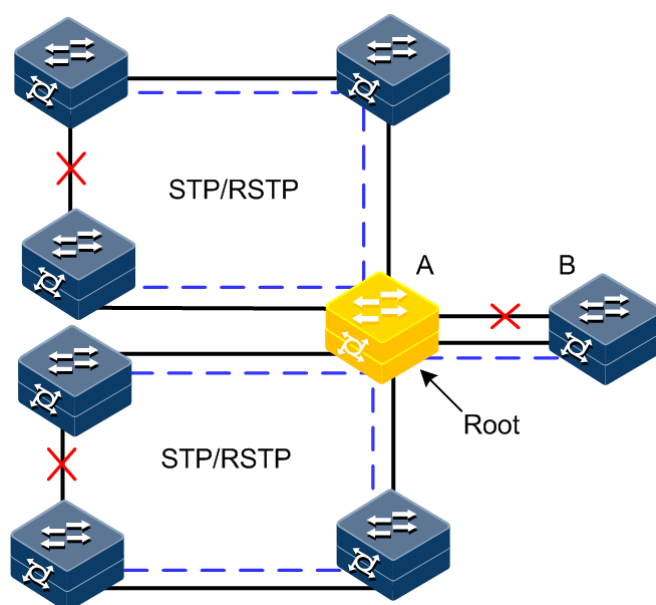
## 2.8 MRSTP

### 2.8.1 Introduction

RSTP aims to trim a bridged LAN to a logical single spanning tree. A tree network must have a root, so the concept of the root bridge is introduced. There is only one root bridge on the entire network while other devices are called leaf nodes.

As shown in Figure 2-19, when running RSTP, device B is generally elected as the root bridge. When these ring networks do not want or fit to run MSTP, device A is specified as the root bridge of the ring network while device B is the root bridge of device A. You can create multiple MRSTP processes on device A and bind the interfaces connecting these ring networks to the specified processes. In this case, when devices on these ring networks, they will elect device A as the root bridge of each ring network while device A will elect device B as its root bridge.

Figure 2-19 Configuring MRSTP for specifying root bridge



### 2.8.2 Preparing for configurations

#### Scenarios

When device A is connected upstream to device B which has a higher priority, device B will be elected as the root bridge. Device A is concurrently connected to multiple ring networks which run STP/RSTP only, so device A is expected to be specified as the root bridge of devices of multiple ring networks, to forward all traffic, and to choose device B as the root bridge.

#### Prerequisite

N/A

## 2.8.3 Default configurations of MRSTP

Default configurations of MRSTP are as below.

Function	Default value
MRSTP process	0
Interface MRSTP status	Enable
Device MRSTP priority	32768
Interface MRSTP priority	128
Path cost of the interface	0
Max Age timer	20s
Hello Time timer	2s
Forward Delay timer	15s

## 2.8.4 Enabling MRSTP

Enable MRSTP for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree enable</b>	Enable STP.
3	<b>Raisecom(config)#spanning-tree mode mrstp</b>	Configure the mode of the spanning tree to MRSTP.
4	<b>Raisecom(config)#spanning-tree mrstp pro-id</b>	Create an MRSTP.
5	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical layer interface configuration mode.
6	<b>Raisecom(config-gigaethernet1/1/port)#spanning-tree mrstp pro-id</b>	Bind the interface to the specified process.

## 2.8.5 Configuring MRSTP parameters

Configure MRSTP parameters for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#spanning-tree mrstp pro-id priority priority</b>	(Optional) configure the priority of the specified process.

Step	Command	Description
3	<b>Raisecom(config)#spanning-tree root {primary  secondary}</b>	(Optional) configure the device as the root device or secondary root device.
4	<b>Raisecom(config)#interface interface-type interface-number</b> <b>Raisecom(config-gigaethernet1/1/port)#spanning-tree priority priority-value</b>	(Optional) configure the priority of the interface.
5	<b>Raisecom(config-gigaethernet1/1/port)# spanning-tree [ instance instance-id ] inter-path-cost cost</b> <b>Raisecom(config-gigaethernet1/1/port)#exit</b>	(Optional) configure the path cost of the interface.
6	<b>Raisecom(config)#spanning-tree hello-time value</b>	(Optional) configure the Hello timer.
7	<b>Raisecom(config)#spanning-tree transit-limit value</b>	(Optional) configure the maximum transmission rate of the interface.
8	<b>Raisecom(config)#spanning-tree forward-delay value</b>	(Optional) configure the Forward Delay.
9	<b>Raisecom(config)#spanning-tree max-age value</b>	(Optional) configure the Max Age.

## 2.8.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show spanning-tree mrstp pro-id</b>	Show basic configurations of MRSTP.

## 2.9 Loop detection

### 2.9.1 Introduction

Loop detection can address the influence on network caused by a loop, providing the self-detection, fault-tolerance, and robustness.

During loop detection, an interface enabled with loop detection periodically sends loop detection packets (Hello packets). Under normal conditions, the edge interface should not receive any loop detection packets because loop detection is applied to the edge interface. However, if the edge interface receives a loop detection packet, it is believed that a loop occurs on the network. There are two conditions that an edge interface receives a loop detection packet: receiving a loop detection packet from itself or receiving a loop detection

packet from other devices, which can be told by comparing the MAC address of the device and the MAC address carried in the packet.

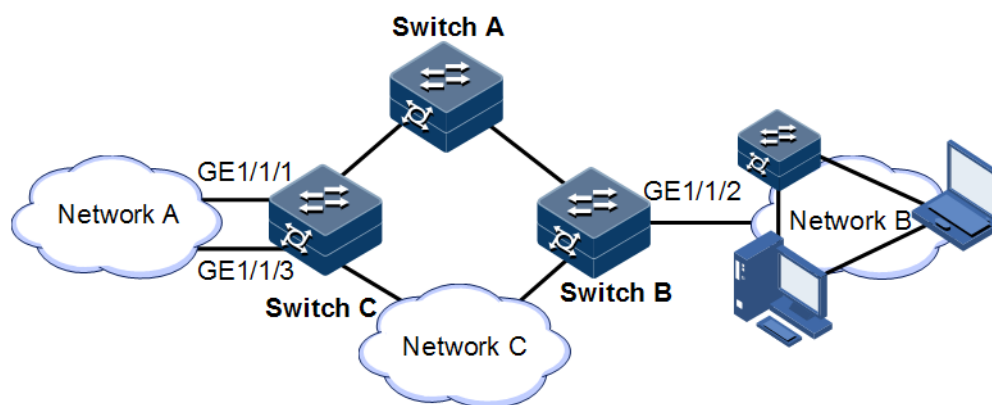
## Loop types

Common loop types include self-loop and inner loop.

As shown in Figure 2-20, Switch B and Switch C are connected to the user network.

- Self-loop: a user loop on the same Ethernet interface of the same device. User network B has a loop, which forms self-loop on GE 1/1/2 on Switch B.
- Inner loop: a loop forming on different Ethernet interfaces of the same device. GE 1/1/1 and GE 1/1/3 on Switch C forms an inner loop with the user network A.

Figure 2-20 Loop detection networking



## Principles for processing loops

The ISCOM2600G-HI series switch processes loops as below:

- If the device sending the loop detection packet is the one receiving the packet but the interface sending the packet and the interface receiving the packet are different, process the interface with the smaller interface ID to eliminate the loop (inner loop).
- If the interface sending the packet and the interface receiving the packet are the same, process the interface to eliminate the loop (self-loop).

In Figure 2-20, assume that both Switch B and Switch C connect user network interfaces enabled with loop detection. The system processes loops for the three loop types as below:

- Self-loop: the interface sending the packet and the interface receiving the packet on Switch B are the same, the configured loop detection action will be taken to eliminate the loop on GE 1/1/2.
- Inner loop: Switch C receives the loop detection packets sent by it and the interface sending the packet and the interface receiving the packet are the same, the configured loop detection action will be taken to eliminate the loop on the interface with a bigger interface number, namely, GE 1/1/3.

## Action for processing loops

The action for processing loops is the method for the ISCOM2600G-HI series switch to use upon loop detection. You can define different actions on the specified interface according to actual situations, including:

- Block: block the interface and send Trap.
- Trap-only: send Trap only.
- Shutdown: shut down the interface and send Trap.

## Loop detection modes

The loop detection modes consist of port mode and VLAN mode:

- Port mode: when a loop occurs, the system blocks the interface and sends Trap in the loopback processing mode of Block, or shuts down the physical interface and sends Trap information in the loopback processing mode of shutdown.
- VLAN mode: when a loop occurs,
  - In loopback processing mode of Block, when a loop occurs on one or more of VLANs to which the interface belongs, the system blocks the VLANs with loop and leaves other VLANs to normally receive or send packets.
  - In loopback processing mode of shutdown, the system shuts down the physical interface and sends Trap information.

If the loop detection processing mode is Trap-only in the previous two modes, the ISCOM2600G-HI series switch sends Trap only.

## Loop restoration

After an interface is blocked or shut down, you can configure it, such as no automatic restoration and automatic restoration after a specified period.

- If an interface is configured as automatic restoration after a specified period, the system will start loop detection after the period. If the loop disappears, the interface will be restored. Otherwise, it will be kept in blocking or shutdown status.
- If an interface is configured as no automatic restoration, in other words, the automatic restoration time is infinite, it will not be automatically restored.

## 2.9.2 Preparing for configurations

### Scenario

On the network, hosts or Layer 2 devices connected to access devices may form a loop intentionally or involuntarily. Enable loop detection on downlink interfaces on all access devices to avoid the network congestion generated by unlimited copies of data traffic. Once a loopback is detected on an interface, the interface will be blocked.

### Prerequisite

Loopback interface, interface backup, STP, G.8032, and RRPS interfere with each other. We do not recommend configuring two or more of them concurrently.

## 2.9.3 Default configurations of loop detection

Default configurations of loop detection are as below.

Function	Default value
Loop detection status	Disable
Automatic recovery time for the blocked interface	Infinite, namely, no automatic recovery
Mode for processing detected loops	trap-only
Loop detection period	4s
Loop detection mode	VLAN

## 2.9.4 Configuring loop detection



### Note

- Loop detection and STP are exclusive, so only one can be enabled at a time.
- Loop detection cannot be concurrently enabled on both two directly-connected devices.

Configure loop detection based on interface+VLAN for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter interface configuration mode. The device also supports batch interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaetherne</b> <b>t1/1/port)#loopback-</b> <b>detection</b> <b>[ pkt-vlan { untag   vlan-</b> <b>id } ] [ hello-time</b> <i>second</i> <b>] [ restore-</b> <b>time</b> <i>second</i> <b>] [ action { block   trap-</b> <b>only   shutdown   shutdown-restore } ]</b> <b>[ log-interval</b> <i>log-interval time</i> <b>]</b>  <b>Raisecom(config-</b> <b>gigaetherne</b> <b>t1/1/port)#loopback-</b> <b>detection detect-vlanlist</b> <i>vlanlist</i> <b>[ hello-time</b> <i>second</i> <b>] [ restore-</b> <b>time</b> <i>second</i> <b>] [ action { block  </b> <b>trap-only   shutdown   shutdown-</b> <b>restore } ] [ log-interval</b> <i>log-</i> <i>interval time</i> <b>]</b>	Enable loop detection on the interface.  Configure the VLAN for sending loop detection packets.  (Optional) configure the period for sending Hello packets.  (Optional) configure the time for automatically restoring the blocked interface due to loop detection and the action for processing loops.
4	<b>Raisecom(config-</b> <b>gigaetherne</b> <b>t1/1/port)#loopback-</b> <b>detection manual restore</b>	Manually restore the interface blocked due to loop detection.



## 2.9.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show loopback-detection</b> [ <b>statistics</b> ] [ <i>interface-type interface-number</i> ] [ <b>details</b> ]	Show configurations and status of loop detection.

## 2.9.6 Maintenance

Use the following commands to maintain the ISCOM2600G-HI series switch.

Command	Description
<b>Raisecom(config)#clear loopback-detection statistic</b> [ <i>interface-type interface-number</i> ]	Clear statistics about loop detection.

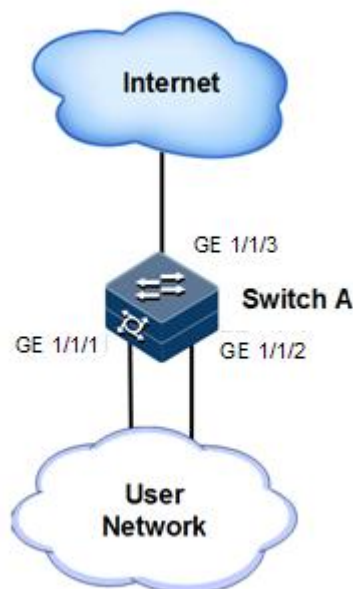
## 2.9.7 Example for configuring inner loop detection

### Networking requirements

As shown in Figure 2-21, GE 1/1/2 and GE 1/1/3 on Switch A are connected to the user network. To avoid loops on the user network, enable loop detection on Switch A to detect loops on user network, and then take actions accordingly. Detailed requirements are as below:

- Enable loop detection on GE 1/1/2 and GE 1/1/3.
- Configure the interval for sending loop detection packets to 3s.
- Configure the VLAN for sending loop detection packets to VLAN 3.
- Configure the loop detection processing action to discarding, namely, sending Trap and blocking the interface.

Figure 2-21 Loop detection networking



## Configuration steps

Step 1 Create VLAN 3, and add interfaces to VLAN 3.

```
Raisecom#config
Raisecom(config)#create vlan 3 active
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#switchport access vlan 3
Raisecom(config-gigabitEthernet1/1/1)#exit
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#switchport access vlan 3
Raisecom(config-gigabitEthernet1/1/2)#exit
```

Step 2 Configure the VLAN for sending loop detection packets, action taken for detected loops, and period for sending loop detection packets.

```
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#loopback-detection pkt-vlan 3 hello-
time 3 action block
Raisecom(config-gigabitEthernet1/1/1)#exit
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#loopback-detection pkt-vlan 3 hello-
time 3 action block
```

## Checking results

Use the **show loopback-detection** command to show loop detection status. GE 1/1/2 is already blocked because of its greater interface ID, so the loop is eliminated.

```
Raisecom#show loopback-detection
Interface pktvlan detect-vlanlist hellotime restoretime loop-act
log-interval Status loop-srcMAC loop-srcPort loop-Duration loop-
vlanlist
-----
-----
GE1/1/1 3 -- 1 5 block 0
no -- -- -- --
GE1/1/2 3 -- 1 5 block 0
no -- -- -- --
```

## 2.10 Interface protection

### 2.10.1 Introduction

With interface protection, you can add an interface, which needs to be controlled, to an interface protection group, isolating Layer 2/Layer 3 data in the interface protection group. This can provide physical isolation between interfaces, enhance network security, and provide flexible networking scheme for users.

After being configured with interface protection, interfaces in an interface protection group cannot transmit packets to each other. Interfaces in and out of the interface protection group can communicate with each other. So do interfaces out of the interface protection group.

### 2.10.2 Preparing for configurations

#### Scenario

Interface protection can implement mutual isolation of interfaces in the same VLAN, enhance network security and provide flexible networking solutions for you.

#### Prerequisite

N/A

### 2.10.3 Default configurations of interface protection

Default configurations of interface protection are as below.

Function	Default value
Interface protection status of each interface	Disable

## 2.10.4 Configuring interface protection



### Caution

Interface protection is unrelated with the VLAN to which the interface belongs.

Configure interface protection for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/port)#switchport protect</b>	Enable interface protection. Interface isolation is supported across devices in the ISF. Interface isolation can be implemented based on LAG interface, namely, between LAG interfaces, and between a LAG interface and common interface.

## 2.10.5 Configuring interface isolation

Configure interface isolation for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#protect-group</b> <i>group-id</i> <b>vlan</b> <i>vlan-id</i> <i>interface-type</i> <i>interface-number</i>	Create an interface isolation group. Configure isolation VLANs associated with the group and the list of isolated interfaces.

## 2.10.6 Checking configurations

Use the following commands to check configuration results.

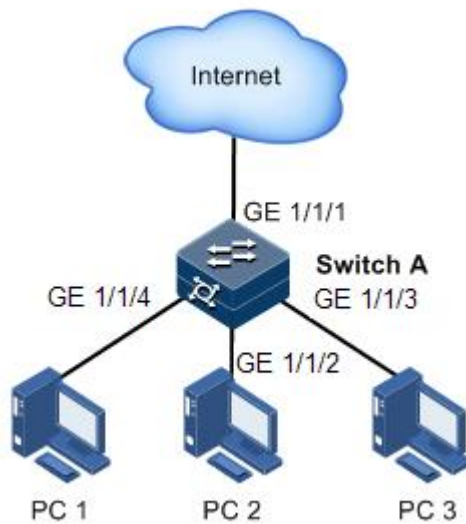
No.	Command	Description
1	<b>Raisecom#show switchport protect</b>	Show configurations of interface protection.
2	<b>Raisecom#show protect-group</b> { <b>all</b>   <i>group-id</i> }	Show configurations of interface isolation.

## 2.10.7 Example for configuring interface protection

### Networking requirements

As shown in Figure 2-22, to prevent PC 1 and PC 2 from interconnecting with each other and to enable them to interconnect with PC 3 respectively, enable interface protection on GE 1/1/1 and GE 1/1/2 on Switch A.

Figure 2-22 Interface protection networking



### Configuration steps

Step 1 Enable interface protection on the GE 1/1/1.

```
Raisecom#config
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#switchport protect
Raisecom(config-gigabitEthernet1/1/1)#exit
```

Step 2 Enable interface protection on the GE 1/1/2.

```
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#switchport protect
```

### Checking results

Use the **show switchport protect** command to show configurations of interface protection.

```
Raisecom#show switchport protect
Port                Protected State
-----
gigaethernet1/1/1   enable
gigaethernet1/1/2   enable
gigaethernet1/1/3   disable
gigaethernet1/1/4   disable
gigaethernet1/1/5   disable
gigaethernet1/1/6   disable
.....
```

Check whether PC 1 and PC 2 can ping PC 3 successfully.

- PC 1 can ping PC 3 successfully.
- PC 2 can ping PC 3 successfully.

Check whether PC 1 can ping PC 2 successfully.

PC 1 fails to ping PC 3, so interface protection has taken effect.

## 2.11 Port mirroring

### 2.11.1 Introduction

Port mirroring refers to assigning some packets mirrored from the source port to the destination port, such as from the monitor port without affecting the normal packet forwarding. You can monitor sending and receiving status for packets on a port through this function and analyze the related network conditions.

Figure 2-23 Principles of port mirroring

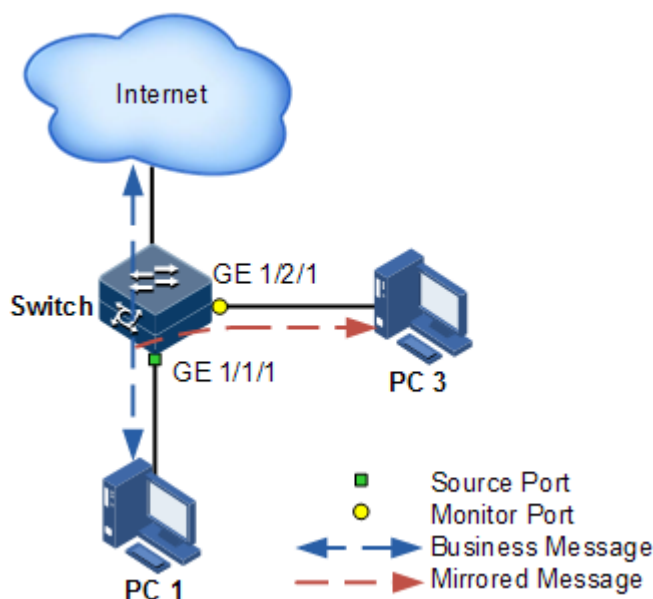


Figure 2-23 shows principles of port mirroring. PC 1 is connected to the external network by the GE 1/1/1; PC 3 is the monitor PC, connecting the external network by GE 1/2/1.

When monitoring packets from the PC 1, you need to assign GE 1/1/1 to connect to PC 1 as the mirror source port, enable port mirroring on the ingress port and assign GE 1/2/1 as monitor port to mirror packets to destination port.

When service packets from PC 1 enter the ISCOM2600G-HI series switch, the ISCOM2600G-HI series switch will forward and copy them to monitor port (GE 1/2/1). The monitor device connected to mirror the monitor port can receive and analyze these mirrored packets.

The ISCOM2600G-HI series switch supports mirroring data stream on the ingress port and egress port. The packets on the ingress/egress mirroring port will be copied to the monitor port after the switch is enabled with port mirroring. The monitor port and mirroring port cannot be the same one.

## 2.11.2 Preparing for configurations

### Scenario

Port mirroring is used to monitor the type and flow of network data regularly for the network administrator.

Port mirroring copies the port flow monitored to a monitor port or CPU to obtain the ingress/egress port failure or abnormal flow of data for analysis, discovers the root cause, and solves them timely.

### Prerequisite

N/A

## 2.11.3 Default configurations of port mirroring

Default configurations of port mirroring are as below.

Function	Default value
Port mirroring status	Disable
Mirroring the source port	N/A

## 2.11.4 Configuring port mirroring on local port

Configure local port mirroring for the ISCOM2600G-HI series switch as below.

Step	Configure	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mirror-group group-id</code>	Create a port mirroring group.
3	<code>Raisecom(config)#mirror-group group-id remote-vlan vlan-id</code>	Configure the remote mirroring VLAN for the mirroring group.

Step	Configure	Description
4	<code>Raisecom(config)#<b>mirror-group</b> <i>group-id</i> <b>reflector-port</b> <i>interface-type</i> <i>interface-number</i></code>	Configure the reflector interface for the mirroring group.
5	<code>Raisecom(config)#<b>interface</b> <i>interface-type</i> <i>interface-number</i></code>	Enter physical interface configuration mode.
6	<code>Raisecom(config-gigaethernet1/1/port)#<b>mirror-group</b> <i>group-id</i> <b>monitor-port</b></code>	Configure the monitor port for mirroring.
7	<code>Raisecom(config-gigaethernet1/1/port)#<b>mirror-group</b> <i>group-id</i> <b>source-port</b> { <b>ingress</b>   <b>egress</b> }</code>	Configure the mirroring port of port mirroring, and designate the mirroring rule for port mirroring. Port mirroring supports mirroring packets in both the ingress and egress directions of the port.
8	<code>Raisecom(config-gigaethernet1/1/port)#<b>exit</b></code> <code>Raisecom(config)#<b>mirror-group</b> <i>group-id</i> <b>source-cpu</b> [ <b>ingress</b>   <b>egress</b> ]</code>	Configure port mirroring to mirror packets to or from the CPU.

## 2.11.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#<b>show mirror-group</b> [ <i>group-id</i> ]</code>	Show configurations of port mirroring.

## 2.11.6 Example for configuring port mirroring

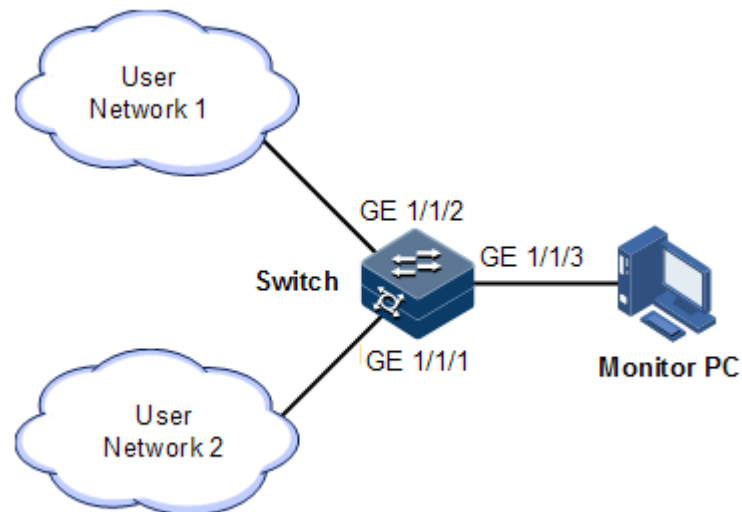
### Networking requirements

As shown in Figure 2-24, the network administrator wants to monitor user network 1 through the monitor device, then to catch the fault or abnormal data flow for analyzing and discovering faults and then solve them in time.

The ISCOM2600G-HI series switch is disabled with storm control and automatic packets sending. User network 1 accesses the ISCOM2600G-HI series switch through GE 1/1/1, user network 2 accesses the ISCOM2600G-HI series switch through GE 1/1/2, and the data monitor device is connected to GE 1/1/3.



Figure 2-24 Port mirroring networking



## Configuration steps

Enable port mirroring on the Switch.

```
Raisecom#config
Raisecom(config)#mirror-group 1
Raisecom(config)#interface gigabitEthernet 1/1/3
Raisecom(config-gigabitEthernet1/1/3)#mirror-group 1 monitor-port
Raisecom(config-gigabitEthernet1/1/3)#exit
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#mirror-group 1 source-port ingress
```

## Checking results

Use the **show mirror** command to show configurations of port mirroring.

```
Raisecom#show mirror-group
Mirror Group 1 :
Monitor Port :
    gigabitEthernet1/1/3
Source Port :
    gigabitEthernet1/1/1      : ingress
    gigabitEthernet1/1/2      : ingress
Remote Vlan: --
```

## 2.12 L2CP

### 2.12.1 Introduction

Metro Ethernet Forum (MEF) introduces service concepts, such as EPL, EVPL, EP-LAN, and EVP-LAN. Different service types have different processing modes for Layer 2 Control Protocol (L2CP) packets.

MEF6.1 defines processing modes for L2CP as below.

- Discard: discard the packet, by applying the configured L2CP profile on the ingress interface of the ISCOM2600G-HI series switch, to complete configuring processing mode.
- Peer: send packets to the CPU in the same way as the discard action.
- Tunnel: send packets to the MAN. It is more complex than discard and peer mode, requiring cooperating profile at network side interface and carrier side interface tunnel terminal to allow packets to pass through the carrier network.

### 2.12.2 Preparing for configurations

#### Scenario

On the access device of MAN, you can configure profile on user network interface according to services from the carrier to configure L2CP of the user network.

#### Prerequisite

N/A

### 2.12.3 Default configurations of L2CP

Default configurations of L2CP are as below.

Function	Default value
Global L2CP status	Disable
Applying the profile on the interface	Disable
Specified multicast destination MAC address	0x0100.0ccd.cdd0
Description of the L2CP profile	N/A

### 2.12.4 Configuring global L2CP

Configure global L2CP for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<b>Raisecom(config)#l2cp-process tunnel destination-address mac-address</b>	(Optional) configure the destination MAC address for transparently transmitted packets.

## 2.12.5 Configuring L2CP profile

Configure the L2CP profile for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#l2cp-process profile profile-number</b>	Create and enter the L2CP profile.
3	<b>Raisecom(config-l2cp-profile)#name string</b>	(Optional) add profile description.
4	<b>Raisecom(config-l2cp-profile)#l2cp-process protocol { oam   stp   dot1x   lacp   lldp   cdp   vtp   pvst   all } action { tunnel   drop   peer }</b>	(Optional) configure the mode for processing L2CP packets.
5	<b>Raisecom(config-l2cp-profile)#tunnel vlan vlan-id</b>	(Optional) configure the specified VLAN for transparent transmission.
6	<b>Raisecom(config-l2cp-profile)#tunnel interface-type interface-number</b>	(Optional) configure the specified egress interface for transparent transmission.
7	<b>Raisecom(config-l2cp-profile)#tunnel tunnel-type mac</b>	(Optional) configure the type of the tunnel for transparent transmission.

## 2.12.6 Configuring L2CP profile on interface

Configure the L2CP profile on the interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/port)#l2cp profile profile-number</b>	Apply the L2CP profile on the interface.



## Note

Applying a profile to an interface takes effect unless global L2CP is enabled. You can configure it but it will not take effect if global L2CP is disabled.

## 2.12.7 Checking configurations

Use the following commands check configuration results.

No.	Command	Description
1	Raisecom# <b>show l2cp-process</b> profile [ <i>profile-number</i> ]	Show information about the created L2CP profile.
2	Raisecom# <b>show l2cp-process</b> [ <i>interface-type interface-number</i> ]	Show configurations of L2CP on the interface.
3	Raisecom# <b>show l2cp-process</b> [ <b>tunnel statistics</b> ] [ <i>interface-type interface-number</i> ]	Show statistics about L2CP packets on the interface.

## 2.12.8 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
Raisecom(config)# <b>clear l2cp-process tunnel statistic</b> [ <i>interface-type interface-number</i> ]	Clear statistics about L2CP packets on the interface.

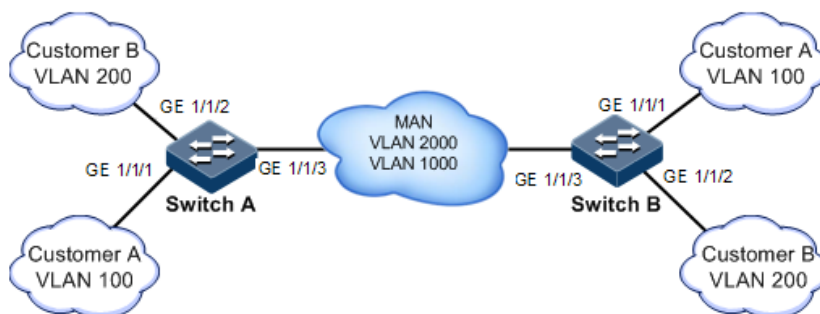
## 2.12.9 Example for configuring L2CP

### Networking requirements

As shown in Figure 2-25, configure L2CP on Switch A and Switch B as below.

- Specify the multicast destination MAC address of them to 0100.1234.1234.
- Configure the STP packets of Customer A to traverse the MAN, and discard other packets.
- Configure the STP and VTP packets of Customer B to traverse the MAN, send elmi packets to the CPU, and discard other packets.

Figure 2-25 L2CP networking



## Configuration steps

Configure Switch A and Switch B.

Configurations of Switch A and Switch B are identical. Take Switch A for example.

Step 1 Configure the switch name.

```
Raisecom#name SwitchA
```

Step 2 Configure the specified multicast destination MAC address.

```
Raisecom(config)#l2cp-process tunnel destination-address 0100.1234.1234
```

Step 3 Configure L2CP profile 1, and apply the profile to GE 1/1/1 for Customer A.

```
Raisecom(config)#l2cp-process profile 1
Raisecom(config-l2cp-profile)#name CustomerA
Raisecom(config-l2cp-profile)#l2cp-process protocol all action drop
Raisecom(config-l2cp-profile)#l2cp-process protocol stp action tunnel
Raisecom(config-l2cp-profile)#exit
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#l2cp-process profile 1
Raisecom(config-gigabitEthernet1/1/1)#exit
```

Step 4 Configure L2CP profile 2, and apply the profile to GE 1/1/2 for Customer B.

```
Raisecom(config)#l2cp-process profile 2
Raisecom(config-l2cp-profile)#name CustomerB
Raisecom(config-l2cp-profile)#l2cp-process protocol all action drop
Raisecom(config-l2cp-profile)#l2cp-process protocol stp action tunnel
Raisecom(config-l2cp-profile)#l2cp-process protocol vtp action tunnel
```

```
Raisecom(config-l2cp-profile)#l2cp-process protocol elmi action peer
Raisecom(config-l2cp-profile)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#l2cp-process profile 2
Raisecom(config-gigaethernet1/1/2)#exit
```

## Checking results

Use the **show l2cp-profile** command to show L2CP configurations.

```
Raisecom#show l2cp-process profile
Destination MAC Address for Encapsulated Packets: 0100.1234.1234
ProfileId: 1
Name: customerA
BpduType      Mac-address      l2cp-process  Mac-vlan  EgressPort  tunneltype
-----
stp           0180.C200.0000  tunnel      --          none
dot1x        0180.C200.0003  drop        --          none
lacp         0180.C200.0002  drop        --          none
oam          0180.C200.0002  drop        --          none
cdp          0100.0CCC.CCCC  drop        --          none
vtp          0100.0CCC.CCCC  drop        --          none
pvst         0100.0CCC.CCCD  drop        --          none
lldp         0180.C200.000E  drop        --          none
elmi         0180.C200.0007  drop        --          none
udld         0100.0CCC.CCCC  drop        --          none
pagp         0100.0CCC.CCCC  drop        --          none
ProfileId: 2
Name: customerB
BpduType      Mac-address      l2cp-process  Mac-vlan  EgressPort  tunneltype
-----
stp           0180.C200.0000  tunnel      --          none
dot1x        0180.C200.0003  drop        --          none
lacp         0180.C200.0002  drop        --          none
oam          0180.C200.0002  drop        --          none
cdp          0100.0CCC.CCCC  drop        --          none
vtp          0100.0CCC.CCCC  tunnel      --          none
pvst         0100.0CCC.CCCD  drop        --          none
lldp         0180.C200.000E  drop        --          none
elmi         0180.C200.0007  peer        --          none
udld         0100.0CCC.CCCC  drop        --          none
pagp         0100.0CCC.CCCC  drop        --          none
...
```

Use the **show l2cp-process** command to show interface configurations.

```
Raisecom#show l2cp-process
L2CP running information
```

Port	ProfileID	BpduType	mac-address	l2cp-process
-----				
-----				
GE1/1/1	1	stp	0180.C200.0000	tunnel
		dot1x	0180.C200.0003	drop
		lACP	0180.C200.0002	drop
		oam	0180.C200.0002	drop
		cdp	0100.0CCC.CCCC	drop
		vtp	0100.0CCC.CCCC	drop
		pvst	0100.0CCC.CCCD	drop
		lldp	0180.C200.000E	drop
		elmi	0180.C200.0007	drop
		udld	0100.0CCC.CCCC	drop
		pagp	0100.0CCC.CCCC	drop
GE1/1/2	2	stp	0180.C200.0000	tunnel
		dot1x	0180.C200.0003	drop
		lACP	0180.C200.0002	drop
		oam	0180.C200.0002	drop
		cdp	0100.0CCC.CCCC	drop
		vtp	0100.0CCC.CCCC	tunnel
		pvst	0100.0CCC.CCCD	drop
		lldp	0180.C200.000E	drop
		elmi	0180.C200.0007	peer
		udld	0100.0CCC.CCCC	drop
		pagp	0100.0CCC.CCCC	drop
GE1/1/3	--	--	--	--
GE1/1/4	--	--	--	--
GE1/1/5	--	--	--	--
...				

## 2.13 Voice VLAN

### 2.13.1 Introduction

With increasing growth of voice technologies, voice devices are more and more widely used, especially in broadband residential communities. The network usually transmits voice traffic and data traffic concurrently, but voice traffic requires a higher priority than data traffic in transmission to avoid delay and packet loss.

A voice VLAN is especially partitioned for voice traffic of users. By partitioning voice VLANs and add interfaces of the voice device to voice VLANs, you can configure QoS of voice traffic to increase the priority of transmitting voice traffic and guarantee call quality.

Compared with other methods for managing voice traffic, the voice VLAN has the following advantages:

- Easy configuration: after you configure the voice device in global configuration mode and interface configuration mode and enable the voice VLAN, the voice device can classify and process voice traffic.
- Easy maintenance: you can modify rules (voice VLAN OUI address) for matching voice traffic in global configuration mode. When a new IP voice device joins the network, its interfaces can rapidly identify voice traffic by updated matching rules.

- Flexible implementation: The voice VLAN supports safe mode and common mode in global configuration mode and automatic mode and manual mode on the interface, so it is flexible in implementation. You can combine these modes as required to meet users' requirements to the maximum extent.
  - Secure mode: in the voice VLAN, the packets mismatching OUI are discarded while the packets matching OUI are modified with the priority and then forwarded.
  - Common mode: in the voice VLAN, the packets mismatching OUI are not modified with the priority and are normally forwarded while the packets matching OUI are modified with the priority and then forwarded.
  - Automatic mode: in this mode, the interface automatically joins the voice VLAN. You do not need to add the interface to the voice LAN; when the switch receives voice packets, it will automatically add the interface to the voice VLAN. When the interface fails to receive voice packets for a specified period, it will automatically quit the voice VLAN.
  - Manual mode: in this mode, you need to manually add the interface to the voice VLAN. The interface does not automatically join and leave the voice VLAN.

The ISCOM2600G-HI series switch supports the following two networking modes.

Figure 2-26 shows the networking mode for IP phone (with its interfaces transmitting voice traffic only) to connect to the switch. This mode enables these interfaces to transmit voice traffic only, thus minimizing the impact on voice traffic from data traffic.

Figure 2-26 Networking for IP phone to connect to switch

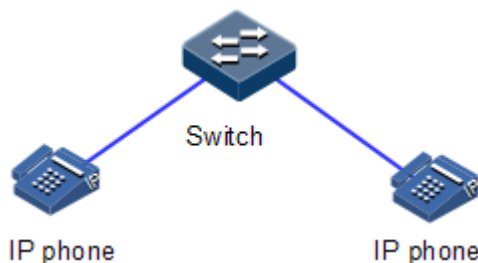
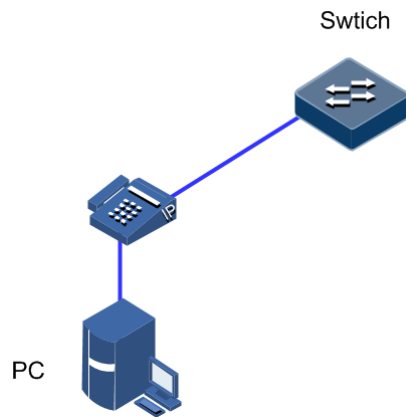


Figure 2-27 shows the networking mode for the IP phone to connect the PC to the switch (transmitting voice packets only), so the link transmits both voice traffic and data traffic. In this networking mode, voice traffic and data traffic are transmitted in the voice VLAN and data VLAN respectively with affecting each other. When office staff need data communication through PCs and also need voice communication through IP phones, you can adopt this networking mode.



Figure 2-27 Networking for IP phone to connect PC to the switch



## 2.13.2 Preparing for configurations

### Scenario

The voice VLAN can transmit voice traffic. You can choose one of the following networking schemes according to whether voice packets are tagged or not:

- If the IP phone sends untagged voice packets, see section Example for adding interface to voice VLAN and configuring it to work in manual mode.
- If the IP phone supports obtaining the voice VLAN configured on the switch through LLDP, it will send tagged voice packets. For details, see section 2.13.9 Example for configuring IP phone to access voice VLAN packets through LLDP.

### Prerequisite

Create a VLAN, and configure its parameters.

## 2.13.3 Default configurations of voice VLAN

Default configurations of Organizationally Unique Identifier (OUI) of the voice VLAN are as below.

OUI-Address	Mask address	Description
0001.E300.0000	FFFF.FF00.0000	Siemens-phone
0003.6B00.0000	FFFF.FF00.0000	Cisco-phone
0004.0D00.0000	FFFF.FF00.0000	Avaya-phone
00D0.1E00.0000	FFFF.FF00.0000	Pingtel-phone
0060.B900.0000	FFFF.FF00.0000	Philips/NEC-phone
00E0.7500.0000	FFFF.FF00.0000	Verilink-phone
00E0.BB00.0000	FFFF.FF00.0000	NBX-phone

Other default configurations of the voice VLAN are as below.

Function	Default value
Voice VLAN	Disable
Voice VLAN secure working mode	Disable
Voice VLAN common working mode	Enable
Automatic mode for the interface to join the voice VLAN	Disable
Manual mode for the interface to join the voice VLAN	Enable
CoS and DSCP of Voice VLAN packets	6 and 46 respectively
QoS trust priority of Voice VLAN	N/A

## 2.13.4 Configuring QoS of voice VLAN

Configure the QoS of the voice VLAN for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#voice-vlan</b> <b>qos cos cos value dscp dscp value</b>	Configure CoS and DSCP of voice VLAN packets.
4	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#voice-vlan</b> <b>qos trust</b>	Configure QoS trust priority of the voice VLAN. Then, the interface does not modify the priority of voice VLAN packets.

## 2.13.5 Enabling voice VLAN

Enable the voice VLAN for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.

Step	Command	Description
3	Raisecom(config-gigaetherne1/1/port)# <b>voice-vlan <i>vlan-id</i> enable</b> [ <b>include-untagged</b> ]	Enable the voice VLAN. After the voice VLAN is enabled, the device in include-untag mode will add a voice VLAN Tag to untagged packets of which the source MAC address matches the OUI address. When the IP phone sends untagged voice packets, you should configure the <b>include-untagged</b> parameter.
4	Raisecom(config-gigaetherne1/1/port)# <b>voice-vlan auto { enable   disable }</b>	Configure the working mode for the interface to join the voice VLAN.
5	Raisecom(config)# <b>voice-vlan aging-time <i>time</i></b>	Configure the aging time for the interface to leave the voice VLAN in automatic mode.

## 2.13.6 Configuring OUI address

Configure the OUI address for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>voice-vlan mac-address <i>mac-address</i> [ <i>mask address</i> ] [ <b>description word</b> ]</b>	Configure the OUI of the voice VLAN.

## 2.13.7 Checking configurations

Use the following commands check configuration results.

No.	Command	Description
1	Raisecom# <b>show voice-vlan mac-address</b>	Show the OUI address, its mask, and description.
2	Raisecom# <b>show voice-vlan status</b>	Show the status of the voice VLAN on the current device.
3	Raisecom# <b>show voice-vlan auto</b>	Show the automatic mode of the voice VLAN on the current device.

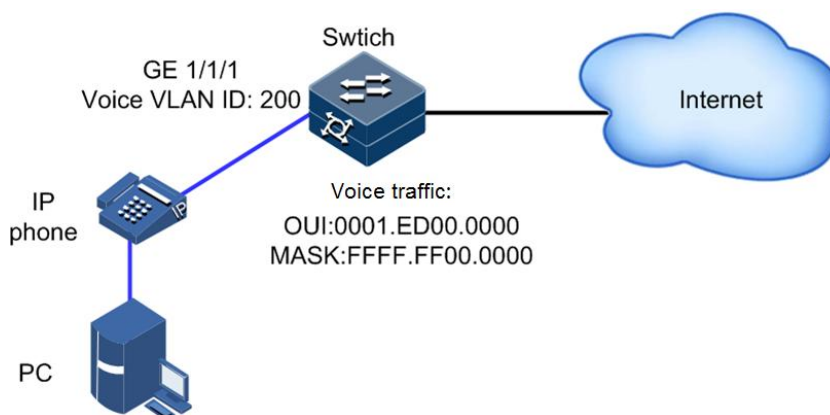
## 2.13.8 Example for adding interface to voice VLAN and configuring it to work in manual mode

### Networking requirements

GE 1/1/1 on the Switch connects the IP phone and PC to the Internet. It is required to concurrently forward and isolate voice traffic and data traffic.

You can configure GE 1/1/1 as a Trunk interface, making the Native VLAN forward data traffic and voice VLAN forward voice traffic. The PC sends untagged packets which are transmitted in the Native VLAN of GE 1/1/1. Configure VLAN 100 as the Native VLAN to transmit data traffic sent from the PC. The IP phone also sends untagged packets. Configure the source MAC address to the OUI address of the voice VLAN so that the device can add voice VLAN Tag when these packets pass the voice VLAN interface. Configure VLAN 200 as the voice VLAN to transmit voice traffic sent from the IP phone.

Figure 2-28 Networking with adding interface to voice VLAN and configuring it to work in manual mode



### Configuration steps

- Step 1 Create VLAN 100 and VLAN 200, activate them, and configure VLAN 200 as the voice VLAN.

```
Raisecom(config)#create vlan 100,200 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan 100
Raisecom(config-gigaethernet1/1/1)#switchport trunk untag vlan 200
Raisecom(config-gigaethernet1/1/1)#voice-vlan 200 enable include-untagged
```

- Step 2 Configure the MAC address (supporting the mask) of the IP phone as the OUI address of the voice VLAN on the switch, namely, 0001.ED00.0000. Configure the mask to FFFF.FF00.0000. For the OUI supported by the device by default, see section 2.13.3 Default configurations of voice VLAN.

```
Raisecom(config)#voice-vlan mac-address 0001.ED00.0000 FFFF.FF00.0000
```

- Step 3 (Optional) by default, the interface modifies the CoS and DSCP of voice packets to 6 and 46 respectively. To modify them to other values, you should use the following command in the interface view before the voice VLAN is enabled on the interface.

```
Raisecom(config-gigaetherne1/1/1)#voice-vlan qos cos 6 dscp 46
```

- Step 4 (Optional) by default, the interface modifies the CoS and DSCP of voice packets to 6 and 46 respectively. To prevent the interface from modifying them, you should use the following command:

```
Raisecom(config-gigaetherne1/1/1)#voice-vlan qos trust
```

## Checking configurations

Use the **show voice-vlan status** command to view the current status of the voice VLAN.

Use the **show voice-vlan mac-address** command to view the OUI address of the voice VLAN.

```
Raisecom(config)#show voice-vlan mac-address
```

OUI-Address	Mask	Description
0001.E300.0000	FFFF.FF00.0000	Siemens-phone
0003.6B00.0000	FFFF.FF00.0000	Cisco-phone
0004.0D00.0000	FFFF.FF00.0000	Avaya-phone
00D0.1E00.0000	FFFF.FF00.0000	Pingtel-phone
0060.B900.0000	FFFF.FF00.0000	Philips/NEC-phone
00E0.7500.0000	FFFF.FF00.0000	verilink-phone
00E0.BB00.0000	FFFF.FF00.0000	NBX-phone
0001.ED00.0000	FFFF.FF00.0000	

## 2.13.9 Example for configuring IP phone to access voice VLAN packets through LLDP

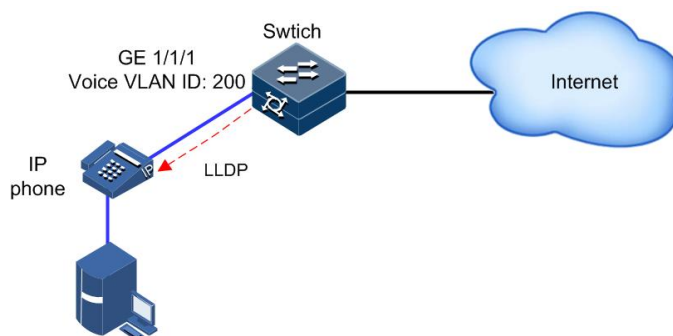
### Networking requirements

As shown in Figure 2-29, when the IP phone supports LLDP, it can obtain the voice VLAN through LLDP. You can configure LLDP and voice VLAN on the switch to connect the IP phone. Configure LLDP on the switch to advertise the voice VLAN of the interface to the IP phone. To guarantee call quality, configure the voice VLAN to prioritize voice packets.

GE 1/1/1 on the Switch connects the IP phone and PC to the Internet. It is required to concurrently forward and isolate voice traffic and data traffic.

You can configure GE 1/1/1 as a Trunk interface, making the Native VLAN forward data traffic and voice VLAN forward voice traffic. The PC sends untagged packets which are transmitted in the Native VLAN of GE 1/1/1. Configure VLAN 100 as the Native VLAN to transmit data traffic sent from the PC. Configure VLAN 200 as the voice VLAN to transmit voice traffic sent from the IP phone. The IP phone obtains the voice VLAN through LLDP and sends packets with the voice VLAN Tag.

Figure 2-29 Configuring IP phone to access voice VLAN packets through LLDP



## Configuration steps

- Step 1 Create VLAN 100 and VLAN 200, activate them, and configure VLAN 200 as the voice VLAN.

```
Raisecom(config)#create vlan 100,200 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan 100
Raisecom(config-gigaethernet1/1/1)#voice-vlan 200 enable
```

- Step 2 Enable global LLDP and interface LLDP to advertise the voice VLAN of the interface to the IP phone.

```
Raisecom(config)#lldp enable
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#lldp enable
```

- Step 3 Configure the MAC address (supporting the mask) of the IP phone as the OUI address of the voice VLAN on the switch, namely, 0001.ED00.0000. Configure the mask to FFFF.FF00.0000. For the OUI supported by the device by default, see section 2.13.3 Default configurations of voice VLAN.

```
Raisecom(config)#voice-vlan mac-address 0001.ED00.0000 FFFF.FF00.0000
```

- Step 4 (Optional) by default, the interface modifies the CoS and DSCP of voice packets to 6 and 46 respectively. To modify them to other values, you should use the following command in the interface view before the voice VLAN is enabled on the interface.

```
Raisecom(config-gigaetherne1/1/1)#voice-vlan qos cos 6 dscp 46
```

- Step 5 (Optional) by default, the interface modifies the CoS and DSCP of voice packets to 6 and 46 respectively. To prevent the interface from modifying them, you should use the following command:

```
Raisecom(config-gigaetherne1/1/1)#voice-vlan qos trust
```

## Checking configurations

Use the **show voice-vlan status** command to view the current status of the voice VLAN.

Use the **show voice-vlan mac-address** command to view the OUI address of the voice VLAN.

```
Raisecom(config)#show voice-vlan mac-address
```

OUI-Address	Mask	Description
0001.E300.0000	FFFF.FF00.0000	Siemens-phone
0003.6B00.0000	FFFF.FF00.0000	Cisco-phone
0004.0D00.0000	FFFF.FF00.0000	Avaya-phone
00D0.1E00.0000	FFFF.FF00.0000	Pingtel-phone
0060.B900.0000	FFFF.FF00.0000	Philips/NEC-phone
00E0.7500.0000	FFFF.FF00.0000	Verilink-phone
00E0.BB00.0000	FFFF.FF00.0000	NBX-phone
0001.ED00.0000	FFFF.FF00.0000	

## 2.14 GARP

### 2.14.1 Introduction

Generic Attribute Registration Protocol (GARP) provides a mechanism to help GARP members in the same LAN to distribute, broadcast, and register information (such as VLAN and multicast information).

GARP is not an entity on a device. Those applications complying with GARP are called GARP applications. GARP VLAN Registration Protocol (GVRP) is a GARP application. When a GARP application entity is connected to an interface of a device, the interface is mapped into the GARP application entity.

Packets of the GARP application entity use a specific multicast MAC address as its destination MAC address. When receiving packets of the GARP application entity, a device

distinguishes them by the destination MAC address and transmits them to different GARP applications (such as GAVP) for processing.

## GARP messages

GARP members exchange data by transmitting messages, including the following three types of messages:

- Join message: a GARP application entity sends a Join message when:
  - It needs another device to register its attributes (such as VLAN information).
  - It receives a Join message from other entities; or it has been statically configured with some parameters, and needs another GARP application entity to register.
- Leave message: a GARP application entity sends a Leave message when:
  - It needs another device to register its attributes.
  - It receives a Join message from other entities to deregister its attributes or it statically deregisters its attributes.
- LeaveAll message: when the GARP application entity is started, the LeaveAll timer starts. It sends a LeaveAll message when this timer expires. The LeaveAll message is used to deregister all attributes so that other GARP application entities can register all attributes of the GARP application entity. When the GARP application entity receives a LeaveAll message from the peer, its LeaveAll time is restored and then starts.
- The Leave message or LeaveAll message cooperates with the Join message to deregister or reregister attributes. Through message exchange, all attributes to be registered can be transmitted to all GARP entities in the same LAN.

## GARP timer

The interval for sending the GARP message is controlled by timers. GARP defines three timers to control the interval.

- Join timer: if no message is replied to the first Join message sent by the GARP application entity, this entity will send another Join message to ensure secure transmission. The interval between sending these two messages is controlled by the Join timer. If the entity has received reply from other GARP application entities, it will not send the Join message.
- Leave timer: when a GARP application entity needs to deregister an attribute, it sends a Leave message to another GARP application entity which will later start a Leave timer. It deregisters the attribute if failing to receive the Join message to deregister the attribute before the Leave timer expires.
- LeaveAll timer: when a GARP application entity starts, its LeaveAll timer also starts. When the LeaveAll timer expires, the GARP application entity sends a LeaveAll message so that other GARP application entities can register all attributes of the GARP application entity. Then, the LeaveAll timer is restored and starts retiming.

## GVRP

GARP VLAN Registration Protocol (GVRP) is a GARP application. Based on GARP working mechanism, it maintains VLAN dynamic registration information of the switch, and sends the information to other switches.

All GVRP-supportive switches can receive VLAN registration information from other switches, and dynamically update local VLAN registration information. In addition, all



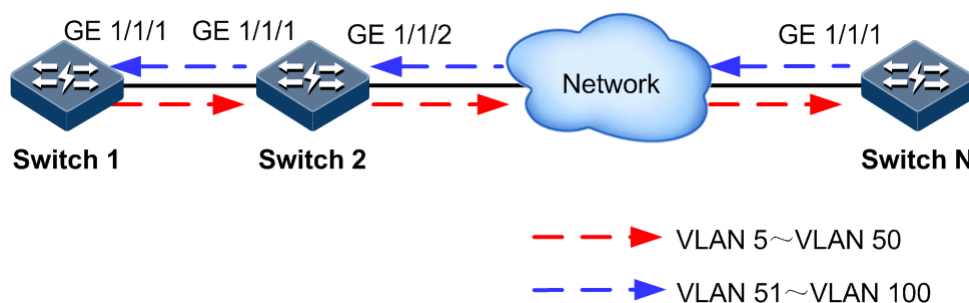
GVRP-supportive switches can send local VLAN registration information to other switches so that they have consistent VLAN registration information in the same VLAN. VLAN registration information sent by GVRP includes manually configured local static registration information and dynamic registration information from other switches.

GVRP has three registration modes:

- Normal: in this mode, GVRP allows dynamic registration and deregistration of VLANs, and sends dynamic and static VLAN information.
- Fixed: in this mode, GVRP forbids dynamic registration and deregistration of VLANs, and sends static VLAN information rather than dynamic VLAN information.
- Forbidden: in this mode, GVRP forbids dynamic registration and deregistration of VLANs, forbids creating static VLANs on the interface, deletes all VLANs except VLAN 1, allows packets of the default VLAN (VLAN 1) to pass, and transmits packets of the default VLAN to other GARP members.

As shown in Figure 2-30, to configure VLANs on multiple devices on a network and allow packets of the specified VLAN to pass are complex. By using GVRP to dynamically register and transmit the specified VLAN, the network administrator can improve working efficiency and accuracy.

Figure 2-30 Principles of GVRP



As shown in Figure 2-30, GE 1/1/1 on Switch 1, GE 1/1/1 and GE 1/1/2 on Switch 2, and GE 1/1/1 on Switch N are Trunk interfaces. Create VLANs 5–50 on Switch 1, and then these VLANs will be dynamically registered on the Rx interface along the red direction until Switch N is registered. Create VLANs 51–100 on Switch N, and then these VLANs will be dynamically registered on the Rx interface along the blue direction so that each switch can completely process packets of VLANs 5–100.

## 2.14.2 Preparing for configurations

### Scenario

GARP enables configurations of a GARP member to fast spread to all GARP-enabled devices in the LAN.

The values of the Join timer, Leaver timer, and LeaveAll timer configured through GARP will be applied to all GARP applications in the LAN, including GVRP and GMRP features.

### Prerequisite

N/A

## 2.14.3 Default configurations of GARP

Default configurations of GARP are as below.

Function	Default value
GARP Join timer	20 (in units of 10ms)
GARP Leave timer	600 (in units of 10ms)
GARP LeaveAll timer	1000 (in units of 10ms)
Global GVRP status	Enable
Interface GVRP status	Disable
GVRP registration mode	Normal
Global GMRP status	Disable
Interface GMRP status	Disable
GMRP registration mode	Normal

## 2.14.4 Configuring basic functions of GARP

Configure basic functions of GARP for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-num</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#garp timer</b> <b>{ join   leave   leaveall } time-</b> <b>value</b>	Configure the GARP timer.

### Caution

- The value of the Join timer must be smaller than half of that of the Leave timer.
- The value of the Leave timer must be greater than twice of that of the Join timer, and smaller than that of the LeaveAll timer.
- The value of the LeaveAll timer must be greater than that of the Leave timer.
- In actual networking, we recommend configuring the Join timer, Leave timer, and LeaveAll timer to 600, 3000, and 12000, in units of 10ms.
- We recommend configuring the LeaveAll timer, Leave timer, and Join timer in sequence, otherwise the restriction among their length may cause configuration failure.

## 2.14.5 Configuring GVRP

Configure GVRP for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#gvrp enable</b>	Enable global GVRP.
3	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#switchport</b> <b>mode trunk</b>	Configure the interface to Trunk mode.
5	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#gvrp</b> <b>registration { fixed   forbidden  </b> <b>normal }</b>	(Optional) configure GVRP registration mode.
6	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#gvrp enable</b>	Enabling interface GVRP.



### Caution

- Interface GVRP can be enabled only after the interface is configured to Trunk mode.
- We do not recommend enabling GVRP on a LAG member interface.

## 2.14.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show garp</b> [ <i>interface-type interface-number</i> ]	Show configurations of the GARP timer.
2	<b>Raisecom#show garp</b> [ <i>interface-type interface-number</i> ] <b>statistics</b>	Show GARP statistics.
3	<b>Raisecom#show gvrp</b> [ <i>interface-type interface-number</i> ]	Show GVRP configurations.
4	<b>Raisecom#show gvrp</b> [ <i>interface-type interface-number</i> ] <b>statistics</b>	Show GVRP statistics.
5	<b>Raisecom#show gvrp local-vlan</b> <i>interface-type interface-number</i>	Show the local VLAN of GMRP.

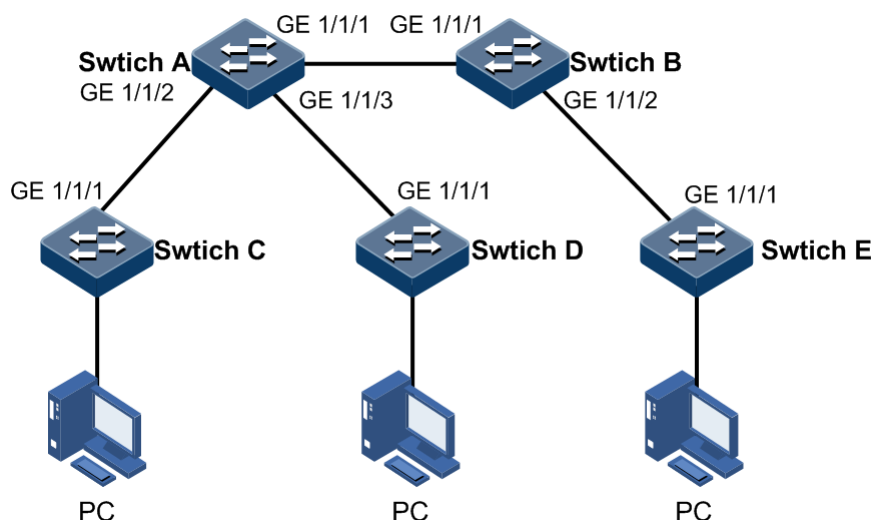
## 2.14.7 Example for configuring GVRP

### Networking requirements

As shown in Figure 2-31, to dynamically register, deregister, and update VLAN information between switches, configure GVRP on these switches. Detailed requirements are as below:

- Configure static VLANs 5–10 on Switch A and Switch C.
- Configure static VLANs 15–20 on Switch D.
- Configure static VLANs 25–30 on Switch E.
- Configure the interfaces that are connected to other switches to Trunk mode, and enable GVRP on these interfaces.
- Configure the Join timer, Leave timer, and LeaveAll timer of GARP on each interface to 600, 3000, and 12000, in units of 10ms.

Figure 2-31 GVRP networking



### Configuration steps

Step 1 Create VLANs and enable global GVRP.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 5-10 active
SwitchA(config)#gvrp enable
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
```

```
SwitchB(config)#gvrp enable
```

Configure Switch C.

```
Raisecom#hostname SwitchC
SwitchC#config
SwitchC(config)#create vlan 5-10 active
SwitchC(config)#gvrp enable
```

Configure Switch D.

```
Raisecom#hostname SwitchD
SwitchD#config
SwitchD(config)#create vlan 15-20 active
SwitchD(config)#gvrp enable
```

Configure Switch E.

```
Raisecom#hostname SwitchE
SwitchE#config
SwitchE(config)#create vlan 25-30 active
SwitchE(config)#gvrp enable
```

- Step 2 Configure GE 1/1/1, GE 1/1/2, and GE 1/1/3 on Switch A, GE 1/1/1, GE 1/1/2, and GE 1/1/3 on Switch B, GE 1/1/1 on Switch C, and GE 1/1/1 on Switch D to Trunk mode, and enable GVRP on them. Take GE 1/1/1 on Switch A for example. Configurations of other interfaces are the same.

```
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/1)#gvrp enable
SwitchA(config-gigabitEthernet1/1/1)#exit
```

- Step 3 Configure GARP timers of GE 1/1/1, GE 1/1/2, and GE 1/1/3 on Switch A, GE 1/1/1, GE 1/1/2, and GE 1/1/3 on Switch B, GE 1/1/1 on Switch C, and GE 1/1/1 on Switch D, and enable GVRP on them. Take GE 1/1/1 on Switch A for example. Configurations of other interfaces are the same.

```
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#garp timer leaveall 12000
SwitchA(config-gigabitEthernet1/1/1)#garp timer leave 3000
SwitchA(config-gigabitEthernet1/1/1)#garp timer join 600
```

## Checking results

Use the **show gvrp** command to show GVRP configurations on the interface.

Take Switch A for example.

```
SwitchA#show gvrp gigaethernet 1/1/1
```

Port	PortStatus	RegMode	LastPduOrigin	FailedTimes	PortRunStatus
GE1/1/1	Enable	Normal	0000.0000.0000	0	Enable

# 3 ISF

---

This chapter describes basic principles and configuration procedures for Intelligent Stacking Framework (ISF), and provides related configuration examples, including the following sections:

- Introduction
- ISF concepts
- Establishing ISF environment
- Configuring ISF
- Preconfiguring ISF in standalone mode
- Configuring ISF in ISF mode
- Checking configurations
- Configuration examples

## 3.1 Introduction

ISF, a typical stack protocol, is a virtualization technology developed by Raisecom. It connects multiple devices and virtualizes them into one device after necessary configurations. In this case, it combines hardware and software processing capabilities of multiple devices, and implements coordinated working, uniform management, and uninterrupted maintenance of multiple devices.

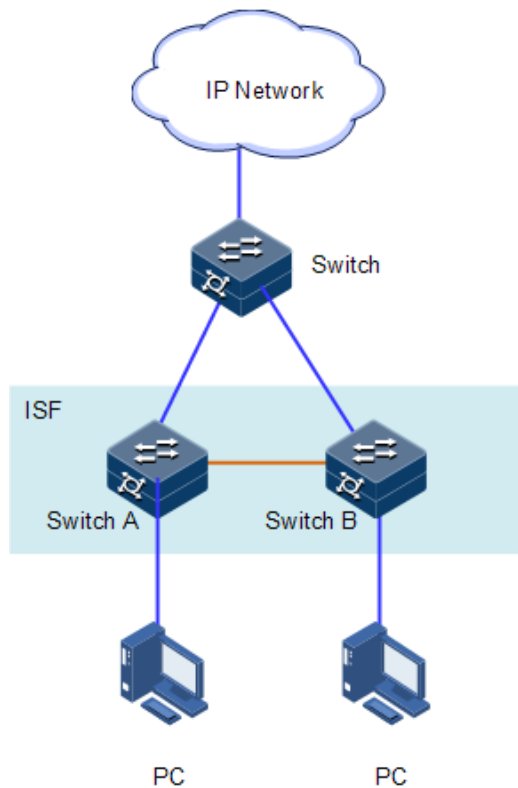
### 3.1.1 ISF advantages

- Simplified management: after an ISF is formed, you can log in from any interface on any member switch to manage all members in the ISF.
- Powerful network scalability: you can increase interfaces, network bandwidth, and processing capability of an ISF simply by adding member switches.
- High reliability: the ISF is reliable in many aspects. The ISF consists of multiple member switches. The master switch operates, manages, and maintains the ISF while the backup switch and slave switch work as backup and meanwhile process services. When the master switch fails, the ISF will rapidly elect a new master switch to resume services and implement 1:1 device backup. ISF links between member switches support link aggregation, and the physical links between the ISF and the upstream or downstream device also support link aggregation. Multiple links can back up each other and balance load with each other. In this way, backup of multiple links improves ISF reliability.

### 3.1.2 ISF application

As shown in Figure 3-1, the master switch and backup switch form an ISF, so they appear as only one device, the ISF, for the upstream or downstream devices.

Figure 3-1 ISF networking

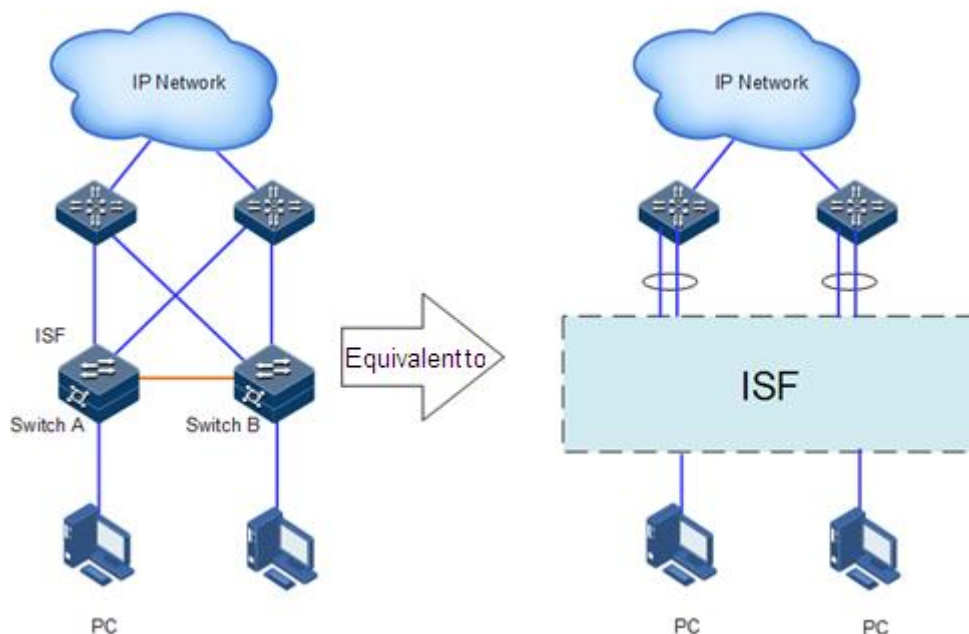


### 3.2 ISF concepts

As shown in Figure 3-2, connect Switch A with Switch B, and configure them properly to form an ISF. The ISF manages physical and software resources of Switch A and Switch B.



Figure 3-2 ISF visualization



Basic concepts of ISF are as below.

## Operating modes

An ISF device supports two operating modes:

- Standalone mode: it runs independently, unable to form an ISF with other devices.
- ISF mode: it can be connected with other devices to form an ISF device.

Use commands to switch an ISF device between the previous two modes.

## Roles

Each ISF device is a member of ISF. There are three roles as below:

- Master: it manages the entire ISF.
- Backup: it works as a backup for the master device. In other words when the master device fails, it becomes the master device.
- Slave: it works as a backup for the backup device. In other words when the master and backup device fail, the ISF will automatically elect a new master device from all slave devices to replace the original master device.

The master device, backup device, and slave device are elected as roles. An ISF contains only one master device, only one backup device, and multiple slave devices.

## Member ID

An ISF uses member IDs to identify and manage member devices. Each member ID is unique in the ISF. For example, the member ID is used in the interface ID in the ISF. When a switch runs in standalone mode, the ID of an interface is `tengigabitethernet1/1/1`. When the switch joins the ISF and its member ID is 2, the interface ID will be `tengigabitethernet2/1/1`.

When a switch runs in standalone mode, its default member ID is 1. When it joins the ISF but its member ID conflicts with that of an existing ISF member, it will fail to join the ISF. In this case, you should plan and configure member IDs uniformly to ensure uniqueness of ISF member IDs.



### Note

The member ID ranges from 1 to 9.

## ISF interfaces

An ISF interface is a logical interface specially used for the ISF. If the member ID of an ISF interface is N, its interface IDs will be ISF-PortN/1/1 and ISF-PortN/1/2. The interface ID will take effect after the ISF interface is bound with a physical interface. An ISF interface can be bound with one or more ISF physical interfaces to increase bandwidth and reliability of ISF links. At present, the ISCOM2600G-HI series switch support binding an ISF interface with up to 8 physical interfaces. For a dual-chip device, physical interfaces connected to different chips cannot be bound with the same ISF interface while those connected to the same chip cannot be bound with different ISF interfaces.



### Note

In standalone mode, IDs of ISF interfaces are ISF-Port1/1/1 and ISF-Port1/1/2. In ISF mode, IDs of ISF interfaces are ISF-PortN/1/1 and ISF-PortN/2/1; in the IDs, N is the member ID. To be brief, this document uses ISF-Port1 and ISF-Port2 uniformly.

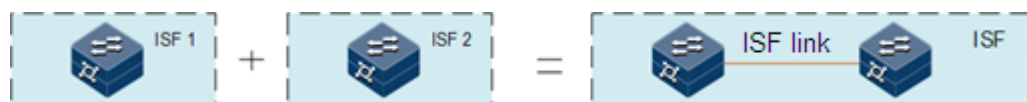
## ISF physical interface

An ISF physical interface is a physical interface used for the ISF. A physical interface can be an optical interface which usually forwards service packets. When a physical interface is bound with an ISF interface, it becomes an ISF physical interface which forwards packets between member devices. These packets include negotiation packets related to the ISF and service packets forwarded between member devices.

## ISF merge

As shown in Figure 3-3, two ISFs run stably. The process of physically connecting and configuring these two ISFs to form a new ISF is called ISF merge.

Figure 3-3 ISF merge



## ISF split

As shown in Figure 3-4, an ISF has formed, but it has a link fault which causes two neighboring members of the ISF to be disconnected. The process of an ISF to be split into two ISFs is called ISF split.

Figure 3-4 ISF split



## ISF domain

An ISF domain is a logical concept. To satisfy various networking applications, you can deploy multiple ISFs, distinguished by domain IDs and independent of each other, in a network. ISF involves the process of discovering devices, detecting device connectivity, electing the master device and backup device, generating topology based on collected information, and monitoring connectivity of member devices, thus ensuring normal operation of the virtualization system.

## Member priority

Member priority determines the role of a member device in role election. The greater the priority value is, the higher the priority is and the more probably it can be elected as the master device. The default priority of a device is 0. The greater the value is, the higher the priority is. To make a device be elected as the master device, you can modify its member priority to a high value on CLI before establishing an ISF. When two master devices have the same priority, the one with a longer up time of the ISF will be elected as the master device. In ISF mode, you can configure the priority of other devices on the master device.

## 3.2.2 Principles of ISF

Establishing an ISF consists of the following four phases:

- Physical connection: connect member devices physically.
- Topology collection: the ISF automatically collects information to form topology.
- Role election: the ISF automatically elects roles.
- Management and maintenance

### Physical connection

- Connection medium

To form an ISF, connect ISF physical interfaces of member devices. The connection medium varies with the type of ISF physical interfaces supported by the ISCOM2600G-HI series switch. When the ISF physical interface is an optical interface, connect it with fiber. In this connection mode, you can connect distant member devices to form an ISF, thus making networking more flexible.

- Connection topology

ISF topology consists of two types: chain networking and ring networking, as shown in Figure 3-5 and Figure 3-6.

Figure 3-5 Chain networking

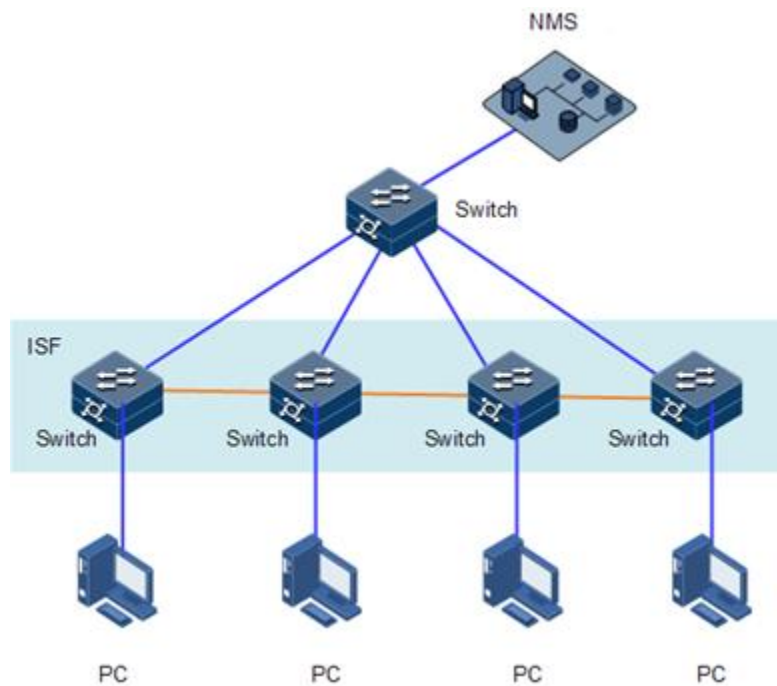
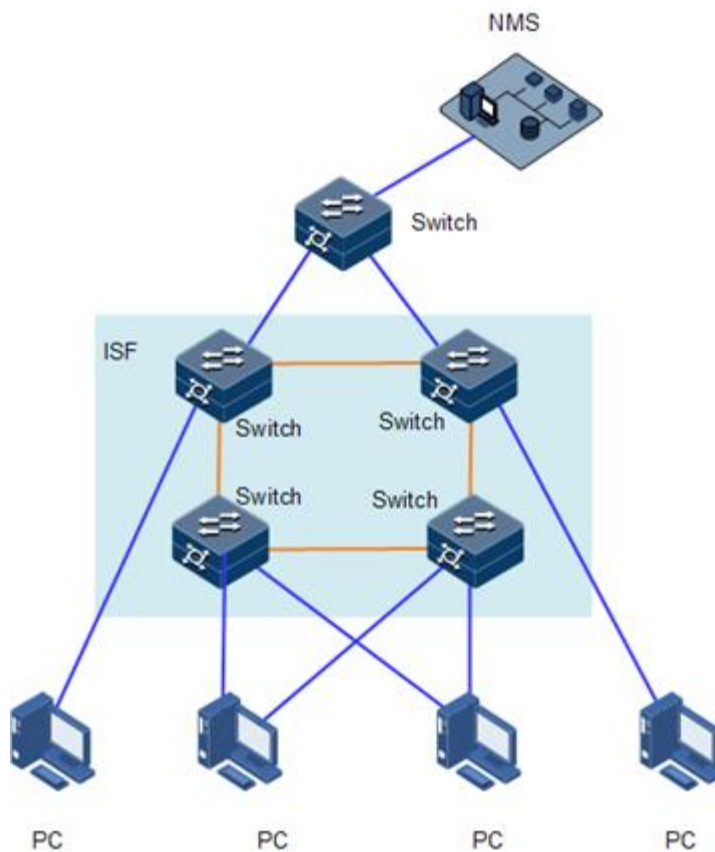


Figure 3-6 Ring networking

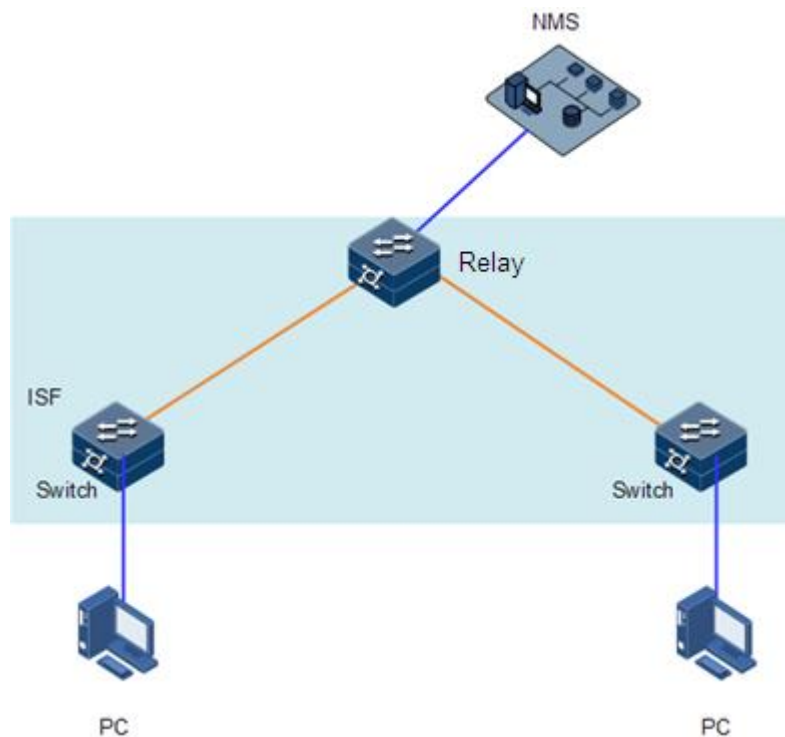


Chain networking: it has a lower physical location than the ring networking, so it is used when members are scattered.

Ring networking: it is more reliable than the chain network because a fault in chain networking disconnects the ISF while a fault in ring networking produces chain networking from the ring networking without affecting ISF services.

If two member devices are far away from each other, such as in Beijing and Hangzhou, you can use a relay device to form an ISF, as shown in Figure 3-7.

Figure 3-7 ISF relay networking



### Note

If the ISCOM2600G-HI series switch is configured with ISF enhancement, the ISF connection topology must be the ring type and exclude ISF relay networking.

## Topology collection

A member device and its neighbors exchange ISF Probe packets to collect the entire ISF topology.

The ISF Route packet carries topology information, including connection relation of ISF interfaces, ID of member device, priority of member device, and bridge MAC addresses of member interfaces.

When a member switch is started, the local master MCC will perform the following operations:

- Periodically send known topology information from the Up ISF interface.
- Update topology information recorded locally after collecting topology information about neighbors.

In this way, all member devices can collect the entire ISF topology after a period (called topology convergence). Then, the ISF enters the role election phase.

## Role election

The process for determining a member device as the master or backup device is called role election, which occurs when the topology changes as below:

- ISF is established.
- A device joins the ISF.
- The master device leaves or fails.
- Two ISFs are merged.

Roles are elected in the following roles in descending order:

1. The current master device, even if a new member device has a higher priority (when an ISF is established, all member devices consider themselves as the master because there is no master. Thus this rule is skipped for the next rule).
2. The device that has been running for the longest time (the up time of each device is carried by the ISF Hello packet)
3. The device with a lowest bridge MAC address

Role election follows the previous rules from the first rule. If multiple member devices are equivalently optimal according to a rule, the following rules will not stop working until a unique optimal member device is elected. Then, this optimal member device is the master, the second optimal one is the backup device, and others are slave devices.

After role election is complete, the master device sends a Config packet to check whether communication is normal. After the ISF is completely established, it enters management and maintenance phase.



### Note

When two ISF merge, ISF election will occur by following rules of role election. The devices in the loser ISF join the winner ISF as the backup device or slave devices, and forming a new ISF with the master member device. The restart during ISF merge is manually operated.

No matter a device forms an ISF with other devices or joins an ISF, it will be initialized and restarted by using configurations of the master device to synchronize with the master device if it works as the slave device, regardless of what configurations it has nor whether it has saved current configurations.

## 3.2.3 ISF merge and split

### ISF merge

ISF merge occurs under the following conditions:

- A device is powered on but it is not connected to the ISF. In this case, it will be elected as the backup device or slave device (depending on whether there is a slave device in the ISF because the ISF can contain only one backup device). For example, device A is elected as the master device (ISF takes effect upon power-on, so it elects itself as the master device if there is no new member); then, device B joins the ISF after being restarted, and is elected as the backup device (according to role election rule 1). The MAC address of the ISF is that of device A.
- The new device is already the master device (ISF is already effective. The device is connected with the other device). There two devices will compete to elect for the master

device. The one that fails will be restarted (by default, automatic device restart upon ISF merge or ISF split is enabled) and then join the ISF as a backup device or slave device (due to lower priority or shorter running time). The MAC address of the ISF is that of the master device. You can configure MAC address synchronization between ISF devices. By default, MAC address synchronization is disabled.

After ISF merge is complete, the MAC address of the ISF is that of the master device, and backup device and slave devices just forward management packets and protocol packets to the master device.

After the ISF runs stably, the master device will back up configurations in batches by issuing its configurations to the backup device and slave devices to synchronize configurations.

After batch backup is complete, realtime backup will start; in other words, the master device processes services while the backup device and slave devices back up data and configurations of the master device. The ISF adopts strict synchronization to reliably issue data and configurations to the backup device and slave devices. In this way, when the master device fails, the backup device will replace it within 15s to improve system stability.

## ISF split

ISF split occurs under the following conditions:

- Two neighboring devices periodically send heartbeat packets to each other. If a device fails to receive heartbeat packets from its neighbor for multiple periods (usually 16 periods), it considers that the neighbor has left the ISF. Thus new topology will form.
- If a stack interface in the ISF becomes Down, the ISF will re-elect members to form a new topology. If the master device leaves, the ISF will elect the backup device as the master device preferentially. If the backup device leaves, the ISF will elect a slave device as the backup device. If a slave device leaves, roles of other devices will remain the same.

After ISF split is complete, two connected devices will delete related physical interfaces of each other and become independent. Then, they do not need to be restarted or reconfigured.

After ISF split is complete, its MAC address will be those of each device. The original backup device and slave devices will not forward management packets and protocol packets to the original master device.

## 3.2.4 ISF management and maintenance

After role election is complete, an ISF has formed. All member devices form a virtual device on the network, and their resources are possessed by the virtual device and managed by the master device.

### Member ID

When working, an ISF uses member IDs to identify and manage member devices. For example, the interface ID in the ISF is used in the member ID. When a switch works in standalone mode, the ID of an interface changes (such as from tengigabitethernet 1/1/1 to tengigabitethernet 2/1/1). Thus, you must guarantee uniqueness of all member IDs, otherwise the ISF will fail to form.

### Maintaining ISF topology

If member device A becomes Down or an ISF link becomes Down, its neighbor devices will broadcast the message that member device A leaves to other member devices in the ISF. These

member devices receiving the message, according to the local ISF topology information table, will determine whether member device A is the master or slave device.

- If member device A is the master device, its leave triggers role election and then its neighbor devices will update local ISF topology.
- If member device A is the slave device, its neighbor devices will update local ISF topology to guarantee rapid convergence of ISF topology.



### Note

The status of an ISF interface depends on that of the bound ISF physical interface. When all ISF physical interfaces become Down, the ISF interface will be Down.

## 3.2.5 MAD

Multi-Active Detection (MAD) is a detection and processing mechanism. When an ISF link is faulty, the ISF will be split to two new ISFs which have the same IP address and thus conflict with each other and amplify the fault. Thus, a mechanism is required to improve system availability when ISF split occurs. MAD can detect whether there are multiple ISFs on the network, take actions accordingly to minimize impact of ISF split on services, and enable the ISF at the master device side before ISF split to work properly. MAD has the following functions:

- Detect ISF split: use Bidirectional Forwarding Detection (BFD) to detect whether there are multiple ISFs on the network.
- Eliminate conflict: after ISF split occurs, the original ISF can detect other ISFs in Active status (indicating the ISF is working). This function allows the ISF with the minimum unit ID of the master device to continue to work while converting other ISFs to Recovery status (indicating the ISF is disabled) and shuts down all physical interfaces except the reserved interface in the Recovery ISFs to prevent these ISFs from forwarding packets.
- Clear MAD faults: when an ISF link is faulty, the ISF will be split to two new ISFs. In this case, you can clear the fault by resuming the faulty link to merge two conflicting ISFs to one. If a Recovery ISF becomes faulty before an existing MAD fault is cleared, you must resume the faulty ISF and faulty link to merge two conflicting ISFs to one. If the Active ISF becomes faulty before an existing MAD fault is cleared, you can use command lines to enable the Recovery ISF to replace the original ISF to minimize impact on services, and then clear the existing MAD fault.

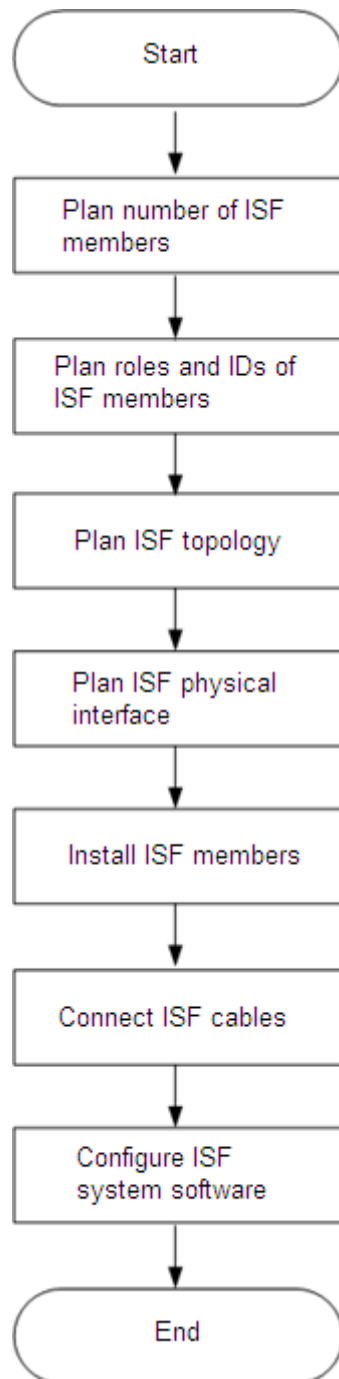
## 3.3 Establishing ISF environment

### 3.3.1 Establishment flow

Figure 3-8 shows the flow for establishing the ISF environment. We recommend planning the ISF topology and then installing devices to facilitate physical connection of cables in the ISF.



Figure 3-8 Flow for establishing the ISF environment



### 3.3.2 Planning number of ISF members

After multiple member devices form an ISF, the sum of their switching capacity is the switching capacity of the ISF. Determine the number and model of ISF members according to access and uplink requirements for the network. An ISF supports up to 9 members.

### 3.3.3 Planning roles and IDs of ISF members

#### Determining master device

You can configure a device with a higher priority as required. In this way, it can be elected as the master among multiple devices when these devices form an ISF for the first time.

#### Determining member IDs

When working, an ISF uses member IDs to identify and manage member devices. In this case, before adding devices to the ISF, you should plan and configure member IDs uniformly to ensure uniqueness of ISF member IDs.

### 3.3.4 Planning ISF topology

The ISF supports chain topology and ring topology. The ring topology is more reliable than chain topology, so it is recommend.

### 3.3.5 Planning ISF physical interfaces

An ISF interface can be bound with 8 physical interfaces. We recommend bounding an ISF interface with at least 2 physical interfaces to increase bandwidth and reliability of the ISF interface. The two ISF interfaces that connect two neighbor devices should be bound with the same number of ISF physical interfaces so that these ISF physical interfaces can be interconnected with those on the neighbor device. For example, the number of ISF physical interfaces bound with ISF-Port2 on Device A should be equal to that of ISF physical interfaces bound with ISF-Port1 on Device B.



#### Note

In standalone mode, a physical interface on the device works as an ISF physical interface. When the device enters ISF mode, services configured on the physical interface will be invalid. In this case, you should plan ISF topology to prevent services from being affected.

### 3.3.6 Installing ISF members

After planning ISF topology, install ISF members.

### 3.3.7 Connecting ISF cables

When you use an Ethernet optical interface as the ISF physical interface, insert an optical module into the Ethernet optical interface, and then connect the fiber. For optical modules corresponding to Ethernet optical interfaces of different types, see *ISCOM2600G-HI (A) Series Product Description*.

### 3.3.8 Configuring ISF system software

After installing ISF members, start them. Log in to them respectively to configure ISF system software as planned.

## 3.4 Configuring ISF

There are two modes for configuring the ISF: preconfiguration mode and non-preconfiguration mode. In preconfiguration mode, an ISF member is restarted for only one time, so this mode is recommended.

### 3.4.1 Preparing for configurations

#### Scenario

- Before establishing an ISF, ensure that multiple devices work in the same mode, otherwise the ISF will fail to form.
- Ensure that all member IDs are different.

#### Prerequisite

Connect physical interfaces on member devices.

### 3.4.2 Default configurations of ISF

Default configurations of ISF are as below.

Function	Default value
Stacking mode	Standalone
Unit ID	1
Domain ID	0
Priority	0
Automatic upgrade	Disable
Restart upon ISF split or merge	Enable

### 3.4.3 Preconfiguration mode

In preconfiguration mode, you can configure a standalone device with the ISF interface ID, member ID, and member priority. These configurations do not affect the running of the standalone device, but will take effect after the standalone device enter ISF mode. Before forming an ISF, you should configure the standalone device in preconfiguration mode. You can configure the standalone device with high priority. In this way, it can be elected as the master among multiple devices when these devices form an ISF for the first time. Configure the ISF interface to switch the operating mode to ISF mode so that the device can form an ISF with other devices (only one restart is needed to form the ISF).

Task		Description
Configuring the ISF interface	Configuring the ISF interface	Required
	Configuring the member ID	Required

Task		Description
	Configuring the member priority	Optional
Configuring the ISF mode		Required
Configuring the ISF in ISF mode	Configuring the reservation time for the bridge MAC address of the ISF	Optional
	Enabling restart upon ISF merge	Optional
	Enabling auto-loading of the startup file of the ISF	Optional
	Configuring MAD	Optional

### 3.4.4 Non-preconfiguration mode

In non-preconfiguration mode, you can configure a standalone device with the member ID, switch the device to the ISF mode, and configure ISF parameters, such as the ISF interface and member priority (multiple restarts are required during the entire process). This configuration method is used to modify current configurations. For example,

- Modify the ID of a member device to a specified value (note that after device restart the modification takes effect and the original member ID becomes invalid).
- Modify the priority of a member device to make the device be elected as the master device.
- Modify the existing binding of an ISF (deleting a binding or add a binding). The configuration of the ISF interface may affect the running of the local device (such as causing ISF split or ISF merge).

Task		Description
Configuring ISF member ID in standalone mode		Required
Configuring ISF mode		Required
Configuring the ISF in ISF mode	Configuring the reservation time for the bridge MAC address of the ISF	Optional
	Enabling restart upon ISF merge	Optional
	Enabling auto-loading of the startup file of the ISF	Optional
	Configuring MAD	Optional

## 3.5 Preconfiguring ISF in standalone mode

To make a device form an ISF with other devices after switching of the operating mode, you can preconfigure parameters of the device in standalone mode, such as the unit ID, member priority, member domain ID, and ISF interface. Configurations of these parameters do not take effect in standalone mode but will take effect after switching to ISF mode.

## 3.5.1 Configuring ISF interface

The ISF interface is a logical concept. After you create an ISF interface and bind it with a physical interface, the physical interface is an ISF physical interface which can be connected to another device through an ISF connection. An ISF interface can be bound with up to 8 physical interfaces through multiple binding commands. The ISF interface aggregated from multiple physical interfaces is called the aggregation ISF interface. In this way, up to 16 Ethernet cables or fibers can connect two devices to increase bandwidth and reliability of the ISF interface.

Configure the ISF interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface isf-port <i>interface-number</i></b>	Create an ISF interface, and enter ISF interface configuration mode.
3	<b>Raisecom(config-isf-port1/1/1)#isf port-group <i>interface-number</i></b> <b>Raisecom(config-isf-port1/1/1)#exit</b>	Bind a physical interface with the ISF interface.



### Note

Save the configuration to the startup configuration file so that it can take effect when the device switches to the ISF mode and load the startup configuration file.

In standalone mode, binding an ISF interface with an ISF physical interface does not affect current services of the ISF physical interface. When the device switches to ISF mode, configurations of the ISF physical interface will be restored to the default ISF status (configurations of current services will be deleted).

When a device leaves the factory, it is in standalone mode without a member ID. You must configure a member ID and then switch the device from standalone mode to ISF mode. Use the **show isf configuration** command to show the member ID. To avoid conflicts of member IDs upon adding the member to the ISF, you should plan ISF member IDs.

## 3.5.2 Configuring member priority

The member priority is used in role election. A device with high priority can be elected as the master device with high probability.

Configure the member priority for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#isf priority <i>priority-number</i></b>	Configure the member priority.

### 3.5.3 Configuring ISF mode

Configure the ISF mode for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>isf-mode isf</b> Set successfully. The device will switch to isf mode,take effect after reboot	Configure the ISF mode.



#### Note

When the configuration command is executed, the system prompts "Set successfully. The device will switch to single mode, take effect after reboot". To prevent the device from being restarted, type "no", and press **Enter**. The device will not be restarted, so you can further configure it.

## 3.6 Configuring ISF in ISF mode

### 3.6.1 Configuring ISF mode

Configure the ISF mode for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>isf-mode isf</b>	Configure the ISF mode.



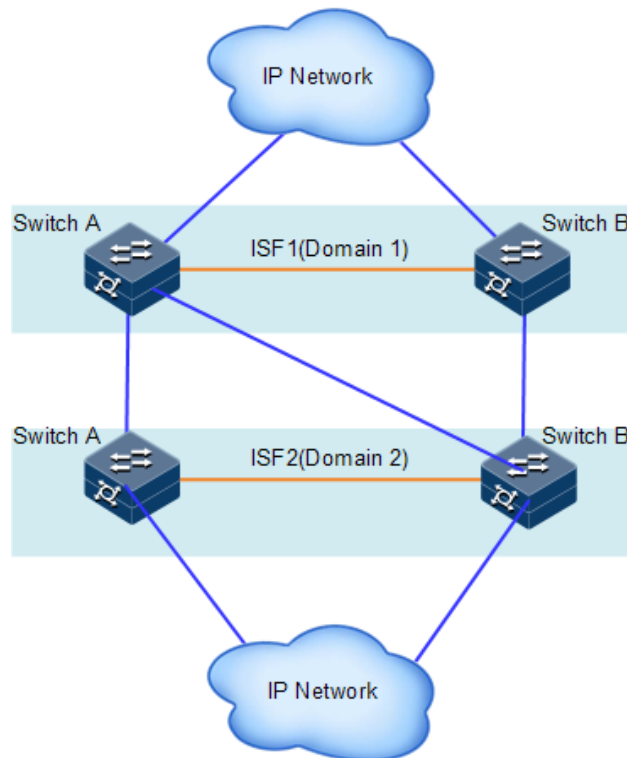
#### Note

When the configuration command is executed, the system prompts "Set successfully. The device will switch to isf mode, take effect after reboot". To prevent the device from being restarted, type "no", and press **Enter**. The device will not be restarted, so you can further configure it.

### 3.6.2 Configuring ISF domain ID

An ISF domain is a logical concept. Multiple devices form an ISF through ISF links, and the set of these devices is an ISF domain. To meet requirements for different networking applications, you can deploy multiple ISFs on a network. These ISFs are identified by ISF domain IDs. As shown in Figure 3-9, Switch A and Switch B form ISF 1 while Switch C and Switch D form ISF 2. If there is a MAD link between ISF 1 and ISF 2, these two ISFs send MAD packets to each other, thus affecting their status and operation. In this case, you can configure two different ISF domain IDs to prevent them from affecting each other.

Figure 3-9 Multi-ISF-domain networking



Configure the ISF domain ID for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#isf unit number domain domain-number</code>	Configure the domain ID.

### 3.6.3 Configuring ISF interface

After switching multiple devices to ISF mode, create their ISF interfaces respectively, and bind these ISF interfaces with their physical interfaces to form ISF physical interfaces. Use ISF cables to connect these ISF physical interfaces. Then, ISF on these devices will take effect. ISF-Port1 (ISF-Port2/1/1 as used in ISF mode) on one device can be connected to ISF-Port2 (ISF-Port2/1/2 as used in ISF mode) only on the other device.

An ISF interface can be bound with up to 8 physical interfaces through multiple execution of the **isf port-group interface** command. The ISF interface aggregated from multiple physical interfaces is called the aggregation ISF interface. In this way, up to 16 Ethernet cables or fibers can connect two devices to increase bandwidth and reliability of the ISF interface.

Configure the ISF interface for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<b>Raisecom(config)#interface isf-port</b> <i>interface-number</i>	Enter ISF interface configuration mode, and create an ISF interface.
3	<b>Raisecom(config-isf-port1/1/1)#isf port-group</b> <i>interface-number</i>	Bind a physical interface with the ISF interface.



## Note

When a physical interface is bound with an ISF interface, services configured on the physical interface will be invalid. You should plan the binding to prevent original services from being affected.

An ISF interface can be bound with multiple physical interfaces through multiple executions of the **port-group interface** command to implement backup or load balancing of ISF links and to increase bandwidth and reliability of ISF links. An ISF interface can be bound with up to 8 physical interfaces. When the number of bound physical interfaces reaches the upper limit, the execution of the **port-group interface** command will fail.

After binding or unbinding a physical interface with an ISF interface, use the **write** command to save this configuration to the startup configuration file, otherwise this configuration will not take effect upon next device startup.

## 3.6.4 Configuring member ID

The ISF uses the member ID to uniquely identify member devices. Information and configurations of the device are related to the member ID, such as the interface ID (including the physical interface and logic interface), interface configurations, and member priority.

- If you modify the member ID but do not restart the device, the original member ID will still take effect and be used by physical resources. In the configuration file, all configurations, except the ISF interface ID, configurations of the ISF interface, and member priority, will remain the same.
- If you modify the member ID and restart the device, the new member ID will take effect and be used by physical resources. In the configuration file, the ISF interface ID, configurations of the ISF interface, and member priority will take effect; other configurations related to the member ID (such as configurations of the physical interface, configurations of a chassis parameter value equal to the original member ID, and so on) will be invalid and need reconfiguration.

Configure the member ID for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#isf unit</b> <i>old-number</i> <b>renumber</b> <i>new-number</i>	(Optional) modify the unit number from the original unit number to a new unit number in ISF mode.
3	<b>Raisecom(config)#isf renumber</b> <i>number</i>	(Optional) modify the unit number from the original unit number to a new unit number in standalone mode.





## Note

The new member ID takes effect after device restart.

The ISF uses the member ID to uniquely identify member devices. Configurations of the ISF interface and member priority are related to the member ID, so modification of the member ID may cause configurations to change or loss. Use the command with caution.

### 3.6.5 Configuring member priority

The member priority is used in role election. A device with higher priority can be elected as the master device with high probability.

Configure the member priority for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#isf unit <i>number</i> priority <i>priority-number</i></b>	Configure the member priority.

### 3.6.6 Configuring reservation time for ISF bridge MAC address

The bridge MAC address is the MAC address when a device communicates as a bridge. Some Layer 2 protocols (such as LACP) use bridge MAC addresses to identify devices, so a bridge device on the network must have a unique bridge MAC address. If there are multiple devices with the same bridge MAC address on the network, the bridge MAC address will conflict with each other and thus the network communication will fail.

An ISF communicates with the external network as a virtual device, so it should have a unique bridge MAC address, called the ISF bridge MAC address. It usually uses the bridge MAC address of the master device as the ISF bridge MAC address.

Conflict with the bridge MAC address causes communication failure, but switching of the bridge MAC address causes service interruption. In this case, you should configure the reservation time for the ISF bridge MAC address according to actual network conditions:

- When the reservation time for the ISF bridge MAC address is configured to 10min, the ISF bridge MAC address remains the same within 10min if the master device leaves the ISF. If the master device fails to return to the ISF, the bridge MAC address of the newly elected master device will be the ISF bridge MAC address. This configuration is suitable when the master device leaves the ISF for a short time and then returns (for example, the master device is restarted or a link is faulty temporarily), and can thus avoid service interruption due to switching of the bridge MAC address.
- When the reservation time for the ISF bridge MAC address is permanent, the ISF bridge MAC address remains the same regardless of whether the master leaves the ISF.
- When the ISF bridge MAC address is configured to unreserved, the bridge MAC address of the newly elected master device will be the ISF bridge MAC address when the master leaves the ISF.

Configure the reservation time for ISF bridge MAC address for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#isf mac-address persistent always</b>	Configure the ISF bridge MAC address to be permanent when the master device leaves the ISF.
3	<b>Raisecom(config)#isf mac-address persistent timer</b>	Configure the reservation time for the ISF bridge MAC address to 10min when the master device leaves the ISF.
4	<b>Raisecom(config)#no isf mac-address persistent</b>	Configure the ISF bridge MAC address to be updated immediately when the master device leaves the ISF.



### Note

The change of the bridge MAC address may interrupt services for a short time. If bridge MAC addresses of two ISFs are the same, these two ISFs cannot be merged into an ISF. When VRRP load balancing is configured in ISF mode, you must configure the ISF bridge MAC address to be permanently reserved (also permanently reserved by default).

## 3.6.7 Configuring MAC address synchronization

In ISF mode, after a switch interface quits a VLAN, it will delete the MAC address corresponding to the VLAN on the interface. During the deleting process, it does not process the MAC address synchronization request from other ISF member switches until it deletes the MAC address. After the period for synchronizing MAC addresses expires, the interface will receive and process the MAC address synchronization request from other ISF member switches and add the MAC address to its MAC address table.

Configure MAC address synchronization for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#1#config</b>	Enter global configuration mode.
2	<b>Raisecom#1(config)#mac-address synchronizing enable</b>	Enable MAC address synchronization.
3	<b>Raisecom#1(config)#mac-address synchronizing long-interval <i>time</i></b>	Configure the period for synchronizing MAC addresses.

## 3.6.8 Enabling automatic device restart upon ISF merge

When multiple ISFs merge, they will elect according to role election rules. All member devices of the loser ISF have to be restarted before joining the winner ISF.

- If automatic device restart upon ISF merge is disabled, you have to restart devices as prompted by the system during ISF merge.

- If automatic device restart upon ISF merge is enabled, the system will automatically restart devices during ISF merge.

Enable automatic device restart upon ISF merge for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#isf auto-merge enable</b>	Enable automatic device restart upon ISF merge.



## Note

All member devices in the loser ISF are restarted and join the winner ISF to merge into one ISF if automatic device restart upon ISF merge is enabled under the following conditions that trigger ISF merge:

- The ISF link fault is cleared.
- Multiple physical interfaces and ISF interfaces are bound in startup configuration files of multiple ISFs, and then establishing the ISF physical connection makes the ISF interface Up.

To keep automatic device restart upon ISF merge in normal operation, enable this function on all ISFs to be merged.

By default, automatic device restart upon ISF merge is enabled.

## 3.6.9 Configuring MAD

Multi-Active Detection (MAD) is a detection and process mechanism. When an ISF link is faulty, the ISF splits into two new ISFs. These two ISFs have the same IP address, which causes IP address conflict and thus enlarges the fault. In this case, a mechanism is required to improve system availability and detect whether there are multiple ISFs on the network, and take actions accordingly to minimize impact of ISF split on services.

The MAD mode supported by the ISF is Bidirectional Forwarding Detection (BFD) MAD.

### BFD MAD

- Principles of BFD MAD

BFD MAD works based on BFD. To make BFD MAD work properly, enable BFD MAD on the VLAN interface, and configure the MAD IP address of the VLAN interface. Different from a common IP address, a MAD IP address is bound with a member device of an ISF. MAD IP addresses must be configured on all member devices and belong to the same network segment.

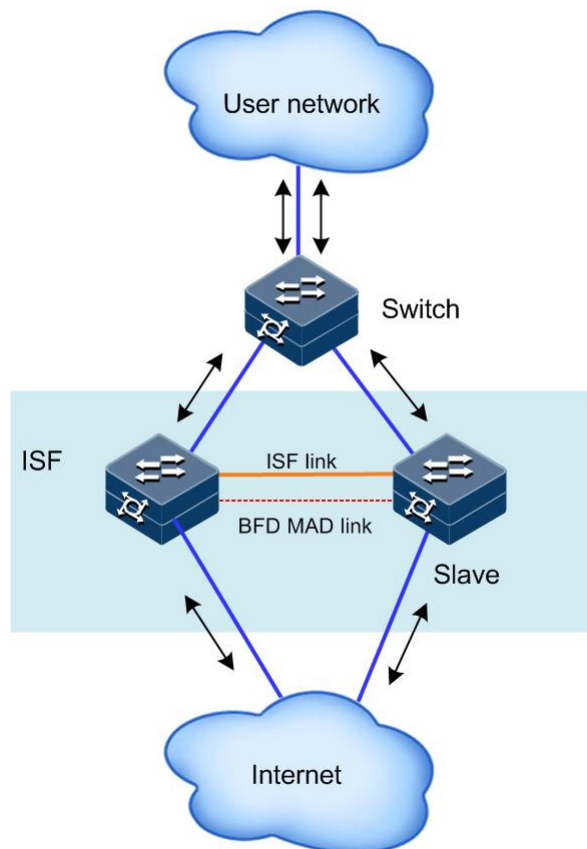
When an ISF works properly, the MAD IP address of the master device takes effect, that of the slave device does not take effect, and thus the BFD session is Down (use the **show bfd state** command to show the status of a BFD session. If the session status is Up, the session is Up. If the session status is Down, the session is Down).

When the ISF splits into multiple ISFs, MAD IP addresses of master devices in different ISFs take effect, BFD sessions become Up, and then multi-active conflict is detected.

- Networking requirements for BFD MAD

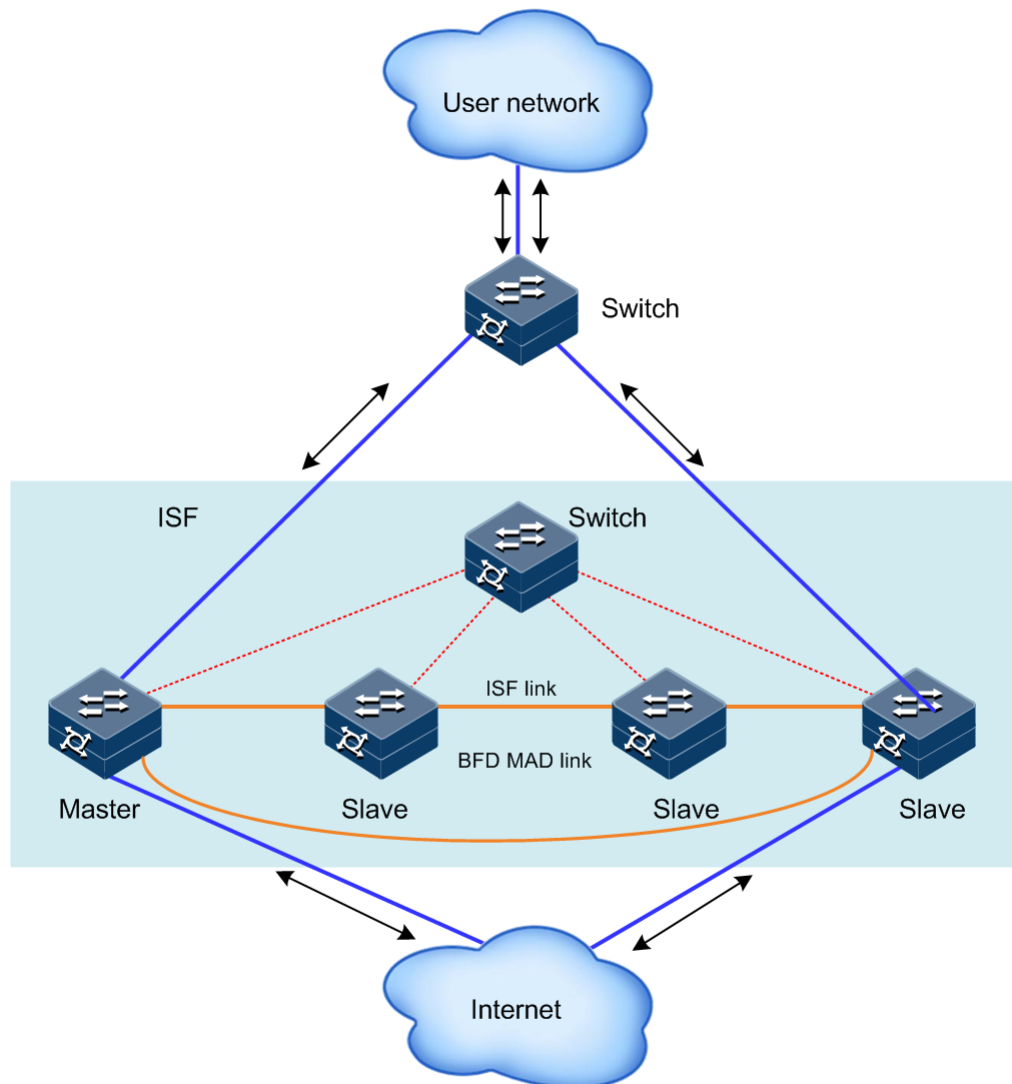
If there are only two member devices in an ISF, you can use an intermediate device or not to configure BFD MAD. As shown in Figure 3-10, there must be one BFD MAD link between any two member devices. The interfaces of these BFD MAD links must belong to the same VLAN. Configure these member devices with different IP addresses in the same network segment in VLAN interface configuration mode.

Figure 3-10 BFD MAD networking (without intermediate device)



If there are 3 or 4 member devices in an ISF, you must use an intermediate device to configure BFD MAD. As shown in Figure 3-11, there must be one BFD MAD link between any member device and the intermediate switch. The interfaces of these BFD MAD links must belong to the same VLAN. Configure these member devices with different IP addresses in the same network segment in VLAN interface configuration mode.

Figure 3-11 BFD MAD networking (with intermediate device)



## Configuring BFD MAD

Configure BFD MAD as below:

- Step 1 Create a VLAN specially for BFD MAD (if an intermediate device is used for networking, you should also configure it with this step).
- Step 2 Determine physical interfaces (at least one on each member device) used for BFD MAD, and add them to the VLAN specially used for BFD MAD (if an intermediate device is used for networking, you should also configure it with this step)
- Step 3 Create a VLAN interface for the VLAN specially used for BFD MAD. Enable BFD MAD on the VLAN interface. Configure the MAD IP address.

Configure BFD MAD for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#2#config</code>	Enter global configuration mode.

Step	Command	Description
2	<code>Raisecom#2(config)#interface vlan <i>vlan-id</i></code>	Enter VLAN interface configuration mode.
3	<code>Raisecom#2(config-vlan2)#mad bfd enable</code>	Enable MAD BFD.
4	<code>Raisecom#2(config-vlan2)#mad ip address <i>ip-address</i> [ <i>ip- mask</i> ] unit <i>number</i></code>	Configure the MAD IP address of the specified ISF among all ISFs.
5	<code>Raisecom#2(config)#mad restore</code>	(Optional) restore a device disabled due to MAD to normal status.



## Note

- After BFD MAD is enabled, the special VLAN should be reserved for this feature only, instead of other usage.
- If the VLAN specially used for BFD MAD contains a Trunk interface which allows packets of multiple VLANs to pass, you must ensure that the default VLAN of the Trunk interface is different from the special VLAN. Otherwise, other services configured on the Trunk interface will be affected.
- BFD MAD cannot be enabled on VLAN 1 interface.
- The interface used for BFD MAD must be configured with the MAD IP address through the **mad ip address** command, instead of other IP addresses (common IP address configured through the **ip address** command and VRRP IP address), to prevent from affecting MAD.
- BFD MAD and STP are mutually exclusive, so do not enable STP on the physical interface that is in the VLAN corresponding to the VLAN interface enabled with BFD MAD. Ensure that there is no physical loop.
- Plan the MAD IP address to avoid conflict with the externally learnt route.

## Configuring reserved interface

When multiple ISFs conduct MAD, it will shut down all services interfaces in the Recovery ISF. If any interface (such as the Telnet login interface and interface for MAD) has to be Up due to special usage, you can configure the interface as reserved interface through commands.

Configure the reserved interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mad exclude interface <i>interface-type interface- number</i></code>	Configure an interface as the reserved interface which will not be shut down when the device enters Recovery status.



## Note

The ISF physical interface and Console interface are automatically regarded as reserved interfaces, needless of manual configuration.

To make a VLAN interface in a Recovery ISF continue to receive and send packets (such as using the VLAN interface for remote login), configure the VLAN interface and its corresponding Layer 2 Ethernet interface as reserved interfaces.

## Clearing MAD fault

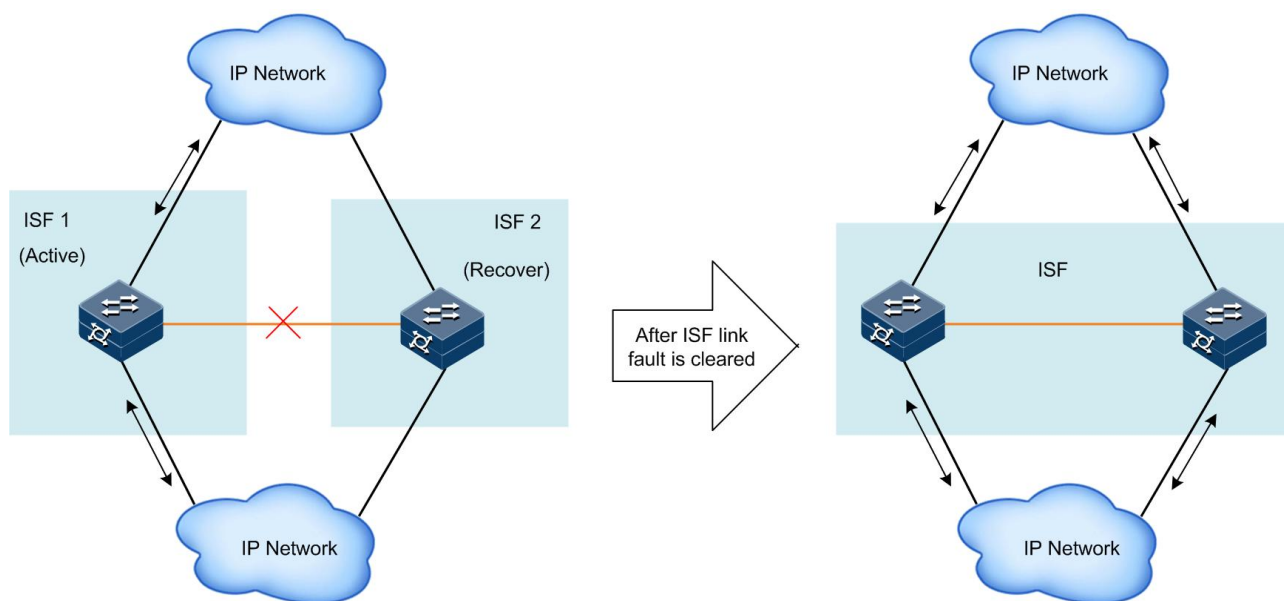
When an ISF link is faulty, the ISF splits into two ISFs, and thus multi-active conflict occurs. When the ISF system detects multi-active conflict, these two conflicting ISFs will elect as below:

- Step 1 Compare the number of member devices in these two ISFs. The ISF with more member devices will win and resume working. The loser ISF transits to Recovery status, in which it fails to forward service packets.
- Step 2 If these two ISFs have the same number of member devices, the ISF system will compare the member ID of the master device. The ISF with the master device of a greater member ID will win and resume working. The loser ISF transits to Recovery status, in which it fails to forward service packets.

In this case, you can clear the ISF link fault to resume the ISF system (devices will automatically try to clear the ISF link fault. If failed, it needs manual restoration).

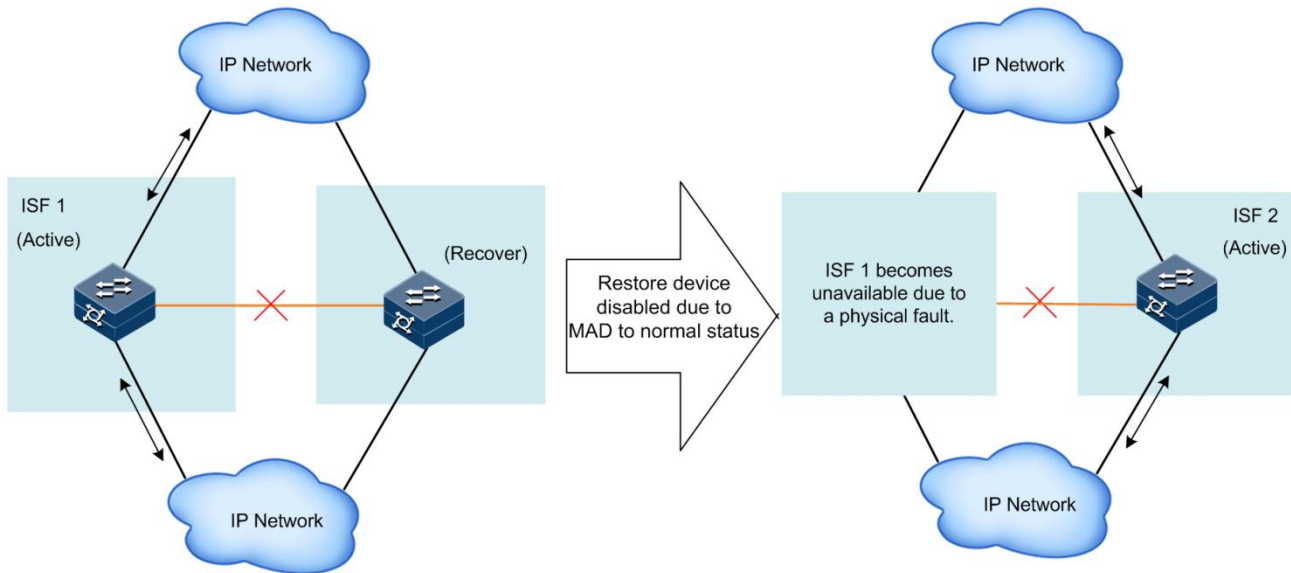
After the ISF link fault is cleared, the Active ISF and the Recovery ISF will merge into an ISF. The ISF system prompts you to restart the Recovery ISF. After the Recovery ISF is restarted, its services interfaces forcibly shut down will be restored to the actual physical status, and the ISF system will resume. As shown in Figure 3-12, if you restart the Active ISF, the two ISFs will merge into one. Then, you need to use the **mad restore** command to restore services interfaces, which are forcibly shut down, in the Recovery ISF to the actual physical status, and the ISF system will resume.

Figure 3-12 Clearing MAD fault (clearing ISF link fault)



As shown in Figure 3-13, if the Active ISF (ISF 1) becomes faulty (device fault or uplink/downlink fault) before the MAD fault is cleared, you can use the **mad restore** command on the Recovery ISF (ISF 2) to restore it and make it replace ISF 1. Then, clear the fault of the link between ISF 1 and ISF 2. Then, these two ISFs merge and the ISF system is restored.

Figure 3-13 Clearing MAD fault (ISF link fault and Active ISF fault)



Restore service interfaces shut down due to MAD to normal status for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mad restore</b>	Restore service interfaces shut down due to MAD to normal status.

## 3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show isf</b>	Show all collected ISF information.
2	<b>Raisecom#show isf topology</b>	Show information about ISF topology.
3	<b>Raisecom#show isf packet</b>	Show statistics on ISF packets.
4	<b>Raisecom#show isf configuration</b>	Show ISF preconfigurations.
5	<b>Raisecom#show mad info</b>	Show configurations and status of MAD.
6	<b>Raisecom#show mac-address synchronizing config</b>	Show configurations of MAC address synchronization.



## 3.8 Configuration examples



### Note

By default, the Ethernet interface, VLAN interface, and aggregation interface are in Down status. To configure these interfaces, use the **undo shutdown** command to make them Up. Take the ISCOM2624G-HI for example.

### 3.8.1 Example for configuring ISF in preconfiguration mode with BFD MAD

#### Networking requirements

When the network grows rapidly, the central switch (Switch A) fails to meet forwarding requirements. To double forwarding capability based on protecting the existing investment with easy management and maintenance, you can configure ISF.

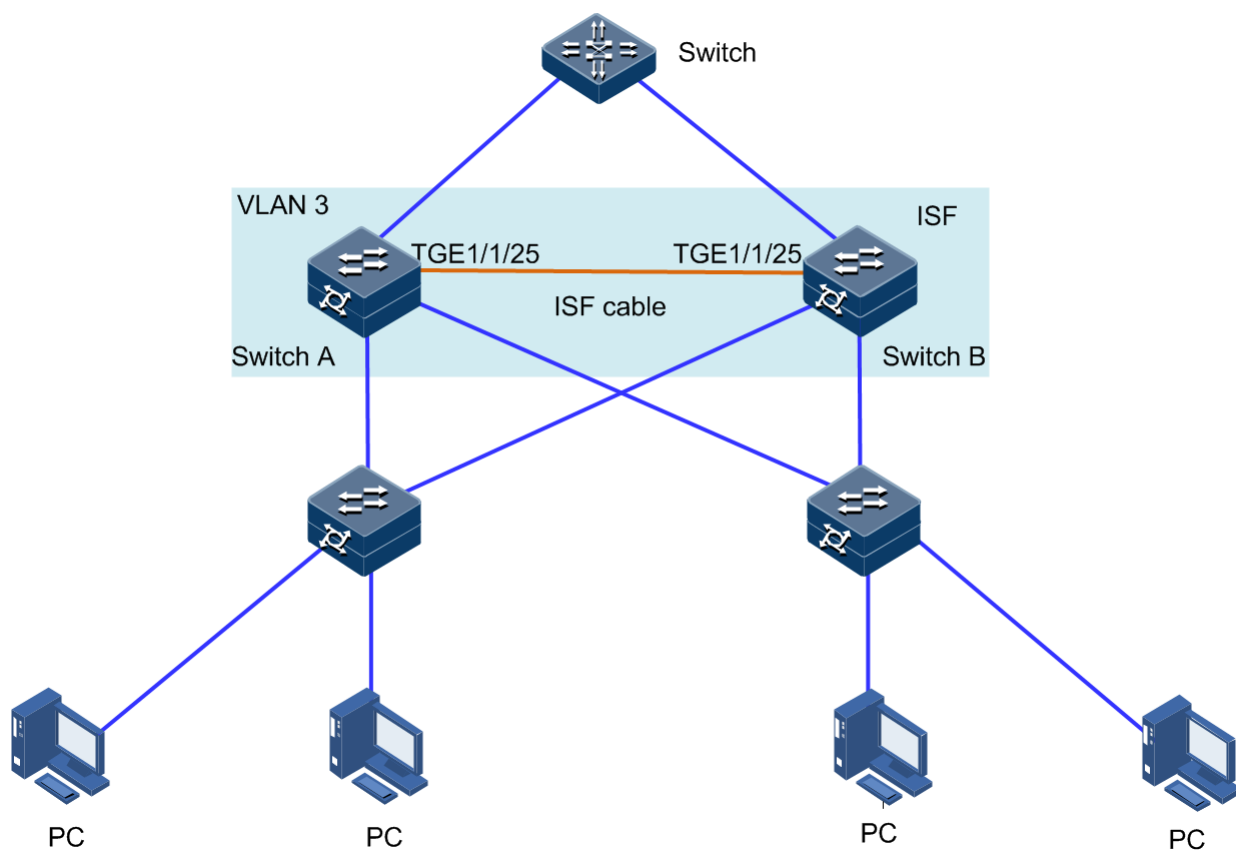
#### Configuration thought

To double forwarding capability of Switch A, add Switch B to the network, and then configure ISF on them.

When an ISF splits into two ISFs due to an ISF link fault, these two ISFs will conflict with each other. To prevent this, configure MAD. You can configure BFD MAD to monitor the ISF status.

## Networking topology

Figure 3-14 ISF networking (BFD MAD mode)



## Configuration steps

Step 1 Configure switches in standalone mode.

1. Configure Switch A.

Configure the member ID to 1 and member priority to 12. Create ISF interface 2. Binding it with the physical interface Tengigabitethernet 1/1/25.

```
Raisecom#config
Raisecom(config)#isf renumber 1
Raisecom(config)#isf priority 12
Raisecom(config)#interface tengigabitethernet 1/1/25
Raisecom(config-tengigabitethernet1/1/25)#exit
Raisecom(config)#interface isf-port 1/1/1
Raisecom(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom(config-isf-port1/1/1)#exit
Raisecom(config)#exit
```

Save running configurations to the startup configuration file.

```
Raisecom#write
```

Configure Switch A to ISF mode.

```
Raisecom#config
Raisecom(config)#isf mode isf
next unit is: 9, please input 'yes':yes
This configuration will go into effect after reboot, Please input 'yes'
to reboot:yes
Will you change start-config ? please input 'yes' to change:yes

1970-01-01,08:06:46 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
Raisecom(config)#
BOOTROM starting ..
```

After Switch A is restarted, it forms an ISF that has only one member device.

- Configure Switch B.

Configure the member ID to 2 and member priority to 26. Create ISF interface 1. Bind it with the physical interface Tengigabitethernet 1/1/25.

```
Raisecom#config
Raisecom(config)#isf renumber 2
Member ID change will take effect after the switch reboots and work in
ISF mode
Will you change start-config ? please input 'yes' to change:no
Raisecom(config)#isf priority 26
Raisecom(config)#interface tengigabitethernet 1/1/25

Raisecom(config)#interface isf-port 1/1/1
Raisecom(config-if-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom(config)#exit
```

Save running configurations to the startup configuration file.

```
Raisecom#write
```

Configure Switch B to ISF mode.

```
Raisecom#config
Raisecom(config)#isf mode isf
next unit is: 2, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
Will you change start-config ? please input 'yes' to change:yes
```

```
1970-01-01,08:10:05 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
Raisecom(config)#
BOOTROM starting ..
```

## Step 2 Configure switches in ISF mode.

Configure BFD MAD.

- Configure Switch A.

Create VLAN 3. Configure the MAD IP address. Enable BFD MAD on Switch A (with the member ID as 1).

```
Raisecom#1#config
Raisecom#1(config)#create vlan 3 active
Raisecom#1(config)#interface vlan 3
Raisecom#1(config-vlan3)#mad ip address 192.168.2.1 unit 1
Raisecom#1(config-vlan3)#mad bfd enable
1970-01-01,08:17:21 BFD-5-BFD_SESSIONID_DOWN:unit1: Bfd session 65 is
down.#
```

- Configure Switch B.

Create VLAN 3. Configure the MAD IP address. Enable BFD MAD on Switch B (with the member ID as 2).

```
Raisecom#2#config
Raisecom#2(config)#create vlan 3 active
Raisecom#2(config)#interface vlan 3
Raisecom#2(config-vlan3)#mad ip address 192.168.2.2 unit 2
Raisecom#2(config-vlan3)#mad bfd enable
1970-01-01,08:17:21 BFD-5-BFD_SESSIONID_DOWN:unit1: Bfd session 65 is
down.#
```

## 3.8.2 Example for configuring ISF in non-preconfiguration mode with BFD MAD

### Networking requirements

When the network grows rapidly, the central switch (Switch A) fails to meet forwarding requirements. To double forwarding capability based on protecting the existing investment with easy management and maintenance, you can configure ISF.

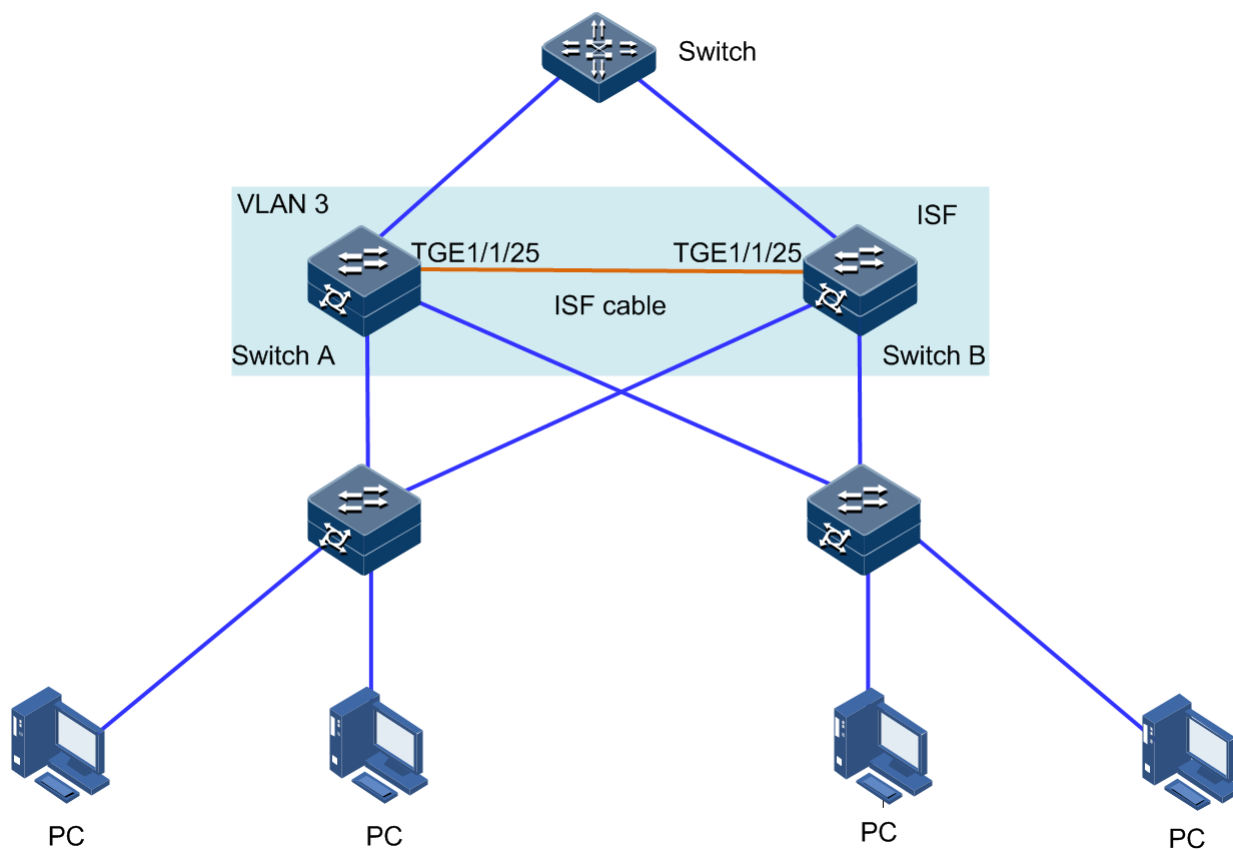
## Configuration thought

Disconnect the ISF link by manually removing the ISF cable or using CLI to shut down all ISF physical interfaces on the master device. This example takes CLI for example.

After the ISF splits, switch the two member devices from ISF mode to standalone mode.

## Networking topology

Figure 3-15 ISF networking with member device changing from ISF mode to standalone mode



## Configuration steps

Step 1 Determine the master device.

```
Raisecom#1#show isf
Raisecom#1(config)#isf renumber 1
Raisecom#1(config)#isf mode isf
next unit is: 1, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
BOOTROM starting ..
```

Configure ISF interface 1/1/1, and bind it with physical interface Tengigabitethernet 1/1/25.

```
Raisecom#1(config)#interface tengigabitethernet 1/1/25
Raisecom#1(config-tengigabitethernet1/1/25)#exit
Raisecom#1(config)#interface isf-port 1/1/1
Raisecom#1(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom#1(config-isf-port1/1/1)#exit
Raisecom#1(config)#isf unit 1 priority 64
Raisecom#1(config)#exit
```

Save running configurations to the startup configuration file.

```
Raisecom#1#write
```

## Step 2 Configure Device B.

Configure Switch B to ISF mode.

```
Raisecom#1#config
Raisecom#1(config)#isf renumber 2
Raisecom#1(config)#isf-mode isf
next unit is: 2, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
BOOTROM starting ..
```

Configure ISF interface 1/1/1, and bind it with physical interface Tengigabitethernet 1/1/25.

```
Raisecom#2(config)#interface tengigabitethernet 1/1/25
Raisecom#2(config-tengigabitethernet1/1/25)#exit
Raisecom#2(config)#interface isf-port 1/1/1
Raisecom#2(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom#2(config-isf-port1/1/1)#exit
Raisecom#2(config)#isf unit 1 priority 255
Raisecom#2(config)#exit
```

Save running configurations to the startup configuration file.

```
Raisecom#1#write
```

## Step 3 Configure switches in ISF mode.

Configure BFD MAD detection.

- Configure Switch A.

Create VLAN 3. Configure the MAD IP address. Enable BFD MAD on Switch A (with the member ID as 1).

```
Raisecom#1#config
Raisecom#1(config)#create vlan 3 active
Raisecom#1(config)#interface vlan 3
Raisecom#1(config-vlan3)#mad ip address 192.168.2.1 unit 1
Raisecom#1(config-vlan3)#mad bfd enable
1970-01-01,08:17:21 BFD-5-BFD_SESSIONID_DOWN:unit1: Bfd session 65 is
down.#
```

- Configure Switch B.

Create VLAN 3. Configure the MAD IP address. Enable BFD MAD on Switch A (with the member ID as 2).

```
Raisecom#2#config
Raisecom#2(config)#create vlan 3 active
Raisecom#2(config)#interface vlan 3
Raisecom#2(config-vlan3)#mad ip address 192.168.2.2 unit 2
Raisecom#2(config-vlan3)#mad bfd enable
1970-01-01,08:17:21 BFD-5-BFD_SESSIONID_DOWN:unit1: Bfd session 65 is
down.#
```

If the intermediate device is an ISF, you must configure it with a domain ID that is different from the domain ID of the target ISF system.

### 3.8.3 Example for switching member device from ISF mode to standalone mode

#### Networking requirements

An ISF runs stably with two member devices: Switch A and Switch B. Due to network adjustment, you need to switch them from ISF mode to standalone mode.

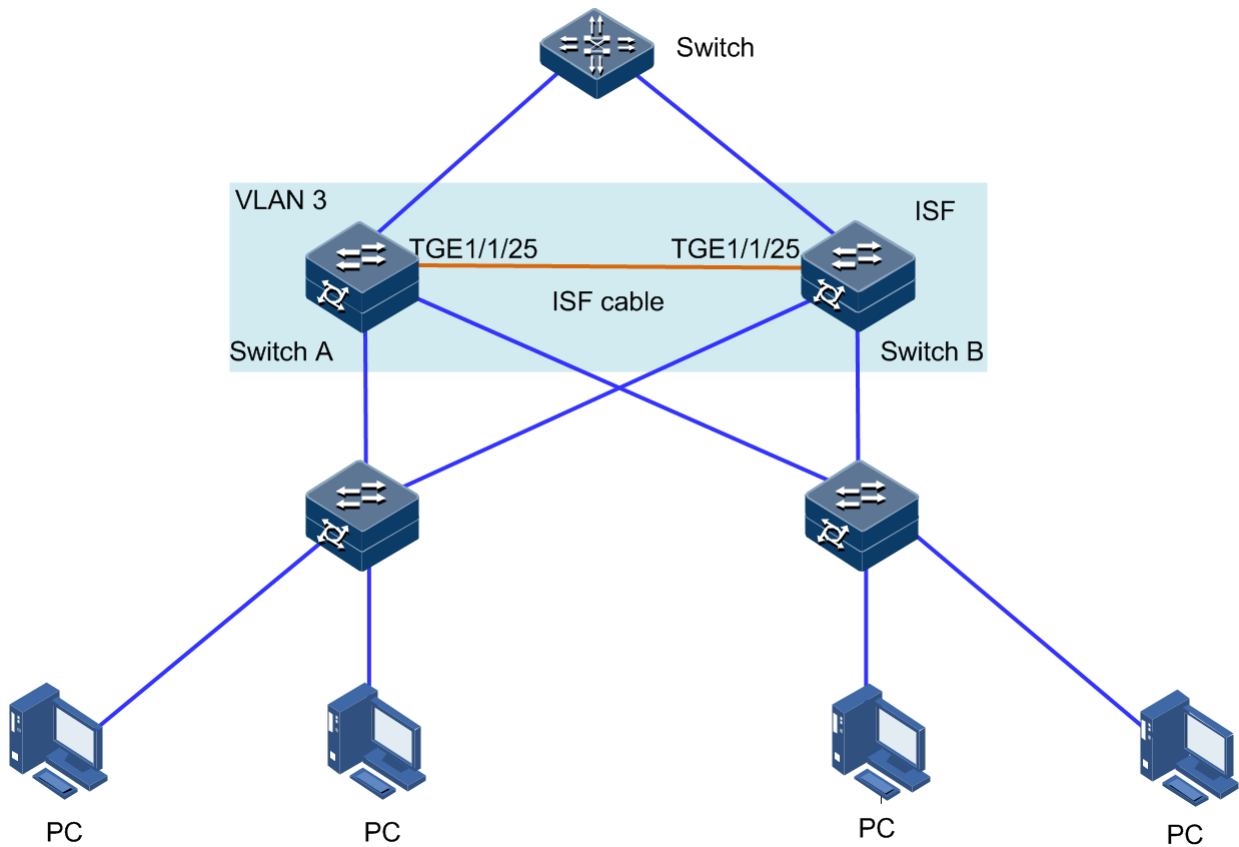
#### Configuration thought

To double forwarding capability of Switch A, add Switch B to the network, and then configure ISF on them.

When an ISF splits into two ISFs due to an ISF link fault, these two ISFs will conflict with each other. To prevent this, configure MAD. You can configure BFD MAD to monitor the ISF status.

## Networking topology

Figure 3-16 ISF networking (BFD MAD mode)



## Configuration steps

Step 1 Determine the master device. Configure Switch A as below:

```
Raisecom#1#show isf
MODE:ISF mode
ISF MAC:00:01:22:44:76:78
-----
Isf-port1/1/1
Tengigabitethernet1/1/25
Number  MAC Address      Domain  Unit  Priority  Role
stk Time  Version  Minversion
1        00:01:22:44:76:78    0       2     255     master
18              2          9
2        00:0e:5e:61:91:cf    0       1     64     backup
30              2          9
```

Previous information shows that Switch B is the master device.

Step 2 Disconnect the ISF link by manually shutting down ISF physical interface Tengigabitethernet 1/1/25 on the master device.



Step 3 Configure Switch A to standalone mode.

Configure Switch A as below:

```
Raisecom#1#config
Raisecom#1#(config)#isf-mode single
This config reboot go into effect, Please input 'yes' to reboot:yes
Will you change start-config ? please input 'yes' to change:yes
1970-01-01,08:36:35 System-4-SYSTEM_REBOOT:unit2: Change work Mode
reboot !
Operation successfully
BOOTROM starting ..
```

Step 4 Log in to Switch B. Configure it to standalone mode.

```
Raisecom#2#config
Raisecom#2(config)#isf-mode single
This config reboot go into effect, Please input 'yes' to reboot:yes
Will you change start-config ? please input 'yes' to change:yes
1970-01-01,08:36:35 System-4-SYSTEM_REBOOT:unit2: Change work Mode
reboot !
Operation successfully
BOOTROM starting ..
```

## 3.8.4 Example for configuring four devices to form ISF

### Networking requirements

When the network grows rapidly, the central switch (Switch A) fails to meet forwarding requirements. To implement easy management and maintenance, add three devices to form an ISF with Switch A, as shown in Figure 3-17.

## Networking topology

Figure 3-17 Networking topology before configuring ISF

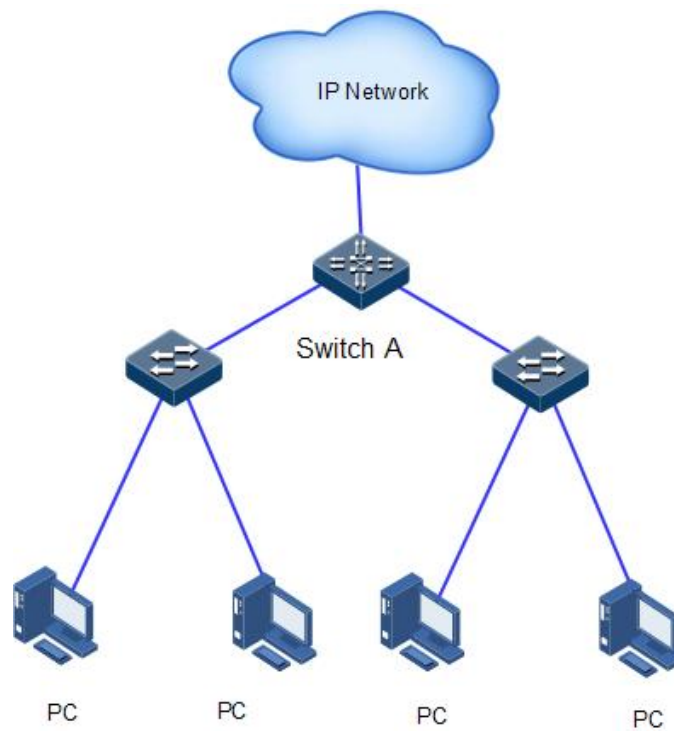
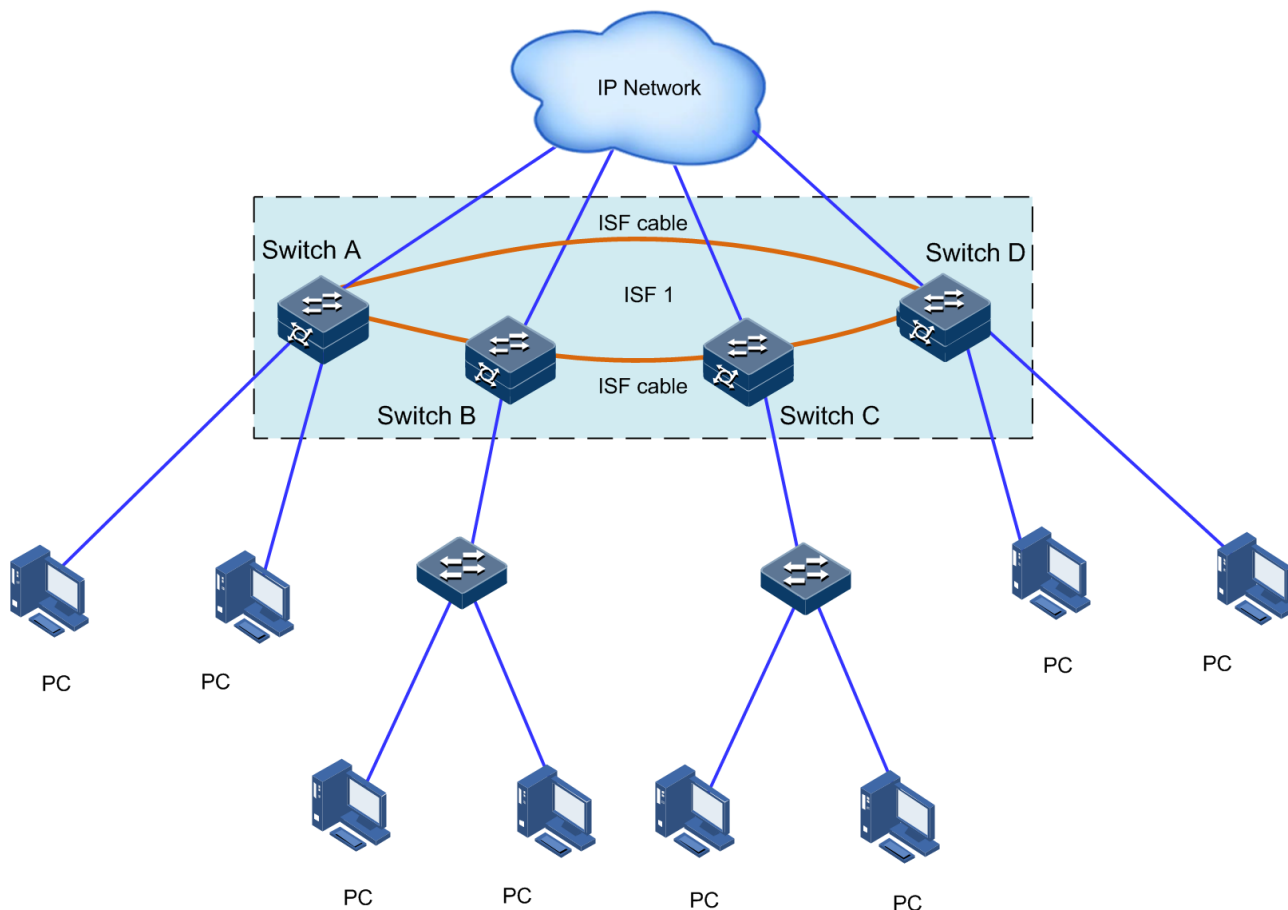


Figure 3-18 Networking topology after adding Switch A to ISF



## Configuration thought

- Configure the member ID, member priority, and ISF interface of these four member devices.
- Configure ISF on them. Connect them according to the previous networking topology.
- Switch them to ISF mode.

## Configuration steps

### Step 1 Configure Switch A.

1. Configure the member ID of Switch A to 1 and member priority to 12.

```
Raisecom#config
Raisecom(config)#isf renumber 1
Raisecom(config)#isf priority 12
Raisecom(config)#interface tengigabitethernet 1/1/25
Raisecom(config-tengigabitethernet1/1/25)#exit
Raisecom(config)#interface tengigabitethernet 1/1/27
Raisecom(config-tengigabitethernet1/1/27)#exit
Raisecom(config)#interface isf-port 1/1/1
Raisecom(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
```

```
Raisecom(config-isf-port1/1/1)#exit
Raisecom(config)#interface isf-port 1/1/2
Raisecom(config-isf-port1/1/2)#isf port-group tengigabitethernet 1/1/27
Raisecom(config-isf-port1/1/2)#exit
```

2. Save running configurations to the startup configuration file.

```
Raisecom#write
```

3. Configure Switch A to ISF mode.

```
Raisecom#config
Raisecom(config)#isf mode isf
next unit is: 1, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
BOOTROM starting ..
```

After Switch A is restarted, it forms an ISF that has only one member device.

## Step 2 Configure Device B.

1. Configure the member ID of Switch B to 2 and member priority to 26.

```
Raisecom#config
Raisecom(config)#isf renumber 2
Raisecom(config)#isf priority 26
Raisecom(config)#interface tengigabitethernet 1/1/25
Raisecom(config-tengigabitethernet1/1/25)#exit
Raisecom(config)#interface tengigabitethernet 1/1/27
Raisecom(config-tengigabitethernet1/1/27)#exit
Raisecom(config)#interface isf-port 1/1/1
Raisecom(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom(config-isf-port1/1/1)#exit
Raisecom(config)#interface isf-port 1/1/2
Raisecom(config-isf-port1/1/2)#isf port-group tengigabitethernet 1/1/27
Raisecom(config-isf-port1/1/2)#exit
```

2. Save running configurations to the startup configuration file.

```
Raisecom#write
```

3. Configure Switch B to ISF mode.

```
Raisecom#config
Raisecom(config)#isf mode isf
next unit is: 9, please input 'yes':yes
This configuration will go into effect after reboot, Please input 'yes'
to reboot:yes
Will you change start-config ? please input 'yes' to change:yes

1970-01-01,08:06:46 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
Raisecom(config)#
BOOTROM starting ..
```

After Switch B is restarted, it joins the ISF with Switch A.

### Step 3 Configure Switch C.

1. Configure the member ID of Switch C to 3 and member priority to 6.

```
Raisecom#config
Raisecom(config)#isf renumber 3
Raisecom(config)#isf priority 6
Raisecom(config)#interface tengigabitethernet 1/1/25
Raisecom(config-tengigabitethernet1/1/25)#exit
Raisecom(config)#interface tengigabitethernet 1/1/27
Raisecom(config-tengigabitethernet1/1/27)#exit
Raisecom(config)#interface isf-port 1/1/1
Raisecom(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom(config-isf-port1/1/1)#exit
Raisecom(config)#interface isf-port 1/1/2
Raisecom(config-isf-port1/1/2)#isf port-group tengigabitethernet 1/1/27
Raisecom(config-isf-port1/1/2)#exit
```

2. Save running configurations to the startup configuration file.

```
Raisecom#write
```

3. Configure Switch C to ISF mode.

```
Raisecom#config
Raisecom(config)#isf mode isf
next unit is: 3, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
```

```
operation successfully
BOOTROM starting ..
```

After Switch C is restarted, it joins the ISF with Switch A and Switch B.

#### Step 4 Configure Switch D.

1. Configure the member ID of Switch D to 4 and member priority to 2.

```
Raisecom#config
Raisecom(config)#isf renumber 4
Raisecom(config)#isf priority 2
Raisecom(config)#interface tengigabitethernet 1/1/25
Raisecom(config-tengigabitethernet1/1/25)#exit
Raisecom(config)#interface tengigabitethernet 1/1/27
Raisecom(config-tengigabitethernet1/1/27)#exit
Raisecom(config)#interface isf-port 1/1/1
Raisecom(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom(config-isf-port1/1/1)#exit
Raisecom(config)#interface isf-port 1/1/2
Raisecom(config-isf-port1/1/2)#isf port-group tengigabitethernet 1/1/27
Raisecom(config-isf-port1/1/2)#exit
```

2. Save running configurations to the startup configuration file.

```
Raisecom#write
```

3. Configure Switch D to ISF mode.

```
Raisecom#config
Raisecom(config)#isf mode isf
next unit is: 4, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
BOOTROM starting ..
```

After Switch D is restarted, it joins the ISF with Switch A, Switch B, and Switch C.

# 4 Ring network protection

---

This chapter describes basic principles and configuration procedures for ring network protection, including the following section:

- G.8032
- ELPS (G.8031)

## 4.1 G.8032

### 4.1.1 Introduction

G.8032 Ethernet Ring Protection Switching (ERPS) is an APS protocol based on the ITU-T G.8032 recommendation. It is a link-layer protocol specially used in Ethernet rings. Generally, ERPS can avoid broadcast storm caused by data loopback in Ethernet rings. When a link/device on the Ethernet ring fails, traffic can be quickly switched to the backup link to ensure restoring services quickly.

G.8032 uses the control VLAN on the ring network to transmit ring network control information. Meanwhile, combining with the topology feature of the ring network, it discovers network fault quickly and enable the backup link to restore service fast.

### 4.1.2 Preparing for configurations

#### Scenario

With development of Ethernet to telecom-grade network, voice and video multicast services bring higher requirements on Ethernet redundant protection and fault-recovery time. The fault-recovery time of current STP system is in second level that cannot meet requirements.

By defining different roles for nodes on a ring, G.8032 can block a loopback to avoid broadcast storm in normal condition. Therefore, the traffic can be quickly switched to the protection line when working lines or nodes on the ring fail. This helps eliminate the loop, perform protection switching, and automatically recover from faults. In addition, the switching time is shorter than 50ms.

The ISCOM2600G-HI series switch supports the single ring, intersecting ring, and tangent ring.

G.8032 provides a mode for detecting faults based on physical interface status. The ISCOM2600G-HI series switch learns link fault quickly and switches services immediately, so this mode is suitable for detecting the fault between neighboring devices.

## Prerequisite

- Connect the interface.
- Configure its physical parameters to make it Up.
- Create VLANs.
- Add interfaces to VLANs.

## 4.1.3 Default configurations of G.8032

Default configurations of G.8032 are as below.

Function	Default value
Protocol VLAN	1
Protection ring mode	Revertive
Ring WTR timer	6min
Ring protocol version	2
Guard timer	500ms
Ring Hold-off timer	0ms
G.8032 fault reported to NMS	Enable
Tributary ring virtual channel mode in intersecting node	With
Ring Propagate switch in crossing node	Disable

## 4.1.4 Creating G.8032 ring

Configure G.8032 for the ISCOM2600G-HI series switch as below.





### Caution

- Only one device on the protection ring can be configured to the Ring Protection Link (RPL) Owner and one device is configured to the RPL neighbor. Other devices are configured to ring forwarding nodes.
- The tangent ring consists of 2 independent single rings. Configurations on the tangent ring are identical to the ones on the common single ring. The intersecting ring consists of a main ring and a tributary ring. Configurations on the main ring are identical to the ones on the common single ring. For detailed configurations of the tributary ring, see section 4.1.6 (Optional) creating G.8032 tributary ring.

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



Step	Command	Description
2	<pre>Raisecom(config)#<b>ethernet</b> <b>ring-protection</b> <i>ring-id</i> <b>east</b> { <i>interface-type</i> <i>interface-</i> <i>number</i>   <b>port-channel</b> <i>port-</i> <i>channel-number</i> } <b>west</b> { <i>interface-type</i> <i>interface-</i> <i>number</i>   <b>port-channel</b> <i>port-</i> <i>channel-number</i> } [ <b>node-type</b> <b>rpl-owner</b> <b>rpl</b> { <b>east</b>   <b>west</b> } ] [ <b>not-revertive</b> ] [ <b>protocol-vlan</b> <i>vlan-id</i> ] [ <b>block-vlanlist</b> <i>vlan-list</i> ]</pre>	<p>Create a protection ring and configure the node as the RPL Owner.</p> <p> <b>Note</b> The east and west interfaces cannot be the same one.</p>
	<pre>Raisecom(config)#<b>ethernet</b> <b>ring-protection</b> <i>ring-id</i> <b>east</b> { <i>interface-type</i> <i>interface-</i> <i>number</i>   <b>port-channel</b> <i>port-</i> <i>channel-number</i> } <b>west</b> { <i>interface-type</i> <i>interface-</i> <i>number</i>   <b>port-channel</b> <i>port-</i> <i>channel-number</i> } <b>node-type</b> <b>rpl-neighbour</b> <b>rpl</b> { <b>east</b>  <b>west</b> } [ <b>not-revertive</b> ] [ <b>protocol-vlan</b> <i>vlan-id</i> ] [ <b>block-vlanlist</b> <i>vlan-list</i> ]</pre>	Create a protection ring, and configure the node as the RPL Neighbour.
	<pre>Raisecom(config)#<b>ethernet</b> <b>ring-protection</b> <i>ring-id</i> <b>east</b> { <i>interface-type</i> <i>interface-</i> <i>number</i>   <b>port-channel</b> <i>port-</i> <i>channel-number</i> } <b>west</b> { <i>interface-type</i> <i>interface-</i> <i>number</i>   <b>port-channel</b> <i>port-</i> <i>channel-number</i> } [ <b>not-</b> <b>revertive</b> ] [ <b>protocol-vlan</b> <i>vlan-id</i> ] [ <b>block-vlanlist</b> <i>vlan-list</i> ]</pre>	Create a protection line, and configure the node as the protection forwarding node.
3	<pre>Raisecom(config)#<b>ethernet</b> <b>ring-protection</b> <i>ring-id</i> <b>name</b> <i>string</i></pre>	(Optional) configure a name for the protection ring. Up to 32 bytes are available.
4	<pre>Raisecom(config)#<b>ethernet</b> <b>ring-protection</b> <i>ring-id</i> <b>version</b> { <b>1</b>   <b>2</b> }</pre>	<p>(Optional) configure the protocol version. The protocol version of all nodes on a protection ring should be identical.</p> <p>In protocol version 1, protection rings are distinguished based on the protocol VLAN. Therefore, you need to configure different protocol VLANs for protection rings.</p> <p>We recommend configuring different protocol VLANs for protection rings even if protocol version 2 is used.</p>

Step	Command	Description
5	<b>Raisecom(config)#ethernet ring-protection ring-id guard-time guard-time</b>	(Optional) after the ring Guard timer is configured, the failed node does not process APS packets during a period. In a bigger ring network, if the failed node recovers from a fault immediately, it may receive the fault notification sent by the neighbor node on the protection ring. Therefore, the node is in Down status again. You can configure the ring Guard timer to solve this problem.
6	<b>Raisecom(config)#ethernet ring-protection ring-id wtr-time wtr-time</b>	(Optional) configure the ring WTR timer. In revertive mode, when the working line recovers from a fault, traffic is not switched to the working line unless the WTR timer times out.
7	<b>Raisecom(config)#ethernet ring-protection ring-id holdoff-time holdoff-time</b>	<p>(Optional) configure the ring Hold-off timer. After the Hold-off timer is configured, when the working line fails, the system will delay processing the fault. It means that traffic is delayed to be switched to the protection line. This helps prevent frequent switching caused by working line vibration.</p> <p> <b>Note</b> If the ring Hold-off timer value is too great, it may influence 50ms switching performance. Therefore, we recommend configuring the ring Hold-off timer value to 0.</p>

## 4.1.5 Configuring ERPS fault detection mode

Configure the ERPS fault detection mode for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ethernet ring-protection ring-id { east   west } failure-detect physical-link</b>	Configure the ERPS fault detection mode to physical link. By default, it is physical link.
	<b>Raisecom(config)# ethernet ring-protection ring-id { east   west } failure-detect cc [ md md-name ] ma ma-name level level mep local-mep-id remote-mep-id</b>	Configure the ERPS fault detection mode to CFM.

Step	Command	Description
	<b>Raisecom(config)# ethernet ring-protection ring-id { east   west } failure-detect physical-link-or-cc [ md md-name ] ma ma-name level level mep local-mep-id remote-mep-id</b>	Configure the ERPS fault detection mode to physical link or CC. In other words, the fault detected by physical link or CC is reported.


## 4.1.6 (Optional) creating G.8032 tributary ring



### Caution

- Only the intersecting ring consists of a main ring and a tributary ring.
- Configurations of the main ring are identical to those of the single/tangent ring. For details, see section 4.1.4 Creating G.8032 ring.
- For the intersecting ring, configure its main ring and then the tributary ring. Otherwise, the tributary ring will fail to find the interface of the main ring, thus failing to establish the virtual channel of the tributary ring.
- The ID of the tributary ring must be greater than that of the main ring.
- Configurations of non-intersecting nodes of the intersecting ring are identical to those of the single/tangent ring. For details, see section 4.1.4 Creating G.8032 ring.

Configure G.8032 intersecting rings for ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ethernet ring-protection ring-id { east   west } { interface-type interface-number   port-channel port-channel-number } node-type rpl-owner [ not-revertive ] [ protocol-vlan vlan-id ] [ block-vlanlist vlan-list ]</b>	<p>Create the tributary ring on the intersecting node and configure the intersecting node as the RPL Owner.</p> <p>The protection ring is in non-revertive mode if you configure the non-revertive parameter.</p> <ul style="list-style-type: none"> <li>• In revertive mode, when the working line recovers from a fault, traffic is switched from the protection line to the working line.</li> <li>• In non-revertive mode, when the working line recovers from a fault, traffic is not switched from the protection line to the working line.</li> </ul> <p>By default, the protection ring is in revertive mode.</p> <div style="margin-top: 10px;">  <b>Note</b> </div> <p>The links between 2 intersecting nodes belong to the main ring. Therefore, when you configure the tributary ring on the intersecting node, you can only configure the west or east interface.</p>

Step	Command	Description
	<pre>Raisecom(config)#<b>ethernet</b> <b>ring-protection</b> <i>ring-id</i> { <b>east</b>   <b>west</b> } { <i>interface-type</i> <i>interface-number</i>   <b>port-</b> <b>channel</b> <i>port-channel-</i> <i>number</i> } <b>node-type</b> <b>rpl-</b> <b>neighbour</b> [ <b>not-</b> <b>revertive</b> ] [ <b>protocol-</b> <b>vlan</b> <i>vlan-id</i> ] [ <b>block-</b> <b>vlanlist</b> <i>vlan-list</i> ]</pre>	Create the tributary ring on the intersecting node and configure the intersecting node as the RPL Neighbour.
	<pre>Raisecom(config)#<b>ethernet</b> <b>ring-protection</b> <i>ring-id</i> { <b>east</b>   <b>west</b> } { <i>interface-type</i> <i>interface-number</i>   <b>port-</b> <b>channel</b> <i>port-channel-</i> <i>number</i> } [ <b>not-</b> <b>revertive</b> ] [ <b>protocol-</b> <b>vlan</b> <i>vlan-id</i> ] [ <b>block-</b> <b>vlanlist</b> <i>vlan-list</i> ]</pre>	Create the tributary ring on the intersecting node and configure the intersecting node as the protection forwarding node.
3	<pre>Raisecom(config)#<b>ethernet</b> <b>ring-protection</b> <i>ring-id</i> <b>raps-vc</b> { <b>with</b>   <b>without</b> }</pre>	<p>(Optional) configure the tributary ring virtual channel mode on the intersecting node. Because the intersecting node belongs to the main ring, transmission modes of protocol packets in the tributary ring are different from the ones of the main ring. In the tributary ring, transmission modes are divided into with and without modes.</p> <ul style="list-style-type: none"> <li>• with: the main ring provides channels for APS packets of the tributary ring; the tributary ring intersecting node transmits APS packets of the tributary ring to the main ring to use the main ring to complete communications among intersecting nodes of the tributary ring.</li> <li>• without: APS packets of the tributary ring on intersecting nodes need to be ended and cannot be transmitted to the main ring. This mode requires the tributary ring not to block the protocol VLAN of the tributary ring (to ensure tributary ring packets to traverse Owner).</li> </ul> <p>By default, the virtual channel of the tributary ring adopts the with mode. Transmission modes on 2 intersecting nodes must be identical.</p>

Step	Command	Description
4	<b>Raisecom(config)#ethernet ring-protection ring-id propagate enable</b>	Enable the ring Propagate switch on the intersecting node.  Because data of the tributary ring needs to be transmitted through the main ring, there is a MAC address table of the tributary ring on the main ring. When the tributary ring fails, it needs to use the Propagate switch to inform the main ring of refreshing the MAC address table to avoid traffic loss.

### 4.1.7 (Optional) configuring G.8032 switching control

Configure G.8032 switching control for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ethernet ring-protection ring-id force-switch { east   west }</b>	Switch the traffic on the protection ring to the west/east interface forcedly.  FS can be configured on multiple interfaces of multiple ring nodes.
3	<b>Raisecom(config)#ethernet ring-protection ring-id manual-switch { east   west }</b>	Switch the traffic on the protection ring to the west/east interface manually. Its priority is lower than the one of FS and APS.  MS can be configured on one interface of a ring node.
4	<b>Raisecom(config)#clear ethernet ring-protection ring-id { command   statistics }</b>	Clear switching control commands, including <b>force-switch</b> , <b>manual-switch</b> , WTR timer, and WTB timer.



#### Note

By default, traffic is automatically switched to the protection line when the working line fails. Therefore, you need to configure G.8032 control in some special cases.

### 4.1.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show ethernet ring-protection</b>	Show configurations of the G.8032 ring.
2	<b>Raisecom#show ethernet ring-protection status</b>	Show G.8032 ring status.

No.	Command	Description
3	<b>Raisecom#show ethernet ring-protection statistics</b>	Show G.8032 ring statistics.

## 4.1.9 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
<b>Raisecom(config)#clear ethernet ring-protection ring-id statistics</b>	Clear statistics about the protection ring.

## 4.2 ELPS (G.8031)

### 4.2.1 Introduction

Ethernet Linear Protection Switching (ELPS) is an Automatic Protection Switching (APS) protocol based on the ITU-TG.8031 recommendation. It is an end-to-end protection technology used to protect an Ethernet connection.

ELPS deploys protection resources for working resources, such as path and bandwidth. It takes a simple, fast, and predictable mode to switch network resources, which is easier for carriers to plan networks more efficiently and learn network active status.

### 4.2.2 Preparing for configurations

#### Scenario

Configuring ELPS feature in Ethernet can make Ethernet reliability up to telecommunication level (network self-heal time less than 50ms). It is an end-to-end protection technology used for protecting an Ethernet link.

ELPS supports 1+1 protection switching and 1:1 protection switching modes:

- 1+1 protection switching: each working line is assigned with a protection line. In the protection domain, the source end sends traffic through the working and protection lines while the destination end receives the traffic from one line.
- 1:1 protection switching: each working line is assigned with a protection line. The source end sends traffic through the working/protection line. In general, the source sends traffic through the working line. The protection line is a backup line. When the working line fails, the source end and destination end communicate through APS protocol to switch traffic to the protection line simultaneously.

Based on whether the source end and destination end switch traffic simultaneously, ELPS is divided into unidirectional switching and bidirectional switching:

- Unidirectional switching: when one direction of a line fails, one end can receive the traffic while the other end fails to receive the traffic. The end failing to receive the traffic

detects a fault and switches the traffic. And the other end does not detect the fault and switch traffic. Therefore, both ends may receive the traffic through different lines.

- Bidirectional switching: when a line fails, even in one direction, both ends communicate through APS protocol to switch traffic to the protection line. Therefore, both ends receive and send the traffic through the same line.

This ISCOM2600G-HI series switch does not distinguish one-way and bidirectional switching until in 1+1 mode; only bidirectional switching is available in 1:1 mode.

ELPS provides two modes for fault detection:

- Detecting fault over physical interface status: to get link fault quickly and switching in time, available to neighboring devices.
- Detecting fault over CC: available to one-way detection or multi-devices crossing detection.

## Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.
- Create VLANs.
- Add interfaces to VLANs.
- Configure CFP detection among devices and make them as neighbors (for CFM detection mode only).

## 4.2.3 Default configurations of ELPS



Default configurations of ELPS are as below.

Function	Default value
Protection group mode	Revertive mode
WTR timer	5min
Hold-off timer	0
Reporting ELPS failure information to network management system	Enable
Fault detection mode	Physical link

## 4.2.4 Creating ELPS pair

Enable the ELPS pair for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<pre>Raisecom(config)#<b>ethernet</b> <b>line-protection</b> <i>line-id</i> <b>working</b> <i>interface-type</i> <i>interface-number</i> <i>vlan-list</i> <b>protection</b> <i>interface-type</i> <i>interface-number</i> <i>vlan-list</i> <b>one-to-one</b> [ <b>non-revertive</b> ] [ <b>protocol-vlan</b> <i>vlan-id</i> ]</pre>	<p>Create an ELPS protection line and configure the protection mode.</p> <p>The protection group is in non-revertive mode if you configure the <b>non-revertive</b> parameter.</p> <ul style="list-style-type: none"> <li>• In revertive mode, when the working line recovers from a fault, traffic is switched from the protection line to the working line.</li> <li>• In non-revertive mode, when the working line recovers from a fault, traffic is not switched from the protection line to the working line.</li> </ul> <p>By default, the protection group is in revertive mode.</p>
3	<pre>Raisecom(config)#<b>ethernet</b> <b>line-protection</b> <i>line-id</i> <b>name</b> <i>string</i></pre>	<p>(Optional) configure a name for the ELPS protection line.</p>
4	<pre>Raisecom(config)#<b>ethernet</b> <b>line-protection</b> <i>line-id</i> <b>wtr-</b> <b>timer</b> <i>wtr-timer</i></pre>	<p>(Optional) configure the WTR timer. In revertive mode, when the working line recovers from a fault, traffic is not switched to the working line unless the WTR timer times out.</p> <p>By default the WTR time value is 5min.</p> <p> <b>Note</b></p> <p>We recommend keeping WTR timer configurations on both ends consistent. Otherwise, 50ms quick switching may fail.</p>
5	<pre>Raisecom(config)#<b>ethernet</b> <b>line-protection</b> <i>line-id</i> <b>hold-off-timer</b> <i>hold-off-</i> <i>timer</i></pre>	<p>(Optional) configure the Hold-off timer. After the Hold-off timer is configured, when the working line fails, the system will delay processing the fault. In other words, traffic is delayed to be switched to the protection line. This helps prevent frequent switching caused by working line vibration.</p> <p>By default, the Hold-off timer value is 0.</p> <p> <b>Note</b></p> <p>If the Hold-off timer value is over great, it may affect 50ms switching performance. Therefore, we recommend setting the Hold-off timer value to 0.</p>



Step	Command	Description
6	<b>Raisecom(config)#ethernet line-protection trap enable</b>	(Optional) enable ELPS Trap to be reported to the NMS. By default, ELPS Trap to be reported to the NMS is disabled. Use the <b>ethernet line-protection trap disable</b> command to disable ELPS Trap.

## 4.2.5 Configuring ELPS fault detection mode

Configure the ELPS fault detection mode for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ethernet line-protection line-id { working   protection } failure-detect physical-link</b>	Configure the fault detection mode of the working line/protection line to physical link. By default, it is physical link.
	<b>Raisecom(config)#ethernet line-protection line-id { working   protection } failure-detect cc [ md md-name ] ma ma-name level level mep local-mep-id remote-mep-id</b>	Configure the fault detection mode of the working line/protection line to CC. This fault detection mode cannot take effect unless you finish related configurations on CFM.
	<b>Raisecom(config)#ethernet line-protection line-id { working   protection } failure-detect physical-link-or-cc [ md md-name ] ma ma-name level level mep local-mep-id remote-mep-id</b>	Configure the fault detection mode of the working line/protection line to failure-detect physical-link-or-cc. In this mode, a Trap is reported when a fault is detected on the physical link/CC. This fault detection mode cannot take effect unless you finish related configurations on CFM.



### Note

Fault detection modes of the working line and protection line can be different. However, we recommend keeping fault detection mode configurations of the working line and protection line consistent.

## 4.2.6 (Optional) configuring ELPS control

Configure ELPS control for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ethernet line-protection line-id lockout</b>	Lock protection switching. After this configuration, the traffic is not switched to the protection line even the working line fails.
3	<b>Raisecom(config)#ethernet line-protection line-id force-switch</b>	Switch the traffic from the working line to the protection line forcedly.
4	<b>Raisecom(config)#ethernet line-protection line-id manual-switch</b>	Switch the traffic from the working line to the protection line manually. Its priority is lower than the one of FS and APS.
5	<b>Raisecom(config)#ethernet line-protection line-id manual-switch-to-work</b>	In non-revertive mode, switch the traffic from the protection line to the working line.
6	<b>Raisecom(config)#clear ethernet line-protection line-id end-to-end command</b>	Clear end-to-end switching control commands, including <b>lockout</b> , <b>force-switch</b> , <b>manual-switch</b> , and <b>manual-switch-to-work</b> .



### Note

By default, traffic is automatically switched to the protection line when the working line fails. Therefore, you need to configure ELPS switching control in some special cases.

## 4.2.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show ethernet line-protection [ line-id ]</b>	Show configurations of the protection line.
2	<b>Raisecom#show ethernet line-protection [ line-id ] statistics</b>	Show protection line statistics.
3	<b>Raisecom#show ethernet line-protection [ line-id ] aps</b>	Show APS information.

## 4.2.8 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

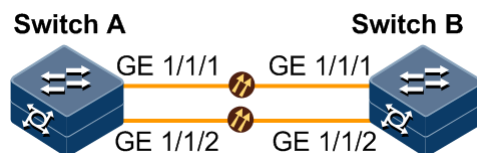
Command	Description
<b>Raisecom(config)#clear ethernet line-protection [ line-id ] statistics</b>	Clear protection line statistic, including Tx APS packets, Rx APS packets, latest switching time, latest status switching time.

## 4.2.9 Example for configuring 1:1 ELPS protection

### Networking requirements

As shown in Figure 4-1, to improve link reliability between Switch A and Switch B, configure 1:1 ELPS on the two Switch devices and detect fault based on physical interface status. GE 1/1/1 and GE 1/1/2 belong to VLANs 100–200.

Figure 4-1 1:1 ELPS networking



### Configuration steps

Step 1 Create VLANs 100–200 and add interfaces to VLANs 100–200.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100-200 active
SwitchA(config)# interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 100-200
confirm
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)# interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#switchport trunk allowed vlan 100-200
confirm
SwitchA(config-gigaethernet1/1/2)#exit
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#create vlan 100-200 active
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#switchport trunk allowed vlan 100-200
confirm
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#switchport trunk allowed vlan 100-200
confirm
SwitchB(config-gigaethernet1/1/2)#exit
```

Step 2 Create a 1:1 mode ELPS pair.

Configure Switch A.

```
SwitchA(config)#ethernet line-protection 1 working gigasethernet 1/1/1  
100-200 protection gigasethernet 1/1/2 100-200 one-to-one
```

Configure Switch B.

```
SwitchB(config)#ethernet line-protection 1 working gigasethernet 1/1/1  
100-200 protection gigasethernet 1/1/2 100-200 one-to-one
```

Step 3 Configure fault detection mode.

Configure Switch A.

```
SwitchA(config)#ethernet line-protection 1 working failure-detect  
physical-link  
SwitchA(config)#ethernet line-protection 1 protection failure-detect  
physical-link
```

Configure Switch B.

```
SwitchB(config)#ethernet line-protection 1 working failure-detect  
physical-link  
SwitchB(config)#ethernet line-protection 1 protection failure-detect  
physical-link
```

## Checking results

Use the **show ethernet line-protection** command to show configurations of 1:1 ELPS on the ISCOM2600G-HI series switch.

Take Switch A for example.

```
SwitchA#show ethernet line-protection 1  
Trap State:Enable  
  
Id:1  
Name:--  
ProtocolVlan:1  
working Entity Information:
```

```

Port:    gigaethernet1/1/1
Vlanlist: 1
FailureDetect:physical
MAID:    --
MdLevel: 0
LocalMep: 0
RemoteMep:0
State/LCK/M:Active/N/N
Link State:failure
Protection Entity Information:
Port:    gigaethernet1/1/2
Vlanlist: 1
FailureDetect:physical
MAID:    --
MdLevel: 0
LocalMep: 0
RemoteMep:0
State/F/M:Standby/N/N
Link State:failure
Wtr(m):5
Holdoff(100ms):0

```

Use the **show ethernet line-protection aps** command to show configurations of the 1:1 ELPS APS on the ISCOM2600G-HI series switch.

Take Switch A for example.

```

SwitchA#show ethernet line-protection 1 aps
Trap State:Enable

```

```

C-Direction: Configuration Direction
N-Direction: Negotiated Direction
R-Signal: Requested Signal
B-Signal: Bridged Signal
Id          Type C-Direction N-Direction Revert Aps State R-Signal B-Signal
-----
1-Local    1:1 bi          bi          yes    yes SF-P null    null

```

# 5 IP services

---

This chapter describes basic principles and configuration procedures for IP services, and provides related configuration examples, including the following sections:

- IP basis
- Loopback interface
- ARP
- NDP
- Static route
- RIP
- OSPFv2

## 5.1 IP basis

### 5.1.1 Introduction

The IP interface is the virtual interface based on VLAN. Configuring Layer 3 interface is generally used for network management or routing link connection of multiple devices.

The ISCOM2600G-HI series switch supports double-tagged management VLAN packets; in other words, it can send and process double-tagged packets.

### 5.1.2 Preparing for configurations

#### Scenario

Configure the IP address of each VLAN interface and loopback interface.

#### Prerequisite

- Create VLANs.
- Activate them.

### 5.1.3 Default configurations of Layer 3 interface

Default configurations of the Layer 3 interface are as below.

Function	Default value
Management VLAN inner TPID	0x8100
Management VLAN inner VLAN	1
Management VLAN CoS	0

## 5.1.4 Configuring IPv4 address of VLAN interface

Configure the IPv4 address of the VLAN interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlan <i>vlan-id</i></b>	Enter VLAN interface configuration mode.
3	<b>Raisecom(config-vlan1)#ip address <i>ip-address</i> [ <i>ip-mask</i> ] [ <i>sub</i> ]</b>	Configure the IP address of the VLAN interface. Use the <b>no ip address <i>ip-address</i></b> command to delete configuration of the IP address.

## 5.1.5 Configuring IPv6 address of VLAN interface

Configure the IPv6 address of the VLAN interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlan <i>vlan-id</i></b>	Enter Layer 3 interface configuration mode.
3	<b>Raisecom(config-vlan1)#ipv6 address <i>ipv6-address</i> link-local</b> <b>Raisecom(config-vlan1)#ipv6 address <i>ipv6-address/prefix-length</i> [ <i>eui-64</i> ]</b>	Configure the IPv6 address of the VLAN interface.

## 5.1.6 Configuring attributes of management VLAN

Configure attributes of the management VLAN for the Gazelle S1508i-PWR as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlan <i>vlan-id</i></b>	Enter VLAN interface configuration mode.

Step	Command	Description
3	<b>Raisecom(config-vlan1)#ip management-traffic cos <i>cos-value</i></b>	Configure CoS of the management VLAN. By default, it is 6.
4	<b>Raisecom(config-vlan1)#ip management-traffic mode double- tagging [ inner-vlan <i>vlan-id</i> ] [ inner-cos <i>cos-id</i> ]</b>	Configure the double-tagged mode for management packets.

## 5.1.7 Checking configurations

Use the following commands to check configuration results.

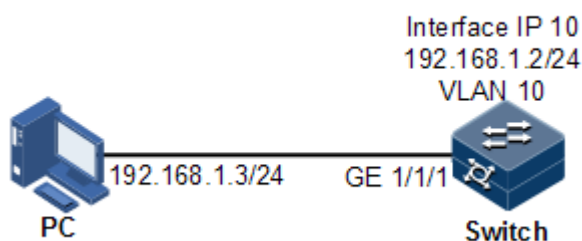
No.	Command	Description
1	<b>Raisecom#show ip interface brief</b>	Show configurations of the IP address of the VLAN interface.
2	<b>Raisecom#show ipv6 interface brief</b>	Show configurations of the IPv6 address of the VLAN interface.
3	<b>Raisecom#show ip management- traffic</b>	Show information about management packets on the VLAN interface.

## 5.1.8 Example for configuring VLAN interface to interconnect with host

### Networking requirements

As shown in Figure 5-1, configure the VLAN interface to the switch so that the host and the ISCOM2600G-HI series switch can ping each other.

Figure 5-1 VLAN interface networking



### Configuration steps

Step 1 Create a VLAN and add the interface to the VLAN.



```
Raisecom#config
Raisecom(config)#create vlan 10 active
```

- Step 2 Configure Layer 3 interface on the ISCOM2600G-HI series switch, configure its IP address, and associate the interface with the VLAN.

```
Raisecom(config)#interface VLAN 10
Raisecom(config-VLAN10)#ip address 192.168.1.2 255.255.255.0
```

## Checking results

Use the **show vlan** command to show mapping between the physical interface and VLAN.

```
Raisecom#show vlan 10
```

VLAN Name	State	Status	Priority	Member-Ports
10 VLAN0010	active	static	--	

Use the **show ip interface brief** to show configurations of the Layer 3 interface.

```
Raisecom#show ip interface brief
```

VRF	IF	Address	NetMask
Default-IP-Routing-Table	fastethernet1/0/1	192.168.0.1	255.255.255.0
primary			
Default-IP-Routing-Table	vlan10	192.168.1.2	255.255.255.0
primary			

Use the **ping** command to check whether the ISCOM2600G-HI series switch and PC can ping each other.

```
Raisecom#ping 192.168.1.3
Type CTRL+C to abort
Sending 5, 8-byte ICMP Echos to 192.168.1.3, timeout is 3 seconds:
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms

---- PING Statistics----
5 packets transmitted, 5 packets received,
```

Success rate is 100 percent(5/5),  
round-trip (ms) min/avg/max = 0/0/0.

## 5.2 Loopback interface

### 5.2.1 Introduction

The loopback interface is a virtual interface and can be classified into two types:

- Loopback interface automatically created by the system: the IP address is fixed to 127.0.0.1. This type of interfaces receives packets sent to the device. It does not broadcast packets through routing protocols.
- Loopback interface created by users: without affecting physical interface configurations, configure a local interface with a specified IP address, and make the interface Up permanently so that packets can be broadcasted through routing protocols.

The loopback interface status is independent from the physical interface status (Up/Down). As long as the ISCOM2600G-HI series switch is working normally, the loopback interface will not become Down. Thus, it is used to identify the physical device as a management address.

### 5.2.2 Preparing for configurations

#### Scenario

Use the IP address of the loopback interface to log in through Telnet so that the Telnet operation does not become Down due to change of physical status. To enable the PC to ping through the IP address of the loopback interface, configure the corresponding static route entry on the PC. The loopback interface ID is also used as the router ID of dynamic routing protocols, such as OSPF, to uniquely identify a device.

#### Prerequisite

N/A

### 5.2.3 Default configurations of loopback interface

N/A

### 5.2.4 Configuring IP address of loopback interface

Configure the IP address of the loopback interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface loopback <i>lb-number</i></b>	Enter loopback interface configuration mode.

Step	Command	Description
3	<b>Raisecom(config-loopback)#ip address</b> <i>ip-address</i> [ <i>ip-mask</i> ]	Configure the IP address of the loopback interface.
4	<b>Raisecom(config-loopback)#ipv6 address</b> <i>ipv6-address link-local</i> <b>Raisecom(config-loopback)#ipv6 address</b> <i>ipv6-address/prefix-length</i> [ <i>eui-64</i> ]	Configure the IPv6 address of the loopback interface.

## 5.2.5 Configuring interface loopback

Configure interface loopback for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter loopback interface configuration mode.
3	<b>Raisecom(config-gigaetherne</b> t1/1/port) <b>#loopback external</b> [ <i>cvlan vlan-id</i> [ <i>cos cos-value</i> ] <i>svlan vlan-id</i> [ <i>cos cos-value</i> ] ] [ <i>dmac mac-address</i> ] [ <i>smac mac-address</i> ] [ <b>swap</b> [ <i>smac mac-address</i> <b>swap</b> ] <b>dmac-disable</b> ]	Configure interface loopback.

## 5.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show interface loopback</b>	Show configurations of the loopback interface.

## 5.3 ARP

### 5.3.1 Introduction

In TCP/IP network environment, each host is assigned with a 32-bit IP address that is a logical address used to identify hosts between networks. To transmit packets in physical link, you must know the physical address of the destination host, which requires mapping the IP address to the physical address. In Ethernet environment, the physical address is 48-bit MAC address. The system has to transfer the 32-bit IP address of the destination host to the 48-bit Ethernet address for transmitting packet to the destination host correctly. Then Address

Resolution Protocol (ARP) is applied to resolve IP address to MAC address and configure mapping between IP address and MAC address.

The ARP address table contains the following two types:

- Static entry: bind the IP address and MAC address to avoid ARP dynamic learning cheating.
  - The static ARP address entry needs to be added/deleted manually.
  - The static ARP address entry is not aged.
- Dynamic entry: MAC address automatically learned through ARP.
  - This dynamic ARP address entry is automatically generated by switch. You can adjust partial parameters of it manually.
  - The dynamic ARP address entry will be aged after the aging time if not used.

The ISCOM2600G-HI series switch supports the following two modes of dynamically learning ARP address entries:

- Learn-all: in this mode, the ISCOM2600G-HI series switch learns both ARP request packets and response packets. When device A sends its ARP request, it writes mapping between its IP address and physical address in ARP request packets. When device B receives ARP request packets from device A, it learns the mapping in its address table. In this way, device B will no longer send ARP request when sending packets to device A.
- learn-reply-only mode: in this mode, the ISCOM2600G-HI series switch learns ARP response packets with corresponding ARP request only sent by itself. For ARP request packets from other devices, it responds with ARP response packets only rather than learning ARP address mapping entry. In this way, network load is heavier but some network attacks based on ARP request packets can be prevented.

## 5.3.2 Preparing for configurations

### Scenario

The mapping of IP address and MAC address is saved in the ARP address mapping table.

Generally, ARP address mapping table is dynamically maintained by the ISCOM2600G-HI series switch. The ISCOM2600G-HI series switch searches for the mapping between IP address and MAC address automatically according to ARP. You just need to configure the ISCOM2600G-HI series switch manually for preventing ARP dynamic learning from cheating and adding static ARP address entries.

### Prerequisite

N/A

## 5.3.3 Default configurations of ARP

Default configurations of ARP are as below.

Function	Default value
Static ARP entry	N/A
Dynamic ARP entry learning mode	learn-all

### 5.3.4 Configuring static ARP entries



#### Caution

- The IP address in static ARP entry must belong to the IP network segment of Layer 3 interface on the switch.
- The static ARP entry needs to be added and deleted manually.

Configure static ARP entries for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#arp ip-address mac-address</b>	Configure static ARP entry.

### 5.3.5 Configuring dynamic ARP entries

Configure dynamic ARP entries for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#arp mode { learn-all   learn-reply-only }</b>	Configure the aging time of dynamic ARP entries.
3	<b>Raisecom(config)#arp aging-time time</b>	Configure the aging time of dynamic ARP entries.
4	<b>Raisecom(config)#arp max-learning-num number</b>	(Optional) configure the maximum number of dynamic ARP entries allowed to learn on the Layer 3 interface.
5	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical layer interface configuration mode.

### 5.3.1 Configuring proxy ARP

Configure proxy ARP for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlan vlan-id</b>	Enter VLAN interface configuration mode.
3	<b>Raisecom(config-vlan1)#arp local-proxy enable</b>	Enable local proxy ARP.

## 5.3.2 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# <b>show arp</b> [ <i>ip-address</i>   <b>interface</b> <i>interface-type</i> <i>interface-number</i>   <b>static</b> ]	Show information about entries in the ARP address table.
2	Raisecom# <b>show arp local-proxy</b> [ <b>interface</b> <i>vlan</i> <i>vlan-id</i> ]	Show information about local proxy ARP.

## 5.3.3 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
Raisecom(config)# <b>clear arp</b>	Clear all entries in the ARP address table.

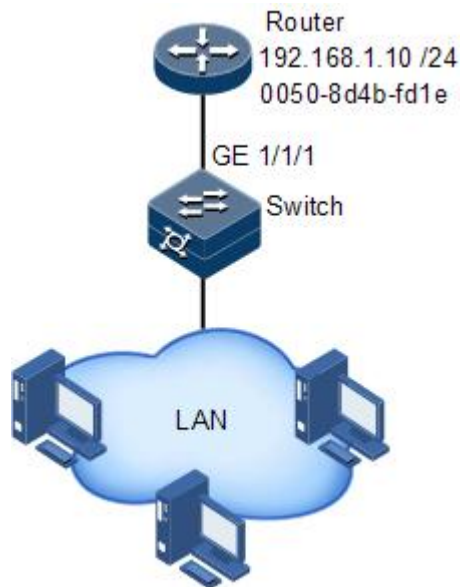
## 5.3.4 Example for configuring ARP

### Networking requirements

As shown in Figure 5-2, the ISCOM2600G-HI series switch is connected to the host, and is also connected to the upstream Router through GE 1/1/1. For the Router, the IP address and submask are 192.168.1.10/24, and the MAC address is 0050-8d4b-fd1e.

To improve communication security between the Switch and Router, you need to configure related static ARP entry on the ISCOM2600G-HI series switch.

Figure 5-2 Configuring 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 configurations of the ARP address table.

```
Raisecom#show arp
ARP aging-time: 1200 seconds(default: 1200s)
ARP mode: Learn all
ARP table:
Total: 1    Static: 1    Dynamic: 0
Age(s)  status
-----
192.168.1.10  0050.8D4B.FD1E  vlan10          static  --  PERMANENT
```

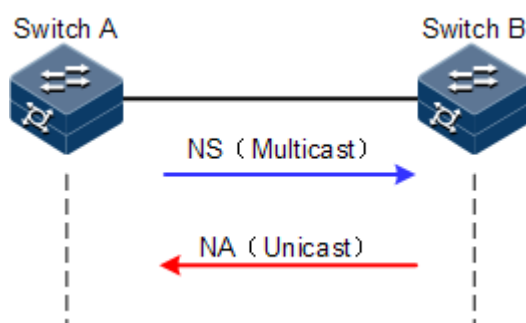
## 5.4 NDP

### 5.4.1 Introduction

Neighbor Discovery Protocol (NDP) is a neighbor discovery mechanism used on IPv6 devices in the same link. It is used to discover neighbors, obtain MAC addresses of neighbors, and maintain neighbor information.

NDP obtains data link layer addresses of neighbor devices in the same link, namely, MAC address, through the Neighbor Solicitation (NS) message and Neighbor Advertisement (NA) message.

Figure 5-3 Principles of NDP address resolution



As shown in Figure 5-3, take Switch A for example. Switch A obtains the data link layer address of Switch B as below:

- Step 1 Switch A sends a NS message in multicast mode. The source address of the NS message is the IPv6 address of Layer 3 interface on Switch A, and the destination address of the NS message is the multicast address of the requested node of the Switch B. The NS message even contains the data link layer address of Switch A.
- Step 2 After receiving the NS message, Switch B judges whether the destination address of the NS message is the multicast address of the request node corresponding to the IPv6 address of Switch B. If yes, Switch B can obtain the data link layer address of Switch A, and sends a NA message which contains its data link layer address in unicast mode.
- Step 3 After receiving the NA message from Switch B, Switch A obtains the data link layer address of Switch B.

By sending ICMPv6 message, IPv6 NDP even has the following functions:

- Verify whether the neighbor is reachable.
- Detect duplicated addresses.
- Discover routers or prefix.
- Automatically configure addresses.
- Support redirection.

### 5.4.2 Preparing for configurations

#### Scenario

IPv6 NDP not only implements IPv4 ARP, ICMP redirection, and ICMP device discovery, but also supports detecting whether the neighbor is reachable.



## Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.
- Configure the IPv6 address of the Layer 3 interface.

### 5.4.3 Default configurations of NDP

Default configurations of NDP are as below.

Function	Default value
Times of sending NS messages for detecting duplicated addresses	1
Maximum number of NDPs allowed to learn	512

### 5.4.4 Configuring static neighbor entries

To resolute the IPv6 address of a neighbor into the data link layer address, you can use the NS message and NA message, or manually configure static neighbor entries.

Configure static neighbor entries for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ipv6 neighbor</b> <i>ipv6-address mac-address</i>	configure static neighbor entries

### 5.4.5 Configuring times of sending NS messages for detecting duplicated addresses

Configure times of sending NS messages for detecting duplicated addresses for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config-vlan1)#ipv6</b> <b>nd dad attempts</b> <i>value</i>	Configure times of sending NS messages for detecting duplicated addresses.



#### Note

When the ISCOM2600G-HI series switch obtains an IPv6 address, it uses the duplicated address detection function to determine whether the IPv6 address is already used by another device. After sending NS messages for a specified times and receiving no response, it determines that the IPv6 address is not duplicated and thus can be used.

## 5.4.6 Configuring maximum number of NDPs allowed to be learnt on Layer 3 interface

Configure the maximum number of NDPs allowed to be learnt on the Layer 3 interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ipv6 neighbors max-learning-num number</b>	Configure the maximum number of NDPs allowed to be learnt on the Layer 3 interface.

## 5.4.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show ipv6 neighbors</b>	Show all NDP neighbor information.
2	<b>Raisecom#show ipv6 neighbors ipv6-address</b>	Show neighbor information about a specified IPv6 address.
3	<b>Raisecom#show ipv6 neighbors vlan vlan-id</b>	Show neighbor information about a specified layer 3 interface.
4	<b>Raisecom#show ipv6 neighbors static</b>	Show information about IPv6 static neighbor.
5	<b>Raisecom#show ipv6 interface nd [ ip if- number ]</b>	Show ND information configured on the interface.

## 5.4.8 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
<b>Raisecom(config)#clear ipv6 neighbors</b>	Clear information about all IPv6 neighbors.

## 5.5 Static route

### 5.5.1 Introduction

A route is required for communication among different devices in one VLAN, or different VLANs. The route is used to transmit packets through network to destination, which adopts routing table for forwarding packets.

#### Default route

The default route is a special route that can be used only when there is no matched item in the routing table. The default route appears as a route to network 0.0.0.0 (with mask 0.0.0.0) in the routing table. You can show configurations of the default route by using the **show ip route** command. If the ISCOM2600G-HI series switch has not been configured with default route and the destination IP of the packet is not in the routing table, the ISCOM2600G-HI series switch will discard the packet and return an ICMP packet to the Tx end to inform that the destination address or network is unavailable.

#### Static route

A static route is the route configured manually, thus bringing low requirements on the system. It is available to simple, small, and stable network. The disadvantage is that it cannot adapt to network topology changes automatically and needs manual intervention.

### 5.5.2 Preparing for configurations

#### Scenario

Configure the static route for simple network topology manually to establish an intercommunication network.

#### Prerequisite

Configure the IP address of the VLAN interface correctly.

### 5.5.3 Configuring static route

Configure the static route for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>ip route ip-address mask-address next-hop</b> [ <i>interface-type interface-num</i> ] [ <b>distance distance</b> ] [ <b>description text</b> ] [ <b>tag tag</b> ] [ <b>track bfd-session session-id</b> ]	Configure the IPv4 static route. The device supports BFD. When the interface is Down, BFD becomes Down and the static route is deleted. When the interface is Up, BFD becomes Up and the static route is added to the routing table.

Step	Command	Description
	<b>Raisecom(config)#ipv6 route</b> <i>ipv6-address/prefix-length</i> <i>ipv6-address</i> [ <b>distance</b> <i>distance</i> ] [ <b>description text</b> ]	Configure the IPv6 static route.
3	<b>Raisecom(config)#ip route</b> <b>static distance</b> <i>distance</i>	(Optional) configure the default administrative distance of the IPv4 static route.
	<b>Raisecom(config)#ipv6 route</b> <b>static distance</b> <i>distance</i>	(Optional) configure the default administrative distance of the IPv6 static route.

## 5.5.4 Configuring route mangement

Configure route management for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router id</b> <i>router-id</i>	Configure the router ID. By default, it is 192.168.1.1.
3	<b>Raisecom(config)#route</b> <b>recursive-lookup tunnel</b> [ <b>ip-prefix</b> <i>listname</i> ]	Configure non-labeled public network routes to be recursive to a LSP tunnel.

## 5.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	<b>Raisecom#show router id</b>	Show information about IPv4 routes.
2	<b>Raisecom#show ip route protocol</b> { <b>static</b>   <b>connected</b>   <b>bgp</b>   <b>ospf</b>   <b>isis</b>   <b>rip</b> } [ <b>detail</b> ]	Show information about the routing table.
	<b>Raisecom#show ipv6 route</b> [ <b>protocol</b> { <b>static</b>   <b>connected</b>   <b>bgp</b>   <b>ospf</b>   <b>isis</b>   <b>rip</b> } ] [ <b>detail</b> ]	
3	<b>Raisecom#show ip route</b> <i>ip-address1</i> [ <i>mask-address1</i> ] <i>ip-address2</i> [ <i>mask-</i> <i>address2</i> ] [ <b>detail</b> ]	Show information about routes between two IP addresses.
4	<b>Raisecom#show { ip   ipv6 } route</b> <b>summary</b>	Show route statistics.
5	<b>Raisecom#show ip route</b> <i>ip-address</i> [ <i>mask-address</i> ] [ <b>longer-prefixes</b> ]	Show information about a

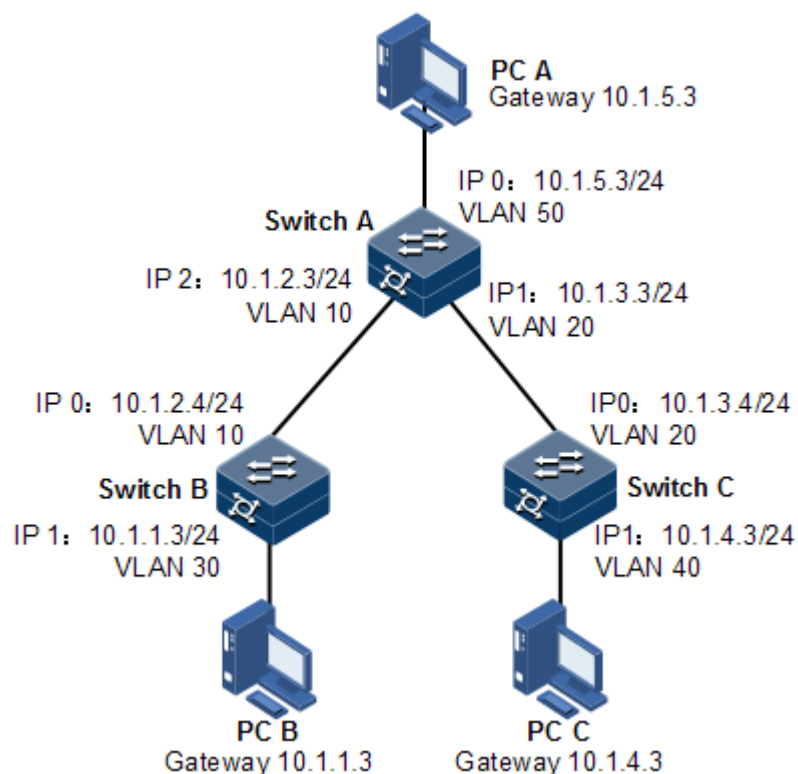
No.	Item	Description
	Raisecom# <b>show ipv6 route</b> { <i>ipv6-address</i>   <i>ipv6-address/prefix-length</i> }	route to a destination.
6	Raisecom# <b>show ip fib</b> [ <i>ip-address</i>   <b>nexthop</b> <i>ip-address</i> ]	Show information about FIB entries.
	Raisecom# <b>show ipv6 fib</b> [ <i>ipv6-address</i>   <b>nexthop</b> <i>ipv6-address</i> ]	
7	Raisecom# <b>show ip fib summary</b>	Show statistics in the routing table.
	Raisecom# <b>show ipv6 fib summary</b>	

## 5.5.6 Example for configuring static route

### Networking requirements

Configure the static route to enable any two hosts or ISCOM2600G-HI series switch devices successfully to ping through each other, as shown in Figure 5-4.

Figure 5-4 Configuring static route



### Configuration steps

- Step 1 Configure the IP address of each device. Detailed configurations are omitted.
- Step 2 Configure the static route on Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.4
SwitchA(config)#ip route 10.1.4.0 255.255.255.0 10.1.3.4
```

Step 3 Configure the default gateway on Switch B.

```
Raisecom#name SwitchB
SwitchB#config
SwitchB(config)#ip route 0.0.0.0 0.0.0.0 10.1.2.3
```

Step 4 Configure the default gateway on Switch C.

```
Raisecom#name SwitchC
SwitchC#config
SwitchC(config)#ip route 0.0.0.0 0.0.0.0 10.1.3.3
```

Step 5 Configure the default gateway of host A to 10.1.5.3. Detailed configurations are omitted.

Configure the default gateway of host B to 10.1.1.3. Detailed configurations are omitted.

Configure the default gateway of host C to 10.1.4.3. Detailed configurations are omitted.

## Checking results

Use the **ping** command to check whether any two of all devices can ping through each other.

```
SwitchA#ping 10.1.1.3
Type CTRL+C to abort
Sending 5, 8-byte ICMP Echos to 10.1.1.3, timeout is 3 seconds:
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms

---- PING Statistics----
5 packets transmitted, 5 packets received,
Success rate is 100 percent(5/5),
round-trip (ms) min/avg/max = 0/0/0.
```

## 5.6 RIP

### 5.6.1 Introduction

Routing Information Protocol (RIP) is a simple Interior Gateway Protocol (IGP) based on distance-vector algorithm.

#### Definition of distance

RIP defines the distance as below:

- The distance from a route to its directly connected network is 1.
- The distance from a route to its indirectly connected network increases by 1 every time when the distance covers a router.

The distance is also called hops. RIP allows a path to cover up to 15 routers, so the distance of 16 indicates an unreachable network.

If two routes with unequal rate or bandwidth to the same destination are present but hops are the same, RIP regards them as the same distance.

#### Working principles

- Step 1 RIP starts initialization. When RIP starts initialization, it sends a request packet on every participant interface. The request packet is used to request a complete routing table from all RIP routers. It is broadcasted in a LAN or sent to the next hop in a point-to-point link. As a special request, it requests complete route update from neighboring devices.
- Step 2 Receive the request. RIP has two types of messages: the response message and receiving message. Each route entry in the request packet will be processed to establish matrix and path for routes. RIP uses hops as matrix; in other words, the value 1 indicates a directly connected network while the value 16 indicates an unreachable network. The router sends back the entire routing table as the response message.
- Step 3 Receive the message and respond. The router receives and processes the response message by adding, deleting, or modifying routing entries in the routing table.
- Step 4 Update common routes and configure timers. By default, the router sends the entire routing table as a response message to neighboring routers. When it receives a new route or updated route, it will start a timer of 180s. If it receives no update message within 180s, it will configure hops to 16. It then advertises the route with the matrix of 16 and deletes the route after the Flush timer expires. The Flush timer is usually 240s, 60s longer than the expiration timer. The device also supports the suppression timer which is 180s and starts after it receive a route with a higher matrix. During the suppression time, the router will not update the routing table according to its new received route. In this case, it provides an extra time for network convergence.
- Step 5 Trigger route update. When the matrix of a route changes, the routers sends related routes rather than the entire routing table.

#### Features

The router running RIP exchanges information with neighboring routers only. If two routers communicate without passing another router, they are neighbors to each other. As defined by RIP, non-neighboring routers do not exchange information.

The information to be exchanged by the router is all information that it knows, namely, its routing table.

Routers exchange routing information periodically (every 30s by default) and update their routing tables according to received routing information (or according to triggering conditions).

- The largest advantage is easy implementation and small overhead.
- RIP has the following disadvantages:
  - The maximum available distance is 15 (the value 16 indicates an unreachable distance), so RIP restricts the network scale.
  - The information to be exchanged by routers is the entire routing table. When the network scale grows, the overhead will increase.
  - "The bad news is transmitted slowly", so the convergence time for the update process is too long.

Based on previous advantages and disadvantages, RIP is applicable to small-scale networks.

## Version

There are three RIP versions: RIPv1, RIPv2, and RIPng. RIPv1 and RIPv2 are applicable to the IPv4 network while RIPng is applicable to the IPv6 network. The ISCOM2600G-HI series switch supports RIPv1 and RIPv2.

RIPv1	RIPv2
Classful routing protocol	Classless routing protocol
The packet does not contain the subnet mask, so devices on the network must use the same subnet mask. Otherwise, errors will occur.	Support VLSM. The update message carries the subnet mask.
RIPv1 uses broadcast packets for update. The broadcast address is 255.255.255.255.	RIPv2 uses multicast packets for update. The multicast address is 224.0.0.9.
Support automatic route aggregation rather than manual route aggregation.	Support both automatic route aggregation and manual route aggregation. You can manually disable automatic route aggregation.
RIPv1 does not support inter-router authentication.	Support authenticating protocol packets in plaintext or MD5 authentication mode, thus enhancing security.
RIPv1 does not support tagging routes.	Support tagging routes for filtering and making policies.

## Anti-loop mechanism

RIP supports the following anti-loop mechanisms:

- Maximum number of hops: a maximum number of hops is defined (15). When it is 16, it indicates an unreachable destination.



- Split horizon: a route learned from one interface is not broadcasted to the interface.
- Route poisoning: when the topology changes, the router marks an invalid route as possibly down status and assign an unreachable matrix for it.
- Poison reverse: when the router learned from one interface is sent back to the interface, it will be poisoned; in other words, its number of hops is configured to 16, which indicates an unreachable destination.
- Triggered update: when route crash is detected, the router immediately broadcasts route update packets rather than wait for the next update period.
- Suppression timer: it prevents the routing table from changing frequently and thus enhances network reliability.

## 5.6.2 Configuring basic RIP functions

Configure basic RIP functions for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router rip</b>	Enable RIP, and enter RIP configuration mode.
3	<b>Raisecom(config-rip)#network <i>ip-address</i></b>	Configure a directly-connected and effective network based on RIP.
4	<b>Raisecom(config-rip)#offset-list <i>access-list-name</i> { in   out } <i>offset-value</i> [ <i>interface-type interface-number</i> ]</b>	Configure the additional metrics when the interface receives or sends RIP routes. By default, it is 0.
5	<b>Raisecom(config-rip)#passive-interface { <i>interface-type interface-number</i>   default }</b>	(Optional) configure the interface to be a passive interface. By default, it is a non-passive interface.

## 5.6.3 Configuring RIP version

Configure the RIP version for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router rip</b>	Enable RIP, and enter RIP configuration mode.

Step	Command	Description
3	<code>Raisecom(config-rip)#<b>version</b> <i>version-id</i></code>	Configure global RIP version ID. By default, global RIP version is not configured. In this case, interfaces which are configured with RIP but not configured with the RIP version in the Tx direction will send V1 packets. Interfaces which are enabled with RIP but not configured with the RIP version in the Rx direction will receive packets of any version.
4	<code>Raisecom(config-rip)#<b>exit</b></code> <code>Raisecom(config)#<b>interface</b> <i>interface-type interface-number</i></code>	Enter interface configuration mode.
5	<code>Raisecom(config-vlan1)#<b>ip rip receive version</b> { 1   2 }*</code>	Configure the receiving RIP version. By default, the receiving RIP version is subjected to the global RIP version.
6	<code>Raisecom(config-vlan1)#<b>ip rip send version</b> { 1   2 } *</code>	Configure the sending RIP version. By default, the sending RIP version is subjected to the global RIP version.
7	<code>Raisecom(config-vlan1)#<b>ip rip v2-broadcast</b></code>	Configure the interface which runs RIPv2 to send broadcast updates. By default, it sends multicast updates.



## Note

You can configure RIP version globally and on the interface of the iTN8800. If the interface is configured with RIP version, then this RIP version prevails.

## 5.6.4 Redistributing external routes

Redistribute external routes for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#<b>config</b></code>	Enter global configuration mode.
2	<code>Raisecom(config)#<b>router rip</b></code>	Enable RIP, and enter RIP configuration mode.
3	<code>Raisecom(config-rip)#<b>host-route</b></code>	Enable the function of receiving host routes. By default, it is enabled.
4	<code>Raisecom(config-rip)#<b>default-information originate</b></code>	Enable broadcasting the default route. By default, it is disabled.

Step	Command	Description
5	<code>Raisecom(config-rip)#redistribute { static   connected   isis   bgp   ospf } [ metric metric ] [ route-map map-name ] [ tag tag-value ]</code>	Configure the policy for redistributing RIP routes.
6	<code>Raisecom(config-rip)#default-metric metric</code>	Configure the default metrics of redistributing external routes. By default, it is 1.
7	<code>Raisecom(config-rip)#auto-summary</code>	Enable automatic aggregation (support RIPv2 only). By default, it is enabled.
8	<code>Raisecom(config-rip)#validate-update-source</code>	Enable the function of checking the source IP address of received RIP packets. By default, it is enabled.

## 5.6.5 Configuring RIP timer

Configure the RIP timer for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router rip</code>	Enable RIP, and enter RIP configuration mode.
3	<code>Raisecom(config-rip)#timers basic update-time invalid-time holddown-time flush-time</code>	Configure the RIP timer. By default, the update interval is 30s. The invalid interval is 180s. The suppression interval is 120s. The refreshing interval is 120s.

## 5.6.6 Configuring loop suppression

Configure loop suppression for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.

Step	Command	Description
3	<b>Raisecom(config-vlan1)#ip rip split-horizon</b>	Enable split horizon on the interface; in other words, the route learned from one interface will not be advertised back to the interface again. By default, it is enabled.
4	<b>Raisecom(config-vlan1)#ip rip poisoned-reverse</b>	Enable poison reverse on the interface, that is, the route learned from one interface can be advertised to other interfaces through this interface. However, the metrics of those routes is configured to 16, namely, unreachable. By default, it is disabled.



### Note

If poison reverse and split horizon are enabled together, split horizon will be invalid.

## 5.6.7 Configuring authentication

Configure authentication for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter interface configuration mode.
3	<b>Raisecom(config-vlan1)#ip rip authentication mode</b> <b>{ text   md5 }</b>	Configure the packet authentication mode on the interface. By default, the authentication mode of RIPv2 packets on the interface is no authentication.
4	<b>Raisecom(config- vlan1)#ip rip authentication string</b> <i>password-string</i>	Configure the interface-associated password.
5	<b>Raisecom(config- vlan1)#ip rip authentication key-chain</b> <i>key-chain-name</i>	Configure the interface-associated authentication secret string.

## 5.6.8 Configuring routing policy

Configure the routing policy for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	Raisecom(config)# <b>router rip</b>	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)# <b>distribute-list</b> { <b>ip-access-list</b> <i>acl-number</i>   <b>prefix-list</b> <i>list-name</i>   <b>route-map</b> <i>rmap-name</i> } <b>in</b> [ <i>interface-type interface-number</i> ]	Configure RIP ingress routing policy.
4	Raisecom(config-rip)# <b>distribute-list</b> { <b>ip-access-list</b> <i>acl-number</i>   <b>prefix-list</b> <i>list-name</i>   <b>route-map</b> <i>rmap-name</i> } <b>out</b> [ <i>interface-type interface-number</i> ]	Configure RIP egress routing policy.
5	Raisecom(config-rip)# <b>distribute-list gateway</b> <i>list-name</i> <b>in</b> [ <i>interface-type interface-number</i> ]	Execute routing policies on the source address of the received packets through RIP.

## 5.6.9 Configuring route calculation

Configure route calculation for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>router rip</b>	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)# <b>distance</b> <i>administrative-distance</i> [ <i>ip-address wild-card-mask</i> ]	Configure the administrative distance of RIP, namely, the protocol priority. The shorter the administrative distance is, the higher the priority will be. By default, the administrative distance is 120.
4	Raisecom(config-rip)# <b>maximum load-balancing</b> <i>number</i>	Configure the maximum number of IP equal-cost multi-path load balancing paths.

## 5.6.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# <b>show ip rip</b>	Show basic information about RIP.
2	Raisecom# <b>show ip rip database</b>	Show information about RIP routing database.
3	Raisecom# <b>show ip rip interface</b>	Show configurations and status of the interface which runs RIP.

## 5.6.11 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
Rasiecom#clear rip database	Clear information about RIP routing database.
Rasiecom#clear rip statistics	Clear RIP interface statistics.

## 5.7 OSPFv2

### 5.7.1 Introduction

Open Shortest Path First (OSPF) is a dynamic route selection protocol based on link status. OSPF referred to in this document is OSPFv2 used for IPv4.

RIP has disadvantages of slow convergence, route loop, and weak expansibility, so it is unfit for large networks. Compared with RIP, OSPF has the following advantages:

- Wide application range: support networks of various sizes, especially large networks.
- Fast convergence: after network topology changes, OSPF immediately sends an update packet, and synchronizes the change in the Autonomous System (AS, the system composed of routing devices running the same routing protocol for exchanging information).
- No routing loop: according to collected link status, OSPF uses the shortest path tree algorithm to calculate routes, which guarantees no routing loop.
- Area division: OSPF divides the network into different areas for layering management, and routing information transmitted across areas is further abstracted, thus reducing occupied network bandwidth.
- Equivalent route: OSPF supports multiple equivalent routes to the same destination address.
- Multicast: OSPF supports sending protocol packets with a multicast address in links of certain types, thus reducing impact on other devices.
- Dynamic learning and advertising of public network routes
- BFD for OSPF

### Network type of OSPF

By types of data link layer protocols, OSPF divides the network into the following types:

- Broadcast: when the data link layer protocol is Ethernet or FDDI, OSPF takes network type as broadcast by default. In such networks, OSPF sends protocol packets in multicast mode (multicast address: 224.0.0.5 and 224.0.0.6).
- Point-to-MultiPoint (P2MP): no data link layer protocol is taken as P2MP by default; instead, this type is forcibly changed from other types. A common method is to change NBMA to P2MP. In such networks, OSPF sends protocol packets in multicast mode (multicast address: 224.0.0.5) by default. You can configure OSPF to send packets in unicast mode as needed.

- Point-to-Point (P2P): when the data link layer protocol is PPP or High-Level Data Link Control (HDLC), OSPF takes network type as P2P by default. In such networks, OSPF sends protocol packets in multicast mode (multicast address: 224.0.0.5).

## Router ID

To run OSPF, a router must have a router ID which is a 32-bit symbol-free integer. The router ID can uniquely identify a router in an AS.



### Note

The router ID can be elected by the system or manually configured. The election rules are as below:

- If there are loopback interfaces configured with IP address, choose the maximum IP address of loopback interface as the router ID.
- If there are loopback interfaces without IP addresses, choose the maximum IP address of IP interface as the router ID.
- If the IP address is used by other OSPF process, it cannot be used by this OSPF process.
- If no IP address is configured, the route ID cannot be elected, the process cannot be created; you have to manually configure the router ID.

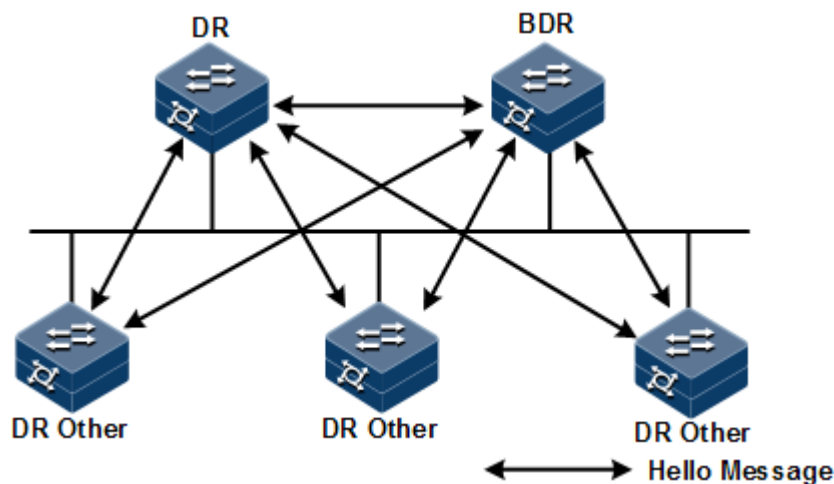
## DR/BDR

In a broadcast network, any two routers need to exchange routing information. Thus route change on a router causes multiple transmissions, which wastes bandwidth resources. To solve this problem, OSPF defines the Designated Router (DR), which receives information from all routers and then advertises link status.

When the DR fails due to a fault, OSPF use a Backup Designated Router (BDR) to avoid incorrect calculation of routes in DR re-election time. Thus a BDR is elected while the corresponding DR is elected. The BDR establishes adjacency relation with all routers in the network segment and exchanges route information with them. When the DR fails, the BDR immediately becomes the DR. Then, a new BDR is elected, but this does not impact route calculation.

On a network running OSPF, a router not DR nor BDR is called DR Other. A DR Other establishes adjacency relation with DR and BDR only rather than another DR Other, as shown Figure 5-5. It reduces the number of relations between routers in the broadcast network and NBMA network, reduces network traffic, and saves bandwidth resource.

Figure 5-5 Roles of broadcast interface



### Note

- Only broadcast interfaces elect the DR. P2MP or P2P interfaces do not elect the DR.
- DR is a concept of a network segment and targeted for an interface on a router. A router may be a DR for an interface and a BDR or DR Other for another interface.
- The DR and BDR are elected by all routers in the same network segment through Hello packets according to router priority and router ID. Devices with a priority above 0 can be candidates for election. If priorities of two routers are the same, the router with the larger router ID is preferential. Devices with priority of 0 cannot be elected as the DR or BDR.
- Router priority affects DR/BDR election. When election ends, a router with higher priority may become effective for election. In this case, it does not replace the elected DR/BDR, and has to wait for next DR/BDR election.

## OSPF packets

OSPF packets are divided into the following types:

- Hello packet: sent periodically, used to discover and maintain OSPF neighbor relations. It carries timer values, DR, BDR, priority, and known neighbor information.
- Database Description (DD) packet: used to synchronize database between two routers. It describes abstract of each Link State Advertisement (LSA) in local LSDB, namely, LSA packet header.
- Link State Request (LSR) packet: used to request required LSA from the peer. After exchanging DD packet, two routers learn the lack LSA for local LSDB compared to the peer LSDB, and then send LSR packet to the peer to request required LSA. The content is LSA abstract.
- Link State Update (LSU) packet: used to send LSA required by the peer. The content is a set of multiple LSAs.
- Link State Acknowledgment (LSAck) packet: used to acknowledge received LSA. The content is the header of the LSA to be acknowledged. An LSAck packet can acknowledge multiple LSAs.



## LSA type

OSPF describes link status, encrypts the information in LSA, and advertises LSA. There are 5 types of common LSAs:

- Router LSA (Type1): generated by each router, used to describe link status and cost, and speeded in the originating area.
- Network LSA (Type2), generated by the DR, used to describe link status of all routers in this segment, advertised in the originating area.
- Network Summary LSA (Type3), generated by the Area Border Router (ABR), used to describes routes of a network segment in the area and notify other areas.
- ASBR Summary LSA (Type4), generated by the ABR, used to describe routes to Autonomous System Boundary Router (ASBR) and notify related areas.
- AS External LSA (Type5), generated by the ASBR, used to describe routers out of AS and notify all areas except Stub area.

## Neighbor and adjacency

After being started, an OSPF router sends Hello packets out through the OSPF interface. After receiving Hello packet, a device checks parameters (interval for sending Hello packets, invalidation time, and area mask information) defined in the Hello packet. If it has the same parameters, it forms a neighbor relation with the OSPF router.

A neighbor is not necessarily in an Adjacency relation, and it depends on the network type. Only when the two devices exchange DD packets and LSAs, and synchronize to the peer LSDB can they become in adjacency relation.

The ISCOM2600G-HI series switch supports up to 32 neighbors.

## Calculating OSPF routes

OSPF calculates routes as below:

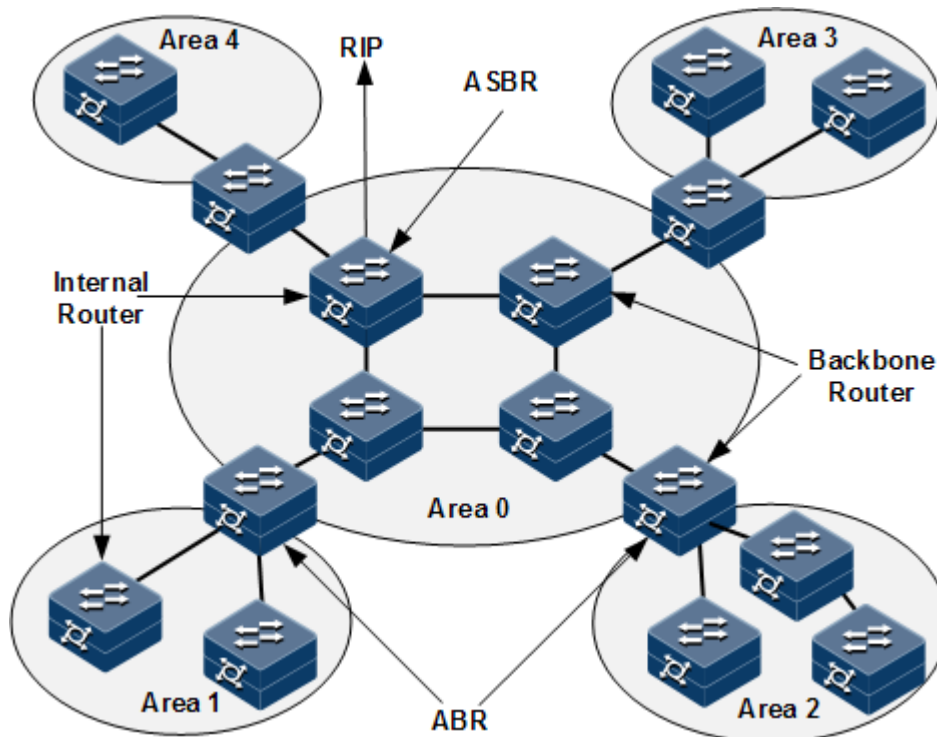
- Step 1 Each OSPF router generates LSAs according to network topology, and sends LSAs to other OSPF routers through updating packets.
- Step 2 Each OSPF router collects LSAs from other OSPF routers. All LSAs form LSDB. LSA describes network topology around the router. LSDB describes network topology of the entire AS.
- Step 3 Each OSPF route transfers LSDB to a weighted diagram, which reflects topology of the entire network. Each OSPF router obtains the same weighted diagram.
- Step 4 Each router uses the Shortest Path First (SPF) algorithm based on the weighted diagram, and then calculates a shortest path tree with itself as root. This tree provides routes to all nodes in the AS.

## Area division

When routers on a large network run OSPF, increment of routers leads to a huge LSDB which occupies much storage space and causes the CPU to work in heavy burden. When the network grows larger, topology changes more frequently, the network is always in oscillation status, a large number of OSPF packets are transmitted, network bandwidth is wasted, and each change causes recalculation of routes for all routers.

OSPF divides an AS into different areas to solve the previous problem. An area logically contains some routers and is identified by the area ID. As shown in Figure 5-5, a route in an area maintains routing information of the area instead of the entire AS.

Figure 5-6 OSPF area and router type



The border of each area is a router instead of a link. A router may belong to different areas, but a network segment (link) must belong to only one area, or an interface running OSPF must belong to a specific area. After the network is divided into different areas, aggregate routes on border routers to reduce the number of LSAs advertised to other areas and minimize impact from changes of network topology.

## Router types

As shown in Figure 5-6, OSPF routers can be divided into four types according to location in the AS:

- Internal router: all interfaces of an interval router belong to only one OSPF area.
- Area Border Router (ABR): this router may belong to two or more areas which must contain a backbone area. The ABR can connect a backbone area and a non-backbone area. It can be physically or logically connected to a backbone area.
- Backbone router: at least one interface of this router belongs to the backbone area, so all ABRs and internal routers in Area 0 are backbone routers.
- Autonomous System Border Router (ASBR): the router exchanges information with other AS is called the ASBR. The ASBR is not necessarily located at the border of an AS, and may be an internal router or ABR. When an OSPF router imports external routes, it becomes the ASBR.

## Backbone area

After OSPF divides areas, not all areas are equal. A special area with area ID as 0 is called the backbone area. The backbone area transmits inter-area routes. Routing information from non-backbone area must be forwarded by the backbone area. The backbone area has the following information:

- All non-backbone areas must be interconnected with the backbone area.
- The backbone area must be internally interconnected.

## Stub area

The border router has low performance, so its routing table must be limited. Configuring the Stub area is used to prevent external LSAs from entering the area to the minimum extend.

In the Stub area, only Type1, Type2, and Type3 LSAs are advertised, and Type5 LSAs are not allowed to enter, which reduces the size of the routing table and the number of transmitted routes. In addition, you can configure the area to Totally Stub area which allows Type1 and Type2 LSAs and a default Type3 LSA. This further reduces the size and the number. In the Totally Stub area, the ABR does not transmit inter-area routes and external routes to the area.

Not each area complies with the (Totally) Stub area. Generally, the (Totally) Stub area is at the border of an AS. To make routes from other areas to the AS or external routes of the AS reachable, the ABR generates a default route, and advertises it to non-ABR routers in the area.

## Route types

OSPF divides routes into four types by priority in descending order: Intra Area route, Inter Area route, Type1 External route, and Type2 External route.

The Intra Area route and Inter Area route describe network topology of the AS. External routes describe how to choose the route to a destination address out of the AS. Whether to calculate interval path cost of AS makes OSPF divide external routes into Type1 External route or Type2 External route.

- Cost of Type1 External route = cost from the local router to the corresponding ASBR + cost from the ASBR to the destination address of the route
- Cost of Type2 External route = cost from the ASBR to the destination address of the route

OSPF takes Type 1 External route with high credibility, so it chooses Type1 External route when Type 1 External route and Type2 External route for the same destination address co-exist regardless of the costs of these two routes.

## 5.7.2 Configuring basic functions of OSPF

Configure basic functions of OSPF for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router ospf process-id [ router-id router-id ]</b>	Start OSPF process, and enter OSPF configuration mode.

Step	Command	Description
3	<code>Raisecom(config-router-ospf)#network ip-address wild-card-mask area area-id</code>	Configure the network segment included by the OSPF area.



## Note

- If you manually configure the *router-id* by configuring optional parameters in the **router ospf process-id [ router-id router-id ]** command, the OSPF process will use the *router-id* by precedence. Otherwise, the process will automatically elect a *router-id*.
- If the process has configured or elected the *router-id*, and you modify the *router-id*, the modification will take effect after restart.

## 5.7.3 Configuring OSPF route attributes

### Configuring interface cost

Configure the interface cost for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter Layer 3 interface configuration mode.
3	<code>Raisecom(config-gigabitethernet1/1/port)#ip ospf cost cost</code>	Configure the route cost of the IP interface. By default, it is not configured.

### Configuring reference bandwidth

Configure the OSPF reference bandwidth for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ospf process-id [ router-id router-id ]</code>	Start an OSPF process, and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#reference-bandwidth bandwidth</code>	Configure the reference bandwidth of the link. By default, it is 110 Mbit/s.



## Note

- After the routing cost is manually configured through the **ip ospf cost** command, the manually-configured routing cost takes effect.
- If the routing cost is not configured manually but the link bandwidth reference value is configured, the routing cost is automatically configured based on link bandwidth reference value. The formula is: cost = link bandwidth reference value (bit/s) / link bandwidth. If the cost value is greater than 65535, it is configured to 65535. If no link bandwidth reference value is configured, it is configured to 100 Mbit/s by default.

## Configuring OSPF administrative distance

Configure the OSPF administrative distance for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router ospf process-id [ router-id router-id ]</b>	Enable an OSPF process and enter OSPF configuration mode.
3	<b>Raisecom(config-router-ospf)#distance administrative-distance</b>	Configure the OSPF administrative distance. By default, it is 110.
4	<b>Raisecom(config-router-ospf)#distance ospf { intra-area   inter-area   external } distance</b>	Configure the administrative distance of OSPF specified route. By default, it is 0. However, it takes 110 provided by RM as the standard.

## Configuring OSPF to be compatible with RFC1583

Configure OSPF to be compatible with RFC1583 for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router ospf process-id [ router-id router-id ]</b>	Enable an OSPF process, and enter OSPF configuration mode.
3	<b>Raisecom(config-router-ospf)#compatible rfc1583</b>	Configure OSPF to be compatible with RFC1583. By default, OSPF is compatible with RFC1583.

## 5.7.4 Configuring load balancing

Configure load balancing for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router ospf process-id [ router-id router-id ]</b>	Enable an OSPF process, and enter OSPF configuration mode.
3	<b>Raisecom(config-router-ospf)#maximum load-balancing number</b>	Configure the maximum number of paths for IP equivalent multi-path load balancing.

## 5.7.5 Configuring OSPF network

### Configuring OSPF network type

Configure the OSPF network type for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/port)#ip ospf network { broadcast   non-broadcast   ptmp   ptp }</b>	Configuring the network type of the Layer 3 interface. By default, it is the broadcast network.

### Configuring DR election priority

Configure the DR election priority for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/port)#ip ospf priority priority</b>	Configure the DR election priority on the IP interface. By default, it is 1.

## Configuring OSPF NBMA network neighbor

Configure the OSPF NBMA network neighbor for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaetherent1/1/port)#ip ospf</b> <b>network non-broadcast</b> <b>Raisecom(config-</b> <b>gigaetherent1/1/port)#exit</b>	Configure the Layer 3 interface network mode to NBMA and exit Layer 3 interface configuration mode.
4	<b>Raisecom(config)#router ospf</b> <i>process-id [ router-id router-id ]</i>	Enable an OSPF process and enter OSPF configuration mode.
5	<b>Raisecom(config-router-</b> <b>ospf)#neighbor ip-address</b> <b>[ priority priority ]</b>	Configure the NBMA neighbor and its priority.  By default, no NBMA neighbor is configured and the priority is 0 when you configure the NBMA neighbor.



### Caution

Priorities configured by the **neighbour** and **ip ospf priority priority** commands are different:

- The priority configured by the **neighbor** command indicates that whether the neighbor has the right to vote. If you configure the priority to 0 when configuring the neighbor, the local router judges that the neighbor has no right to vote and will not sent Hello packets to the neighbor. This method helps reduce the number of Hello packets transmitted through the network during DR and BDR election processes. However, if the local router is a DR or BDR, it will send the Hello packet to the neighbor, whose priority is configured to 0, to establish the neighboring relationship.
- The priority configured by the **ip ospf priority priority** command is used for actual DR election.

## 5.7.6 Optimizing OSPF network

### Configuring OSPF packet timer

Configure the OSPF packet timer for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/port)#ip ospf dead-interval seconds</code>	Configure the OSPF neighbor dead interval. By default, it is 4 times of Hello packet delivery interval. If no Hello packet delivery interval is configured, it is 40s for P2P and Broadcast interfaces and 120s for P2MP and NBMA interfaces by default.
4	<code>Raisecom(config- gigaethernet1/1/port)#ip ospf hello-interval seconds</code>	Configure the ODPF Hello packet delivery interval. By default, it is 10s for P2P and Broadcast interfaces and 30s for P2MP and NBMA interfaces
5	<code>Raisecom(config- gigaethernet1/1/port)#ip ospf poll-interval seconds</code>	Configure the OSPF Poll timer interval. By default, it is 120s.
6	<code>Raisecom(config- gigaethernet1/1/port)#ip ospf retransmit-interval seconds</code>	Configure the LAS retransmission interval on the IP interface. By default, it is 5s.
7	<code>Raisecom(config- gigaethernet1/1/port)#ip ospf transmit-delay seconds</code>	Configure the LSA retransmission delay on the IP interface. By default, it is 1s.

## Caution

- When the dead-interval is not manually configured, the dead-interval and poll-interval are changed to 4 times of the hello-interval after the hello-interval is configured.
- When the dead-interval is manually configured, no effect is brought to the dead-interval and poll-interval after hello-interval is configured. No matter whether you configure the poll interval or not, the poll-interval changes with the dead-interval. Therefore, we recommend configuring these 3 values in the following order: hello-interval, dead-interval, and poll-interval.

## Configuring SPF calculation interval

When the OSPF Link State Database (LSDB) changes, it needs to re-calculate the shortest path. If the network changes frequently and it needs to calculate the shortest path immediately, it will occupy a great amount of system resources and affect efficiency of the router. By adjusting the SPF calculation interval, you can prevent some effects brought by frequent network changes.

Configure the SPF calculation interval for the ISCOM2600G-HI series switch as below.



Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router ospf process-id [ router-id router-id ]</b>	Enable an OSPF process and enter OSPF configuration mode.
3	<b>Raisecom(config-router-ospf)#timers spf delay-time hold-time</b>	Configure the calculation delay and interval of the OSPF route.  By default, the calculation delay is 2s and the calculation interval is 3s.

## Configuring OSPF passive interface

To prevent some OSPF routing information from being obtained by some routers on the network, you can configure the interface to an OSPF passive interface to disable the interface to send OSPF packets.

Configure the OSPF passive interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/port)#ip ospf passive-interface enable</b>	Enable passive interface on the OSPF interface.  By default, it is disabled.

## Configuring MTU ignorance

By default, the value of MTU domain in the DD packet is the MTU value of the interface, which sends the DD packet. Default MTU values may vary on devices. In addition, if the MTU value of the DD packet is greater than the one of the interface, the DD packet will be discarded. To ensure receiving the DD packet properly, enable MTU ignorance to configure the MTU value to 0. Therefore, all devices can receive the DD packet.

Configure MTU ignorance for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/port)#ip ospf mtu-ignore enable</b>	Enable MTU ignorance on the IP interface.  By default, MTU ignorance is disabled on the IP interface to check MTU of the OSPF Hello packet.

## 5.7.7 Configuring OSPF authentication mode

### Configuring OSPF area authentication mode

All routers in an area need to be configured with the identical area authentication mode (non-authentication, simple authentication, or MD5 authentication). The OSPF area has no authentication password but adopts the interface authentication password. If no interface authentication password is configured, the empty password will be used for authentication.

Configure the OSPF area authentication mode for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router ospf</b> <i>process-id [ router-id router-id ]</i>	Enable an OSPF process and enter OSPF configuration mode.
3	<b>Raisecom(config-router-ospf)#area area-id</b> <b>authentication { md5   simple }</b>	Configure the area authentication mode. By default, it is non-authentication.

### Configuring OSPF interface authentication mode

Packet authentication prioritizes selecting the interface authentication mode. If the interface authentication mode is configured to non-authentication mode, the area authentication mode will be selected. OSPF interfaces cannot establish the neighbor relationship unless the authentication mode and authentication password are identical.

Configure the OSPF interface authentication mode for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#ip ospf</b> <b>authentication { md5   simple }</b>	Configure the authentication mode of the IP interface. By default, it is non-authentication. It means adopting the area authentication mode.
4	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#ip ospf</b> <b>authentication-key { simple [ 0  </b> <b>7 ] password   md5 { [ key-id [ 0</b> <b>  7 ] password ]   keychain</b> <b>keychain-name } }</b>	Configure the authentication password of the IP interface.

## 5.7.8 Configuring Stub area

For the non-backbone area at the edge of Autonomous System (AS), you can configure the **stub** command on all routers in the area to configure the area to a Stub area. In this case, Type5 LSA, which is used to describe external routes of the AS, cannot be flooded in the Stub area. This facilitates reducing the routing table size.

Configure the Stub area for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router ospf process-id</b> [ <b>router-id router-id</b> ]	Enable an OSPF process and enter OSPF configuration mode.
3	<b>Raisecom(config-router-ospf)#area area-id stub</b> [ <b>no-summary</b> ]	Configure the area to a Stub area. The <b>no-summary</b> parameter is used to disable the ABR to send Summary LSA to the Stub area. It means that it is a Totally Stub area and the ABR is available for the Stub only. By default, no area is the Stub area.
4	<b>Raisecom(config-router-ospf)#area area-id default-cost cost</b>	Configure the default route cost of the Stub area. This command is available for the ABR in the Stub area only. By default, it is 1.
5	<b>Raisecom(config-router-ospf)#area area-id nssa</b> [ <b>no-summary</b> ]	(Optional) configure the area to NSSA.



### Caution

- All routers in the Stub area must be configured with the Stub property through the **area area-id stub** command.
- To configure an area to a Totally Stub area, all routers in the area must be configured by the **area area-id stub** command. In addition, all ABRs in the area must be configured by the **area area-id stub no-summary** command.
- The backbone area cannot be configured to the Stub area.
- ASBR should not be in the Stub area. It means that routers besides the AS cannot be transmitted in the Stub area.

## 5.7.9 Controlling OSPF routing information

### Configuring OSPF redistributed routes

Configure OSPF redistributed routes for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router ospf process-id</b> [ <b>router-id router-id</b> ]	Enable an OSPF process and enter OSPF configuration mode.
3	<b>Raisecom(config-router-ospf)#redistribute</b> { <b>static</b>   <b>connected</b>   <b>isis</b>   <b>bgp</b> } [ <b>metric metric</b> ] [ <b>metric-type { 1   2 }</b> ] [ <b>tag tag-value</b> ] [ <b>route-map map-name</b> ] <b>Raisecom(config-router-ospf)#redistribute ospf</b> [ <b>process-id</b> ] [ <b>metric metric</b> ] [ <b>metric-type { 1   2 }</b> ] [ <b>tag tag-value</b> ] [ <b>route-map map-name</b> ]	Configure OSPF route redistribution polity. By default, no external route is redistributed. When an external route is redistributed: <ul style="list-style-type: none"> <li>• When the directly-connected and static route is redistributed, the metric is 1 by default. When other routes are redistributed, take the original metric of the external route as the metric of the LSA.</li> <li>• If no Metric-type is specified, the Metric-type is Type2 by default.</li> <li>• If no Tag is specified, take the original Tag of the external route as the Tag of the LSA.</li> </ul>
4	<b>Raisecom(config-router-ospf)#redistribute limit limit-number</b>	Configure the threshold of redistributed OSPF external routes. By default, no threshold is configured.

## Configuring inter-area route aggregation

If there are sequent network segments in the area, you can configure route aggregation on the ABR to aggregate these network segments to a network segment. When sending routing information, the ABR generates Type3 LSA in units of network segment.

Configure inter-area route aggregation for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router ospf process-id</b> [ <b>router-id router-id</b> ]	Enable an OSPF process and enter OSPF configuration mode.
3	<b>Raisecom(config-router-ospf)#area area-id range ip-address ip-mask</b> [ <b>not-advertise</b> ]	Configure the inter-area route aggregation. By default, no inter-area route aggregation is configured. When you configure the aggregated route, the cost is the maximum Metric of the LSA by default. In addition, the aggregated route is redistributed.

## Configuring redistributed external route aggregation

After the external route is redistributed, configure route aggregation on the ASBR. The ISCOM2600G-HI series switch just puts the aggregated route on the ASE LSA. This helps reduce the number of LSAs in the LSDB.

Configure inter-area route aggregation for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router ospf process-id</b> [ <b>router-id router-id</b> ]	Enable an OSPF process and enter OSPF configuration mode.
3	<b>Raisecom(config-router-ospf)#summary-address ip-address ip-mask</b> [ <b>not-advertise</b> ] [ <b>metric metric</b> ]	Aggregate external routes. By default, external routes are not aggregated. When external aggregates are aggregated, the Metric is the maximum Metric of the LSA by default.

## Configuring default route redistribution

Configure default route redistribution for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#router ospf process-id</b> [ <b>router-id router-id</b> ]	Enable an OSPF process and enter OSPF configuration mode.
3	<b>Raisecom(config-router-ospf)#default-information originate</b> [ <b>always</b> ] [ <b>metric metric</b> ] [ <b>type { 1   2 }</b> ]	Redistribute the default route. By default, no default route is generated. When the default LSA is generated, if the <b>always</b> key word is specified, the default Metric is 1. If the <b>always</b> key word is not specified, the Metric is 10.

## 5.7.10 Configuring OSPF routing policy

### Configuring OSPF receiving policy

Configure the OSPF receiving policy for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<code>Raisecom(config)#ip prefix-list list-name { permit   deny } ip-address mask-length [ ge ge-length ] [ le le-length ]</code>	Configure the IP prefix list.
3	<code>Raisecom(config)#access-list acl-number</code>	Create an IP ACL, and enter ACL configuration mode. When the acl-number is between 1000 and 1999, this operation enters basic IP ACL configuration mode.
	<code>Raisecom(config-ipv4-std)#rule [ rule-id ] { deny   permit } { source-ip-address source-ip-mask   any }</code>	Configure basic IP ACL rules.
4	<code>Raisecom(config)#router ospf process-id [ router-id router-id ]</code>	Enable an OSPF process, and enter OSPF configuration mode.
5	<code>Raisecom(config-router-ospf)#distribute-list { ip-access-list acl-number   prefix-list list-name } in</code>	Configure the OSPF filtering policy for receiving the OSPF inter-area routes, intra-area routes, and AS external routes.



## Note

- Before configuring OSPF receiving policy, ensure that the IP ACL used by the OSPF receiving policy has been created.
- When the ISCOM2600G-HI series switch performs filtering based on IP ACL, all routes, which match with the ACL, can pass if the ACL mode is configured to permit. Others are filtered.
- You cannot modify the IP ACL unless it is not used by any routing policy.
- Different from IP ACL, the IP prefix-list can be modified even if it is being used.
- If the configured IP prefix list does not exist, the ISCOM2600G-HI series switch does not filter received routes.

## Configuring OSPF advertising policy

Configure the OSPF advertising policy for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip prefix-list list-name { permit   deny } ip-address mask-length [ ge ge-length ] [ le le-length ]</code>	Configure the IP prefix-list. You can use the <b>no ip prefix-list list-name [ index number ]</b> command to delete the configuration.

Step	Command	Description
3	Raisecom(config)# <b>access-list</b> <i>acl-number</i>	Configure the IP ACL rule.  At present, the ISCOM2600G-HI series switch just supports matching the address prefix information of the route by specifying the destination IP address and subnet mask.
	Raisecom(config-ipv4-basic)# <b>rule</b> [ <i>rule-id</i> ] { <b>deny</b>   <b>permit</b> } { <i>source-ip-address</i> <i>source-ip-mask</i>   <b>any</b> }	Configure basic IP ACL rules.
4	Raisecom(config)# <b>router ospf</b> <i>process-id</i> [ <b>router-id</b> <i>router-id</i> ]	Enable an OSPF process and enter OSPF configuration mode.
5	Raisecom(config-router-ospf)# <b>distribute-list</b> { <b>ip-access-list</b> <i>acl-number</i>   <b>prefix-list</b> <i>list-name</i> } <b>out</b>	Configure the filtering policy that the OSPF releases 5 types of LSAs to the AS.
6	Raisecom(config-router-ospf)# <b>distribute-list</b> { <b>ip-access-list</b> <i>acl-number</i>   <b>prefix-list</b> <i>list-name</i> } <b>out</b> [ <b>static</b>   <b>connected</b>   <b>isis</b>   <b>bgp</b> ]	Configure the OSPF advertising policy.
	Raisecom(config-router-ospf)# <b>distribute-list</b> { <b>ip-access-list</b> <i>acl-number</i>   <b>prefix-list</b> <i>list-name</i> } <b>out ospf</b> <i>process-id</i>	



## Note

- Before configuring OSPF global distributing policy, ensure that the IP ACL used by the OSPF global distributing policy has been created.
- You cannot modify the IP ACL unless it is not used by any routing policy.
- Different from IP ACL, the IP prefix-list can be modified even it is being used.
- After global advertising policy is configured, routes cannot be redistributed to the local LSDB unless it passes the global advertising policy. After protocol advertising policy is configured, the route can be redistributed through the protocol advertising policy.
- After protocol advertising policy is configured, the redistributed protocol route can be redistributed to the local LSDB through the protocol advertising policy. If global advertising policy is also configured, the route must be redistributed through the global advertising policy.

## Configuring Type3 LSA filtering policy

Configure the Type3 LSA filtering policy for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>ip prefix-list</b> <i>list-name { permit   deny } ip-</i> <i>address mask-length [ ge ge-</i> <i>length ] [ le le-length ]</i>	Configure the IP prefix-list. You can use the <b>no ip prefix-list</b> <i>list-name [ index number ]</i> command to delete the configuration.
3	Raisecom(config)# <b>router ospf</b> <i>process-id [ router-id router-id ]</i>	Enable an OSPF process and enter OSPF configuration mode.
4	Raisecom(config-router-ospf)# <b>area</b> <i>area-id filter prefix-list list-</i> <i>name { in   out }</i>	Configure Type3 LSA filtering policy in the area.



## Note

If the configured filtering policy does not exist, it is believed that the command fails to configure the filtering policy and no filtering operation is performed on received routes.

## 5.7.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# <b>show ip ospf</b> [ <i>process-id</i> ]	Show OSPF basic information.
2	Raisecom# <b>show ip ospf</b> [ <i>process-id</i> ] <b>interface</b> [ <i>interface-type interface-</i> <i>number</i> ]	Show OSPF interface information.
3	Raisecom# <b>show ip ospf</b> [ <i>process-id</i> ] <b>neighbor</b> [ <i>interface-type interface-</i> <i>number</i> ] [ <i>neighbor-id</i> ]	Show OSPF neighbor information.
4	Raisecom# <b>show ip ospf</b> [ <i>process-id</i> ] <b>route</b>	Show OSPF routing information.
5	Raisecom# <b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <i>max-age</i>   <i>self-originate</i> ] Raisecom# <b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <i>router</i>   <i>network</i>   <i>summary</i>   <i>asbr-summary</i>   <i>external</i> ] [ <i>linkstate-</i> <i>id</i> ] [ <i>adv-router ip-address</i>   <i>self-</i> <i>originate</i> ] Raisecom# <b>show ip ospf</b> [ <i>process-id</i> ] <b>database statistics</b>	Show OSPF link status database information and statistics.
6	Raisecom# <b>show ip ospf</b> [ <i>process-id</i> ] <b>border-routers</b>	Show information about routers at edges of the area and AS.



No.	Command	Description
7	Raisecom# <b>show ip ospf</b> [ <i>process-id</i> ] <b>neighbor statistics</b>	Show OSPF statistics or OSPF neighbor statistics.
8	Raisecom# <b>show ip ospf</b> [ <i>process-id</i> ] <b>summay-address</b>	Show OSPF ASBR external route aggregation information.

## 5.7.12 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
Raisecom# <b>clear ip ospf</b> [ <i>process-id</i> ] <b>process</b> [ <i>graceful</i> ]	Restart the OSPF process.

# 6 DHCP

---

This chapter describes basic principles and configurations procedures of DHCP, and providing related configuration examples, including the following sections:

- DHCP Client
- Zero-configuration
- DHCP Snooping
- DHCP Options
- DHCP Server
- DHCP Relay

## 6.1 DHCP Client

### 6.1.1 Introduction

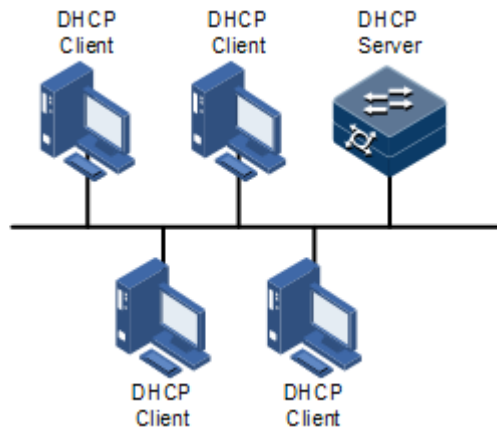
Dynamic Host Configuration Protocol (DHCP) refers to the protocol which assigns configurations, such as the IP address, to users on the TCP/IP network. Based on BOOTP (Bootstrap Protocol) protocol, it has additional features, such as automatically assigning available network addresses, reusing network addresses, and other extended configuration features.

With the enlargement of network scale and development of network complexity, the number of PCs on a network usually exceeds the maximum number of distributable IP addresses. Meanwhile, the widely use of laptops and wireless networks lead to frequent changes of locations and also related IP addresses must be updated frequently. As a result, network configurations become more and more complex. DHCP is developed to solve these problems.

DHCP adopts client/server communication mode. A client applies for configurations to the server (including the IP address, subnet mask, and default gateway), and the server replies with IP address to the client and other related configurations to implement dynamic configurations.

Typical applications of DHCP usually include a set of DHCP server and multiple clients (such as the PC or laptop), as shown in Figure 6-1.

Figure 6-1 DHCP typical networking



DHCP ensures rational allocation, avoid waste, and improve the utilization rate of IP addresses on the entire network.

Figure 6-2 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 6-2 Structure of DHCP packet

0	7	15	23	31
OP	Hardware type	Hardware length	Hops	
Transaction ID				
Seconds		Flags		
Client IP address				
Your(client) IP address				
Server IP address				
Relay agent IP address				
Client hardware address				
Server host name				
File				
Options				

Table 6-1 describes fields of DHCP packets.

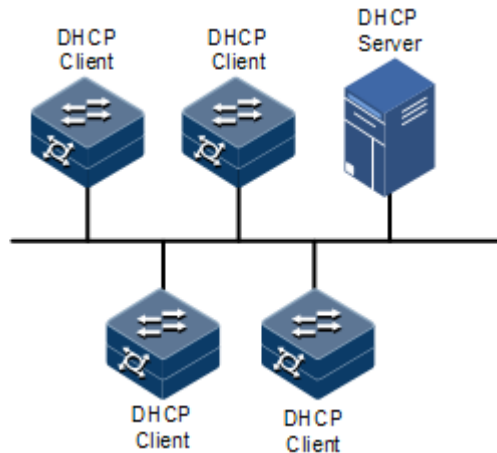
Table 6-1 Fields of a DHCP packet

Field	Length	Description
OP	1	Packet type <ul style="list-style-type: none"> <li>• 1: a request packet</li> <li>• 2: a reply packet</li> </ul>
Hardware type	1	Hardware address type of a DHCP client
Hardware length	1	Hardware address size of a DHCP client
Hops	1	Number of DHCP hops passed by a DHCP packet This field increases by 1 every time the DHCP request packet passes a DHCP hop.

Field	Length	Description
Transaction ID	4	The client chooses a number at random when starting a request, used to mark process of address request.
Seconds	2	Passing time for the DHCP client after starting DHCP request. It is unused now, fixed as 0.
Flags	2	Bit 1 is the broadcast reply flag, used to mark whether the DHCP server replies packets in unicast or broadcast mode. <ul style="list-style-type: none"> <li>• 0: unicast</li> <li>• 1: broadcast</li> </ul> Other bits are reserved.
Client IP address	4	DHCP client IP address, only filled when the client is in bound, updated or re-bind status, used to reply ARP request.
Your (client) IP address	4	IP address of the client distributed by the DHCP server
Server IP address	4	IP address of the DHCP server
Relay agent IP address	4	IP address of the first DHCP hop after the DHCP client sends request packets.
Client hardware address	16	Hardware address of the DHCP client
Server host name	64	Name of the DHCP server
File	128	Name of the startup configuration file of the DHCP client and path assigned by the DHCP server
Options	Modifiable	A modifiable option field, including packet type, available lease period, IP address of the DNS server, and IP address of the WINS server

The ISCOM2600G-HI series switch can be used as a DHCP client to obtain the IP address from the DHCP server for future management, as shown in Figure 6-3.

Figure 6-3 DHCP Client networking



## 6.1.2 Preparing for configurations

### Scenario

As a DHCP client, the ISCOM2600G-HI series switch obtains the IP address from the DHCP server.

The IP address assigned by the DHCP client is limited with a certain lease period when adopting dynamic assignment of IP addresses. The DHCP server will take back the IP address when it is expired. The DHCP client has to renew the IP address for continuous use. The DHCP client can release the IP address if it does not want to use the IP address before expiration.

We recommend configuring the number of DHCP relay devices smaller than 4 if the DHCP client needs to obtain IP address from the DHCP server through multiple DHCP relay devices.

### Prerequisite

- Create VLANs
- Add the Layer 3 interface to the VLANs.
- DHCP Snooping is disabled.
- FE 1/0/1 supports obtaining the IP address through DHCP or zero-configuration.

## 6.1.3 Default configurations of DHCP Client

Default configurations of DHCP Client are as below.

Function	Default value
hostname	Raisecom
class-id	Raisecom-ROS
client-id	Raisecom-SYSMAC-IF0

## 6.1.4 Configuring DHCP Client

Before a DHCP client applies for an IP address, you must create a VLAN, and add the interface of the IP address to the VLAN. Meanwhile you must configure the DHCP server, otherwise the interface will fail to obtain the IP address through DHCP.


For interface IP 0, the IP addresses obtained through DHCP and configured manually can overwrite each other.



### Note

- By default, the ISCOM2600G-HI series switch is enabled with DHCP Client. Use the **no ip address dhcp** command to disable DHCP Client.
- If the ISCOM2600G-HI series switch obtains the IP address from the DHCP server through DHCP previously, it will restart the application process for IP address if you use the **ip address dhcp** command to modify the IP address of the DHCP server.

Configure DHCP Client for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>interface vlan 1</b>	Enter Layer 3 interface configuration mode.
3	Raisecom(config-vlan)# <b>ip dhcp client { class-id class-id   client-id client-id   hostname hostname }</b>	(Optional) configure DHCP client information, including the type identifier, client identifier, and host name.   <b>Caution</b> After the IP address is obtained by a DHCP client, client information cannot be modified.
4	Raisecom(config-vlan)# <b>ip address dhcp [ server-ip ip-address ]</b>	Configure the DHCP client to obtain IP address through DHCP.
5	Raisecom(config-vlan)# <b>ip dhcp client renew</b>	(Optional) renew the IP address. If the Layer 3 interface of the DHCP client has obtained an IP address through DHCP, the IP address will automatically be renewed when the lease period expires.
6	Raisecom(config-ip)# <b>no ip address dhcp</b>	(Optional) release the IP address.

## 6.1.5 Configuring DHCPv6 Client

Configure the DHCPv6 client for the ISCOM2600 series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlan <i>vlan-id</i></b>	Enter VLAN interface configuration mode.
3	<b>Raisecom(config-vlan1)#ipv6 address dhcp [ server-ip <i>ipv6-address</i> ]</b>	Configure applying for IPv6 address through DHCPv6.  If the ISCOM2600G-HI series switch has obtained an IP address from the DHCP server through DHCPv6 before, it will restart the application process for the IP address if you use the command to modify the IPv6 address of the DHCP server.
4	<b>Raisecom(config-vlan1)#ipv6 dhcp client renew</b>	(Optional) renew the IPv6 address.  If the Layer 3 interface on the ISCOM2600G-HI series switch has obtained an IP address through DHCP, the IPv6 address will automatically be renewed when the lease period expires.
5	<b>Raisecom(config-vlan1)#ipv6 dhcp client rapid-commit</b>	(Optional) enable DHCPv6 Client to apply for rapid interaction.

## 6.1.6 Checking configurations

Use the following commands to check configuration results.

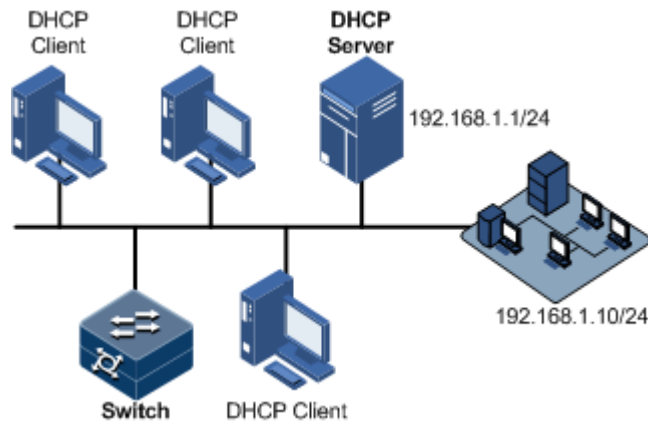
No.	Command	Description
1	<b>Raisecom#show ip dhcp client</b>	Show configurations of DHCP Client.
2	<b>Raisecom#show ipv6 dhcp client</b>	Show configurations of DHCPv6 Client.

## 6.1.7 Example for configuring DHCP Client

### Networking requirements

As shown in Figure 6-4, the Switch is used as a DHCP client, and the host name is raisecom. The Switch is connected to the DHCP server and NMS. The DHCP server should assign IP addresses to the SNMP interface on the Switch and make NMS manage the Switch.

Figure 6-4 DHCP Client networking



## Configuration steps

Step 1 Configure the DHCP client.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip dhcp client hostname raisecom
```

Step 2 Configure applying for IP address through DHCP.

```
Raisecom(config-vlan1)#ip address dhcp server-ip 192.168.1.1
```

## Checking results

Use the **show ip dhcp client** command to show configurations of DHCP Client.

```
Raisecom#show ip dhcp client
DHCP Client Mode:           Normal Mode
Interface :                 vlan1
Hostname:                   Raisecom
Class-ID:                   Raisecom-ROS_5.2.1
Client-ID:                  Raisecom-000e5e112233-IF0
DHCP Client Is Requesting For A Lease.
Assigned IP Addr:           0.0.0.0
Subnet Mask:                0.0.0.0
Default Gateway:            --
Client Lease Starts:        Jan-01-1970 08:00:00
Client Lease Ends:          Jan-01-1970 08:00:00
Client Lease Duration:      0(sec)
DHCP Server:                0.0.0.0
TFTP Server Name:           --
TFTP Server IP Addr:        --
```



```
Bootfile Filename:      --
NTP Server IP Addr:     --
Root Path:              --

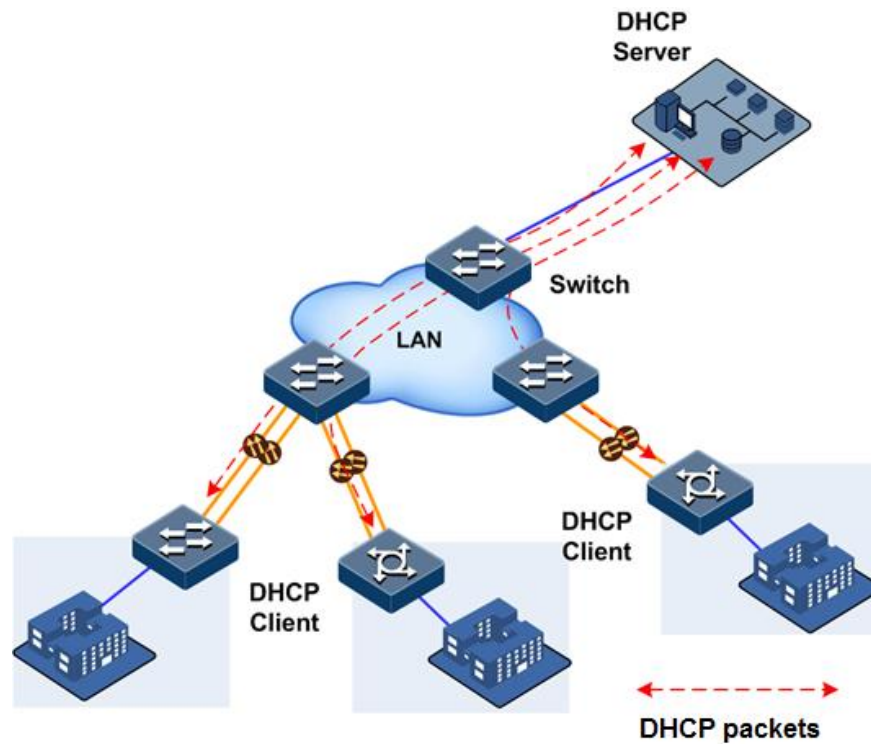
DHCP Client Mode:       Normal Mode
Interface :             vlan10
Hostname:               Raisecom
Class-ID:               Raisecom-ROS_5.2.1
Client-ID:              Raisecom-000e5e112233-IF0
DHCP Client Is Disabled.
Assigned IP Addr:       0.0.0.0
Subnet Mask:            0.0.0.0
Default Gateway:        --
Client Lease Starts:    Jan-01-1970 08:00:00
Client Lease Ends:      Jan-01-1970 08:00:00
Client Lease Duration:  0(sec)
DHCP Server:            0.0.0.0
TFTP Server Name:       --
TFTP Server IP Addr:    --
Bootfile Filename:      --
NTP Server IP Addr:     --
Root Path:              --
```

## 6.2 Zero-configuration

### 6.2.1 Introduction

Zero-configuration refers to that the device needs no manual configurations; it automatically sends DHCP packets for applying for an IP address to the zero-configuration server, and automatically downloads the configurations file from the zero-configuration server to update its configurations after obtaining the IP address from the zero-configuration server. Figure 6-5 shows zero-configuration server networking.

Figure 6-5 Zero-configuration server networking



### Caution

By default, zero-configuration is enabled on the device. To disable it, configure the device to common client mode.

## 6.2.2 Default configurations of zero-configuration

Default configurations of zero-configuration are as below.

Function	Default value
Zero-configuration polling period	2h
Zero-configuration mode	Enable

## 6.2.3 Preparing for configuration

### Scenario

To enable the remote device to automatically apply for the IP address after being powered on, configure zero-configuration. To configure zero-configuration parameters, see the following section.


### Prerequisite

- Connect the device to the DHCP server correctly. Configure the DHCP server correctly.

- Configure the interface connected to the zero-configuration server to be Up.
- Configure the upstream switch to allow packets of a VLAN of the remote device to pass.
- Out-of-band interface FE 1/0/1 supports obtaining the IP address through DHCP or zero-configuration.

## 6.2.4 Configuring DHCP Client

Configure DHCP Client for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip dhcp client mode { zeroconfig   normal }</b> <b>Raisecom(config)#ipv6 dhcp client mode { zeroconfig   normal }</b>	Configure the DHCP client to work in zero-configuration mode or common client mode. By default, it works in zero-configuration mode.   <b>Caution</b> To disable zero-configuration, use the command to configure the DHCP client to common client mode.
3	<b>Raisecom(config)#ip dhcp client { class-id class-id   client-id client-id   hostname host-name }</b>	(Optional) configure information about the DHCP client, including the host name, class ID, and client ID. Packets carry them when being sent by a client.

## 6.2.5 (Optional) configuring zero-configuration polling

Configure zero-configuration polling for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip dhcp client zeroconfig polling period hour</b> <b>Raisecom(config)#ipv6 dhcp client zeroconfig polling period hour</b>	Configure the zero-configuration polling period, in units of hour, ranging from 1 to 24. By default, it is 2h.

## 6.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show ipv6 dhcp client</b> <b>Raisecom#show ip dhcp client</b>	Show configurations and information automatically obtained by the DHCP client.

## 6.2.7 Example for IPv6 zero-configuration

### Networking requirements

As shown in Figure 6-6, the DHCP Server program is installed on a virtual machine and bridged with the Network Interface Card (NIC) of the PC on which the TFTP Server program is installed. Switch A is connected upstream to the TFTP server through GE 1/1/2 and downstream to GE 1/1/1 on Switch B through its GE 1/1/1. Switch B is started without any configurations. It can obtain an IPv6 global unicast address from the DHCP server through zero-configuration when it has no IPv6 address. Then, it automatically downloads the configuration file and system files from the TFTP server in the same network segment and loads them. Table 6-2 lists planned data.

Figure 6-6 Zero-configuration networking

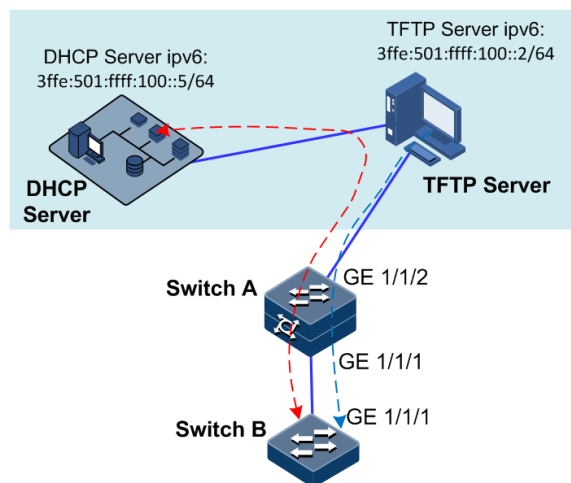


Table 6-2 Planned data

Device	Parameter
DHCP server	<ul style="list-style-type: none"> <li>IPv6 address: 3ffe:501:ffff:100::5/64</li> <li>IPv4 address: 172.16.125.201/24</li> <li>DHCPv6 server pool: 3ffe:501:ffff:100::5/64 to 3ffe:501:ffff:100::102</li> </ul>
TFTP server	<ul style="list-style-type: none"> <li>IPv6 address: 3ffe:501:ffff:100::2/64</li> <li>IPv4 address: 172.16.125.135/24</li> </ul>
Switch A	Interface configurations: <ul style="list-style-type: none"> <li>GE 1/1/2: Access mode, accessing packets of VLAN 10</li> <li>GE 1/1/1: Trunk mode, allowing packets of VLAN 10 to pass</li> </ul>
Switch B	No configurations

### Configuration principles

- Establish a DHCPv6 server, configure the DHCPv6 address pool, and define Option 59 and Option 60.
- Establish a TFTP server. Save the configuration file and system files to be issued to Switch B on the TFTP server.

- Configure Switch A to connect it to the TFTP server.

## Configuration steps

Establish a DHCPv6 server, configure the DHCPv6 address pool, and define Option 59 and Option 60.

- Step 1 Install the virtual machine program. For details, see virtual machine manuals.
- Step 2 Configure the IPv4 address and IPv6 address of the virtual machine to 172.16.125.135/24 and ffe:501:ffff:100::2 respectively.
- Step 3 Install the DHCPv6 Server program on the virtual machine. For details, see its manuals.
- Step 4 Configure the IPv4 address and IPv6 address of the DHCPv6 server.
- Configure the IPv4 address and IPv6 address of the DHCPv6 server to 172.16.125.201/24 and 3ffe:501:ffff:100::5/64 respectively.
  - Configure the NIC of the virtual machine to be bridged with the NIC of the PC.
- Step 5 Configure the DHCPv6 address pool and prefix length. Take a DHCPv6 Server program for example.
- Log in to the DHCPv6 Server console through its management address "https://172.16.125.201".
  - Configure the DHCPv6 address pool to be 3ffe:501:ffff:100::105–3ffe:501:ffff:100::190 and prefix length to 64, as shown in Figure 6-7.
- Step 6 Configure Option 59 and Option 60, as shown in Figure 6-7.
- Configure the format of Option 59: option dhcp6.bootfile-url"3ffe:501:ffff:100::2"
  - Configure the format of Option 60: option dhcp6.bootfile-param"startup-config:zeroconfig\_startup\_config,system-boot:ISCOM2600G-HI\_SYSTEM\_3.11.142\_20170315"

Figure 6-7 Configuring DHCPv6 address pool and prefix

**Subnet details**

Subnet description: Added automatically to match listening network interface

Network address: 3ffe:501:ffff:100:: / 64

Lease time (seconds): Default: Max: Min:

Authoritative for this subnet: ☐ No (default) ☐ Yes ☒ Not set

Unknown client connections: ☐ Allow (default) ☐ Deny ☒ Not set

Subnet location: Top level

Toggle: **Ranges** **Advanced options** **Custom options**

---

**Prefix6**

Low 3ffe:501:ffff:100:: High 3ffe:501:ffff:100:: Bits 64

Low High Bits

**Add new prefix6**

---

**Dynamic ranges**

Low 3ffe:501:ffff:100::105 High 3ffe:501:ffff:100::190

Low High

**Add new range**

---

**Custom options**

Note: The contents of custom options are checked only for syntax errors. Be sure you know what you are doing before editing this data.

```
option dhcp6.bootfile-url "3ffe:501:ffff:100::2";
option dhcp6.bootfile-param "startup-config:zeroconfig_startup_c
```

Use the TFTP program to establish the TFTP server environment which is used to issue the configuration file and system files to be issued to Switch B.

Step 7 On the PC installed with the virtual machine, configure the directory for TFTP Server to read saved files and the IP address of TFTP Server, and enable global IPv6.

- Configure the directory of TFTP Server to bootfile, and save the configuration file and system files in this directory.
- Configure the service address of TFTP Server to the IPv4 address of the NIC on the PC, namely, 172.16.125.135.
- Enable global IPv6 addresses.

Current Directory: E:\bootfile **Browse**

Server interface: 172.16.125.135 **Show Dir**

Tftp Server | Tftp Client | **DHCP server** | Syslog server | DNS server

peer	file	start time	progress

**About** **Settings** **Help**

GLOBAL | TFTP | DHCP | SYSLOG |

Start Services

- ☒ TFTP Server
- ☒ TFTP Client
- ☐ SNTP server
- ☒ Syslog Server
- ☒ DHCP Server
- ☒ DNS Server

☒ Enable IPv6

Configure Switch A.

#### Step 8 Configure switches in standalone mode.

- Configure Switch A.

Configure GE 1/1/1 to Trunk mode, allowing packets of VLAN 10 to pass.

Configure GE 1/1/2 to Access mode, accessing packets of VLAN 10.

```
Raisecom#config
Raisecom(config)#create vlan 10 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk allowed vlan 10
Raisecom(config-gigaethernet1/1/1)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport access vlan 10
```

- Power on Switch B.

After Switch B is powered on, it will automatically obtain the IPv6 address and download files.

## Checking results

After Switch B is powered on, you can see that it automatically obtains the IPv6 address and download the configuration file and system files, as shown in Figure 6-8.

Figure 6-8 Automatically obtaining files through zero-configuration

```
1970-01-01,08:01:06 DHCPC6-5-ACQUIRING_IPV6_ADDR:unit1: Acquiring IP address via DHCPv6.
1970-01-01,08:01:08 DHCPC6-5-ACQUIRING_IPV6_ADDR:unit1: Acquiring IP address via DHCPv6.
1970-01-01,08:01:10 DHCPC6-5-GET_IPADDR_SUCCESSFULLY:unit1: Acquire configuration information successfully.
ISCOM2600G_SYSTEM_3. 7% |** | 1733k 0:06:42 ETA
```

## 6.3 DHCP Snooping

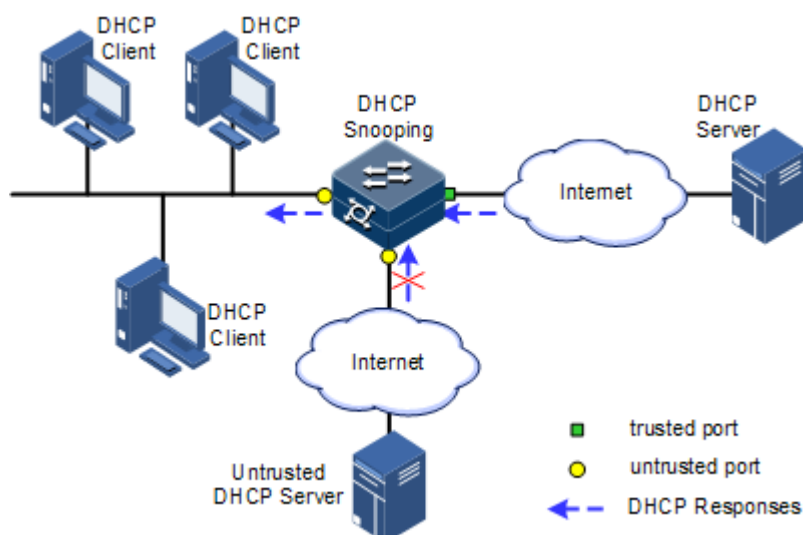
### 6.3.1 Introduction

DHCP Snooping is a security feature of DHCP with the following functions:

- Make the DHCP client obtain the IP address from a legal DHCP server.

If a false DHCP server exists on the network, the DHCP client may obtain incorrect IP address and network configuration parameters, but cannot communicate normally. As shown in Figure 6-9, to make DHCP client obtain the IP address from a legal DHCP server, the DHCP Snooping security system permits you to configure an interface as the trusted interface or untrusted interface: the trusted interface forwards DHCP packets normally; the untrusted interface discards reply packets from the DHCP server.

Figure 6-9 DHCP Snooping



- Record mapping between DHCP client IP address and MAC address.

DHCP Snooping records entries through monitor request and reply packets received by the trusted interface, including client MAC address, obtained IP address, DHCP client connected interface and VLAN of the interface. Then implement following by the record information:

- ARP detection: judge legality of a user that sends ARP packet and avoid ARP attack from illegal users.
- IP Source Guard: filter packets forwarded by interfaces by dynamically getting DHCP Snooping entries to avoid illegal packets to pass the interface.
- VLAN mapping: modify mapped VLAN of packets sent to users to original VLAN by searching IP address, MAC address, and original VLAN information in DHCP Snooping entry corresponding to the mapped VLAN.

The Option field in DHCP packet records position information of DHCP clients. The Administrator can use this Option field to locate DHCP clients and control client security and accounting.

If the ISCOM2600G-HI series switch is configured with DHCP Snooping to support Option function:



- When the ISCOM2600G-HI series switch receives a DHCP request packet, it processes packets according to Option field included or not, filling mode, and processing policy configured by user, then forwards the processed packet to DHCP server.
- When the ISCOM2600G-HI series switch receives a DHCP reply packet, it deletes the Optional field and forwards the rest part of the packet to the DHCP client if the packet contains the Option field, or it forwards the packet directly if the packet does not contain the Option field.

## 6.3.2 Preparing for configurations

### Scenario

DHCP Snooping is a security feature of DHCP, used to make DHCP client obtain its IP address from a legal DHCP server and record mapping between IP address and MAC address of a DHCP client.

The Option field of a DHCP packet records location of a DHCP client. The administrator can locate a DHCP client through the Option field and control client security and accounting. The device configured with DHCP Snooping and Option can perform related process according to Option field status in the packet.

### Prerequisite

N/A

## 6.3.3 Default configurations of DHCP Snooping

Default configurations of DHCP Snooping are as below.

Function	Default value
Global DHCP Snooping status	Disable
Interface DHCP Snooping status	Enable
Interface trusted/untrusted status	Untrust
DHCP Snooping in support of Option 82	Disable

## 6.3.4 Configuring DHCP Snooping

Generally, you must ensure that the ISCOM2600G-HI series switch interface connected to DHCP server is in trusted status while the interface connected to the user is in untrusted status.

If enabled with DHCP Snooping but without the feature of DHCP Snooping supporting DHCP Option, the ISCOM2600G-HI series switch will do nothing to Option fields in packets. For packets without Option fields, the ISCOM2600G-HI series switch does not conduct the insertion operation.

By default, DHCP Snooping is enabled on all interfaces, but only when global DHCP Snooping is enabled can interface DHCP Snooping take effect.

Configure DHCP Snooping for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip dhcp snooping</b>	Enable global DHCP Snooping.
3	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode or aggregation group configuration mode.
4	<b>Raisecom(config-gigaetherne</b> <b>t1/1/port)#ip dhcp</b> <b>snooping</b>	(Optional) enable interface DHCP Snooping. The device supports this configuration on the QinQ interface.
5	<b>Raisecom(config-gigaetherne</b> <b>t1/1/port)#ip dhcp</b> <b>snooping trust</b>	Configure the trusted interface of DHCP Snooping.
6	<b>Raisecom(config-gigaetherne</b> <b>t1/1/port)#ip dhcp</b> <b>snooping binding max</b> <i>number</i>	Configure the maximum number of entries in the DHCP Snooping binding table.
7	<b>Raisecom(config-gigaetherne</b> <b>t1/1/port)#ip dhcp</b> <b>snooping outer</b> <i>vlan-id</i> <b>inner</b> <i>vlan-list</i>	(Optional) enable DHCP Snooping based on interface or double VLAN Tags.
8	<b>Raisecom(config)#ip dhcp snooping</b> <b>option client-id</b>	(Optional) configure DHCP Snooping to support Option 61 field.
9	<b>Raisecom(config)#ip dhcp snooping</b> <b>autosave enable</b>	(Optional) enable auto-saving of the DHCP Snooping binding table.
10	<b>Raisecom(config)#ip dhcp snooping</b> <b>autosave write-interval</b> <i>time</i>	(Optional) configure the interval for automatically saving the DHCP Snooping binding table.

### 6.3.5 Configure DHCP Snooping to support Option 82

Configure DHCP Snooping to support Option 82 for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip dhcp snooping</b> <b>information option</b>	Configure global DHCP Snooping to support Option 82.
3	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config-gigaetherne</b> <b>t1/1/port)#ip dhcp</b> <b>snooping information option</b> <b>vlan-</b> <b>list</b> <i>vlan-list</i>	(Optional) configure the lists of VLANs that support Option 82 through interface DHCP Snooping.

## 6.3.6 Configuring DHCPv6 Snooping

Configure DHCPv6 Snooping for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ipv6 dhcp snooping</b>	Enable global DHCPv6 Snooping.
3	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#ipv6 dhcp</b> <b>snooping</b>	(Optional) enable interface DHCPv6 Snooping.
5	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#ipv6 dhcp</b> <b>snooping trust</b>	Configure the trusted interface of DHCPv6 Snooping.
6	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#ipv6 dhcp</b> <b>snooping vlan</b> <i>vlan-id</i>	Enable IPv6 DHCP Snooping on the specified interface and in the specified VLAN.
7	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#ipv6 dhcp</b> <b>snooping binding max</b> <i>number</i>	Configure the maximum number of entries in the DHCPv6 Snooping binding table.
8	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#exit</b> <b>Raisecom(config)#ipv6 dhcp</b> <b>snooping option</b> <i>number</i>	(Optional) configure DHCPv6 Snooping to support user-defined Options.
9	<b>Raisecom(config)#ipv6 dhcp</b> <b>snooping option interface-id</b>	(Optional) configure DHCP Snooping to support Option 18.

## 6.3.7 Checking configurations

Use the following commands to check configuration results.

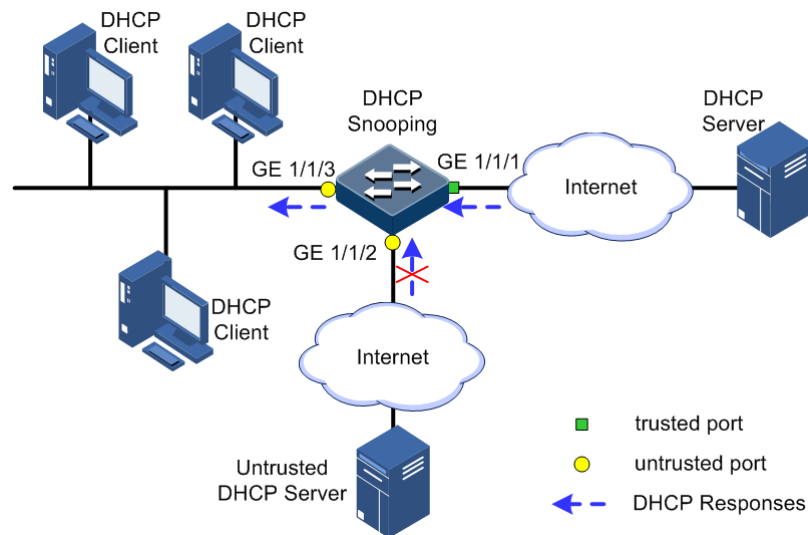
Step	Command	Description
1	<b>Raisecom#show ip dhcp snooping</b>	Show configurations of DHCP Snooping.
2	<b>Raisecom#show ip dhcp snooping binding</b>	Show configurations of the DHCP Snooping binding table.
3	<b>Raisecom#show ipv6 dhcp snooping</b>	Show configurations of DHCPv6 Snooping.
4	<b>Raisecom#show ipv6 dhcp snooping binding</b>	Show configurations of the DHCPv6 Snooping binding table.
5	<b>Raisecom#show ip dhcp snooping autosave</b>	Show auto-saving status of the DHCP Snooping binding table.

## 6.3.8 Example for configuring DHCP Snooping

### Networking requirements

As shown in Figure 6-10, the Switch is used as the DHCP Snooping device. The network requires DHCP clients to obtain the IP address from a legal DHCP server and support Option 82 to facilitate client management. You can configure padding information of about circuit ID sub-option to raisecom on GE 1/1/3, and padding information about remote ID sub-option to user01.

Figure 6-10 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 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#ip dhcp snooping
Raisecom(config-gigabitEthernet1/1/1)#ip dhcp snooping trust
Raisecom(config-gigabitEthernet1/1/1)#quit
```

Step 3 Configure DHCP Relay to support Option 82 field and configure Option 82 field.

```
Raisecom(config)#ip dhcp snooping information option
Raisecom(config)#ip dhcp information option remote-id string user01
```

```
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#ip dhcp information option circuit-id
raisecom
```

## Checking results

Use the **show ip dhcp snooping** command to show configurations of DHCP Snooping.

```
Raisecom#show ip dhcp snooping
DHCP Snooping: Enabled
DHCP Option 82: Enabled
Port          vlan          Enabled Status  Trusted Status
Option82  Vlanlist
-----
gigaethernet1/1/1    --          enabled        yes           1-
4094
gigaethernet1/1/2    --          enabled        no            1-
4094
gigaethernet1/1/3    --          enabled        no            1-
4094
gigaethernet1/1/4    --          enabled        no            1-
4094
gigaethernet1/1/5    --          enabled        no            1-
4094
gigaethernet1/1/6    --          enabled        no            1-
4094
.....
```

## 6.4 DHCP Options

### 6.4.1 Introduction

DHCP transmits control information and network configuration parameters through Option field in packet to dynamically assign addresses to provide abundant network configurations for clients. DHCP has 255 types of options, with the final option as Option 255. Table 6-3 lists frequently used DHCP options.

Table 6-3 Common DHCP options

Options	Description
3	Router option, used to assign the gateway address of DHCP clients
6	DNS server option, used to specify the IP address of the DNS server assigned for DHCP clients

Options	Description
18	IPv6 DHCP client flag option, used to specify interface information about DHCP clients
37	IPv6 DHCP client flag option, used to specify device information about DHCP clients
51	IP address lease option
53	DHCP packet type option, used to mark the type of DHCP packets
55	Request parameter list option, used to indicate network configuration parameters to be obtained from the server, containing values of these parameters
61	DHCP client flag option, used to assign device information for DHCP clients
66	TFTP server name option, used to specify the domain name of the TFTP server assigned for DHCP clients
67	Startup file name option, used to specify the name of the startup file assigned for DHCP clients
82	DHCP client flag option, user-defined, used to mark the position of DHCP clients, including Circuit ID and remote ID
150	TFTP server address option, used to specify the IP address of the TFTP server assigned for DHCP clients
184	DHCP reserved option. At present Option 184 is used to carry information required by voice calling. Through Option 184, the DHCP server can distribute IP addresses for DHCP clients with voice function and meanwhile provide information about voice calling.
255	Complete option

Options 18, 37, 61, and 82 in DHCP Option are relay information options in DHCP packets. When a DHCP client sends request packets to the DHCP server by passing a DHCP Relay or DHCP Snooping device, the DHCP Relay or DHCP Snooping device will add Option fields to the request packets.

Options 18, 37, 61, and 82 implement recording of information about DHCP clients on the DHCP server. By cooperating with other software, it can implement functions, such as limit on IP address distribution and accounting. For example, by cooperating with IP Source Guard, Options 18, 61, 82 can defend deceiving through IP address+MAC address.

Option 82 can include up to 255 sub-options. If the Option 82 field is defined, at least one sub-option must be defined. The ISCOM2600G-HI series switch supports the following two sub-options:

- Sub-Option 1 (Circuit ID): it contains the interface ID, interface VLAN, and additional information about request packets of the DHCP client.
- Sub-Option 2 (Remote ID): it contains interface MAC address (DHCP Relay), or bridge MAC address (DHCP Snooping device) of the ISCOM2600G-HI series switch, or user-defined string in request packets of the DHCP client.

## 6.4.2 Preparing for configurations

### Scenario

Options 18, 37, 61, and 82 in DHCP Option are relay information options in DHCP packets. When request packets from DHCP clients reach the DHCP server, DHCP Relay or DHCP Snooping added Option field into request packets if request packets pass the DHCP relay device or DHCP snooping device is required.

Options 18, 37, 61, and 82 are used to record DHCP client information on the DHCP server. By cooperating with other software, it can implement functions such as limit on IP address distribution and accounting.

### Prerequisite

N/A

## 6.4.3 Default configurations of DHCP Option

Default configurations of DHCP Option are as below.

Function	Default value
attach-string in global configuration mode	N/A
remote-id in global configuration mode	Switch-mac
circuit-id in interface configuration mode	N/A

## 6.4.4 Configuring DHCP Option fields

Configure DHCP Option fields for the ISCOM2600G-HI series switch as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip dhcp information option attach-string <i>attach-string</i></b>	(Optional) configure additional information for Option 82 field.
	<b>Raisecom(config)#interface <i>interface-type interface-number</i></b> <b>Raisecom(config-gigaethernet1/1/port)#ip dhcp information option circuit-id <i>circuit-id</i> [ <i>prefix-mode</i> ]</b>	(Optional) configure circuit ID sub-option information for Option 82 field on the interface.
	<b>Raisecom(config-gigaethernet1/1/port)#ip dhcp option <i>vlan vlan-id description string</i></b> <b>Raisecom(config-gigaethernet1/1/port)#exit</b>	(Optional) configure the interface or VLAN description to be padded into Option 82 fields.

Step	Command	Description
	<b>Raisecom(config)#ip dhcp information option { attach-string   circuit-id format   circuit-id hex } string</b>	(Optional) configure the attached string in Option 82 of DHCP packets.
	<b>Raisecom(config)#ip dhcp information option circuit-id mac-format string</b>	(Optional) configure the format of the MAC address in the variable of Circuit ID in Option 82 of DHCP packets.
	<b>Raisecom(config)#ip dhcp information option remote-id { client-mac   client-mac-string   hostname   string string   switch-mac   switch-mac-string }</b> <b>Raisecom(config)#ip dhcp information option remote-id extend { client-mac   client-mac-string   switch-mac   switch-mac-string }</b>	(Optional) configure remote ID sub-option information for Option 82 field.  DHCP Relay supports the Remote ID of Option 82 to be compatible with the Huawei Default mode.
3	<b>Raisecom(config)#ipv4 dhcp option option-id { ascii ascii-string   hex hex-string   ip-address ip-address }</b>	(Optional) create user-defined Option based on IPv4.
	<b>Raisecom(config)#interface interface-type interface-number</b> <b>Raisecom(config-gigaethernet1/1/port)#ipv4 dhcp option option-id { ascii ascii-string   hex hex-string   ip-address ip-address }</b>	(Optional) create user-defined Option field information on the interface.
4	<b>Raisecom(config-gigaethernet1/1/port)#exit</b> <b>Raisecom(config)#ipv4 dhcp option client-id { ascii ascii-string   hex hex-string   ip-address ip-address }</b>	(Optional) configure Option 61 field information.
	<b>Raisecom(config-gigaethernet1/1/port)#ipv4 dhcp option client-id { ascii ascii-string   hex hex-string   ip-address ip-address }</b>	(Optional) configure Option61 field information on the interface.

## 6.4.5 Configuring DHCP Option 18 over IPv6

Configure DHCP Option 18 over IPv6 for the ISCOM2600G-HI series switch as below.

Option 18 over IPv6 should be configured on the device that is enabled with DHCP Snooping.

All the following steps are optional and in any sequence.

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



Step	Command	Description
2	<b>Raisecom(config)#ipv6 dhcp option interface-id { ascii <i>ascii-string</i>   hex <i>hex-string</i>   ipv6-address <i>ipv6-address</i> }</b>	(Optional) configure information about Option 18.
3	<b>Raisecom(config)#interface <i>interface-type interface-number</i></b> <b>Raisecom(config-gigaethernet1/1/port)#ipv6 dhcp option interface-id { ascii <i>ascii-string</i>   hex <i>hex-string</i>   ipv6-address <i>ipv6-address</i> }</b>	(Optional) configure information about Option 18 on the interface.

## 6.4.6 Configuring DHCP Option 37 over IPv6

Configure DHCP Option 37 over IPv6 for the ISCOM2600G-HI series switch as below.

Option 37 over IPv6 should be configured on the device that is enabled with DHCP Snooping.

All the following steps are optional and in any sequence.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ipv6 dhcp option remote-id { ascii   hex } <i>string</i></b>	(Optional) configure information about Option 37.
3	<b>Raisecom(config)#interface <i>interface-type interface-number</i></b> <b>Raisecom(config-gigaethernet1/1/port)#ipv6 dhcp option remote-id mac-format <i>string</i></b>	(Optional) configure the format of the MAC address of the Remote ID variable in Option 37 in DHCPv6 packets.

## 6.4.7 Configuring user-defined DHCP Option over IPv6

Configure user-defined DHCP Option over IPv6 for the ISCOM2600G-HI series switch as below.

User-defined Option over IPv6 should be configured on the device that is enabled with DHCP Snooping.

All the following steps are optional and in any sequence.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ipv6 dhcp option <i>number</i> { ascii <i>ascii-string</i>   hex <i>hex-string</i>   ipv6-address <i>ipv6-address</i> }</b>	(Optional) create user-defined Option information over IPv6.

Step	Command	Description
3	<pre>Raisecom(config)#<b>interface</b> <i>interface-type</i> <i>interface-number</i> Raisecom(config-gigaethernet1/1/port)#<b>ipv6</b> <b>dhcp option number</b> { <b>ascii</b> <i>ascii-string</i>   <b>hex</b> <i>hex-string</i>   <b>ipv6-address</b> <i>ipv6-address</i> }</pre>	(Optional) create user-defined Option information over IPv6 on the interface.

## 6.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<pre>Raisecom#<b>show ip dhcp</b> <b>information option</b></pre>	Show configurations of DHCP Option fields.
2	<pre>Raisecom#<b>show ip dhcp</b> <b>option port vlan</b> <b>description</b></pre>	Show the interface or VLAN description to be padded into Option 82 fields.

## 6.5 DHCP Server

### 6.5.1 Introduction

Dynamic Host Configuration Protocol (DHCP) refers to assigning IP address configurations dynamically for users on the TCP/IP network. It is based on BOOTP (Bootstrap Protocol) protocol, and automatically adds the specified available network address, network address reuse, and other extended configuration options over BOOTP protocol.

With the enlargement of network scale and development of network complexity, the number of PCs on a network usually exceeds the maximum number of distributable IP addresses. Meanwhile, the widely use of laptops and wireless networks lead to frequent change of PC positions and also related IP addresses must be updated frequently. As a result, network configurations become more and more complex. DHCP is developed to solve these problems.

DHCP adopts client/server communication mode. A client applies configuration to the server (including IP address, subnet mask, and default gateway), and the server replies with an IP address for the client and other related configurations to implement dynamic configurations of IP address.

In DHCP Client/Server communication mode, a specific host is configured to assign IP addresses, and send network configurations to related hosts. The host is called the DHCP server.

### DHCP application

Under normal circumstances, use the DHCP server to assign IP addresses in following situations:

- The network scale is large. It requires much workload for manual configurations, and is difficult to manage the entire network intensively.

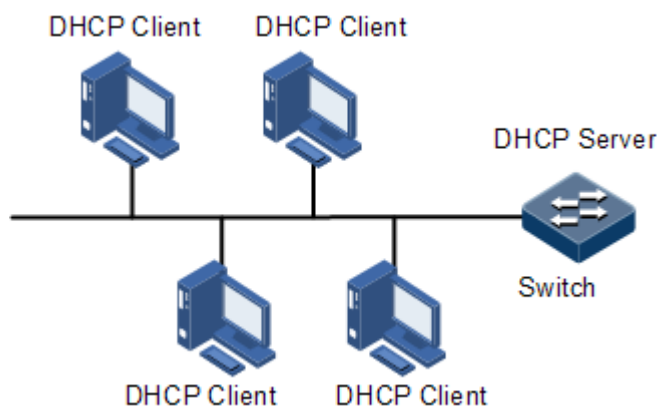
- The number of hosts on the network is greater than that of IP addresses, which makes it unable to assign a fixed IP address for each host and restricts the number of users connected to network simultaneously.
- Only the minority of hosts on the network need fixed IP addresses, most of hosts have no requirement for fixed IP address.

After a DHCP client obtains the IP address from the DHCP server, it cannot use the IP address permanently but in a fixed period, which is called the lease period. You can specify the duration of the lease period.

DHCP ensures rational allocation, avoids waste of IP addresses, and improves the utilization rate of IP addresses on the entire network.

The ISCOM2600G-HI series switch, as the DHCP server, assigns dynamic IP addresses to clients, as shown in Figure 6-11.

Figure 6-11 DHCP Server and Client networking



## DHCP packets

Figure 6-12 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 6-12 Structure of a DHCP packet

0	7	15	23	31
OP	Hardware type	Hardware length	Hops	
Transaction ID				
Seconds		Flags		
Client IP address				
Your(client) IP address				
Server IP address				
Relay agent IP address				
Client hardware address				
Server host name				
File				
Options				

Table 6-4 describes fields of a DHCP packet.

Table 6-4 Fields of a DHCP packet

Field	Length	Description
OP	1	Packet type <ul style="list-style-type: none"> <li>• 1: a request packet</li> <li>• 2: a reply packet</li> </ul>
Hardware type	1	Hardware address type of a DHCP client
Hardware length	1	Hardware address length of a DHCP client
Hops	1	Number of DHCP hops passing by the DHCP packet This field increases 1 every time the DHCP request packet passes a DHCP relay.
Transaction ID	4	A random number selected by the client to initiate a request, used to identify an address request process
Seconds	2	Duration after the DHCP request for the DHCP client, fixed to 0, being idle currently
Flags	2	Bit 1 is the broadcast reply flag, used to mark that the DHCP server response packet is transmitted in unicast or broadcast mode. <ul style="list-style-type: none"> <li>• 0: unicast</li> <li>• 1: broadcast</li> </ul> Other bits are reserved.
Client IP address	4	IP address of the DHCP client, only filled when the client is in bound, updated or re-bound status, used to respond to ARP request
Your (client) IP address	4	IP address of the DHCP client assigned by the DHCP server
Server IP address	4	IP address of the DHCP server
Relay agent IP address	4	IP address of the first DHCP relay passing by the request packet sent by the DHCP client
Client hardware address	16	Hardware address of the DHCP client
Server host name	64	Name of the DHCP server
File	128	Startup configuration file name and path assigned by the DHCP server to the DHCP client
Options	Modifiable	A modifiable option field, including packet type, available lease period, IP address of the DNS server, IP address of the WINS

## 6.5.2 Preparing for configurations

### Scenario

When working as the DHCPv4 server, the ISCOM2600G-HI series switch can assign IP addresses to DHCPv4 clients.

### Prerequisite

- Disable DHCPv4 Client on the ISCOM2600G-HI series switch.
- The DHCP server is a common one.

## 6.5.3 Creating and configuring IPv4 address pool

Configure the IPv4 address pool for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip dhcp server pool pool-name</b>	Create an IPv4 address pool, and enter address pool configuration mode.
3	<b>Raisecom(config-pool)#address start-ip-address end-ip-address mask { mask   mask-length }</b>	Configure the range of IP addresses in the IPv4 address pool. The mask length ranges from 1 to 30.
4	<b>Raisecom(config-pool)#excluded-ip-address start-ip-address [ end-ip-address ]</b>	Configure the range of excluded IP addresses in the IPv4 address pool.
5	<b>Raisecom(config-pool)#lease expired { minute   infinite }</b>	Configure the lease period for the IPv4 address pool.
6	<b>Raisecom(config-pool)#dns-server ip-address [ secondary ]</b>	Configure the DNS server address of the IPv4 address pool.
7	<b>Raisecom(config-pool)#gateway ip-address</b>	Configure the default gateway of the IPv4 address pool.
8	<b>Raisecom(config-pool)#option 60 vendor-string</b>	Configure information carried by Option 60.
9	<b>Raisecom(config-pool)#option 43 [ sub-option option-code ] { ascii ascii-string   hex hex-string }</b>	Configure information carried by Option 43.
10	<b>Raisecom(config-pool)#tftp-server ip-address</b>	Configure the TFTP server of the IPv4 address pool.
11	<b>Raisecom(config-pool)#trap server-ip ip-address</b>	Configure the Trap server of the IPv4 address pool.

## 6.5.4 Enabling DHCPv4 Server on VLAN interface

Enable DHCPv4 Server on the VLAN interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlan <i>vlan-id</i></b>	Enter VLAN interface configuration mode.
3	<b>Raisecom(config-vlan1)#ip dhcp server</b>	Enable DHCPv4 Server on the VLAN interface.

## 6.5.5 Enabling DHCP Server on VLAN interface

Only global DHCP Server and Layer 3 interface DHCP Server are enabled can the Layer 3 interface receive and process DHCP request packets from clients.

Enable DHCP Server on the VLAN interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlan <i>vlan-id</i></b>	Enter VLAN interface configuration mode.
3	<b>Raisecom(config-vlan1)#ip dhcp server</b>	Enable DHCP Server on the VLAN interface.

## 6.5.6 Configuring DHCP Server to support Option 82

Configure DHCP Server to support Option 82 for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip dhcp server information option</b>	Configure DHCP Server to support Option 82.

## 6.5.7 Checking configurations

Use the following commands to check configuration results.

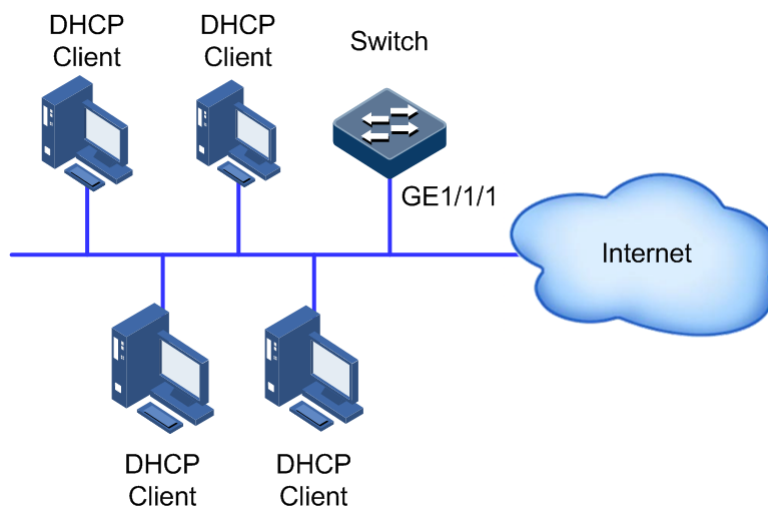
No.	Command	Description
1	<b>Raisecom(config)#show ip dhcp server</b>	Show configurations of DHCP Server.
2	<b>Raisecom(config)#show ip dhcp server lease</b>	Show assigned IPv4 addresses and clients information.
3	<b>Raisecom(config)#show ip dhcp server statistics</b>	Show packet statistics on the DHCPv4 Server.
4	<b>Raisecom(config)#show ip dhcp static-bind</b>	Show information about DHCPv4 static binding.
5	<b>Raisecom(config)#show ip server pool</b>	Show configurations of the address pool of DHCPv4 Server.

## 6.5.8 Example for configuring DHCPv4 Server

### Networking requirements

As shown in Figure 6-13, the switch as a DHCP server assigns IP addresses to DHCP clients. The lease period is 8h. The name of the IP address pool is pool. The range of IP addresses is 172.31.1.2–172.31.1.100. The IP address of the DNS server is 172.31.100.1.

Figure 6-13 DHCP Server networking



### Configuration steps

Step 1 Create an IP address pool, and configure it.

```
Raisecom#config
Raisecom(config)#ip dhcp server pool pool
Raisecom(config-pool)#address 172.31.1.2 172.31.1.100 mask 24
Raisecom(config-pool)#lease expired 480
Raisecom(config-pool)#dns-server 172.31.100.1
```

```
Raisecom(config-pool)#exit
```

Step 2 Configure interface DHCP Server.

```
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 172.31.1.1 255.255.255.0
Raisecom(config-vlan1)#ip dhcp server
```

## Checking results

Use the **show ip dhcp server** command to show configurations of DHCP Server.

```
Raisecom#show ip dhcp server
Interface                Status
-----
vlan 1                   Enable
```

Use the **show ip server pool** command to show configurations of the address pool of the DHCP server.

```
Raisecom#show ip server pool
Pool Name      :    pool1
pool type      :    DHCP
Address Range   :    172.31.1.2~172.31.1.100
Address Mask    :    255.255.255.0
Gateway         :    0.0.0.0
DNS Server      :    172.31.100.1
Secondary DNS   :    0.0.0.0
Tftp Server     :    0.0.0.0
Lease time      :    480 minutes
Trap Server     :    0.0.0.0
interface       :    vlan1
option60        :
```

## 6.6 DHCP Relay

### 6.6.1 Introduction

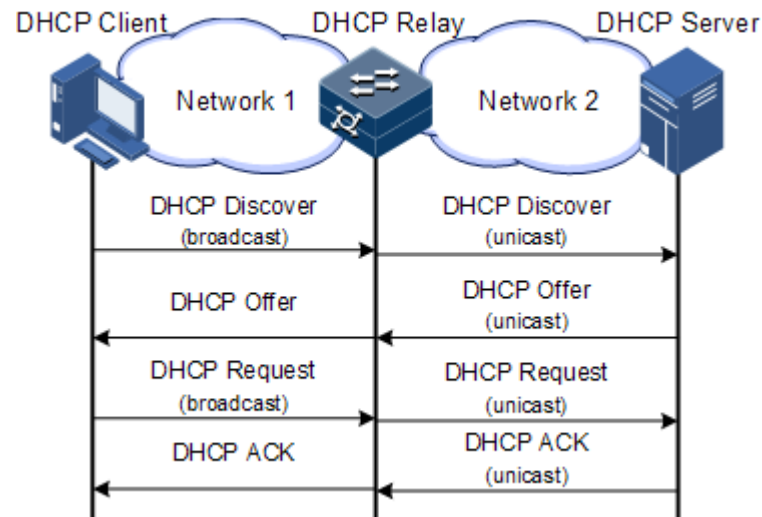
At the beginning, DHCP requires the DHCP server and clients to be in the same segment, instead of different segments. As a result, a DHCP server is configured for all segments for dynamic host configuration, which is not economic.



DHCP Relay is introduced to solve this problem. It can provide relay service between DHCP clients and the DHCP server that are in different segments. It relays packets across segments to the DHCP server or clients.

Figure 6-14 shows typical application of DHCP Relay.

Figure 6-14 Typical application of DHCP Relay



When a DHCP client sends a request packet to the DHCP server through a DHCP relay, the DHCP relay processes the request packet and sends it to the DHCP server in the specified segment. The DHCP server sends required information to the DHCP client through the DHCP relay according to the request packet, thus implementing dynamic configuration of the DHCP client.

## 6.6.2 Preparing for configurations

### Scenario

When DHCP Client and DHCP Server are not in the same segment, you can use DHCP Relay function to make DHCP Client and DHCP Server in different segments carry relay service, and relay DHCP protocol packets across segment to destination DHCP server, so that DHCP Client in different segments can share the same DHCP server.

### Prerequisite

N/A

## 6.6.3 Default configurations of DHCP Relay

Default configurations of DHCP Relay are as below.

Function	Default value
Global DHCP Relay	Disable
Interface DHCP Relay	Disable
Global DHCPv6 Relay	Disable

Function	Default value
Interface DHCPv6 Relay	Disable

## 6.6.4 Configuring global DHCP Relay

Configure global DHCP Relay for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip dhcp relay</b>	Enable global DHCP Relay.

## 6.6.5 Configuring DHCP Relay on VLAN interface

Configure DHCP Relay on the VLAN interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlan</b> <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	<b>Raisecom(config-vlan1)#ip dhcp relay</b>	Enable DHCP Relay on the VLAN interface.
4	<b>Raisecom(config-vlan1)#ip dhcp relay target-ip</b> <i>ip-address</i>	Configure the destination IP address for forwarding packets.

## 6.6.6 Configuring global DHCPv6 Relay

Configure global DHCPv6 Relay for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ipv6 dhcp relay</b>	Enable global DHCPv6 Relay.
3	<b>Raisecom(config)#ipv6 dhcp relay option interface-id</b>	Enable DHCPv6 Relay to support Option 18.
4	<b>Raisecom(config)#ipv6 dhcp relay option remote-id</b>	Enable DHCPv6 Relay to support Option 37.

## 6.6.7 Configuring DHCPv6 Relay on VLAN interface

Configure DHCPv6 Relay on the VLAN interface for forwarding packets for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlan <i>vlan-id</i></b>	Enter VLAN interface configuration mode.
3	<b>Raisecom(config-vlan1)#ipv6 dhcp relay</b>	Enable DHCPv6 Relay on the VLAN interface.
4	<b>Raisecom(config-vlan1)#ipv6 dhcp relay target-ip <i>ip- address</i> [ <i>vlan vlan-id</i> ]</b>	Configure the destination IPv6 address for forwarding packets.

## 6.6.8 (Optional) configuring DHCP Relay to support Option 82

Configure DHCP Relay to support Option 82 for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip dhcp relay information option</b>	Configure DHCP Relay to support Option 82. DHCP Relay supports the Remote ID of Option 82 and is compatible with Huawei Default mode.
3	<b>Raisecom(config)#ip dhcp relay information policy { <b>drop</b>   <b>keep</b>   <b>replace</b> }</b>	Configure the policy for DHCP Relay to process Option 82 request packets
4	<b>Raisecom(config)#interface <i>interface-type interface- number</i></b>	Enter physical layer interface configuration mode.
5	<b>Raisecom(config- gigaethernet1/1/port)#ip dhcp relay information trusted</b>	Configure the trusted interface of DHCP Relay.
6	<b>Raisecom(config- gigaethernet1/1/port)#ip dhcp relay information option vlan- list <i>vlan-list</i></b>	Configure the VLAN list of DHCP Relay to support Option 82.

## 6.6.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show ip dhcp relay</b>	Show configurations of DHCP Relay.

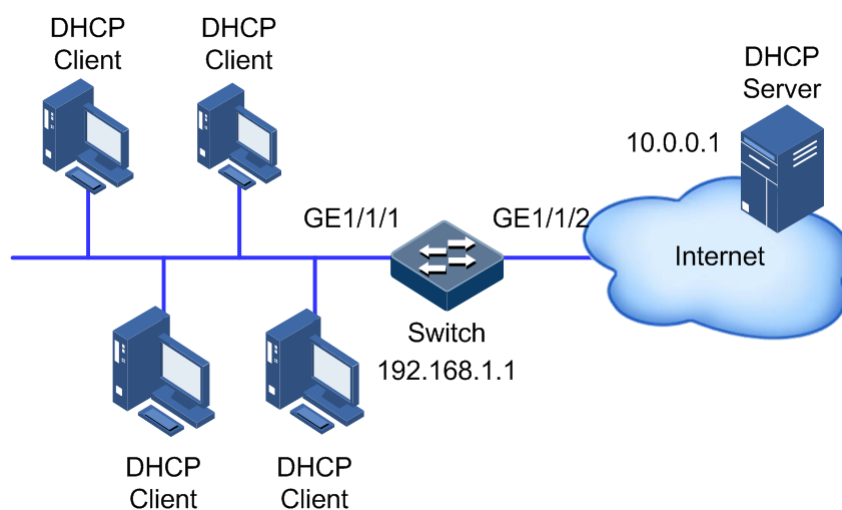
No.	Command	Description
2	<b>Raisecom#show ip dhcp relay information</b>	Show information about Option 82 supported by DHCP Relay.
3	<b>Raisecom#show ipv6 dhcp relay</b>	Show configurations of DHCPv6 Relay.

## 6.6.10 Example for configuring DHCPv4 Relay

### Networking requirements

As shown in Figure 6-15, the switch works as the DHCP relay device. The host name is raisecom. The switch is connected to the DHCP server through a service interface. The DHCP server assigns IP addresses to clients so that the NMS can discover and manage these clients.

Figure 6-15 DHCP Relay networking



### Configuration steps

Step 1 Enable global DHCP Relay and interface DHCP Relay.

```

Raisecom#config
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#ip dhcp relay
Raisecom(config-gigabitEthernet1/1/1)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#ip dhcp relay
Raisecom(config-gigabitEthernet1/1/2)#exit
  
```

Step 2 Configure the destination IP address of DHCP Relay.

```

Raisecom(config)#interface gigabitEthernet 1/1/1
  
```

```
Raisecom(config-gigaethernet1/1/1)#ip dhcp relay target-ip 10.0.0.1
```

## Checking results

Use the **show ip dhcp relay** command to show configurations of DHCP Relay.

```
Raisecom#show ip dhcp relay
Interface                Status                Target Address
-----
gigaethernet1/1/1       Enable                10.0.0.1
```

# 7 QoS

---

This chapter describes basic principles and configuration procedures for QoS, and provides related configuration examples, including the following sections:

- Introduction
- Configuring priority
- Configuring congestion management
- Configuring congestion avoidance
- Configuring traffic classification and traffic policy
- Configuring rate limiting
- Bandwidth rate limiting
- Configuration examples

## 7.1 Introduction

When network applications become more and more versatile, users bring forward different Quality of Service (QoS) requirements on them. In this case, the network should distribute and schedule resources for different network applications as required. When network is overloaded or congested, QoS can ensure service timeliness and integrity and make the entire network run efficiently.

QoS is composed of a group of flow management technologies:

- Service model
- Priority trust
- Traffic classification
- Traffic policy
- Priority mapping
- Congestion management

### 7.1.1 Service model

QoS technical service models:

- Best-effort Service

- Differentiated Services (DiffServ)

## Best-effort

Best-effort service is the most basic and simplest service model on the Internet (IPv4 standard) based on storing and forwarding mechanism. In Best-effort service model, the application can send a number of packets at any time without being allowed in advance and notifying the network. For the Best-effort service, the network will send packets as possible as it can, but it does not guarantee the delay and reliability.

Best-effort is the default Internet service model now, suitable to most network applications, such as FTP and E-mail. It is implemented by First In First Out (FIFO) queue.

## DiffServ

The DiffServ model is a multi-service model, which can satisfy different QoS requirements.

The DiffServ model does not need to maintain state for each flow. It provides differentiated services according to the QoS classification of each packet. Many different methods can be used for classifying QoS packets, such as IP packet priority (IP precedence), the packet source address or destination address.

Generally, DiffServ is used to provide end-to-end QoS services for a number of important applications, which is implemented through the following techniques:

- Committed Access Rate (CAR): CAR refers to classifying the packets according to the preconfigured packet matching rules, such as IP packets priority, the packet source address or destination address. The system continues to send the packets if the flow complies with the rules of token bucket. Otherwise, it discards the packets or remarks IP precedence, DSCP, EXP CAR can not only control the flows, but also mark and remark the packets.
- Queuing technology: the queuing technologies of SP, WRR, DRR, SP+WRR, and SP+DRR cache and schedule the congestion packets to implement congestion management.

### 7.1.2 Priority trust

Priority trust means that the ISCOM2600G-HI series switch uses priority of packets for classification and performs QoS management.

The ISCOM2600G-HI series switch supports packet priority trust based on interface, including:

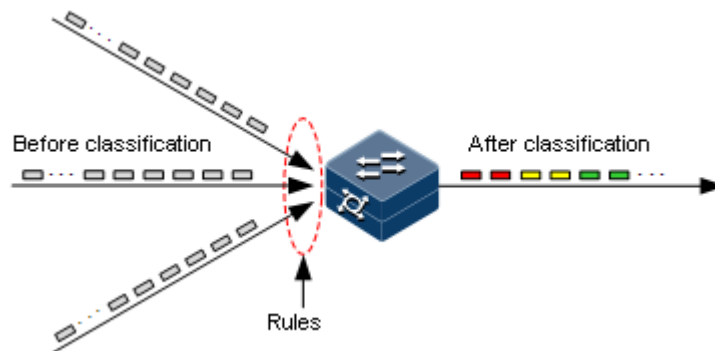
- Differentiated Services Code Point (DSCP) priority
- Class of Service (CoS) priority
- ToS priority

### 7.1.3 Traffic classification

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.

The ISCOM2600G-HI series switch supports traffic classification based on ToS priority, DSCP, and CoS over IP packets, and classification based on Access Control List (ACL) rules and VLAN ID. The traffic classification procedure is shown in Figure 7-1.

Figure 7-1 Traffic classification



## IP precedence and DSCP

Figure 7-2 shows the structure of the IP packet header. The head contains an 8-bit ToS field. Defined by RFC 1122, IP priority (IP Precedence) uses the highest 3 bits (0–3) with value range of 0–7; RFC2474 defines ToS field again, and applies the first 6 bits (0–5) to DSCP with value ranging from 0 to 63, the last 2 bits (bit-6 and bit-7) are reserved. Figure 7-3 shows the structure of ToS and DSCP.

Figure 7-2 Structure of an IP packet header

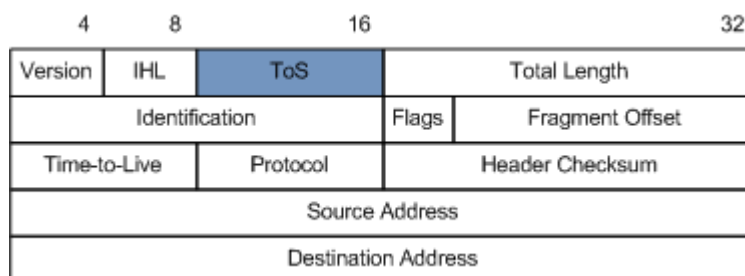
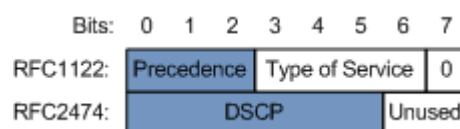


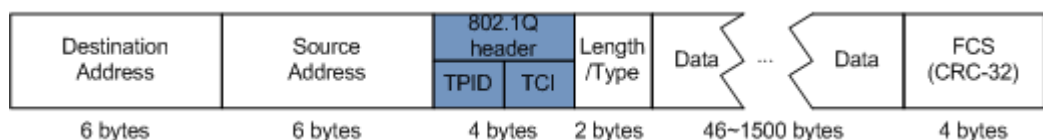
Figure 7-3 Structures of the ToS priority and DSCP



## CoS

IEEE802.1Q-based VLAN packets are modifications of Ethernet packets. A 4-byte 802.1Q header is added between the source MAC address and protocol type, as shown in Figure 7-4. The 802.1Q header consists of a 2-byte Tag Protocol Identifier (TPID, valuing 0x8100) field and a 2-byte Tag Control Information (TCI) field.

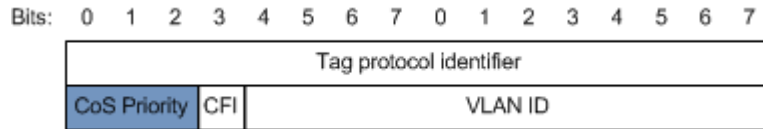
Figure 7-4 Structure of a VLAN packet





The first 3 bits of the TCI field represent CoS, which ranges from 0 to 7, as shown in Figure 7-5. CoS is used to guarantee QoS on the Layer 2 network.

Figure 7-5 Structure of CoS



## 7.1.4 Traffic policy

After performing traffic classification on packets, you need to perform different operations on packets of different categories. A traffic policy is formed when traffic classifiers are bound to traffic behaviours.

### Rate limiting based on traffic policy

Rate limiting refers to controlling network traffic, monitoring the rate of traffic entering the network, and discarding overflow part, so it controls ingress traffic in a reasonable range, thus protecting network resources and carrier interests.

The ISCOM2600G-HI series switch supports rate limiting based on traffic policy in the ingress direction on the interface.

The ISCOM2600G-HI series switch supports using token bucket for rate limiting, including single-token bucket and dual-token bucket.

### Redirection

Redirection refers to redirecting packets to a specified interface, instead of forwarding packets according to the mapping between the original destination address and interface, thus implementing policy routing.

The ISCOM2600G-HI series switch supports redirecting packets to the specified interface for forwarding in the ingress direction of the interface.

### Remarking

Remarking refers to configuring some priority fields in packets again and then classifying packets by user-defined standards. Besides, downstream nodes on the network can provide differentiated QoS service according to remarking information.

The ISCOM2600G-HI series switch supports remarking packets by the following priority fields:

- IP precedence
- DSCP
- CoS

### Traffic statistics

Traffic statistics is used to gather statistics about data packets of a specified service flow; in other words, the number of packets and bytes matching traffic class that pass the network or are discarded.

Traffic statistics is not a QoS control measure, but can be used in combination with other QoS actions to improve network supervision.

## 7.1.5 Priority mapping

Priority mapping refers to sending packets to different queues with different local priorities according to pre-configured mapping from external priority to local priority. Therefore, packets in different queues can be scheduled on the egress interface.

The ISCOM2600G-HI series switch supports performing priority mapping based on DSCP of IP packets or CoS of VLAN packets. The Traffic-Class field of IPv6 packets corresponds to DSCP of IPv4 packets. The mapping from DSCP to local priority is applicable to IPv6 packets. Take the first 6 bits of the Traffic-Class field for use.

By default, the mapping from the DSCP or CoS to local priority of the ISCOM2600G-HI series switch is listed in Table 7-1 and Table 7-2.

Table 7-1 Mapping from DSCP or CoS to local priority

Local priority	0	1	2	3	4	5	6	7
DSCP	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
CoS	0	1	2	3	4	5	6	7

Local priority refers to a kind of packet priority with internal meaning assigned by the ISCOM2600G-HI series switch and is the priority corresponding to queue in QoS queue scheduling.

Local priority ranges from 0 to 7. Each interface of the ISCOM2600G-HI series switch supports 8 queues. Local priority and interface queue are in one-to-one mapping. The packet can be sent to the assigned queue according to the mapping between local priority and queue, as shown in Table 7-2.

Table 7-2 Mapping between local priority and queue

Local priority	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

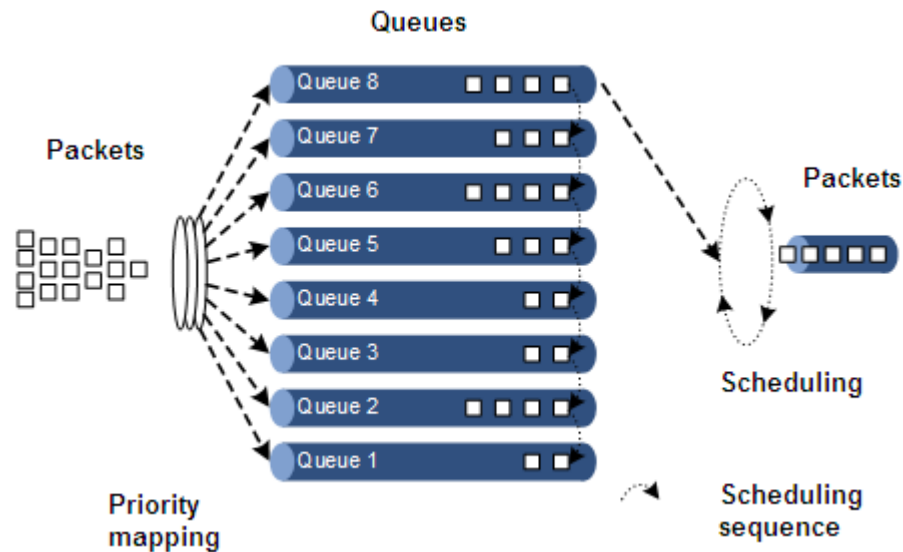
## 7.1.6 Queue scheduling

The ISCOM2600G-HI series switch needs to perform 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 ISCOM2600G-HI series switch 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.

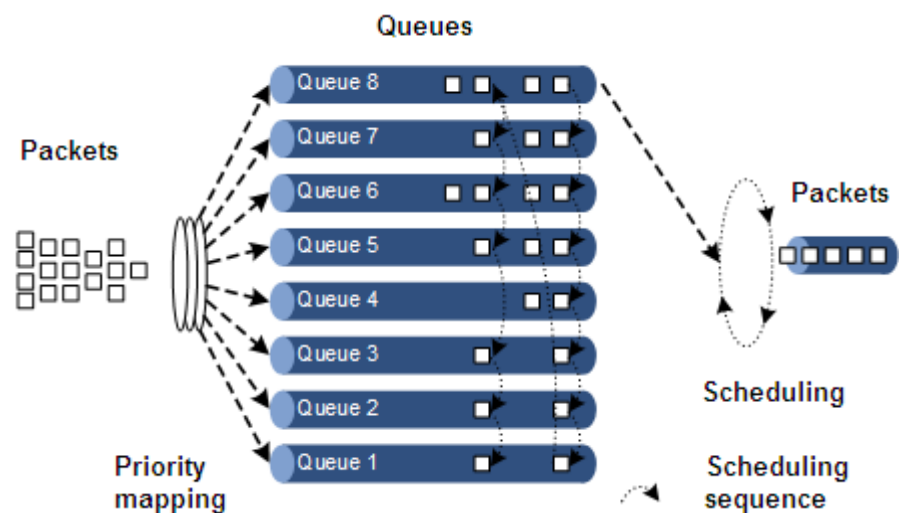
- SP: the ISCOM2600G-HI series switch strictly schedules packets in a descending order of priority. Packets with lower priority cannot be scheduled until packets with higher priority are scheduled, as shown in Figure 7-6.

Figure 7-6 SP scheduling



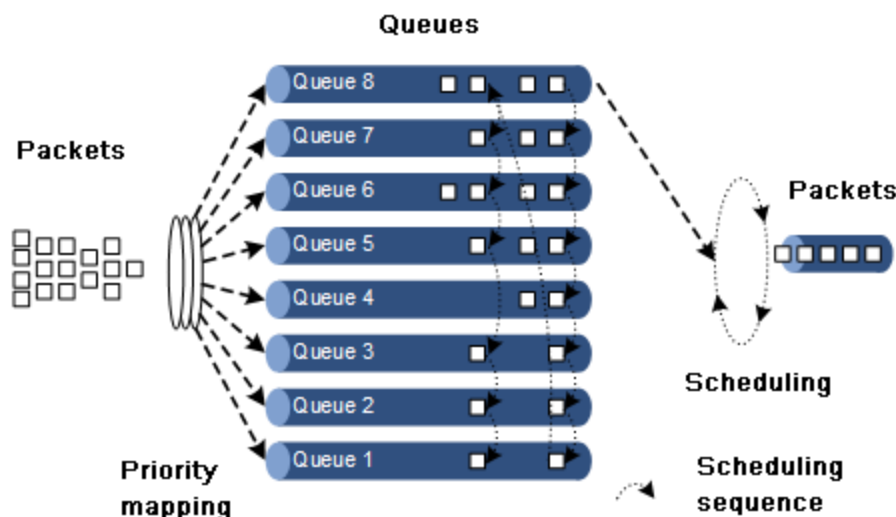
- WRR: on the basis of scheduling packets in a polling manner according to the priority, the ISCOM2600G-HI series switch schedules packets according to the weight (based on bytes) of the queue, as shown in Figure 7-7.

Figure 7-7 WRR scheduling



- DRR: similar with WRR, on the basis of scheduling packets in a polling manner according to the scheduling sequence, the ISCOM2600G-HI series switch schedules packets according to the weight of the queue (based on packet), as shown in DRR scheduling

Figure 7-8 DRR scheduling



- SP+WRR: a scheduling mode combining the SP scheduling and WRR scheduling. In this mode, queues on an interface 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 DRR scheduling. In this mode, queues on an interface are divided into 2 groups. You can specify the queues where SP scheduling/DRR scheduling is performed.

## 7.1.7 Congestion avoidance

By monitoring utilization of network resources (queues/memory buffer), congestion avoidance can discard packets actively when congestion occurs or network traffic increases. It is a traffic control mechanism that is used to resolve network overload by adjusting network traffic.

The traditional packet loss policy uses the Tail-Drop mode to process all packets equally without differentiating class of services. When congestion occurs, packets at the end of a queue are discarded until congestion is resolved.

This Tail-Drop policy may cause TCP global synchronization, making network traffic change between heavy and low and affecting link utilization.

### RED

Random Early Detection (RED) discards packets randomly and prevents multiple TCP connection from reducing transmission rate simultaneously to avoid TCP global synchronization.

The RED algorithm configures a minimum threshold and maximum threshold for length of each queue. In addition:

- Packets are not discarded when the queue length is smaller than the minimum threshold.
- All received packets are discarded when the queue length is greater than the maximum threshold.
- Packets to be received are discarded randomly when the queue length is between the minimum and maximum thresholds. The greater the queue size is, the higher the packet drop probability is.

## 7.1.8 Rate limiting based on interface and VLAN

The ISCOM2600G-HI series switch supports rate limiting both based on traffic policy, interface, or VLAN ID. Similar to rate limiting based on traffic policy, the ISCOM2600G-HI series switch discards the excess traffic.

## 7.1.9 QoS enhancement

QoS enhancement is a subfunction of QoS and is more flexible than basic QoS. It is widely used on switches.

QoS enhancement has the following functions:

- Ingress interface
  - Bandwidth guarantee: QoS enhancement implements the bandwidth service based on interface or flow. It also supports hierarchical bandwidth guarantee and refining bandwidth of different service flows.
  - Awaiting: this function determines whether to conduct color-aware of packets when a flow enters the bandwidth-guaranteed interface.
- Egress interface
  - Bandwidth guarantee: bandwidth service based on interface or flow is implemented. QoS enhancement does not support hierarchical bandwidth guarantee.
  - Marking: this function determines whether to mark a packet with color when a flow leaves the bandwidth-guaranteed interface.

### Bandwidth guarantee

The bandwidth guarantee function guarantees that the traffic entering the network is within the defined range, and it discards or schedules packets. Bandwidth guarantee can meet users' requirements on service bandwidth, and also protect network resources and carriers' benefits.

By configuring the bandwidth guarantee profile and applying it to an interface, you can mark different flows green, yellow, and red. The ISCOM2600G-HI series switch takes different actions over flows of different colors: forward green flows, schedule yellow flows, and discard red flows.

### Hierarchical bandwidth guarantee

Hierarchical bandwidth guarantee is a more flexible bandwidth guarantee. You can configure guaranteed bandwidth for each flow independently and even configure guaranteed bandwidth for sum of multiple flows through hierarchical bandwidth guarantee.

### Color-aware and marking

If enabled with color-aware, the ISCOM2600G-HI series switch is in color-aware status, in which it can identify whether the ingress flow is marked with color. If disabled with color-aware, the ISCOM2600G-HI series switch is in color-blind status, in which it can neglect whether the ingress flow is marked with color, but identify the flow color again.

The function of color marking judges the color of a flow according to Committed Information Rate (CIR), Committed Burst Size (CBS), Excess Information Rate (EIR), and Excess Burst Size (EBS) configured in the bandwidth guarantee profile, and modifies the flag bit to mark it with color according to the packet format defined in IEEE 802.1ad.

## 7.2 Configuring priority

### 7.2.1 Preparing for configurations

#### Scenario

You can choose to trust the priority carried by packets from an upstream device, or process packets with untrusted priority through the traffic class and traffic policy. After being configured to priority trust mode, the ISCOM2600G-HI series switch processes packets according to their priorities and provides services accordingly.

To specify local priority for packets is the prerequisite for queue scheduling. For packets from the upstream device, you can not only map the external priority carried by packets to different local priorities, but also configure local priority for packets based on interface. Then the ISCOM2600G-HI series switch will conduct queue scheduling according to local priority of packets. Generally, IP packets need to be configured with mapping from IP precedence/DSCP to local priority; while VLAN packets need to be configured with mapping from CoS to local priority.

#### Prerequisite

N/A

### 7.2.2 Default configurations of basic QoS

Default configurations of basic QoS are as below.

Function	Default value
Global QoS status	Enable
Interface trust priority type	Trust CoS
Mapping from CoS to local priority	See Table 7-3.
Mapping from DSCP to local priority	See Table 7-4.
Mapping from ToS to local priority and color	See Table 7-5.
Interface priority	0

Table 7-3 Default mapping from CoS to local priority

CoS	0	1	2	3	4	5	6	7
Local priority	0 (green)	1 (green)	2 (green)	3 (green)	4 (green)	5 (green)	6 (green)	7 (green)

Table 7-4 Default mapping from DSCP to local priority

DSCP	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
Local priority	0 (green)	1 (green)	2 (green)	3 (green)	4 (green)	5 (green)	6 (green)	7 (green)

Table 7-5 Default mapping from ToS to local priority and color

ToS	0	1	2	3	4	5	6	7
Local priority	0 (green)	1 (green)	2 (green)	3 (green)	4 (green)	5 (green)	6 (green)	7 (green)

## 7.2.3 Configuring types of priorities trusted by interface

Configure types of priorities trusted by interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaetherne</b> <b>t1/1/1)#mls qos trust</b> <b>{ cos   dscp   dscp-or-cos   port-</b> <b>priority }</b>	Configure types of priorities trusted by interface. CoS exists in the head of 802.1q packets. When you use it, the interface type must be Trunk Tunnel.
4	<b>Raisecom(config-</b> <b>gigaetherne</b> <b>t1/1/1)#mls qos</b> <b>priority</b> <i>portpri-value</i>	Configure the interface priority.

## 7.2.4 Configuring mapping from CoS to local priority

Configure the mapping from CoS to local priority and color for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mls qos mapping</b> <b>cos-to-local-priority</b> <i>profile-id</i>	Create a profile of mapping from CoS to local priority and color, and enter cos-to-pri configuration mode.

Step	Command	Description
3	<b>Raisecom(cos-to-pri)#cos</b> <i>cos-value</i> <b>to local-priority</b> <i>localpri-value</i> [ <b>color</b> { <b>green</b>   <b>red</b>   <b>yellow</b> } ]	(Optional) modify the profile of mapping from CoS to local priority and color.
4	<b>Raisecom(cos-to-pri)#exit</b> <b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	<b>Raisecom(config-</b> <b>gigaethernet1/1/1)#mls qos cos-to-</b> <b>local-priority</b> <i>profile-id</i>	Apply the profile of mapping from CoS to local priority and color on the interface.

## 7.2.5 Configuring mapping from DSCP to local priority and color

Configure the mapping from DSCP to local priority and color for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mls qos</b> <b>mapping dscp-to-local-priority</b> <i>profile-id</i>	Create a profile of mapping from DSCP to local priority and color, and enter dscp-to-pri configuration mode.
3	<b>Raisecom(dscp-to-pri)#dscp</b> <i>dscp-value</i> <b>to local-priority</b> <i>localpri-value</i> [ <b>color</b> { <b>green</b>   <b>red</b>   <b>yellow</b> } ]	(Optional) modify the profile of mapping from DSCP to local priority and color.
4	<b>Raisecom(dscp-to-pri)#exit</b> <b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	<b>Raisecom(config-</b> <b>gigaethernet1/1/1)#mls qos</b> <b>dscp-to-local-priority</b> <i>profile-</i> <i>id</i>	Apply the profile of mapping from DSCP to local priority and color on the interface. The profile used in this configuration is the same profile used by DSCP mutation.

## 7.2.6 Configuring DSCP mutation

Configure DSCP mutation for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mls qos mapping</b> <b>dscp-mutation</b> <i>profile-id</i>	Create a DSCP mutation mapping profile, and enter dscp mutation configuration mode.



Step	Command	Description
3	<code>Raisecom(dscp-mutation)#<b>dscp</b> <i>dscp-value</i> <b>to new-dscp</b> <i>new dscp-value</i></code>	(Optional) modify the DSCP mutation profile. The profile used in this configuration is the same profile used by the mapping from DSCP to local priority.
4	<code>Raisecom(dscp-mutation)#<b>exit</b> Raisecom(config)#<b>interface</b> <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
5	<code>Raisecom(config-gigaetherne1/1/1)#<b>mls qos dscp-mutation</b> <i>profile-id</i></code>	Apply the DSCP mutation profile on the interface.

## 7.2.7 Configuring CoS remarking

Configure CoS remarking for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#<b>config</b></code>	Enter global configuration mode.
2	<code>Raisecom(config)#<b>interface</b> <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaetherne1/1/1)#<b>mls qos cos-remark-mapping enable</b> Raisecom(config-gigaetherne1/1/1)#<b>exit</b></code>	Enable CoS remarking on the interface.
4	<code>Raisecom(config)#<b>mls qos mapping cos-remark</b> <i>profile-id</i></code>	Create a CoS remarking profile, and enter cos-remark configuration mode.
5	<code>Raisecom(cos-remark)#<b>local-priority</b> <i>localpri-value</i> <b>to cos</b> <i>newcos-value</i></code>	Modify the CoS remarking profile.
6	<code>Raisecom(dscp-remark)#<b>exit</b> Raisecom(config)#<b>interface</b> <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
7	<code>Raisecom(config-gigaetherne1/1/1)#<b>mls qos cos-remark</b> <i>profile-id</i></code>	Apply the DSCP remarking profile on the interface.

## 7.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#<b>show mls qos interface</b> [ <i>interface-type interface-number</i> ]</code>	Show QoS priority, trust mode, and scheduling mode on the interface.

No.	Command	Description
2	<b>Raisecom#show mls qos mapping cos-to-local-priority [ default   profile-id ]</b>	Show information about mapping from CoS to local priority and color profile.
3	<b>Raisecom#show mls qos mapping dscp-to-local-priority [ default   profile-id ]</b>	Show information about mapping from DSCP to local priority and color profile.
4	<b>Raisecom#show mls qos mapping dscp-mutation [ profile-id ]</b>	Show mapping information about the DHCP mutation profile
5	<b>Raisecom#show mls qos mapping cos-remark [ default   profile-id ]</b>	Show information about the CoS remarking profile.

## 7.3 Configuring congestion management

### 7.3.1 Preparing for configurations

#### Scenario

When the network is congested, you can configure queue scheduling if you want to:

- Balance delay and delay jitter of various packets, preferentially process packets of key services (such as video and voice).
- Fairly process packets of secondary services (such as Email) with identical priority.
- Process packets of different priorities according to respective weight values.

The scheduling algorithm to be chosen depends on the current service condition and customer requirements.

#### Prerequisite

Enable global QoS.

### 7.3.2 Default configurations of congestion management

Default configurations of congestion management are as below.

Function	Default value
Queue scheduling mode	SP
Queue weight	<ul style="list-style-type: none"> <li>• WRR weight for scheduling 8 queues is 1.</li> <li>• DRR weight for scheduling 8 queues is 81.</li> </ul>

### 7.3.3 Configuring SP queue scheduling

Configure SP queue scheduling for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#mls qos</b> <b>queue scheduler sp</b>	Configure queue scheduling mode as SP on the interface.

### 7.3.4 Configuring WRR or SP+WRR queue scheduling

Configure WRR or SP+WRR for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#mls qos queue</b> <b>scheduler wrr weigh1 weight2</b> <i>weight3...weight8</i>	Configure queue scheduling mode as WRR on the interface and the weight for each queue.

### 7.3.5 Configuring DRR or SP+DRR queue scheduling

Configure DRR or SP+DRR for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#mls</b> <b>qos queue scheduler drr</b> <i>weigh1 weight2</i> <i>weight3...weight8</i>	Configure queue scheduling mode as DRR, and configure weight for various queues. Conduct SP scheduling when priority of a queue is 0.

### 7.3.6 Configuring queue bandwidth guarantee

Configure queue bandwidth guarantee for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#mls qos</b> <b>queue queue-id shaping cir cir</b> <b>pir pir</b>	(Optional) configure queue bandwidth guarantee on the interface and configure burst size.

## 7.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show mls qos queue interface</b> <i>interface-type interface-number</i>	Show the weight of queues on the interface.
2	<b>Raisecom#show mls qos queue statistics</b> <b>interface interface-type interface-</b> <b>number</b>	Show statistics about queues on the interface.
3	<b>Raisecom#show mls qos queue shaping</b> <b>interface interface-type interface-list</b>	Show queue shaping on the interface.

## 7.4 Configuring congestion avoidance

### 7.4.1 Preparing for configurations

#### Scenario

To avoid network congestion and solve the problem of TCP global synchronization, you can configure congestion avoidance to adjust network flow and relieve network overload.

The ISCOM2600G-HI series switch conducts congestion avoidance based on WRED.

#### Prerequisite

Enable global QoS.

### 7.4.2 Default configurations of congestion avoidance

Default configurations of congestion avoidance are as below.

Function	Default value
Global WRED status	Enable

## 7.4.3 Configuring SRED

Configure SRED for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mls qos sred profile profile-id</b>	Create a SRED profile, and enter SRED configuration mode.
3	<b>Raisecom(sred)#sred [ color { red   yellow } ] start-drop-threshold start-drop value drop-probability drop probability value</b>	Modify the SRED profile.
4	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical layer interface configuration mode.
5	<b>Raisecom(config-gigaethernet1/1/1)#mls qos queue queue-id sred profile-id</b>	Apply the SRED profile to the interface.

## 7.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show mls qos sred profile [ profile-list ]</b>	Show information about the SRED profile.
2	<b>Raisecom#show mls qos queue sred interface interface-type interface-number</b>	Show SRED information about the interface.

## 7.5 Configuring traffic classification and traffic policy

### 7.5.1 Preparing for configurations

#### Scenario

Traffic classification is the basis of QoS. You can classify packets from the upstream device according to the priorities and ACL rules. After classification, the ISCOM2600G-HI series switch can perform corresponding operations on packets in different categories and provide corresponding services.

A traffic classification rule will not take effect until it is bound to a traffic policy. You should apply traffic policy according to current network loading conditions and period. Usually, the ISCOM2600G-HI series switch limits the rate for transmitting packets according to CIR when packets enter the network, and remarks priority according to service feature of packets.

## Prerequisite

Enable global QoS.

## 7.5.2 Default configurations of traffic classification and traffic policy

Default configurations of traffic classification and traffic policy are as below.

Function	Default value
Traffic policy status	Disable
Traffic policy statistics status	Disable

## 7.5.3 Creating traffic class

Create a traffic class for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#class-map</b> <i>class-map-name</i> [ <b>match-all</b>   <b>match-any</b> ]	Create a traffic class and enter traffic classification cmap configuration mode.
3	<b>Raisecom(config-cmap)#description</b> <i>string</i>	(Optional) configure the description of traffic class.

## 7.5.4 Configuring traffic classification rules

Configure traffic classification rules for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#class-map</b> <i>class-map-name</i> [ <b>match-all</b>   <b>match-any</b> ]	Create a traffic class and enter traffic classification cmap configuration mode.
3	<b>Raisecom(config-cmap)#match</b> <b>access-list</b> { <i>access-list</i>   <i>name</i> } <b>Raisecom(config-cmap)#exit</b>	(Optional) configure the traffic classification based on the ACL rule. The ACL rule must be defined firstly and the type must be permit.
4	<b>Raisecom(config-cmap)#match</b> <b>cos</b> <i>cos-value</i>	(Optional) configure the traffic class based on CoS of packets.
5	<b>Raisecom(config-cmap)#match</b> <b>inner-vlan</b> <i>inner-vlan-value</i>	(Optional) configure the traffic class based on inner VLAN of packets.
6	<b>Raisecom(config-cmap)#match</b> <b>vlan</b> <i>vlan-value</i>	(Optional) configure the traffic class based on VLANs of packets.

Step	Command	Description
7	<code>Raisecom(config-cmap)#match dscp dscp-value</code>	(Optional) configure the traffic class based on DSCP rule.
8	<code>Raisecom(config)#policy-map policy-map-name</code> <code>Raisecom(config-pmap)#class-map class-map-name</code>	(Optional) configure the traffic class based on traffic policy.  The traffic policy must have been created, and its matching type must be consistent with the matching type of the traffic class.



### Note

- Traffic classification rules must be created for the traffic class; in other words, the **match** parameter must be configured.
- For the traffic class quoted by a traffic policy, do not modify the traffic classification rule; in other words, do not modify the **match** parameter of the traffic class.

## 7.5.5 Creating rate limiting rule and shapping rule

To limit rate of packets based on traffic policy, create a token bucket, configure rate limiting and shaping rules on the token bucket, quote these rules to the traffic class bound to the traffic policy.

Create rate limiting rules and shaping rule for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mls qos policer-profile policer-name [ single   hierarchy   aggregate ]</code>	Create a traffic policer profile, and enter traffic-policer configuration mode.
3	<code>Raisecom(traffic-policer)#cir cir cbs cbs</code>	(Optional) configure flow mode token bucket parameters.  <div data-bbox="997 1462 1093 1547" data-label="Image"> </div> <div data-bbox="1090 1498 1197 1541" data-label="Section-Header"> <h3>Note</h3> </div> <p>Flow mode token bucket is single token bucket, only supporting to configure red and green packets operation.</p>
4	<code>Raisecom(traffic-policer)#cir cir cbs cbs ebs ebs</code>	(Optional) configure RFC2697 mode token bucket parameters.
5	<code>Raisecom(traffic-policer)#cir cir cbs cbs pir pir pbs pbs</code>	(Optional) configure RFC2698 mode token bucket parameters.
6	<code>Raisecom(traffic-policer)#cir cir cbs cbs eir eir ebs ebs [ coupling ]</code>	(Optional) configure RFC4115 mode or MEF token bucket parameters.

Step	Command	Description
7	<code>Raisecom(traffic-policer)#drop-color { red   yellow }</code>	(Optional) configure the token bucket to discard packets with any color.
8	<code>Raisecom(traffic-policer)#recolor { green-recolor { yellow   red }   red-recolor { green   yellow }   yellow-recolor { green   red } }</code>	(Optional) configure packet recoloring.
9	<code>Raisecom(traffic-policer)#set-cos { green cos   red cos   yellow cos }</code>	(Optional) configure the mapping from packets color to CoS.
10	<code>Raisecom(traffic-policer)#set-dscp { green green-value   red red-value   yellow yellow-value }</code>	(Optional) configure the mapping from packets color to DSCP.
11	<code>Raisecom(traffic-policer)#set-pri { green green-value   red red-value   yellow yellow-value }</code>	(Optional) configure the mapping from packets color to local priority.

## 7.5.6 Creating traffic policy

Create a traffic policy for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#policy-map <i>policy-map-name</i></code>	Create a traffic policy, and enter traffic policy pmap configuration mode.
3	<code>Raisecom(config-pmap)#description <i>string</i></code>	(Optional) configure the description of the traffic policy.

## 7.5.7 Defining traffic policy mapping




### Note

Define one or more defined traffic classes to one traffic policy.

Define traffic policy mapping for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#policy-map <i>policy-map-name</i></code>	Create a traffic policy, and enter traffic policy pmap configuration mode.



Step	Command	Description
3	<code>Raisecom(config-pmap)#class-map class-map-name</code>	Bind a traffic class with a traffic policy. The traffic policy is applied to the packets matching the traffic class.   <b>Note</b> At least one rule is required for the traffic class to be bound with a traffic policy, otherwise the binding will fail.



## 7.5.8 Defining traffic policy operation



### Note

Define different operations to different flows in policy.

Define a traffic policy operation for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#policy-map policy-map-name</code>	Create a traffic policy, and enter traffic policy pmap configuration mode.
3	<code>Raisecom(config-pmap)#class-map class-map-name</code>	Bind a traffic class with a traffic policy. The traffic policy is applied to the packets matching the traffic class.   <b>Note</b> At least one rule is required for the traffic class to be bound with the traffic policy, otherwise the binding will fail.
4	<code>Raisecom(config-pmap-c)#police policer-name</code>	(Optional) apply the token bucket on traffic policy and conduct rate limiting and shaping.   <b>Note</b> The token bucket needs to be created in advance and be configured with rate limiting and shaping rules. Otherwise, the operation will fail.
5	<code>Raisecom(config-pmap-c)#redirect-to interface-type interface-number</code>	(Optional) configure redirection rules under the traffic class, forwarding classified packets from assigned interface.

Step	Command	Description
6	<code>Raisecom(config-pmap-c)#set { cos cos-value   dscp dscp-value   local-priority value   vlan vlan-id   inner-vlan inner-vlan-id }</code>	(Optional) configure remarking rules under the traffic class, modify packet CoS, local priority, inner VLAN, DSCP, IP precedence, and VLAN ID.
7	<code>Raisecom(config-pmap-c)#copy-to-mirror mirror-id</code>	(Optional) configure traffic mirroring to the monitor interface.
8	<code>Raisecom(config-pmap-c)#statistics enable</code>	(Optional) configure traffic statistic rules under the traffic class, statistic packets for the matched traffic class.

## 7.5.9 Applying traffic policy to interfaces

Apply a traffic policy to the interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode or VLAN interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/port)#service-policy { ingress   egress } policy-map-name</code>	Apply the configured traffic policy to the ingress or egress direction of the interface.

## 7.5.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show service-policy statistics interface interface-type interface-number { ingress   egress } [ class-map class-map-name ]</code>	Show statistics about applied traffic policy.
2	<code>Raisecom#show service-policy interface [ interface-type interface-number] [ ingress   egress ]</code>	Show information about the applied traffic policy.
3	<code>Raisecom#show class-map [ class-map-name ]</code>	Show information about the traffic class.

No.	Command	Description
4	<b>Raisecom#show policy-map</b> [ <i>policy-map-name</i> ]	Show information about traffic policy.
5	<b>Raisecom#show policy-map</b> [ <i>policy-map-name</i> ] [ <b>class</b> <i>class-map-name</i> ]	Show information about the traffic class in the traffic policy.
6	<b>Raisecom#show mls qos policer</b> [ <i>policer-name</i> ]	Show information about the assigned token bucket (rate limiting and shaping).

## 7.5.11 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
<b>Raisecom(config)#clear service-policy statistics</b> <b>interface</b> <i>interface-type interface-number</i> { <b>ingress</b>   <b>egress</b> }	Clear statistics on QoS packets.

## 7.6 Configuring rate limiting

### 7.6.1 Preparing for configurations

#### Scenario

When the network is congested, you want to restrict burst flow on an interface or VLAN to make packets transmitted at a well-proportioned rate to remove network congestion. In this case, you need to configure rate limiting.

#### Prerequisite

N/A

### 7.6.2 Configuring rate limiting based on interface

Configure rate limiting based on interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter interface configuration mode.

Step	Command	Description
3	<code>Raisecom(config-gigaethernet1/1/port)#rate-limit { ingress   egress } cir <i>cir-value</i> cbs <i>cbs-value</i></code>	Configure rate limiting based on interface.
4	<code>Raisecom(config)#rate-limit mode { 11   12 }</code>	Configure the rate limiting mode.



## Note

- By default, no interface-based rate limiting is configured.
- Adopt the drop processing mode for packets on the ingress interface if they exceed the configured rate limit.
- When you configure the rate limit and burst for an interface, the burst value should not be much greater if the configured rate limit is smaller than 256 kbit/s. Otherwise, packets may be inconsecutive.
- When the rate limit is too small, we recommend that the burst value is 4 times greater than then rate limit. If packets are inconsecutive, reduce the burst value or increase the rate limit.
- Packets discarded due to rate limiting on the egress interface are included in statistics about packet loss of the ingress interface.

## 7.6.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show rate-limit interface</code>	Show configurations of rate limiting on interfaces.
	<code>Raisecom#show rate-limit interface <i>interface-type interface-number</i></code>	

## 7.7 Bandwidth rate limiting

### 7.7.1 Introduction

Bandwidth rate limiting is a subfunction of QoS and is more flexible than basic QoS.

Bandwidth rate limiting has the following functions:

- Ingress interface
  - Bandwidth guarantee: bandwidth rate limiting implements the bandwidth service based on interface or flow. It also supports hierarchical bandwidth guarantee and refining bandwidth of different service flows.
  - Awaiting: this function determines whether to be aware of packet color when a flow enters the bandwidth-guaranteed interface.
- Egress interface

- Bandwidth guarantee: bandwidth service based on interface or flow is implemented. Bandwidth rate limiting does not support hierarchical bandwidth guarantee.

## Bandwidth guarantee

The bandwidth guarantee function guarantees that the traffic entering the network is within the defined range, and it discards or schedules packets. Bandwidth guarantee can meet users' requirements on service bandwidth, and also protect network resources and carriers' benefits.

By configuring the bandwidth guarantee profile and applying it to an interface, you can mark different flows green, yellow, and red. The ISCOM2600G-HI series switch takes different actions over flows of different colors: forward green flows, schedule yellow flows, and discard red flows.

## Hierarchical bandwidth guarantee

Hierarchical bandwidth guarantee is more flexible. You can configure the token bucket action or aggregation token bucket for each flow independently and then configure hierarchical token buckets to limit the sum of multiple flows.

## Color-aware and marking

If enabled with color-aware, the ISCOM2600G-HI series switch is in color-aware status, in which it can identify whether the ingress flow is marked with color. If disabled with color-aware, the ISCOM2600G-HI series switch is in color-blind status, in which it can neglect whether the ingress flow is marked with color, but identify the flow color again.

The function of color marking judges the color of a flow according to Committed Information Rate (CIR), Committed Burst Size (CBS), Excess Information Rate (EIR), and Excess Burst Size (EBS) configured in the bandwidth guarantee profile, and modifies the flag bit to mark it with color according to the packet format defined in IEEE 802.1ad.

## 7.7.2 Preparing for configurations

### Scenario

Bandwidth rate limiting is used to guarantee service bandwidth for users and protect network resources and carriers' profits.

### Prerequisite

N/A

## 7.7.3 Default configurations of bandwidth rate limiting

Default configurations of bandwidth rate limiting are as below.

Function	Default value
Color awaring	Disable

## 7.7.4 Configuring bandwidth guarantee

### Creating bandwidth guarantee profile

Create a bandwidth guarantee profile for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#bandwidth-profile <i>bwp-profile-id</i> cir <i>cir</i> cbs <i>cbs</i> [ color-aware ]</b> <b>Raisecom(config)#bandwidth-profile <i>bwp-profile-id</i> cir <i>cir</i> cbs <i>cbs</i> eir <i>eir</i> ebs <i>ebs</i> [ color-aware [ coupling ] ]</b>	Create a bandwidth guarantee profile.
3	<b>Raisecom(config)#bandwidth-profile <i>bwp-profile-id</i> description <i>word</i></b>	Configure the description of the bandwidth guarantee profile.
4	<b>Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i></b> <b>Raisecom(config-gigaethernet1/1/port)#bandwidth { ingress   egress } <i>bwp-profile-id</i></b>	Apply the bandwidth guarantee profile on the interface.

### Configuring bandwidth guarantee based on interface+VLAN

Configure bandwidth guarantee based on interface+VLAN for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#bandwidth-profile <i>bwp-profile-id</i> cir <i>cir</i> cbs <i>cbs</i> [ eir <i>eir</i> ebs <i>ebs</i> ] [ color-aware ]</b>	Create a bandwidth guarantee profile.
3	<b>Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i></b> <b>Raisecom(config-gigaethernet1/1/port)#bandwidth { ingress   egress } vlan <i>vlan-id</i> <i>bwp-profile-id</i></b>	Apply the bandwidth guarantee profile on the interface+VLAN.

### Configuring bandwidth guarantee based on interface+VLAN+CoS

Configure bandwidth guarantee based on interface+VLAN+CoS for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#bandwidth-profile</b> <i>bwp profile-id cir cir cbs cbs [ eir eir ebs ebs ] [ color-aware ]</i>	Create a bandwidth guarantee profile.
3	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i> <b>Raisecom(config-gigaethernet1/1/port)#bandwidth</b> { <b>ingress</b>   <b>egress</b> } <b>vlan</b> <i>vlan-id coslist cos-value-list bwp-profile-id</i>	Apply the bandwidth guarantee profile on the interface+VLAN+CoS.



### Note

If a bandwidth guarantee profile is used by other profiles or applied, it cannot be deleted.

## 7.7.5 Configuring hierarchical bandwidth guarantee

### Creating hierarchical CoS bandwidth guarantee

Create a hierarchical CoS bandwidth guarantee for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#bandwidth-profile</b> <i>profile-id cir cir cbs cbs [ eir eir ebs ebs ] [ color-aware ]</i>	Create a bandwidth guarantee profile.
3	<b>Raisecom(config)#hierarchy-cos bandwidth-profile</b> <i>hc-profile-id</i>	Create a hierarchical CoS profile, and enter HCoS configuration mode.
4	<b>Raisecom(config-hcos)#bandwidth coslist</b> <i>cos-list bwp-profile-id</i> <b>Raisecom(config-hcos)#exit</b>	Configure the hierarchical CoS profile.
5	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i> <b>Raisecom(config-gigaethernet1/1/port)#bandwidth</b> { <b>ingress</b>   <b>egress</b> } <b>vlan</b> <i>vlan-id bwp-profile-id hierarchy-cos hc-profile-id</i>	Apply the hierarchical CoS profile on the ingress interface+VLAN.

## Configuring hierarchical VLAN bandwidth guarantee

Create a hierarchical VLAN bandwidth guarantee for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#bandwidth-profile</b> <i>profile-id cir cir cbs cbs [ eir eir ebs ebs ] [ color-aware ]</i>	Create a bandwidth guarantee profile.
3	<b>Raisecom(config)#hierarchy-vlan</b> <b>bandwidth-profile</b> <i>hv-profile-id</i>	Create a hierarchical VLAN profile, and enter Hvlan configuration mode.
4	<b>Raisecom(config-hvlan)#bandwidth</b> <b>vlanlist</b> <i>vlan-list profile-id</i> <b>Raisecom(config-hvlan)#exit</b>	Configure the hierarchical VLAN profile.
5	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i> <b>Raisecom(config-</b> <b>gigaethernet1/1/*)#bandwidth { ingress</b> <b>  egress } bwp-profile-id hierarchy-</b> <b>vlan</b> <i>hv-profile-id</i>	Apply the hierarchical VLAN profile on the ingress or egress interface.



### Note

If a hierarchical bandwidth guarantee profile is applied, it cannot be deleted or modified.

## 7.7.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show bandwidth-profile</b> [ <i>bwp-profile-id</i> ]	Show information about the bandwidth guarantee profile.
2	<b>Raisecom#show bandwidth interface</b> <i>interface-type interface-number</i>	Show information about the bandwidth guarantee profile on the interface.
3	<b>Raisecom#show hierarchy-cos-bandwidth profile</b> [ <i>hc-profile-id</i> ]	Show information about the hierarchical CoS bandwidth guarantee profile.
4	<b>Raisecom#show hierarchy-vlan-bandwidth profile</b> [ <i>hv-profile-id</i> ]	Show information about the hierarchical VLAN bandwidth guarantee profile.



## 7.8 Configuration examples

### 7.8.1 Example for configuring congestion management

#### Networking requirements

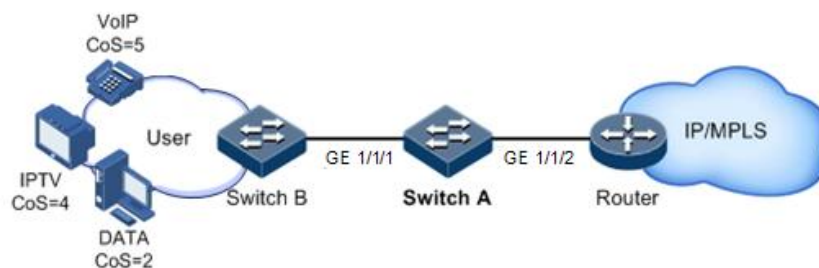
As shown in Figure 7-9, the user use voice, video and data services.

CoS of voice service is 5, CoS of video service is 4, and CoS of data service is 2. The local priorities for these three types of services are mapping 6, 5, and 2 respectively.

Congestion can easily occur on Switch A. To reduce network congestion, make the following rules according to different services types:

- For voice service, perform SP scheduling to grant high priority.
- For video service, perform WRR scheduling, with weight value of 50.
- For data service, perform WRR scheduling, with weight value of 20.

Figure 7-9 Queue scheduling networking



#### Configuration steps

Step 1 Configure interface priority trust mode.

```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#mls qos trust cos
SwitchA(config-gigabitEthernet1/1/2)#quit
```

Step 2 Configure the profile for mapping from CoS to local priority.

```
SwitchA(config)#mls qos mapping cos-to-local-priority 1
SwitchA(cos-to-pri)#cos 5 to local-priority 6
SwitchA(cos-to-pri)#cos 4 to local-priority 5
SwitchA(cos-to-pri)#cos 2 to local-priority 2
SwitchA(cos-to-pri)#quit
```

Step 3 Apply the profile for mapping from CoS to local priority on GE 1/1/2.

```
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#mls qos cos-to-local-priority 1
SwitchA(config-gigabitEthernet1/1/2)#quit
```

Step 4 Conduct SP+WRR queue scheduling in the egress direction of GE 1/1/1.

```
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#mls qos queue scheduler wrr 1 1 20 1 1
50 0 0
SwitchA(config-gigabitEthernet1/1/1)#quit
```

## Checking results

Use the following command to show priority trust mode on the interface.

```
Raisecom#show mls qos interface
```

Interface	TrustMode	Priority	Cos-PriProfile	Dscp-
PriProfile	Dscp-Mutation	Cos-Remark		
gigabitEthernet1/1/1	cos	0	0	0
gigabitEthernet1/1/2	cos	0	1	0
...				

Use the following command to show configurations of mapping from CoS to local priority

```
Raisecom#show mls qos mapping cos-to-local-priority
```

G:GREEN  
Y:YELLOW  
R:RED

cos-to-localpriority(color)

Index	Description	Ref	CoS:	0	1	2	3	4
5	6	7						
1	6(G)	1	localpri(color)	0(G)	1(G)	2(G)	3(G)	5(G)
6(G)	6(G)	7(G)						

Use the following command to show configurations of queue scheduling on the interface.

```
Raisecom#show mls qos queue interface gig Ethernet 1/1/1
gig Ethernet1/1/1
Queue      Weight(WRR)
-----
1
2          1
3          20
4          1
5          1
6          50
7          0
```

## 7.8.2 Example for configuring rate limiting based on traffic policy

### Networking requirements

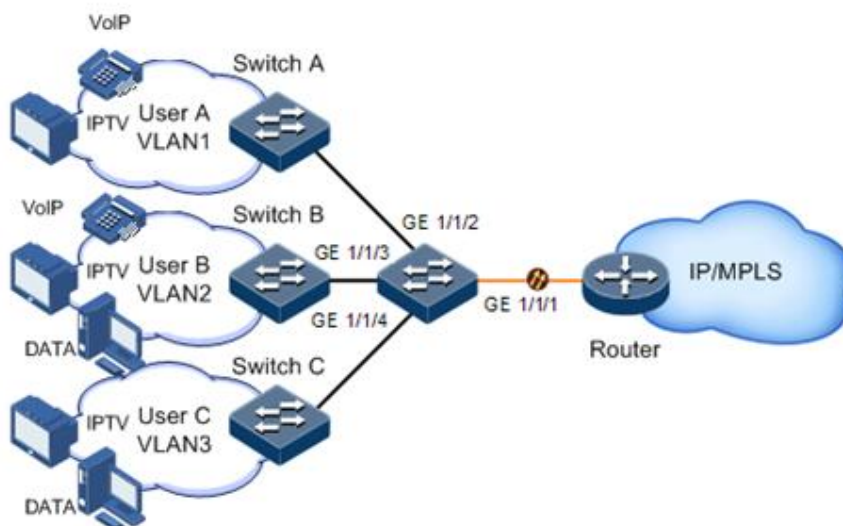
As show in Figure 7-10, User A, User B, and User C respectively belong to VLAN 1, VLAN 2, and VLAN 3, and are connected to the ISCOM2600G-HI series switch by Switch A, Switch B, and Switch C.

User A uses voice and video services, User B uses voice, video and data services, and User C uses video and data services.

According to service requirements, user needs to make rules as below.

- Provide User A with 25 Mbit/s guaranteed bandwidth, permitting burst flow of 100 Kbytes and discarding excess flow.
- Provide User B with 35 Mbit/s guaranteed bandwidth, permitting burst flow of 100 Kbytes and discarding excess flow.
- Provide User C with 30 Mbit/s guaranteed bandwidth, permitting burst flow of 100 Kbytes and discarding excess flow.

Figure 7-10 Rate limiting based on traffic policy



## Configuration steps

Step 1 Create and configure the traffic class, and classify users by VLAN ID.

```
Raisecom#config  
Raisecom(config)#class-map usera match-any  
Raisecom(config-cmap)#match vlan 1  
Raisecom(config-cmap)#quit  
Raisecom(config)#class-map userb match-any  
Raisecom(config-cmap)#match vlan 2  
Raisecom(config-cmap)#quit  
Raisecom(config)#class-map userc match-any  
Raisecom(config-cmap)#match vlan 3  
Raisecom(config-cmap)#quit
```

Step 2 Create rate limiting rules.

```
Raisecom(config)#mls qos policer-profile usera single  
Raisecom(traffic-policer)#cir 25000 cbs 100  
Raisecom(traffic-policer)#drop-color red  
Raisecom(traffic-policer)##quit  
Raisecom(config)#mls qos policer-profile userb single  
Raisecom(traffic-policer)#cir 35000 cbs 100  
Raisecom(traffic-policer)#drop-color red  
Raisecom(traffic-policer)##quit  
Raisecom(config)#mls qos policer-profile userc single  
Raisecom(traffic-policer)#cir 30000 cbs 100  
Raisecom(traffic-policer)#drop-color red  
Raisecom(traffic-policer)##quit
```

Step 3 Create and configure the traffic policy.

```
Raisecom(config)#policy-map usera  
Raisecom(config-pmap)#class-map usera  
Raisecom(config-pmap-c)#police usera  
Raisecom(config-pmap-c)#quit  
Raisecom(config-pmap)#quit  
Raisecom(config)#interface gigabitEthernet 1/1/1  
Raisecom(config-gigabitEthernet1/1/1)#service-policy ingress usera  
Raisecom(config-gigabitEthernet1/1/1)#exit  
Raisecom(config)#policy-map userb  
Raisecom(config-pmap)#class-map userb  
Raisecom(config-pmap-c)#police userb  
Raisecom(config-pmap-c)#quit  
Raisecom(config-pmap)#quit  
Raisecom(config)#interface gigabitEthernet 1/1/2  
Raisecom(config-gigabitEthernet1/1/2)#service-policy ingress userb  
Raisecom(config-gigabitEthernet1/1/2)#exit  
Raisecom(config)#policy-map userc
```

```
Raisecom(config-pmap)#class-map userc
Raisecom(config-pmap-c)#police userc
Raisecom(config-pmap-c)#quit
Raisecom(config-pmap)#quit
Raisecom(config)#interface gigabitEthernet 1/1/3
Raisecom(config-gigabitEthernet1/1/3)#service-policy userc ingress 4
Raisecom(config-gigabitEthernet1/1/1)#exit
```

## Checking results

Use the **show class-map** command to show configurations of traffic classification.

```
Raisecom#show class-map usera
Class Map match-any usera (id 0)(ref 1)
  Match vlan 1
Raisecom#show class-map userb
Class Map match-any userb (id 1)(ref 1)
  Match vlan 2
Raisecom#show class-map userc
Class Map match-any userb (id 2)(ref 1)
  Match vlan 3
```

Use the **show mls qos policer** command to show configurations of rate limiting rules.

```
Raisecom(config)#show mls qos policer
single-policer: USERC      mode:flow   color:blind
cir: 30000 kbps  cbs: 100 kB

single-policer: usera      mode:flow   color:blind
cir: 25000 kbps  cbs: 100 kB

single-policer: userb      mode:flow   color:blind
cir: 35000 kbps  cbs: 100 kB
```

Use the **show policy-map** command to show configurations of traffic policy.

```
Raisecom(config)#show policy-map
Policy Map usera
  Class usera
    police usera

Policy Map userb
  Class userb
    police userb

Policy Map userc
  Class userc
```

police userc

## 7.8.3 Example for configuring rate limiting based on interface

### Networking requirements

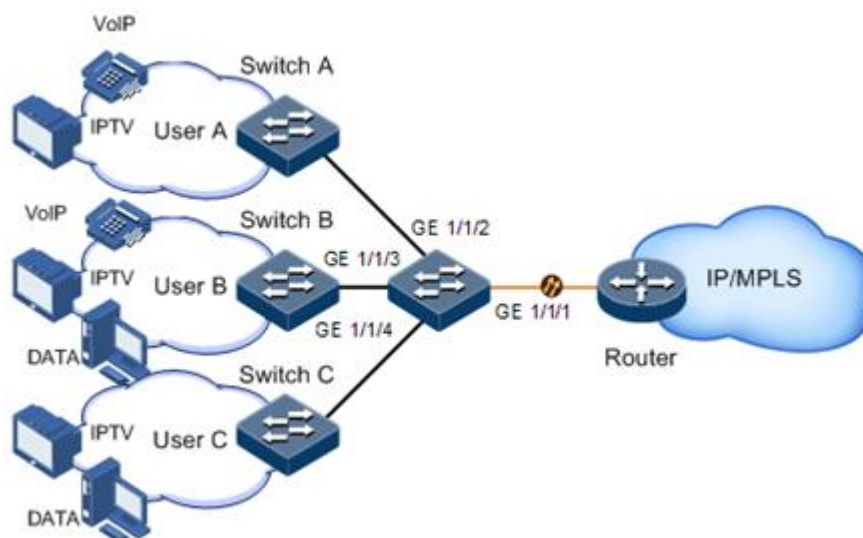
As shown in Figure 7-11, User A, User B, and User C are respectively connected to the ISCOM2600G-HI series switch by Switch A, Switch B, and Switch C.

User A uses voice and video services. User B uses voice, video and data services. User C uses video and data services.

According to service requirements, make rules as below.

- Provide User A with 25 Mbit/s guaranteed bandwidth, permitting burst flow of 100 Kbytes and discarding excess flow.
- Provide User B with 35 Mbit/s guaranteed bandwidth, permitting burst flow of 100 Kbytes and discarding excess flow.
- Provide User C with 30 Mbit/s guaranteed bandwidth, permitting burst flow of 100 Kbytes and discarding excess flow.

Figure 7-11 Rate limiting based on interface



### Configuration steps

Configure rate limiting based on interface.

```
Raisecom#config
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#rate-limit ingress cir 25000 cbs 100
Raisecom(config-gigabitEthernet1/1/1)#exit
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#rate-limit ingress cir 35000 cbs 100
Raisecom(config-gigabitEthernet1/1/2)#exit
```

```
Raisecom(config)#interface gig Ethernet 1/1/3
Raisecom(config-gig Ethernet1/1/3)#rate-limit ingress cir 30000 cbs 100
Raisecom(config-gig Ethernet1/1/3)#exit
```

## Checking results

Use the **show rate-limit port-list** command to show configurations of rate limiting based on interface.

```
Raisecom(config)#show rate-limit interface
```

Interface	Direction	Cir(kbps)	Cbs(kb)
CirOper(kbps)	CbsOper(kb)		
-----			
gig Ethernet1/1/1	ingress	25000	100
101			25024
gig Ethernet1/1/2	ingress	30000	100
101			30016
gig Ethernet1/1/3	ingress	30000	100
101			30016

# 8 Multicast

---

This chapter describes basic principles and configuration procedures for multicast, and provides related configuration examples, including the following sections:

- Multicast
- Basic functions of Layer 2 multicast
- IGMP Snooping
- IGMP Querier
- IGMP MVR
- IGMP filtering
- Multicast VLAN copy
- MLD

## 8.1 Multicast

With the continuous development of Internet, more and more interactive data, voice, and video of various types emerge on the network. On the other hand, the emerging e-commerce, online meetings, online auctions, video on demand, remote learning, and other services also rise gradually. These services bring higher requirements on network bandwidth, information security, and paid feature. Traditional unicast and broadcast cannot meet these requirements well, while multicast has met them timely.

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

### Comparison among unicast, broadcast, and multicast

Multicast is a kind of packets transmission method which is parallel with unicast and broadcast.

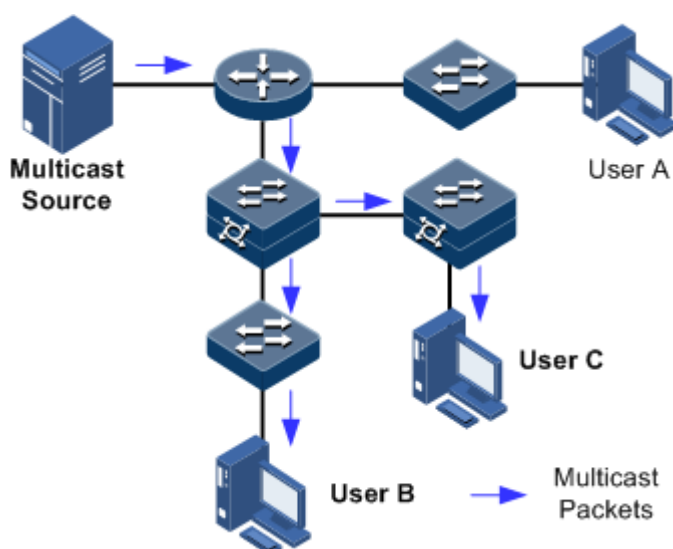
- Unicast: the system establishes a data transmission path for each user who needs the information, and sends separate copy information about them. Through unicast, the amount of information transmitted over the network is proportional to the number of users, so when the number of users becomes huge, there will be more identical information on the network. In this case, bandwidth will become a bottleneck, and unicast will not be conducive to transmission of large-scale information.



- Broadcast: the system sends information to all users regardless of whether they need or not, so any user will receive it. Through broadcast, the information source delivers information to all users in the segment, which fails to guarantee information security and paid service. In addition, when the number of users who require this kind of information decreases, the utilization of network resources will be very low, and the bandwidth will be wasted seriously.
- Multicast: when some users in the network need specific information, the sender only sends one piece of information, then the transmitted information can be reproduced and distributed in fork junction as far as possible.

As shown in Figure 8-1, assume that User B and User C need information, you can use multicast transmission to combine User B and User C to a receiver set, then the information source just needs to send one piece of information. Each switch on the network will establish their multicast forwarding table according to IGMP packets, and finally transmits the information to the actual receiver User B and User C.

Figure 8-1 Multicast transmission networking



In summary, the unicast is for a network with sparse users and broadcast is for a network with dense users. When the number of users in the network is uncertain, unicast and broadcast will present low efficiency. When the number of users are doubled and redoubled, the multicast mode does not need to increase backbone bandwidth, but sends information to the user in need. These advantages of multicast make itself become a hotspot in study of the current network technology.

## Advantages and application of multicast

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

- Improve efficiency: reduce network traffic, relieve server and CPU load.
- Optimize performance: reduce redundant traffic and guarantee information security.
- Support distributed applications: solve the problem of point-point data transmission.

The multicast technology is used in the following aspects:

- Multimedia and streaming media, such as, network television, network radio, and realtime video/audio conferencing

- Training, cooperative operations communications, such as: distance education, telemedicine
- Data warehousing and financial applications (stock)
- Any other point-to-multipoint applications

## Basic concepts in multicast

- Multicast group

A multicast group refers to the recipient set using the same IP multicast address identification. Any user host (or other receiving device) will become a member of the group after joining the multicast group. They can identify and receive multicast data with the destination address as IP multicast address.

- Multicast group members

Each host joining a multicast group will become a member of the multicast group. Multicast group members are dynamic, and hosts can join or leave multicast group at any time. Group members may be widely distributed in any part of the network.

- Multicast source

A multicast source refers to a server which regards multicast group address as the destination address to send IP packet. A multicast source can send data to multiple multicast groups; multiple multicast sources can send to a multicast group.

- Multicast router

A multicast router is a router that supports Layer 3 multicast. The multicast router can achieve multicast routing and guide multicast packet forwarding, and provide multicast group member management to distal segment connecting with users.

- Routed interface

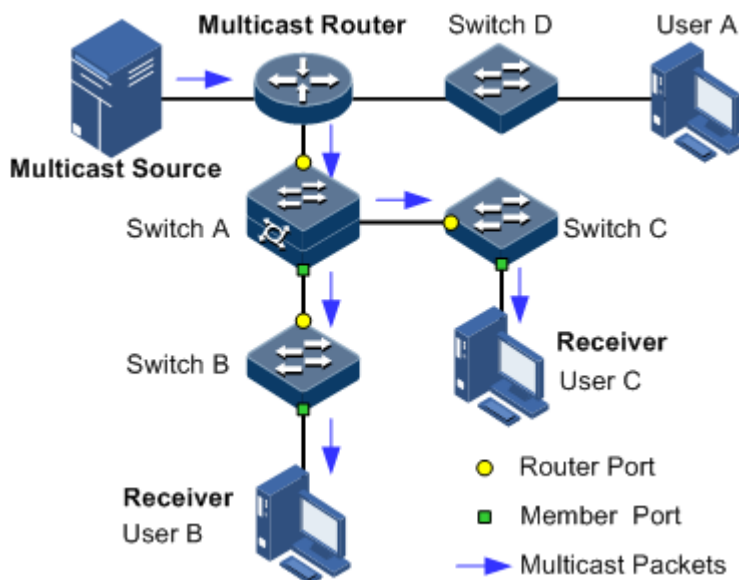
A routed interface refers to the interface towards the multicast router between a multicast router and a host. The ISCOM2600G-HI series switch receives multicast packets from this interface.

- Member interface

Known as the Rx interface, a member interface is the interface towards the host between multicast router and the host. The ISCOM2600G-HI series switch sends multicast packets from this interface.

Figure 8-2 shows basic concepts in multicast.

Figure 8-2 Basic concepts in multicast



## Multicast address

To make multicast source and multicast group members communicate across the Internet, you need to provide network layer multicast address and link layer multicast address, namely, the IP multicast address and multicast MAC address.

- IP multicast address

Internet Assigned Numbers Authority (IANA) assigns Class D address space to IPv4 multicast; the IPv4 multicast address ranges from 224.0.0.0 to 239.255.255.255.

- Multicast MAC address

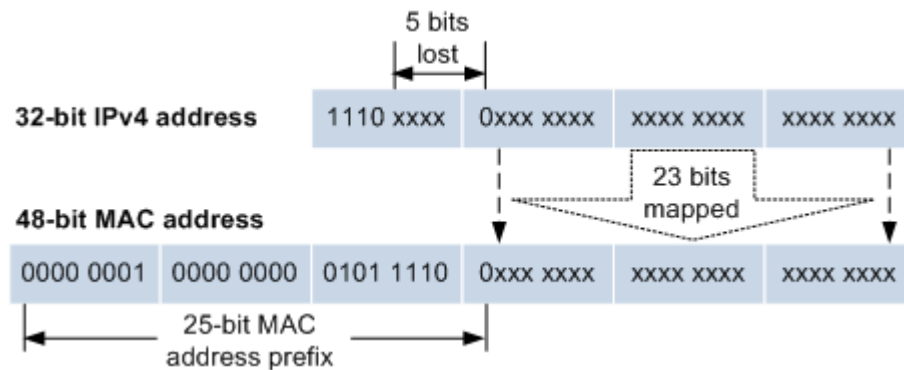
When the Ethernet transmits unicast IP packets, it uses the MAC address of the receiver as the destination MAC address. However, when multicast packets are transmitted, the destination is no longer a specific receiver, but a group with an uncertain number of members, so the Ethernet needs to use the multicast MAC address.

The multicast MAC address identifies receivers of the same multicast group on the link layer.

According to IANA, high bit 24 of the multicast MAC address are 0x01005E, bit 25 is fixed to 0, and the low bit 23 corresponds to low bit 23 of the IPv4 multicast address.

Figure 8-3 shows mapping between the IPv4 multicast address and MAC address.

Figure 8-3 Mapping between IPv4 multicast address and multicast MAC address



The first 4 bits of IP multicast address are 1110, indicating multicast identification. In the last 28 bits, only 23 bits are mapped to the multicast MAC address, and the missing of 5 bits makes 32 IP multicast addresses mapped to the same multicast MAC address. Therefore, in Layer 2, the ISCOM2600G-HI series switch may receive extra data besides IPv4 multicast group, and these extra multicast data needs to be filtered by the upper layer on the ISCOM2600G-HI series switch.

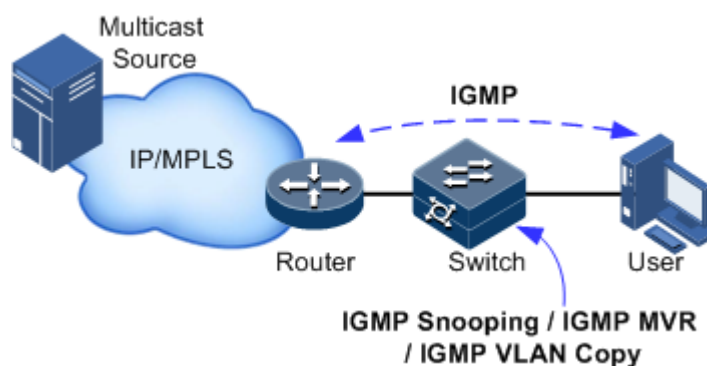
## Basis of multicast protocol

To implement complete set of multicast services, you need to deploy a variety of multicast protocols in various positions of network and make them cooperate with each other.

Typically, IP multicast working at network layer is called Layer 3 multicast, so the corresponding multicast protocol is called Layer 3 multicast protocol, including Internet Group Management Protocol (IGMP). IP multicast working at data link layer is called Layer 2 multicast, so the corresponding multicast protocol is called Layer 2 multicast protocol, including Internet Group Management Protocol (IGMP) Snooping.

Figure 8-4 shows operating of IGMP and Layer 2 multicast features.

Figure 8-4 Operating of IGMP and Layer 2 multicast features



IGMP, a protocol in TCP/IP protocol suite, is responsible for managing IPv4 multicast members. IGMP runs between the multicast router and host, defines the establishment and maintenance mechanism of multicast group membership between hosts and the multicast router. IGMP is not involved in transmission and maintenance of group membership between multicast routers, which is completed by the multicast routing protocol.

IGMP manages group members through interaction of IGMP packets between the host and multicast router. IGMP packets are encapsulated in IP packets, including Query packets, Report packets, and Leave packets. Basic functions of IGMP are as below:

- The host sends Report packets to join the multicast group, sends Leave packets to leave the multicast group, and automatically determines which multicast group packets to receive.
- The multicast router sends Query packets periodically, and receives Report packets and Leave packets from hosts to understand the multicast group members in connected segment. The multicast data will be forwarded to the segment if there are multicast group members, and not forward if there are no multicast group members.

Up to now, IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3. The newer version is fully compatible with the older version. Currently the most widely used version is IGMPv2, while IGMPv1 does not support the Leave packet.

Layer 2 multicast runs on Layer 2 devices between the host and multicast router.

Layer 2 multicast manages and controls multicast groups by monitoring and analyzing IGMP packets exchanged between hosts and multicast routers to implement forwarding multicast data at Layer 2 and suppress multicast data diffusion at Layer 2.

## Supported multicast features

The ISCOM2600G-HI series switch supports the following multicast features:

- Basic functions of IGMP
- IGMP Snooping
- IGMP Multicast VLAN Registration (MVR)
- IGMP filtering



### Note

- Any two of IGMP Snooping, IGMP MVR, and multicast VLAN copy cannot be concurrently enabled in the same multicast VLAN. Multicast VLAN copy and IGMP MVR cannot be enabled concurrently in the same multicast group of the same multicast VLAN.
- The ISCOM2600G-HI series switch supports IGMPv1, IGMPv2, and IGMPv3.

## 8.2 Basic functions of Layer 2 multicast

### 8.2.1 Introduction

Basic IGMP functions are as below:

- Assign the multicast router interface.
- Enable immediate leave.
- Configure multicast forwarding entries and the aging time of router interfaces.
- Enable IGMP ring network forwarding.

Basic functions of Layer 2 multicast provide Layer 2 multicast common features, which must be used on the ISCOM2600G-HI series switch enabled with IGMP Snooping or IGMP MVR.



## Note

Configurations of basic function take effect on IGMP Snooping or IGMP MVR concurrently.

The concepts related to IGMP basic functions are as below.

## Multicast router interface

The router interface can be learnt dynamically (learnt through IGMP query packets, on the condition that the multicast routing protocol is enabled on multicast routers) on Layer 2 multicast switch, or configured manually to forward downstream multicast report and leave packets to the router interface.

The router interface learnt dynamically has an aging time, while the router interface configured manually will not be aged.

## Aging time

The configured aging time takes effect on both multicast forwarding entries and the router interface.

On Layer 2 switch running multicast function, each router interface learnt dynamically starts a timer, of which the expiration time is the aging time of IGMP Snooping. The router interface will be deleted if no IGMP Query packets are received in the aging time. The timer of the router interface will be updated when an IGMP Query packet is received.

Each multicast entry starts a timer, namely, the aging time of a multicast member. The expiration time is IGMP Snooping aging time. The multicast member will be deleted if no IGMP Report packets are received in the aging time. Update timeout for multicast entry when receiving IGMP Report packets. The timer of the multicast entry will be updated when an IGMP Report packet is received.

## Immediate leave

On Layer 2 switch running multicast function, the system will not delete the corresponding multicast entry immediately, but wait until the entry is aged after sending Leave packets. You can enable this function to delete the corresponding multicast entry quickly when there are a large number of downstream users and adding or leaving is more frequently required.



## Note

IGMPv2/v3 supports immediate leave.

## IGMP ring network forwarding

On Layer 2 switch running multicast function, IGMP ring network forwarding can be enabled on any type of interfaces.

Enabling IGMP ring network forwarding can implement multicast backup protection on the ring network, make multicast services more stable, and prevent link failure from causing multicast service failure.

IGMP ring network forwarding can be applied to the RRPS ring, STP/RSTP/MSTP ring, and G.8032 ring.

## 8.2.2 Preparing for configurations

### Scenario

Basic functions of Layer 2 multicast provide common features of Layer 2 multicast, and must be used on the ISCOM2600G-HI series switch enabled with IGMP Snooping or IGMP MVR.

### Prerequisite

- Disable IGMP MVR and multicast VLAN copy in the Snooping multicast VLAN.
- Add related interfaces to VLANs.

## 8.2.3 Default configurations of Layer 2 multicast basic functions

Default configurations of Layer 2 multicast basic functions are as below.

Function	Default value
IGMP immediate leave status	Disable
Aging time of multicast entries	260s
Interface IGMP ring network forwarding status	Disable

## 8.2.4 Configuring basic functions of Layer 2 multicast

Configure basic functions of Layer 2 multicast for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#igmp mrouter vlan <i>vlan-id</i> interface-type interface-number</b>	(Optional) configure the multicast router interface.
3	<b>Raisecom(config)#igmp member- timeout { seconds   infinite }</b>	(Optional) configure the aging time of IGMP members.
4	<b>Raisecom(config)#igmp ring interface-type interface- number-list</b>	(Optional) enable IGMP ring network forwarding on the interface.
5	<b>Raisecom(config)#igmp report- suppression</b>	(Optional) enable Report suppression.
6	<b>Raisecom(config)#igmp version {2 3}</b>	(Optional) configure the IGMP version.
7	<b>Raisecom(config)#igmp snooping mrouter vlan <i>vlan-list</i> priority <i>priority-number</i></b>	(Optional) configure the CoS priority of the IGMP route VLAN.

Step	Command	Description
8	<code>Raisecom(config-gigaethernet1/1/port)#igmp immediate-leave vlan <i>vlan-list</i></code>	(Optional) configure immediate leave. If immediate leave is disabled on the downlink interface, the router interface, after receiving a Leave packet, will calculate the aging time according to robust factor and configure the expiration time for a member to leave the group as Group Membership Interval (GMI). $GMI = robust-value * lastmember-queryinterval$ .

## 8.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show igmp configuration</code>	Show IGMP basic configurations.
2	<code>Raisecom#show igmp mrouter</code>	Show configurations of the multicast route interface.
3	<code>Raisecom#show igmp immediate-leave [ <i>interface-type interface-number</i> ]</code>	Show configuration of immediate leave on Layer 2 multicast.
4	<code>Raisecom#show igmp statistics [ <i>interface-type interface-number</i> ]</code>	Show Layer 2 multicast statistics.
5	<code>Raisecom#show igmp snooping mrouter vlan-priority</code>	Show the CoS priority of the IGMP route VLAN.
6	<code>Raisecom#show igmp ring</code>	Show information about the IGMP ring network.

## 8.2.6 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
<code>Raisecom(config)#clear igmp statistics [ <i>interface-type interface-number</i> ]</code>	Clear statistics about Layer 2 multicast IGMP.
<code>Raisecom(config)#no igmp member <i>interface-type interface-number</i></code>	Delete a specified multicast entry.



## 8.3 IGMP Snooping

### 8.3.1 Introduction

IGMP Snooping is a multicast constraining mechanism running on Layer 2 devices, used for managing and controlling multicast groups, and implementing Layer 2 multicast.

IGMP Snooping allows the ISCOM2600G-HI series switch to monitor IGMP sessions between the host and multicast router. When monitoring a group of IGMP Report from host, the ISCOM2600G-HI series switch will add host-related interface to the forwarding entry of this group. Similarly, when a forwarding entry reaches the aging time, the ISCOM2600G-HI series switch will delete host-related interface from the forwarding table.

IGMP Snooping forwards multicast data through Layer 2 multicast entry. When receiving multicast data, the ISCOM2600G-HI series switch will forward them directly according to the corresponding receiving interface of the multicast entry, instead of flooding them to all interfaces, to save bandwidth of the ISCOM2600G-HI series switch effectively.

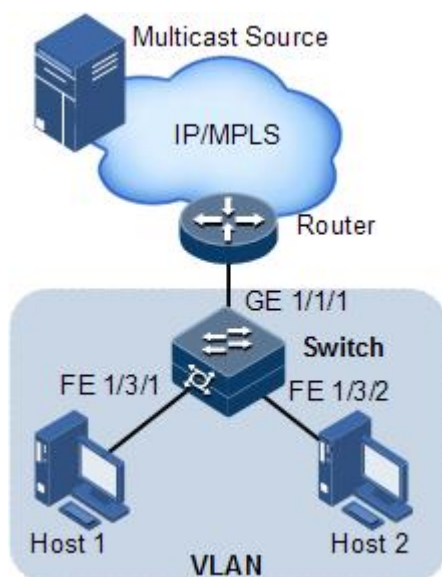
IGMP Snooping establishes a Layer 2 multicast forwarding table, of which entries can be learnt dynamically or configured manually.

### 8.3.2 Preparing for configurations

#### Scenario

As shown in Figure 8-5, multiple hosts belonging to a VLAN receive data from the multicast source. You can enable IGMP Snooping on the Switch that connects the multicast router and hosts. By listening IGMP packets transmitted between the multicast router and hosts, creating and maintaining the multicast forwarding table, you can implement Layer 2 multicast.

Figure 8-5 IGMP Snooping networking



#### Prerequisite

- Disable multicast VLAN copy on the ISCOM2600G-HI series switch.

- Create VLANs.
- Add related interfaces to the VLANs.

### 8.3.3 Default configurations of IGMP Snooping

Default configurations of IGMP Snooping are as below.

Function	Default value
Global IGMP Snooping status	Disable
VLAN IGMP Snooping status	Disable
IGMP robustness	2

### 8.3.4 Configuring IGMP Snooping

Configure IGMP Snooping for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#igmp snooping</b>	Enable global IGMP Snooping.
3	<b>Raisecom(config)#igmp member time-out { seconds   infinite }</b>	(Optional) configure the aging time of IGMP members.
4	<b>Raisecom(config)#igmp snooping vlan vlan-list</b>	(Optional) enable IGMP Snooping on all VLANs.
5	<b>Raisecom(config)#vlan vlan-id</b> <b>Raisecom(config-vlan)#igmp snooping static ip-address [ interface-type interface-number ]</b>	(Optional) configure static members of IGMP Snooping in VLAN mode.
6	<b>Raisecom(config)#interface interface-type interface-number</b> <b>Raisecom(config-gigaethernet1/1/port)#igmp snooping host-join group-address vlan vlan-id</b>	Configure the host joining function.



#### Note

- IGMP Snooping and IGMP MVR cannot be enabled concurrently in the same multicast VLAN. Otherwise, the configuration will fail.
- IGMP Snooping and multicast VLAN copy cannot be enabled concurrently in the same multicast VLAN. Otherwise, the configuration will fail.

### 8.3.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show igmp snooping [ vlan <i>vlan-id</i>   member vlan <i>vlan-list</i>   mrouter <i>vlan-priority</i> ]</b>	Show configurations of IGMP Snooping.
2	<b>Raisecom#show igmp snooping member [ <i>interface-type interface-number</i>   vlan <i>vlan-id</i> ]</b>	Show information about multicast group members of IGMP Snooping.
3	<b>Raisecom#show igmp snooping member count [ <i>interface-type interface-number</i>   vlan <i>vlan-id</i> ]</b>	Show the number of multicast group members of IGMP Snooping.

## 8.3.6 Example for applying multicast on ring network

### Networking requirements

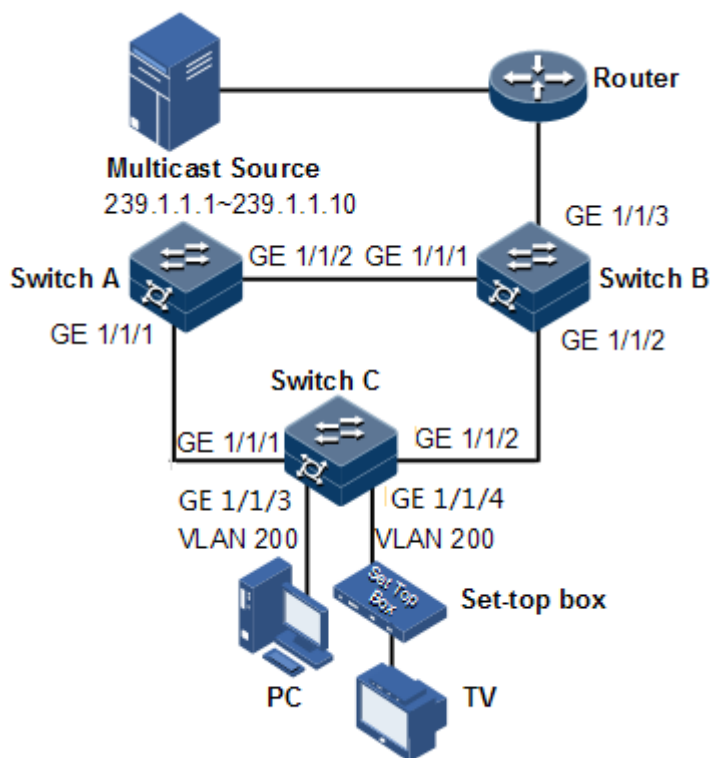
Configure IGMP ring forwarding on single Ethernet ring to make multicast service more stable and prevent multicast service from being disrupted by link failure.

As shown in Figure 8-6, GE 1/1/1 and GE 1/1/2 on Switch A, GE 1/1/1 and GE 1/1/2 on Switch B, GE 1/1/1 and GE 1/1/2 on Switch C form a physical ring. Multicast traffic is input from GE 1/1/1 on Switch B. The customer demands multicast traffic through GE 1/1/3 and GE 1/1/4 on Switch C. By doing this, it will not affect user's on-demand multicast stream whichever link fails in the Switch.

When using single Ethernet ring to provide multicast services, you can adopt IGMP MVR or IGMP Snooping to receive the multicast traffic.

The following example shows that STP provides ring network detection and IGMP Snooping provides multicast function.

Figure 8-6 Ring network multicast networking



## Configuration steps

Step 1 Enable STP, create a VLAN, and add interfaces to the VLAN.

Configure Switch A.

```
SwitchA#config
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree mode stp
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/1)#switchport trunk native vlan 200
SwitchA(config-gigabitEthernet1/1/1)#exit
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/2)#switchport trunk native vlan 200
```

Configure Switch B.

```
SwitchB#config
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree mode stp
SwitchB(config)#interface gigabitEthernet 1/1/1
```

```
SwitchB(config-gigaethernet1/1/1)switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#switchport trunk native vlan 200
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#switchport trunk native vlan 200
```

Configure Switch C.

```
SwitchC#config
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree mode stp
SwitchC(config)#interface gigaethernet 1/1/1
SwitchC(config-gigaethernet1/1/1)#switchport mode trunk
SwitchC(config-gigaethernet1/1/1)#switchport trunk native vlan 200
SwitchC(config-gigaethernet1/1/1)#exit
SwitchC(config)#interface gigaethernet 1/1/2
SwitchC(config-gigaethernet1/1/2)#switchport mode trunk
SwitchC(config-gigaethernet1/1/2)#switchport trunk native vlan 200
```

Step 2 Enable IGMP Snooping and IGMP ring network forwarding on the interface.

Configure Switch A.

```
SwitchA(config)#igmp ring gigaethernet 1/1/1
SwitchA(config)#igmp ring gigaethernet 1/1/2
SwitchA(config)#igmp snooping
SwitchA(config)#igmp snooping vlan 200
```

Configure Switch B.

```
SwitchB(config)#igmp ring gigaethernet 1/1/1
SwitchB(config)#igmp ring gigaethernet 1/1/2
SwitchB(config)#igmp snooping
SwitchB(config)#igmp snooping vlan 200
```

Configure Switch C.

```
SwitchC(config)#igmp ring gigaethernet 1/1/1
SwitchC(config)#igmp ring gigaethernet 1/1/2
SwitchC(config)#igmp snooping
```

## Checking results

Disconnect any link in the ring, and check whether the multicast flow can be received normally.

## 8.4 IGMP Querier

### 8.4.1 Introduction

MVR Querier is an MVR protocol proxy mechanism. It runs on Layer 2 devices to assist in managing and controlling multicast groups. MVR Querier will terminate IGMP packets. It can agent host functions upstream and also proxy multicast router functions downstream. The Layer 2 network device enabled with MVR Querier has two roles:

- At the user side, it is a query builder and undertakes the role of the server, sending Query packets and periodically checking user information, and processing the Report and Leave packets from users.
- At the network routing side, it is a host and undertakes the role of the client, responding the multicast router Query packet and sending Report and Leave packets. It sends the user information to the network as required.

The proxy mechanism can control and access user information effectively, and reduce the network side protocol packet and network load.

IGMP Querier establishes a multicast packet forwarding list by intercepting IGMP packets between the user and multicast routers.



#### Note

IGMP Querier is used in cooperation with IGMP Snooping/MVR.

The following concepts are related to IGMP Querier.

- IGMP packet suppression

IGMP packet suppression means that the switch filters identical Report packets. When receiving multiple Report packets from a multicast group member in a query interval, the switch sends the first Report packet to the multicast router only while it suppresses other identical Report packets, to reduce packet quantity on the network.



#### Note

When IGMP Snooping, IGMP MVR, or multicast VLAN copy is enabled, IGMP packet suppression can be enabled or disabled respectively.

- IGMP Querier

If a switch is enabled with this function, it can actively send IGMP Query packets to query information about multicast members on the interface. If it is disabled with this function, it only forwards IGMP Query packets from routers.



#### Note

When IGMP Snooping, IGMP MVR, or multicast VLAN copy is enabled, IGMP Querier can be enabled or disabled respectively.

- Source IP address of Query packets sent by IGMP Querier

IGMP querier sends the source IP address of Query packets. By default, the IP address of IP interface 0 is used. If the IP address is not configured, 0.0.0.0 is used. When receiving Query packets with IP address of 0.0.0.0, some hosts take it illegal and do not respond. Thus, specifying the IP address for the Query packet is recommended.

- Query interval

It is the query interval for common groups. The query message of common group is periodically sent by the switch in multicast mode to all hosts in the shared network segment, to query which multicast groups have members.

- Maximum response time for 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 added 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 the last member to send Query packets

It is also called the specified group query interval. It is the interval for the switch continues to send Query packets for the specified group when receiving IGMP Leave packet for a specified group by a host.

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 switch 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, the switch judges that the last member of the multicast group has left and thus deletes multicast forwarding entries.

## 8.4.2 Preparing for configurations

### Scenario

On a network with multicast routing protocol widely applied, multiple hosts and client subnets receive multicast information. Enable IGMP Querier on the switch connecting the multicast router and hosts to block IGMP packets between hosts and the multicast router and relieve the network load.

Configure IGMP Querier to relieve configuration and management of client subnet for the multicast router and to implement multicast connection with the client subnet.

IGMP Querier is used in cooperation with IGMP Snooping/MVR.

### Prerequisite

- Create VLANs.
- Add related interfaces to VLANs.

## 8.4.3 Default configurations of IGMP Querier

Default configurations of IGMP Querier area as below.

Function	Default value
IGMP Querier status	Disable
IGMP packet suppression status	Disable
Source IP address for IGMP Querier to send packets	Use the IP address of IP address 0. If IP interface 0 is not configured, use 0.0.0.0.
IGMP query interval	125s
Maximum response time to send Query packets	10s
Interval for the last member to send Query packets	1s

## 8.4.4 Configuring IGMP Querier

Configure IGMP Querier for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#igmp querier</b>	Enable IGMP Querier.
3	<b>Raisecom(config)#igmp source-ip <i>ip-address</i></b>	(Optional) configure the source IP address for the IGMP querier to send Query packets.
4	<b>Raisecom(config)#igmp querier query-interval <i>seconds</i></b>	(Optional) configure the IGMP query interval.
5	<b>Raisecom(config)#igmp querier query-max-response-time <i>seconds</i></b>	(Optional) configure the maximum response time to send Query packets.
6	<b>Raisecom(config)#igmp querier last-member-query-interval <i>seconds</i></b>	(Optional) configure the interval for the last member to send Query packets.
7	<b>Raisecom(config)#igmp proxy</b>	Configure IGMP proxy.



### Note

- When IGMP Querier is disabled, the following parameters can be configured: source IP address, query interval, maximum response time to send Query packets, and interval for the last member to send Query packets. After IGMP Querier is enabled, these configurations will take effect immediately.
- Though IGMP Snooping or IGMP MVR is enabled, IGMP Querier can be still enabled.
- IGMP Proxy and IGMP Querier are mutually exclusive. IGMP Proxy and IGMP report suppression are mutually exclusive.



## 8.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# <b>show igmp querier</b>	Show configurations of IGMP Querier.

## 8.4.6 Example for configuring IGMP Snooping and IGMP Querier

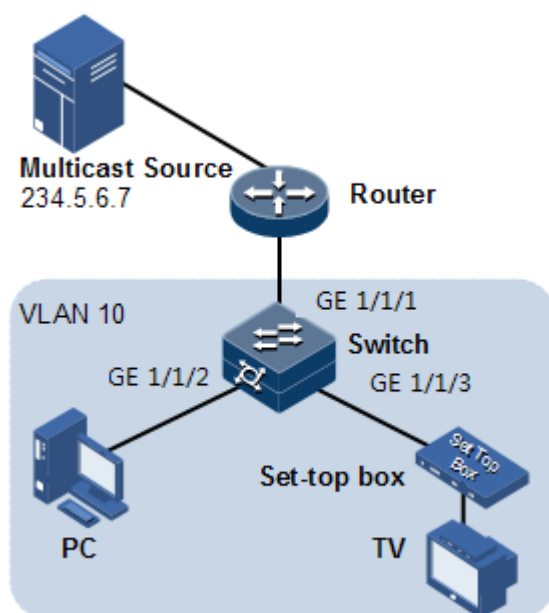
### Networking requirements

As shown in Figure 8-7, GE 1/1/1 on the switch is connected to the multicast router; GE 1/1/2 and GE 1/1/3 are connected to users. All multicast users belong to the same VLAN 10; you need to configure IGMP Snooping on the switch to receive multicast data with the address 234.5.6.7.

Enable the IGMP Querier on the switch to reduce communication between the hosts and multicast routers and implement the multicast function.

When the PC and set-top box are added to the same multicast group, the switch receives two IGMP Report packets and only sends one of them to the multicast router. The IGMP Query packet sent by the multicast router is not forwarded downstream, but the switch periodically sends IGMP Query packets.

Figure 8-7 IGMP Snooping networking



### Configuration steps

Step 1 Create VLANs and add interfaces to VLANs.

```
Raisecom#config
Raisecom(config)#create vlan 10 active
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#switchport mode trunk
Raisecom(config-gigabitEthernet1/1/2)#switchport trunk native vlan 10
Raisecom(config-gigabitEthernet1/1/2)#exit
Raisecom(config)#interface gigabitEthernet 1/1/3
Raisecom(config-gigabitEthernet1/1/3)#switchport access vlan 10
Raisecom(config-gigabitEthernet1/1/3)#exit
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#switchport access vlan 10
Raisecom(config-gigabitEthernet1/1/1)#exit
```

Step 2 Enable IGMP Snooping.

```
Raisecom(config)#igmp snooping
Raisecom(config)#igmp snooping vlan 10
```

Step 3 Configure IGMP Querier.

```
Raisecom(config)#igmp querier
Raisecom(config)#igmp source-ip 192.168.1.2
```

## Checking results

Use the following command to show configurations of IGMP Snooping.

```
Raisecom#show igmp snooping
IGMP snooping           :Enable
IGMP report-suppression :Disable
IGMP version            :v2
IGMP snooping active vlan :10
IGMP aging-time(s)      :260
IGMP ring               :--
```

Use the following command to show information about IGMP Snooping multicast group members.

```
Raisecom#show igmp snooping member vlan 10
R- ring port   D - Dynamic   S - Static
Vlan   Group                                     Port       Live-time(s)  Flag
-----
10     234.5.6.7                                GE1/1/1     --
D
```

Use the following command to show configurations of IGMP Querier.

```
Raisecom#show igmp querier
Global IGMP querier configuration:
-----
Querier Status           : Enable
Querier Source Ip        : 192.168.1.2
Query Interval(s)        :125
Query Max Response Interval(s) :10
Last Member Query Interval(s) :1
Robust Count             :2
Aging Time(s)            :60
Next General Query(s)     :--
```

## 8.5 IGMP MVR

### 8.5.1 Introduction

IGMP Multicast VLAN Registration (MVR) is multicast constraining mechanism running on Layer 2 devices, used for multicast group management and control and achieve Layer 2 multicast.

IGMP MVR adds member interfaces belonging to different user VLAN in switch to multicast VLAN by configuring multicast VLAN and makes different VLAN user uses one common multicast VLAN, then the multicast data will be transmitted only in one multicast VLAN without copying one for each user VLAN, thus saving bandwidth. At the same time, multicast VLAN and user VLAN are completely isolated which also increases the security.

Both IGMP MVR and IGMP Snooping can achieve Layer 2 multicast, but the difference is: multicast VLAN in IGMP Snooping is the same with user VLAN, while multicast VLAN in IGMP MVR can be different with user VLAN.



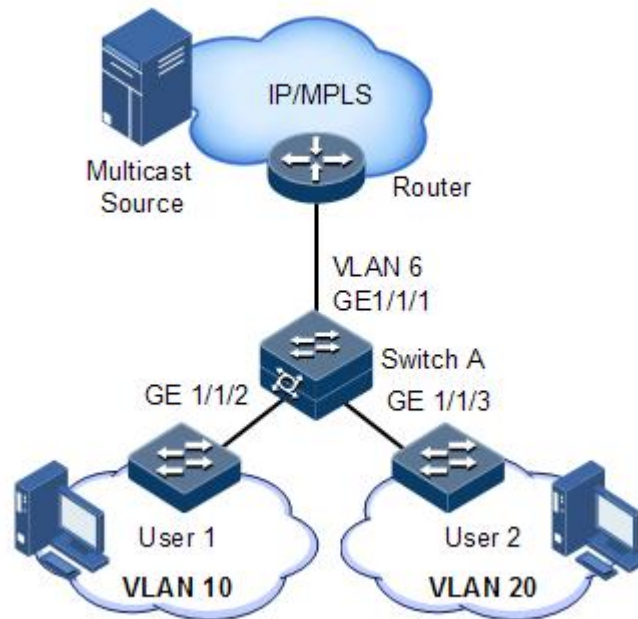
One switch can configure up to 10 multicast VLAN, at least one multicast VLAN and group addresses. The supported maximum number of multicast groups is 1024.

### 8.5.2 Preparing for configurations

#### Scenario

As shown in Figure 8-8, multiple users receive data from the multicast source. These users and the multicast router belong to different VLAN. Enable IGMP MVR on Switch A, and configure multicast VLAN. In this way, users in different VLAN can share a multicast VLAN to receive the same multicast data, and bandwidth waste is reduced.

Figure 8-8 IGMP MVR networking



### Prerequisite

- Disable multicast VLAN copy.
- Create VLANs.
- Add related interfaces to the VLANs.

## 8.5.3 Default configurations of IGMP MVR


Default configurations of MVR are as below.

Function	Default value
Global IGMP MVR status	Disable
Interface IGMP MVR status	Disable
Multicast VLAN and group address set	N/A

## 8.5.4 Configuring IGMP MVR

Configure IGMP MVR for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#igmp mvr</b>	Enable global IGMP MVR.

Step	Command	Description
3	<code>Raisecom(config)#igmp mvr mcast-vlan <i>vlan-id</i> group { <i>start-ip-address</i> [ <i>end-ip-address</i> ]   any }</code>	Configure the group address set for multicast VLAN.   <b>Note</b> After IGMP MVR is enabled, you need to configure multicast VLAN and bind group address set. If the received IGMP Report packet does not belong to a group address set of any VLAN, it is not processed and the user cannot make multicast traffic on demand.
4	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter interface configuration mode.
5	<code>Raisecom(config-gigaetheret1/1/port)#igmp mvr mcast-vlan <i>vlan-id</i> static <i>ip-address</i> user-vlan <i>vlan-id</i></code>	(Optional) configure static multicast members of MVR for a specified customer VLAN.
6	<code>Raisecom(config-gigaetheret1/1/port)#igmp mvr user-vlan <i>vlan-id</i></code>	(Optional) configure the range for multicast inter-VLAN copy to take effect.



### Note

- IGMP Snooping and IGMP MVR cannot be enabled concurrently in the same multicast VLAN. Otherwise, the configuration will fail.
- IGMP Snooping and multicast VLAN copy cannot be enabled concurrently in the same multicast VLAN. Otherwise, the configuration will fail.

## 8.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show igmp mvr { <i>interface</i>   <i>interface-type interface-number</i> }</code>	Show configurations of IGMP MVR on the specified interface.
2	<code>Raisecom#show igmp mvr member [ <i>interface-type interface-number</i>   <i>user-vlan vlan-id</i> ]</code>	Show information about multicast group members of IGMP MVR.
3	<code>Raisecom#show igmp mvr member count { <i>interface-type interface-number</i>   <i>user-vlan vlan-id</i> }</code>	Show the number of multicast group members of IGMP MVR.
4	<code>Raisecom#show igmp mvr vlan-group [ <i>mcast-vlan vlan-id</i> ]</code>	Show multicast VLAN and its group address set.

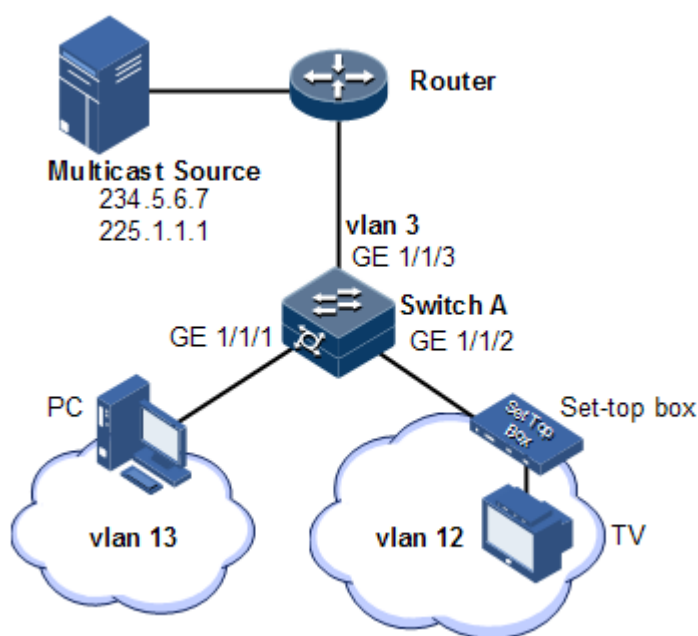
## 8.5.6 Example for configuring IGMP MVR

### Networking requirements

As shown in Figure 8-9, GE 1/1/1 on Switch A connects with the multicast router, and GE 1/1/2 and GE 1/1/3 connect with users in different VLANs to receive data from multicast addresses 234.5.6.7 and 225.1.1.1.

Configure IGMP MVR on Switch A to specify VLAN 3 as a multicast VLAN, and then the multicast data needs to be duplicated with one copy in the multicast VLAN instead of copying for each customer VLAN, thus saving bandwidth.

Figure 8-9 MVR networking



### Configuration steps

Step 1 Create VLANs on Switch A and add interfaces to them.

```
Raisecom(config)#config
Raisecom(config)#create vlan 3,12,13 active
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#switchport mode trunk
Raisecom(config-gigabitEthernet1/1/1)#switchport trunk native vlan 13
Raisecom(config-gigabitEthernet1/1/1)#switchport trunk untagged vlan 12
Raisecom(config-gigabitEthernet1/1/1)#exit
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#switchport mode trunk
Raisecom(config-gigabitEthernet1/1/2)#switchport trunk native vlan 12
Raisecom(config-gigabitEthernet1/1/2)#switchport trunk untagged vlan 13
Raisecom(config-gigabitEthernet1/1/2)#exit
Raisecom(config)#interface gigabitEthernet 1/1/3
```

```
Raisecom(config-gigaethernet1/1/3)#switchport mode trunk
Raisecom(config-gigaethernet1/1/3)#switchport trunk native vlan 3
Raisecom(config-gigaethernet1/1/3)#switchport trunk untagged vlan 12,13
Raisecom(config-gigaethernet1/1/3)#exit
```

Step 2 Configure IGMP MVR on Switch A.

```
Raisecom(config)#igmp mvr
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#igmp mvr
Raisecom(config-gigaethernet1/1/1)#igmp mvr user-vlan 13
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#igmp mvr
Raisecom(config-gigaethernet1/1/2)#igmp mvr user-vlan 12
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#igmp mvr mcast-vlan 3 group 234.5.6.7
Raisecom(config)#igmp mvr mcast-vlan 3 group 225.1.1.1
```

## Checking results

Use the following command to show IGMP MVR configurations on Switch A.

```
Raisecom#show igmp mvr
igmp mvr running           :Enable
igmp mvr port              :GE1/1/1 GE1/1/2
igmp mvr multicast vlan(ref) :3(2)
igmp aging time(s)         :260
igmp ring                  :--
```

Use the following command to show information about the multicast VLAN and group address.

```
Raisecom#show igmp mvr vlan-group
-----
Raisecom(config)#show igmp mvr vlan-group
Mcast-vlan      Start-group      End-group
-----
3                225.1.1.1      225.1.1.1
3                234.5.6.7      234.5.6.7
```

## 8.6 IGMP filtering

### 8.6.1 Introduction

To control user access, you can configure IGMP filtering. IGMP filtering includes limiting the range of accessible multicast groups by using the filtering profile and limiting the maximum number of multicast groups.

- IGMP filtering profile

To ensure information security, the administrator needs to limit the multicast users, such as what multicast data are allowed to receive and what are not.

You can configure IGMP Profile filtering profile to control the interface. One IGMP Profile can be configured one or more multicast group access control restrictions and access the multicast group according to the restriction rules (**permit** and **deny**). If a rejected IGMP Profile filtering profile is applied to the interface, the interface will discard the IGMP report packet from this group directly once receiving it and disallow the interface to receive this group of multicast data.

IGMP filtering profile can be configured on an interface or interface+VLAN.

IGMP Profile only applies to dynamic multicast groups, but not static ones.

- Limit to the maximum number of multicast groups

You can configure the maximum number of multicast groups allowed to join based on interface or interface+VLAN and the rules to restrict the maximum number.

The maximum group number rule defines the actions to be taken for reaching the maximum number of multicast groups jointed by users, namely, disallowing new users to join the multicast group or overriding a joined group.



#### Note

IGMP filtering is generally used with IGMP Snooping/IGMP MVR/multicast VLAN copy.

### 8.6.2 Preparing for configurations

#### Scenario

Different users in the same multicast group receive different multicast requirements and permissions. You can configure filtering rules on the switch which connects the multicast router and user host to restrict multicast users. You also can configure the maximum number of multicast groups jointed by users. IGMP Proxy is generally used with IGMP Snooping or IGMP MVR.

#### Prerequisite

- Create VLANs.
- Add related interfaces to the VLANs.



## 8.6.3 Default configurations of IGMP filtering

Default configurations of IGMP filtering are as below.

Function	Default value
Global IGMP filtering	Disable
IGMP filtering profile Profile	N/A
IGMP filtering profile action	Refuse
IGMP filtering under interface	No maximum group limit, the largest group action is drop, no application filtering profile
IGMP filtering under interface+VLAN	No maximum group limit, the largest group action is drop, no application filtering profile

## 8.6.4 Enabling global IGMP filtering

Enable global IGMP filtering for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode
2	<b>Raisecom(config)#igmp filter</b>	Enable global IGMP filtering



### Note

When configuring IGMP filtering profile or the maximum group number, use the **igmp filter** command to enable global IGMP filtering.

## 8.6.5 Configuring IGMP filtering profile

IGMP filtering profile can be used to interface or interface+VLAN.

Configure IGMP filtering profile for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#igmp filter profile <i>profile-number</i></b>	Create IGMP Profile and enter Profile configuration mode.
3	<b>Raisecom(config-igmp-profile){ <b>permit</b>   <b>deny</b> }</b>	Configure IGMP Profile action.
4	<b>Raisecom(config-igmp-profile)#range <i>range-id start-ip-address</i> [ <i>end-ip-address</i> ]</b>	Configure to control IP multicast address access and range.

Step	Command	Description
5	<code>Raisecom(config-igmp-profile)#exit</code> <code>Raisecom(config)#interface</code> <code>interface-type interface-number</code>	Enter physical layer interface configuration mode or LAG configuration mode.
6	<code>Raisecom(config-gigaetherne1/1/port)#igmp filter profile profile-number [ vlan vlan-list ]</code>	Configure IGMP Profile filtering profile to physical interface or interface+VLAN.
	<code>Raisecom(config-portchannel1)#igmp filter profile profile-number [ vlan vlan-list ]</code> <code>Raisecom(config-portchannel1)#exit</code>	Configure IGMP Profile filtering profile to LAG interface or interface+VLAN.
7	<code>Raisecom(config-gigaetherne1/1/port)# igmp drop [ query   report ]</code>	(Optional) enable IGMP to filter query packets from the user interface or join or leave packets from the upstream interface.



## Note

Perform the command of **igmp filter profile profile-number** in interface configuration mode to make the created IGMP profile apply to the specified interface. One IGMP profile can be applied to multiple interfaces, but each interface can have only one IGMP profile.

## 8.6.6 Configuring maximum number of multicast groups

You can add the maximum number of multicast groups applied to interface or interface+VLAN.

Configure the maximum number of multicast groups for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode
2	<code>Raisecom(config)#interface</code> <code>interface-type interface-number</code>	Enter physical layer interface configuration mode or LAG configuration mode.
3	<code>Raisecom(config-gigaetherne1/1/port)#igmp filter max-groups group-number [ vlan vlan-list ]</code>	Configure the maximum number of multicast groups to physical interface or interface+VLAN.
	<code>Raisecom(config- port-channel1)#igmp filter max-groups group-number [ vlan vlan-list ]</code>	Configure the maximum number of multicast groups to LAG interface or interface+VLAN.

Step	Command	Description
4	<b>Raisecom(config-gigaetherne1/1/port)#igmp filter max-groups action { drop   replace } [ vlan vlan-list ]</b>	(Optional) configure the action over maximum number of multicast groups in physical interface or interface+VLAN.
	<b>Raisecom(config-port-channel1)#igmp filter max-groups action { drop   replace } [ vlan vlan-list ]</b>	(Optional) configure the action over maximum number of multicast groups in LAG interface or interface+VLAN.

## 8.6.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show igmp filter [ interface   interface-type interface-number [ vlan vlan-id ] ]</b>	Show configurations of IGMP filtering.
2	<b>Raisecom#show igmp filter profile [ profile-number ]</b>	Show information about the IGMP profile.

## 8.6.8 Example for applying IGMP filtering on interface

### Networking requirements

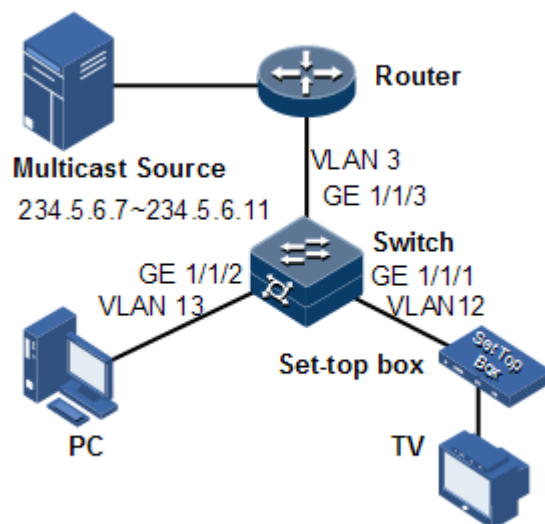
Enable IGMP filtering on the switch. Add filtering rules on the interface to filter multicast users.

As shown in Figure 8-10,

- Create an IGMP filtering rule Profile 1, and configure the action to pass for the multicast group ranging from 234.5.6.7 to 234.5.6.10.
- Apply filtering rule on GE 1/1/1, allow the STB to join the 234.5.6.7 multicast group, forbid it to join the 234.5.6.11 multicast group.
- Apply no filtering rule on Port 3, and allow PCs to join the 234.5.6.11 multicast group.

Configure the maximum number of multicast groups on GE 1/1/1. After the STB is added to the 234.5.6.7 multicast group, add it to the 234.5.6.8 multicast group while it quits the 234.5.6.7 multicast group.

Figure 8-10 Applying IGMP filtering on interface



## Configuration steps

Step 1 Create VLANs, and add interfaces to VLANs.

```

Raisecom#config
Raisecom(config)#create vlan 3,12,13 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan 12
Raisecom(config-gigaethernet1/1/1)#switchport trunk untagged vlan 3
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#switchport trunk native vlan 13
Raisecom(config-gigaethernet1/1/2)#switchport trunk untagged vlan 3
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#switchport mode trunk
Raisecom(config-gigaethernet1/1/3)#switchport trunk native vlan 3
Raisecom(config-gigaethernet1/1/3)#switchport trunk untagged vlan 12,13
Raisecom(config-gigaethernet1/1/3)#exit

```

Step 2 Enable IGMP MVR.

```

Raisecom(config)#igmp mvr
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#igmp mvr
Raisecom(config-gigaethernet1/1/1)#igmp mvr user-vlan 12
Raisecom(config-gigaethernet1/1/1)#exit

```

```
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#igmp mvr
Raisecom(config-tengigabitEthernet1/1/2)#igmp mvr user-vlan 13
Raisecom(config-gigabitEthernet1/1/2)#exit
Raisecom(config)#igmp mvr mcast-vlan 3 group any
```

Step 3 Configure the IGMP filtering profile.

```
Raisecom(config)#igmp filter profile 1
Raisecom(config-igmp-profile)#permit
Raisecom(config-igmp-profile)#range 1 234.5.6.7 234.5.6.10
Raisecom(config-igmp-profile)#exit
```

Step 4 Configure the STB to apply the IGMP filtering profile.

```
Raisecom(config)#igmp filter
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#igmp filter profile 1
```

Step 5 Configure the maximum number of multicast groups on the STB interface.

```
Raisecom(config-gigabitEthernet1/1/1)#igmp filter max-groups 1
Raisecom(config-gigabitEthernet1/1/1)#igmp filter max-groups action replace
```

## Checking results

Use the following command to show configurations of IGMP filtering on the interface.

```
Raisecom#show igmp filter gigabitEthernet 1/1/1
igmp profile: 1
max group: 1
current group: 0
action: replace
```

## 8.7 Multicast VLAN copy

### 8.7.1 Introduction

Multicast VLAN copy refers to specifying different VLANs as one user VLAN of the multicast VLAN when different user VLANs require the same multicast source on the switch.

After multicast VLAN copy is enabled, the upper layer device copies multicast data in the multicast VLAN, instead of copying multicast data for each user VLAN, thus saving bandwidth. The system searches for the egress interface according to the multicast VLAN and multicast group address, and copies multicast data for each user VLAN on the egress interface.

Both multicast VLAN copy and IGMP MVR can implement multicast functions when user VLANs and the multicast VLAN are in different VLANs. Their difference is that multicast data of IGMP MVR can be forwarded in a multicast VLAN but multicast VLAN copy is used to copy multicast data to each user VLAN.

IGMP MVR transmits data in a way as shown in Figure 8-11 while multicast VLAN copy transmits data in a way as shown in Figure 8-12.

Figure 8-11 Data transmission of IGMP MVR

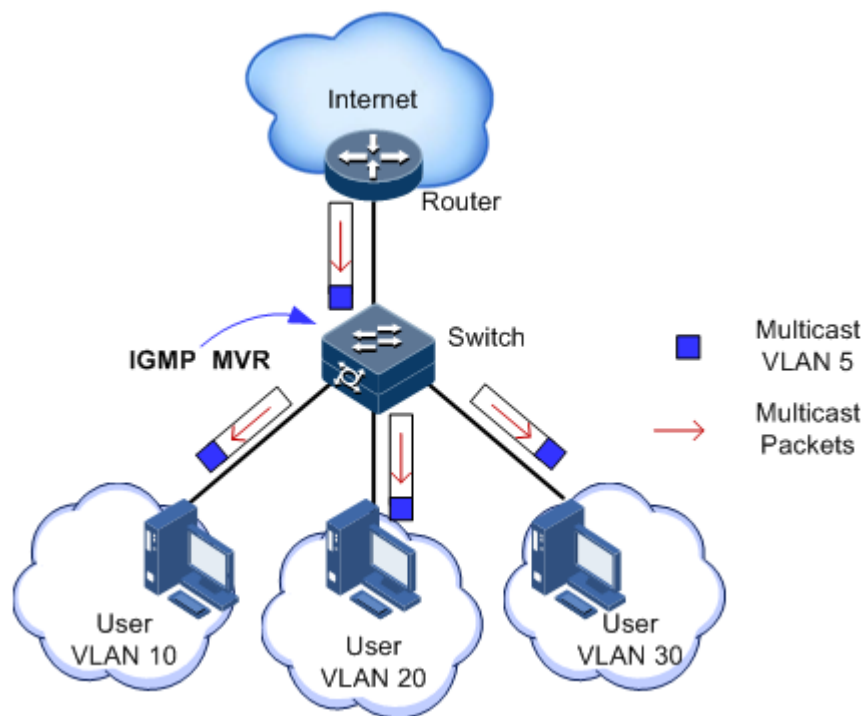
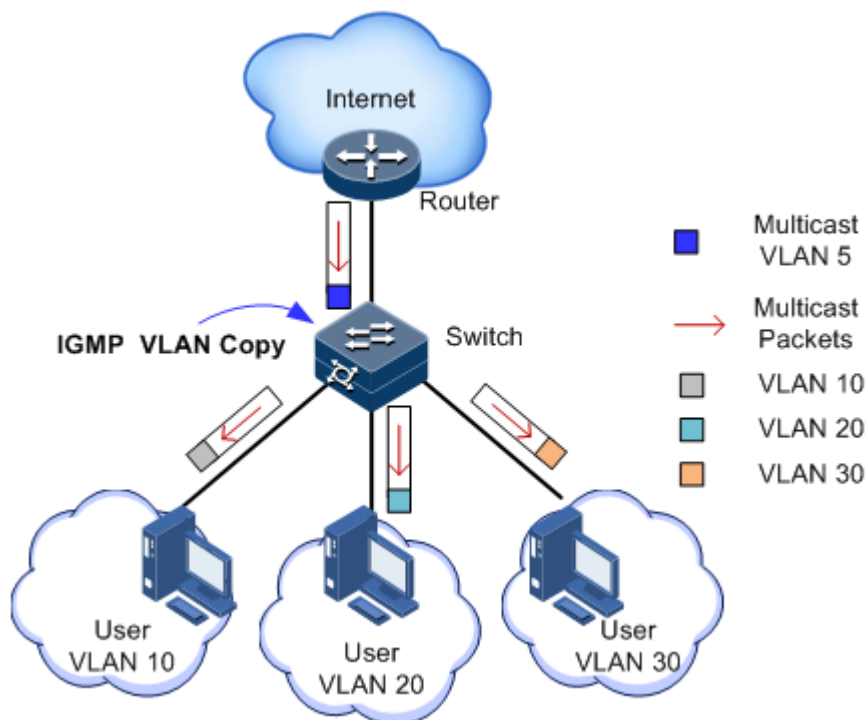


Figure 8-12 Data transmission of multicast VLAN copy



### Note

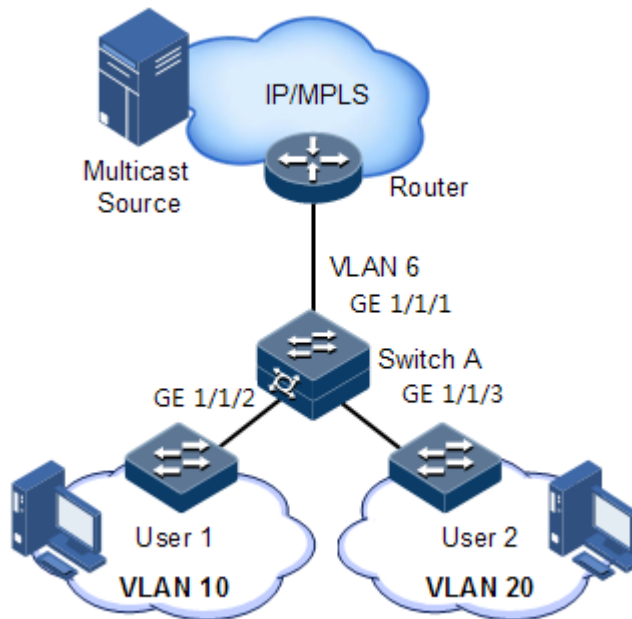
The ISCOM2600G-HI series switch can be configured with 1–10 multicast VLANs and at least one multicast VLAN and corresponding group address set. It supports up to 1024 multicast groups.

## 8.7.2 Preparing for configurations

### Scenario

As shown in Figure 8-13, multiple hosts belonging to different VLANs receive data of the multicast source. Enable multicast VLAN copy on Switch B and configure multicast VLAN so that multicast data is copied on the receiving interface to the user VLAN and users of different VLANs can share a multicast VLAN to receive the same multicast data and reduce waste of bandwidth.

Figure 8-13 Multicast VLAN copy networking



## Prerequisite

Create VLANs, and add related interfaces to VLANs.

### 8.7.3 Default configurations of multicast VLAN copy

Default configurations of multicast VLAN copy are as below.

Function	Default value
Global multicast VLAN copy status	Disable
Interface multicast VLAN copy status	Disable
Multicast VLAN and group address set	N/A




## Note

- To concurrently configure N:1 VLAN mapping and VLAN copy, you must configure VLAN copy and then configure N:1 VLAN mapping.
- To concurrently configure N:1 VLAN mapping and PIM, you must configure PIM and then configure N:1 VLAN mapping.

### 8.7.4 Configuring multicast VLAN copy

Configure multicast VLAN copy for the ISCOM2600G-HI series switch as below.



Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#igmp vlan-copy</b>	Enable global multicast VLAN copy.
3	<b>Raisecom(config)#igmp vlan-copy mcast-vlan vlan-id group { start-ip [ end-ip ]   any }</b>	Configure the group address set of the multicast VLAN.   <b>Note</b> After multicast VLAN copy is enabled, you need to configure the multicast VLAN and bound group address set. If the received IGMP Report packet does not belong to a group address set of any VLAN, it is not processed and the user cannot make multicast traffic on demand.

## 8.7.5 Configuring static multicast members of VLAN copy

Configure static multicast members of VLAN copy for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config- gigaethernet1/1/port)#igmp vlan- copy mcast-vlan vlan-id static ip- address user-vlan vlan-id</b>	Configure static multicast members of VLAN copy.



### Note

- IGMP Snooping and IGMP MVR cannot be enabled concurrently in the same multicast VLAN, otherwise the configuration will fail.
- IGMP Snooping and multicast VLAN copy cannot be enabled concurrently in the same multicast VLAN, otherwise the configuration will fail.

## 8.7.6 Configuring customer VLAN of VLAN copy

Configure the customer VLAN of VLAN copy for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#igmp</b> <b>vlan-copy user-vlan</b> <i>vlan-id</i>	Configure the customer VLAN of multicast VLAN copy.

## 8.7.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show igmp vlan-copy</b>	Show configurations of multicast VLAN copy.
2	<b>Raisecom#show igmp vlan-copy</b> <i>interface-type interface-number</i>	Show configurations of multicast VLAN copy on the specified interface.
3	<b>Raisecom#show igmp vlan-copy member</b>	Show information about multicast group members of multicast VLAN copy.
4	<b>Raisecom#show igmp vlan-copy member</b> <i>interface-type interface-number</i>	Show information about multicast group members of multicast VLAN copy on the specified interface.
5	<b>Raisecom#show igmp vlan-copy member user-vlan</b> <i>vlan-id</i>	Show information about multicast group members of multicast VLAN copy in the specified user VLAN.
6	<b>Raisecom#show igmp vlan-copy vlan-group</b> [ <b>mcast-vlan</b> <i>vlan-id</i> ]	Show the multicast VLAN and bound group address set of multicast VLAN copy.

## 8.8 MLD

### 8.8.1 Introduction

MLD is a network protocol used in multicast technologies. Through MLD, a router can snoop whether there is a snooper of the IPv6 multicast group in the connected network segment, and then record the result in the database. The router also maintains timer information about these IPv6 multicast addresses. Through MLD, the user host and the expected directly-connected multicast router establish and maintain multicast membership.

A MLD router uses the local address of IPv6 unicast link as the source address to send MLD packets, and uses ICMPv6 packets. All MLD packets are limited to local links, with hops of 1.

The ISCOM2600G-HI series switch supports two MLD versions:

- MLDv1: defined by RFC2710, derived from IGMPv2

- MLDv2: defined by RFC3810, derived from IGMPv3

MLDv1 is used to manage IPv6 multicast group members through the querying and response mechanism. Based on MLDv1, MLDv2:

- Additionally support filtering IPv6 multicast sources. When a host joins an IPv6 multicast group, it can request to receive or deny messages from a specified IPv6 multicast source.
- Additionally support configuring the maximum response time. Thus, MLDv2 is applicable to larger networks.
- It does not support response suppression; in other words, the host does not need to process packets from other hosts, thus simplifying hosts operations.
- Add an S flag bit in the querying packet to enhance robustness of the system.
- Add the retransmission mechanism to the querying and response packets.

## 8.8.2 Preparing for configurations

### Scenarios

Multicast arising in the IPv4 era solves the problem of single-point sending and multi-point receiving, and transmits data efficiently point to multiple points on the network, thus saving network bandwidth and lowering network load. It is enhanced on the IPv4 network. By listening MLD messages and thus creating a forwarding table for multicast packets, the ISCOM2600G-HI series switch can manage and control the forwarding of multicast packets, and forward multicast packets to the target host.

### Prerequisite

Configure the IPv6 address of the interface.

## 8.8.3 Default configurations of MLD

Default configurations of MLD are as below.

Function	Default value
MLD ring network forwarding on the interface	Disable
MLD Snooping	Disable
MLD version	1
Aging time of MLD members	260s
MLD robustness	2

## 8.8.4 Configuring basic functions of MLD

Configure basic functions of MLD for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mld mrouter vlan vlan-id interface-type interface-number</b>	Create a multicast router interface on the specified VLAN.
3	<b>Raisecom(config)#mld ring interface-type interface- number</b>	Enable MLD ring network forwarding on the interface.
4	<b>Raisecom(config)#interface interface-type interface- number</b> <b>Raisecom(config- gigaethernet1/1/port)#mld immediate-leave [ vlan vlan- list ]</b>	(Optional) enable immediate leave of MLD on the interface or interface+VLAN.  If immediate leave is disabled on the downlink interface, the router interface, after receiving a Leave packet, will calculate the aging time according to robust factor and configure the expiration time for a member to leave the group as Group Membership Interval (GMI). $GMI = robust-value * lastmember-queryinterval$ .
5	<b>Raisecom(config)#mld report- suppression</b>	(Optional) enable Report suppression. When receiving multiple Report packets from the same group in a specified period, the ISCOM2600G-HI series switch forwards only one Report packet to the router interface while it suppresses others.
6	<b>Raisecom(config)#mld member- timeout { second   infinite }</b>	(Optional) configure the aging time of MLD members.
7	<b>Raisecom(config)#mld version { 1   2 }</b>	Configure the MLD version.
8	<b>Raisecom(config)#interface interface-type interface- number</b> <b>Raisecom(config- gigaethernet1/1/port)#mld snooping host-join group- address vlan vlan-id</b>	Configure the host joining function for MLD Snooping.

## 8.8.5 Configuring MLD Snooping

Configure MLD Snooping for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mld snooping</b>	Enable global MLD Snooping.

Step	Command	Description
3	<code>Raisecom(config)#mld snooping vlan <i>vlan-list</i></code>	(Optional) enable MLD Snooping in all VLANs.
4	<code>Raisecom(config)#vlan <i>vlan-id</i></code> <code>Raisecom(config-vlan)#mld snooping static <i>ip-address</i> [ <i>interface-type interface-number</i> ]</code>	(Optional) configure the static member of MLD Snooping in VLAN mode.
5	<code>Raisecom(config)#interface <i>interface-type interface number</i></code> <code>Raisecom(config-gigaethernet1/1/1)#mld snooping group-address <i>vlan vlan-id</i></code>	(Optional) configure the host joining function for MLD Snooping on the interface.

## 8.8.6 Configuring MLD Querier

Configure MLD Querier for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mld querier</code>	Enable MLD querier.
3	<code>Raisecom(config)#mld source-ip <i>ip-address</i></code>	(Optional) configure the source IP address for MLD Querier to send Query packets.
4	<code>Raisecom(config)#mld query-interval <i>seconds</i></code>	(Optional) configure the MLD query interval.
5	<code>Raisecom(config)#mld query-max-response-time <i>seconds</i></code>	(Optional) configure the maximum response time of Query packets.
6	<code>Raisecom(config)#mld last-member-query-interval <i>seconds</i></code>	(Optional) configure the interval for the last member to send Query packets.
7	<code>Raisecom(config)#mld robust-count <i>value</i></code>	Configure the robustness factor of MLD.
8	<code>Raisecom(config)#mld proxy</code>	Enable MLD Proxy.



### Note

- When IGMP Querier is disabled, the following parameters can be configured: source IP address, query interval, maximum response time to send Query packets, and interval for the last member to send Query packets. After IGMP Querier is enabled, these configurations will take effect immediately.
- MLD proxy and MLD Querier are mutually exclusive. MLD proxy and MLD report-suppression are mutually exclusive.

## 8.8.7 Configuring MLD filtering

### Enable global MLD filtering

Enable global MLD filtering for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mld filter</b>	Enable global MLD filtering.
3	<b>Raisecom(config-gigaethernet1/1/port)# mld drop [ query   report ]</b>	(Optional) enable IGMP to filter Query packets from the user interface or Join or Leave packets from the upstream interface.



### Note

Before applying the MLD filtering profile or configuring the maximum number of groups, use the **mld filter** command to enable global MLD filtering.

### Configuring MLD filtering profile

The MLD filtering profile can be used on the interface or interface+VLAN.

Configure the MLD filtering profile for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mld filter profile <i>profile-number</i></b>	Create a MLD profile, and enter profile configuration mode.
3	<b>Raisecom(config-mld-profile)#{ permit   deny }</b>	Configure the action of the MLD profile.
4	<b>Raisecom(config-mld-profile)#range <i>range-id start-ip-address [ end-ip-address ]</i></b>	Configure the IPv6 multicast address or range for access control.
5	<b>Raisecom(config-mld-profile)#exit</b> <b>Raisecom(config)#interface <i>interface-type interface-number</i></b>	Enter physical layer interface configuration mode or LAG configuration mode.
6	<b>Raisecom(config-gigaethernet1/1/port)#mld filter profile <i>profile-number</i> [ vlan <i>vlan-list</i> ]</b>	Apply the MLD filtering profile to the physical interface or interface+VLAN.
	<b>Raisecom(config-port-channel1)#mld filter profile <i>profile-number</i> [ vlan <i>vlan-list</i> ]</b> <b>Raisecom(config-port-channel1)#exit</b>	Apply the MLD filtering profile to the LAG interface or interface+VLAN.



## Note

By using the **mld filter profile** *profile-number* command in interface configuration mode, you can apply a created MLD profile to the specified interface. A MLD profile can be applied to multiple interfaces, but only one MLD profile can be applied to one interface.

## Configuring maximum number of groups

The maximum number of groups for the user to join can be applied to the interface or interface+VLAN.

Configure maximum number of groups for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
3	<b>Raisecom(config-gigaetherne</b> <b>t1/1/port)#mld</b> <b>filter max-groups</b> <i>group-number</i> [ <b>vlan</b> <i>vlan-list</i> ]	Apply the maximum number of groups to the physical interface or interface+VLAN.
	<b>Raisecom(config-port-channel)#mld filter max-groups</b> <i>group-number</i> [ <b>vlan</b> <i>vlan-list</i> ]	Apply the maximum number of groups to the LAG interface or interface+VLAN.
4	<b>Raisecom(config-gigaetherne</b> <b>t1/1/port)#mld</b> <b>filter max-groups action</b> { <b>drop</b>   <b>replace</b> } [ <b>vlan</b> <i>vlan-list</i> ]	(Optional) configure the action to be taken when the number of groups for the physical interface or interface+VLAN to join exceeds the maximum number of groups.
	<b>Raisecom(config-port-channel)#mld filter max-groups action</b> { <b>drop</b>   <b>replace</b> } [ <b>vlan</b> <i>vlan-list</i> ]	(Optional) configure the action to be taken when the number of groups for the LAG interface or interface+VLAN to join exceeds the maximum number of groups.

## 8.8.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show mld immediate-leave</b> [ <i>interface-type interface-number</i>   <b>port-channel</b> <i>port-channel-id</i> ]	Show configurations of immediate leave of MLD.
2	<b>Raisecom#show mld mrouter</b>	Show information about the multicast router interface of MLD.

No.	Command	Description
3	Raisecom# <b>show mld snooping</b> [ <b>vlan</b> <i>vlan-id</i> ]	Show configurations of MLD Snooping.
4	Raisecom# <b>show mld snooping member</b> [ <i>interface-type interface-number</i>   <b>vlan</b> <i>vlan-id</i> ]	Show information about multicast group members of MLD Snooping.
5	Raisecom# <b>show mld snooping member count</b> [ <i>interface-type interface-number</i>   <b>vlan</b> <i>vlan-id</i> ]	Show the number of multicast group members of MLD Snooping.
6	Raisecom# <b>show mld statistics</b> [ <i>interface-type interface-number</i> ]	Show statistics of MLD statistics.
7	Raisecom# <b>show mld filter</b> [ <b>interface</b>   <b>gigaethernet</b> <i>interface-number</i> [ <b>vlan</b> <i>vlan-id</i> ] ]	Show configuration of MLD filtering.
8	Raisecom# <b>show mld filter profile</b> [ <i>profile-number</i> ]	Show configurations of the MLD filtering profile.
9	Raisecom# <b>show mld configuration</b>	Show basic configurations of MLD.

## 8.8.9 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
Raisecom# <b>clear mld statistics</b> [ <i>interface-type interface-number</i> ]	Clear MLD statistics.
Raisecom# <b>no mld member</b> <i>interface-type interface-number</i>	Clear multicast entries of the specified interface.



# 9 OAM

---

This chapter describes basic principles and configuration procedures for OAM and provide related configuration examples, including the following sections:

- Introduction
- EFM
- CFM (IEEE 802.1ag/ITU-Y.1731)
- SLA
- BFD

## 9.1 Introduction

Initially, Ethernet is designed for LAN. Operation, Administration and Maintenance (OAM) is weak because of its small size and a NE-level administrative system. With continuous development of Ethernet technology, the application scale of Ethernet in Telecom network becomes wider and wider. Compared with LAN, the link length and network size of Telecom network is bigger and bigger. The lack of effective management and maintenance mechanism has seriously obstructed Ethernet technology applying to the Telecom network.

To confirm connectivity of Ethernet virtual connection, effectively detect, confirm, and locate faults on network, balance network utilization, measure network performance, and provide service according Service Level Agreement (SLA), implementing OAM on Ethernet has becoming an inevitable developing trend.

### Working mode

An interface enabled with EFM OAM is called an OAM entity. EFM OAM supports the following two working modes:

- Active mode: initialized by the OAM entity that is in active mode
- Passive mode: the OAM entity in passive mode just waits for connection request of the active OAM entity. If OAM entities of both ends of a link are in passive mode, the OAM link cannot be established.

## OAM discovery

The Ethernet OAM connection process is the OAM discovery phase, where an OAM entity discovers a remote OAM entity and establishes a session with it.

This phase is initiated by an OAM entity that is in active mode. One end informs the other of its Ethernet OAM configurations and Ethernet OAM capabilities supported by the local node by exchanging OAM PDU. Both ends determine whether to establish OAM connection. If yes, Ethernet OAM protocol will work on the link layer.

Only the OAM entity in active mode can initiate OAM connection.

After the OAM connection is established, both ends keep connected by exchanging OAM PDU. If one end fails to receive OAM PDU within the timeout time, it believes that connection expires and reconnection is required.

## Monitoring link

In the OAM connection, an OAM entity keeps sending Information OAM PDUs. The local OAM entity can inform the peer OAM entity of threshold events through Information OAM PDUs. In this way, the network administrator can learn the link state and take actions accordingly.

The network administrator monitors Ethernet OAM through the Event Notification OAM PDU. When a link fails, the passive OAM entity detects the failure, and actively sends Event Notification OAM PDU to the peer active OAM entity to inform the following threshold events. By default, 3 Dying Gasp Traps are sent. Therefore, the network administrator can dynamically master the network status through the link monitoring process.

- Error frame event: the number of error frames exceeds the threshold in a time unit.
- Error frame period event: the number of error frames exceeds the threshold in a period (specified N frames).
- Error frame second event: the number of error frames in M seconds exceeds the threshold. The second when an errored frame is generated is called the errored frame second.
- Error symbol period event: the number of error symbols received in a period (monitor window) exceeds the threshold.

## Informing of peer fault

When a device is faulty or fails, it may cause network failure. Thus a flag is defined in OAM PDU packet to allow an OAM entity to transmit fault information to the peer. The flag may stand for the following threshold events:

- Link fault: signals from the peer are lost. OAM PDUs are sent every 1s.
- Dying gasp: an unpredictable event occurs which causes the system to be irrevocable, such as power failure. In this case, OAM PDUs are sent ceaselessly.
- Critical event: an uncertain critical event occurs, such as abnormal temperature. In this case, OAM PDUs are sent ceaselessly.

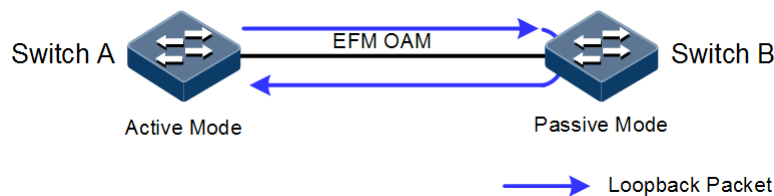
## Remote loopback

Remote loopback is used to locate the area with the fault and help you test link quality with instruments. Periodical loop detection helps you find network faults in time and segmental loop detection helps you locate the specified area with the fault and clear the fault.

OAM loopback occurs only after the Ethernet OAM connection is established. When connected, the active OAM entity initiates the OAM loopback command, and the peer OAM entity responds to the command. When the peer OAM entity is in loopback mode, all packets except OAM PDU will be retraced.

Switch A, in active mode, determines link status through returned packets, as shown in Figure 9-1.

Figure 9-1 OAM loopback



## 9.2 EFM

### 9.2.1 Introduction

Complying with IEEE 802.3ah protocol, Ethernet in the First Mile (EFM) is a link-level Ethernet OAM technology. It provides link connectivity detection, link fault monitoring, and remote fault notification for a link between two directly connected devices. EFM is mainly used for Ethernet links on edges of the network accessed by users.

### 9.2.2 Preparing for configurations

#### Scenario

Deploying EFM feature between directly connected devices can efficiently improve Ethernet link management and maintenance capability and ensure stable network operation.

#### Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.

### 9.2.3 Default configurations of EFM

Default configurations of EFM are as below.

Function	Default value
EFM working mode	Passive mode
Interval for sending messages	10 × 100ms
Link timeout	5s
OAM	Disable

Function	Default value
Remote OAM event alarm	Disable
EFM remote loopback status	Not response
Monitor window of errored frame event	1s
Monitor threshold of errored event	1 errored frame
Monitor window of errored frame period event	1000ms
Monitor threshold of errored frame period event	1 errored frame
Monitor window of link errored frame second statistics event	60s
Monitor threshold of link errored frame second statistics event	1s
Monitor window of link errored coding statistics event	1s
Monitor threshold of errored coding statistic event	1s
Fault indication	Enable
Local OAM event alarm	Disable

## 9.2.4 Configuring basic functions of EFM

Configure basic functions of EFM for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-gigaetherne</b> t1/1/1) <b>#oam</b> { <b>active</b>   <b>passive</b> } <b>Raisecom(config-gigaetherne</b> t1/1/1) <b>#exit</b>	Configure the working mode of EFM OAM. At least one end should be in active mode, otherwise link detection will fail.
4	<b>Raisecom(config)#oam</b> <b>send-period</b> <i>period-number</i>	(Optional) Configure the period for sending OAM PDUs.
5	<b>Raisecom(config)#oam</b> <b>timeout</b> <i>period-number</i>	(Optional) configure the timeout of EFM OAM links.  When the duration of failing to receive OAM packets by one end of the OAM link is greater than the timeout, the end regards that the OAM link is disconnected.
6	<b>Raisecom(config)#interface</b> <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.

Step	Command	Description
7	<code>Raisecom(config-gigaetherne1/1/1)#oam enable</code>	Enable interface OAM.

## 9.2.5 Configuring active functions of EFM



### Note

The active function of EFM OAM can be configured only when the ISCOM2600G-HI series switch is in active mode.

### Configuring OAM remote loopback

OAM provides a link-layer remote loopback mechanism for locating link faults and measuring performance and quality. In link loopback status, the ISCOM2600G-HI series switch sends back all packets except OAM packets received by the link to the peer device. The local device initiates or disables remote loopback through the OAM remote loopback command. The remote device, through the loopback configuration command, controls whether to respond to the loopback command.

Configure OAM remote loopback for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaetherne1/1/1)#oam remote-loopback</code>	Configure the interface to start EFM OAM remote loopback. Only the active OAM end can initiate remote loopback.
4	<code>Raisecom(config-gigaetherne1/1/1)#oam loopback timeout time-out</code>	(Optional) configure the timeout for remote loopback. If the remote end fails to respond within the timeout time, the local end will retry. After the local end fails in retry, it will send a timeout alarm.
5	<code>Raisecom(config-gigaetherne1/1/1)#oam loopback retry times</code>	(Optional) configure the retry times for remote loopback.
6	<code>Raisecom(config-gigaetherne1/1/1)#no oam remote-loopback</code>	(Optional) disable remote loopback. After loop detection is complete, disable remote loopback in time.

## Configuring peer OAM event alarm

Configure the peer OAM event alarm for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/1)#oam peer event trap enable</b>	Enable peer OAM event alarm to send link monitoring events to the NMS.

### (Optional) configuring OAM variable obtaining

OAM variable obtaining is a link monitoring method. By obtaining the current variable of the peer, you can learn status of current link. IEEE802.3 Clause 30 defines and explains supported variable and its denotation obtained by OAM in details. The variable takes object as the maximum unit. Each object contains Package and Attribute. A package contains several attributes. Attribute is the minimum unit of a variable. When getting an OAM variable, it defines object, package, branch, and leaf description of attributes by Clause 30 to describe requesting object, and the branch and leaf are followed by variable to denote object responds variable request.

The ISCOM2600G-HI series switch supports obtaining OAM information and interface statistics.

Configure OAM variable obtaining for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#show oam peer { link-statistic   oam-info }</b> <i>[ interface-type interface-number ]</i>	Obtain EFM OAM information about the peer device or interface statistical variable.



#### Note

Peer variable cannot be obtained until EFM is connected.

## 9.2.6 Configuring EFM passive function



#### Note

The EFM passive function can be configured regardless the ISCOM2600G-HI series switch is in active or passive mode.

## Configuring device to respond with EFM remote loop

Configure the ISCOM2600G-HI series switch to respond with EFM remote loop as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/1)#oam</b> <b>loopback { ignore   process }</b>	Configure the Layer 2 physical interface to ignore or process EFM remote loopback.



## Caution

Only when the local end is configured with remote loopback response can EFM OAM remote loopback of the peer end take effect.

## Configuring OAM link monitoring

OAM link monitoring is used to detect and report link error in different conditions. When the detection link has a fault, the ISCOM2600G-HI series switch notifies the peer of the error generated time, window and threshold by OAM event, the peer receives event notification and reports the NView NNM system through SNMP Trap. Besides, the local device can directly report events from a specified interface to the NView NNM system center through SNMP Trap.

Configure OAM link monitoring for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/1)#oam errored-frame</b> <b>window window threshold threshold</b>	Configure errored frame monitor window and threshold.
4	<b>Raisecom(config-</b> <b>gigaethernet1/1/1)#oam errored-</b> <b>frame-period window window threshold</b> <b>threshold</b>	Configure errored frame period event monitor window and threshold.
5	<b>Raisecom(config-</b> <b>gigaethernet1/1/1)#oam errored-</b> <b>frame-seconds window window</b> <b>threshold threshold</b>	Configure link errored frame second window and threshold.
6	<b>Raisecom(config-</b> <b>gigaethernet1/1/1)#oam errored-</b> <b>symbol-period window window</b> <b>threshold threshold</b>	Configure errored code window and threshold.

## (Optional) configuring OAM fault indication

OAM fault indication is used by the local device to inform the peer device of local abnormalities, such as link fault, power failure, abnormal temperature, which cause faulty link and device restart.

You can enable or disable fault indications except link fault which must be sent to the peer end.

Configure OAM fault indication for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/1)#oam</b> <b>notify { critical-event   dying-gasp  </b> <b>errored-frame   errored-frame-period  </b> <b>errored-frame-seconds   errored-symbol-</b> <b>period } enable</b>	Enable the OAM fault notification to notify the peer device of local fault.

## Configuring local OAM event Trap

Configure local OAM event alarm for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interfac</b> <b>e</b> <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/1)#oam</b> <b>event trap enable</b>	Enable local OAM event Trap to report link monitoring events to the NView NNM system immediately.

## 9.2.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show oam [</b> <b>gigaethernet</b> <i>interface-number</i> <b>]</b>	Show basic configurations of EFM OAM.
2	<b>Raisecom#show oam event</b> <b>[</b> <b>gigaethernet</b> <i>interface-number</i> <b>]</b> <b>[</b> <b>critical</b> <b>]</b>	Show remote loopback configurations of EFM OAM.



No.	Command	Description
3	Raisecom# <b>show oam loopback</b> [ <b>gigaethernet</b> <i>interface-number</i> ]	Show configurations of link monitoring and fault indication of EFM OAM.
4	Raisecom# <b>show oam notify</b> [ <b>gigaethernet</b> <i>interface-number</i> ]	Show statistics on EFM OAM packets.
5	Raisecom# <b>show oam peer event</b> [ <b>gigaethernet</b> <i>interface-number</i> ] [ <b>critical</b> ]	Show configurations of EFM OAM event Trap.
6	Raisecom# <b>show oam peer link-statistic</b> [ <b>gigaethernet</b> <i>interface-number</i> ]	Show information about local critical faults detected by the EFM OAM interface.
7	Raisecom# <b>show oam statistics</b> [ <b>gigaethernet</b> <i>interface-number</i> ]	Show information about the peer EFM OAM device.
8	Raisecom# <b>show oam trap</b> [ <b>gigaethernet</b> <i>interface-number</i> ]	Show information about the peer EFM OAM and interface statistical variable.

## 9.2.8 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
Raisecom(config-gigaethernet1/1/1)# <b>clear oam statistics</b>	Clear statistics on links of the EFM OAM interface.
Raisecom(config-gigaethernet1/1/1)# <b>clear oam event</b>	Clear EFM OAM link events.
Raisecom(config)# <b>clear oam config</b>	Clear EFM OAM configurations.

## 9.3 CFM (IEEE 802.1ag/ITU-Y.1731)

### 9.3.1 Introduction

Connectivity Fault Management (CFM) is a network-level Ethernet OAM technology, providing end-to-end connectivity fault detection, fault notification, fault judgement, and fault location. It is used to diagnose fault actively for Ethernet Virtual Connection (EVC), provide cost-effective network maintenance solution, and improve network maintenance through the fault management function.

The ISCOM2600G-HI series switch provides CFM that is compatible with both ITU-Y.1731 and IEEE 802.1ag standards.

## CFM concepts

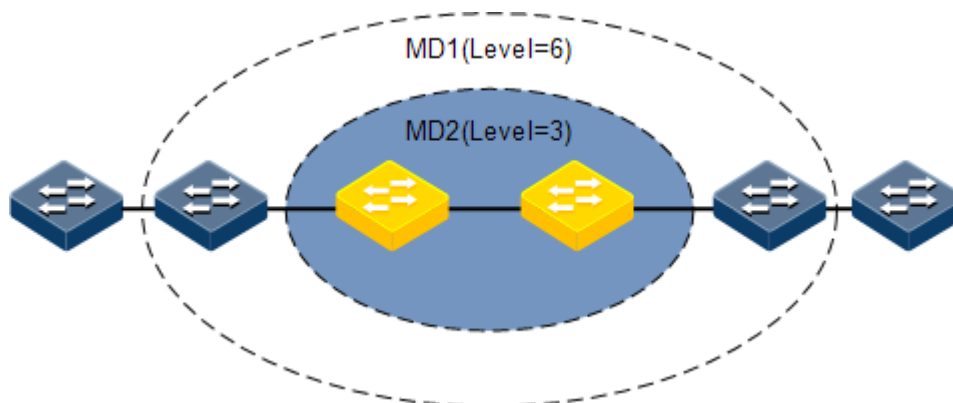
CFM consists of following components:

- MD

Maintenance Domain (MD), also called Maintenance Entity Group (MEG), is a network that runs CFM. It defines network range of OAM management. MD has a level property, with 8 levels (level 0 to level 7). The bigger the number is, the higher the level is and the larger the MD range is. Protocol packets in a lower-level MD will be discarded after entering a higher-level MD. If no Maintenance association End Point (MEP) but a Maintenance association Intermediate Point (MIP) is in a high-level MD, the protocol can traverse the higher-level MD. However, packets in a higher-level MD can traverse lower-level MDs. In the same VLAN range, different MDs can be adjacent, embedded, but not crossed.

As shown in Figure 9-2, MD 2 is in MD 1. Packets in MD 1 need to traverse MD 2. Configure MD 1 to be at level 6, and MD 2 to be at level 3. Then packets in MD 1 can traverse MD 2 and implement connectivity fault management of the whole MD 1. However, packets in MD 2 cannot diffuse into MD 1. MD 2 is a server layer while MD 1 is a client layer.

Figure 9-2 MDs at different levels



- Service instance

The service instance is also called Maintenance Association (MA). It is a part of a MD. One MD can be divided into one or multiple service instances. One service instance corresponds to one service and is mapped to a group of VLANs. VLANs of different service instances cannot cross. Though a service instance can be mapped to multiple VLANs, one service instance can only use a VLAN for sending or receiving OAM packets. This VLAN is the master VLAN of the service instance.

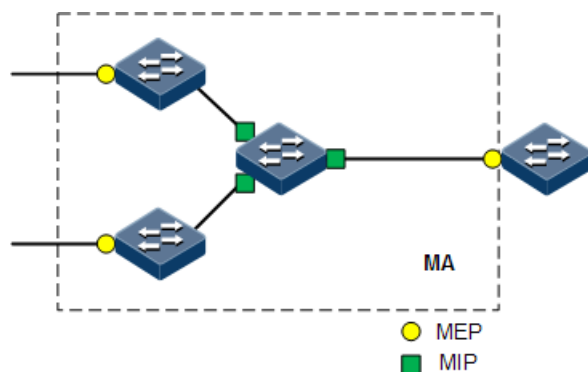
- MEP

As shown in Figure 9-3, the MEP is an edge node of a service instance. MEPs can be used to send and process CFM packets. The service instance and the MD where the MEP locates decide VLANs and levels of packets received and sent by the MEP.

For any device that runs CFM on the network, the MEP is called local MEP. For MEPs on other devices of the same service instance, they are called Remote Maintenance association End Points (RMEP).

Multiple MEPs can be configured in a service instance. Packets sent by MEPs in one instance carry an identical S-VLAN Tag, priority, and C-VLAN Tag. A MEP can receive OAM packets sent by other MEPs in the instance, intercept packets at the same or lower level, and forward packets of a higher level.

Figure 9-3 MEP and MIP



- MIP

As shown in Figure 9-3, the MIP is the internal node of a service instance, which is automatically created by the device. MIP cannot actively send CFM packets but can process and response to LinkTrace Message (LTM) and LoopBack Message (LBM) packets.

- MP

MEP and MIP are called Maintenance Point (MP).

## CFM functions

CFM can provide following OAM functions:

- Fault detection (Continuity Check, CC)

The function is implemented by periodically sending Continuity Check Messages (CCMs). One MEP sends CCM and other MEPs in the same service instance can verify the RMEP status when receiving this packet. If the ISCOM2600G-HI series switch fails or a link is incorrectly configured, MEPs cannot properly receive or process CCMs sent by RMEPs. If no CCM is received by a MEP during 3.5 CCM intervals, it is believed that the link fails. Then a fault Trap will be sent according to configured alarm priority.

- Fault acknowledgement (LoopBack, LB)

This function is used to verify the connectivity between two MPs through the source MEP sending LoopBack Message (LBM) and the destination MP sending LoopBack Reply (LBR). The source MEP sends a LBM to a MP who needs to acknowledge a fault. When receiving the LBM, the MP sends a LBR to the source MEP. If the source MEP receives this LBR, it is believed that the route is reachable. Otherwise, a connectivity fault occurs.

- Fault location (LinkTrace, LT)

The source MEP sends LinkTrace Message (LTM) to the destination MP and all MPs on the LTM transmission route will send a LinkTrace Reply (LTR) to the source MEP. By recording valid LTR and LTM, this function can be used to locate faults.

- Alarm Indication Signal (AIS)

This function is used to inhibit alarms when a fault is detected at the server layer (sub-layer, as shown in Figure 9-2). When detecting a fault, the MEP (including the server MEP) sends an AIS frame to the client MD. By transmitting ETH-AIS frames, the device can inhibit or stop an alarm on MEP (or server MEP).

When receiving an AIS frame, the MEP must inhibit alarms for all peer MEPs regardless of connectivity, because this frame does not include information about MEPs that are at the same level with the failed MEP. With AIS, the device can inhibit the alarm at the client level when the server layer (sub-layer) fails. Therefore, the network is easy for maintenance and management.

- Ethernet locked signal (Lock, LCK)

This function is used to notify managed lock and service interruption of server layer (sub-layer) MEPs. The data traffic is sent to a MEP that expects to receive it. This function helps the MEP that receives ETH-LCK frame to identify a fault. It is a managed lock action for server layer (sub-layer) MEP. Lock is an optional OAM management function. One typical scenario for applying this function is used to perform detection when services are interrupted.

- Client Signal Fail (CSF)

This function is used to inform the server layer of signal faults on the client layer.

When an Up MEP has a fault occurs at the client side, it will periodically send CSF packets with LOS labels to the peer MEP. After receiving these packets, the peer MEP will report CSF alarms. When the client-side fault is cleared, the local MEP will send 3 consecutive CSF packets with DCI labels. When receives these packets, the peer MEP will exit the CSF status and report the CSF clearance alarm. This function can be used to suppress alarms.

In general, CFM is an end-to-end OAM technology at the server layer. It helps reduce operation and maintenance cost. In addition, it improves the competitiveness of service providers.

## 9.3.2 Preparing for configurations

### Scenario

To expand application of Ethernet technologies on a carrier-grade network, the Ethernet must ensure the same QoS as the carrier-grade transport network does. CFM implements this by providing overall OAM tools for the carrier-level Ethernet.

### Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.
- Create VLANs.
- Add interfaces to the VLAN.

## 9.3.3 Enabling CFM

Enable CFM for the ISCOM2600G-HI series switch as below.



### Note


CFM functions, such as fault detection and location, cannot take effect unless CFM is enabled.


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

Step	Command	Description
2	<b>Raisecom(config)#ether net cfm enable</b>	Enable global CFM. By default, this function is disabled. Use the <b>ethernet cfm disable</b> command to disable this function.
3	<b>Raisecom(config)#inter face interface-type interface-number</b>	Enter physical layer interface configuration mode.
	<b>Raisecom(config)#inter face port-channel port-channel</b>	Enter aggregation group configuration mode.
4	<b>Raisecom(config- gigaethernet1/1/*)#eth ernet cfm enable</b>	(Optional) enable CFM on the interface. By default, this function is disabled.
	<b>Raisecom(config-port- channel1)#ethernet cfm enable</b>	(Optional) enable CFM on the LAG interface. By default, this function is disabled.

## 9.3.4 Configuring basic functions of CFM

Configure basic functions of CFM for the ISCOM2600G-HI series switch as below.


Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#e thernet cfm domain [ md-name domain- name ] level level</b>	Create a MD. If a MD name is assigned by the <b>md-name</b> parameter, it indicates that the MD is in IEEE 802.1ag style and all MAs and CCMs in the MD are in 802.1ag style. Otherwise, the MD is in Y.1731 style and all MAs and CCMs in the MD are in Y.1731 style. If a name is specified for a MD, the name must be globally unique. Otherwise the MD is configured unsuccessfully.  <b>Note</b> Levels of different MDs must be different, otherwise the MD will fail to be configured.
3	<b>Raisecom(config)#s ervice cis-id level level</b>	Create a service instance and enter service instance configuration mode. Character strings composed by MD name/service instance name are globally unique. If a service instance has existed, you can use this command to enter service instance configuration mode directly.

Step	Command	Description
4	<code>Raisecom(config-service)#service vlan-list <i>vlan-list</i> [ <b>primary-vlan</b> <i>vlan-id</i> ]</code>	<p>Configure VLAN mapping based on the service instance.</p> <p>The VLAN list contains up to 32 VLANs. If you do not use the <b>primary-vlan</b> parameter to specify the primary VLAN, the minimum VLAN is taken as the primary VLAN of the service instance. All MEPs in the service instance send and receive packets through this primary VLAN.</p> <p> <b>Note</b></p> <p>The primary VLAN is used to send and receive packets. Therefore, all non-primary VLANs are logically mapped to the primary VLAN. This logical VLAN mapping is global, but VLANs cannot be crossed. For example, service instance 1 is mapped to VLANs 10–20 and service instance 2 is mapped to VLANs 15–30. Therefore, VLANs 15–20 are crossed. This configuration is illegal.</p>
5	<code>Raisecom(config-service)#service mep [ <b>up</b>   <b>down</b> ] mpid <i>mep-id</i> [ <i>interface-type</i> <i>interface-number</i>   <b>port-channel</b> <i>port-channel</i> ] [ <b>priority</b> <i>priority</i> ]</code>	<p>Configure MEPs based on a service instance.</p> <p>When configuring a MEP based on a service instance, you must ensure that the service instance is mapped to a VLAN.</p> <p>By default, the MEP is Up. It indicates detecting faults in the uplink direction.</p>
6	<code>Raisecom(config-service)#service sdp { <i>interface-type</i> <i>backup-interface-number</i>   <b>port-channel</b> <i>port-channel-list</i> } { <i>interface-type</i> <i>backup-interface-number</i>   <b>port-channel</b> <i>port-channel-list</i> } <b>secondary</b></code>	<p>Configure the distribution interface based on service instance.</p> <p>Only the uplink interface can be configured as the distribution interface.</p>

## 9.3.5 Configuring CFM fault detection

Configure CFM fault detection on the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<b>Raisecom(config)#ether net cfm errors archive-hold-time</b> <i>minute</i>	(Optional) configure the hold time of errored CCMs. Fault information reported by all MEPs is saved on the ISCOM2600G-HI series switch.  By default, the hold time of errored CCMs is 100min. When a new hold time is configured, the system will detect the database immediately. The data will be deleted if exceeding the hold time.
3	<b>Raisecom(config)#service cis-id level</b> <i>level</i>	Enter service instance configuration mode.
4	<b>Raisecom(config-service)#service cc interval { 3ms   10ms   100ms   1   10   60   600 }</b>	(Optional) configure the interval for sending CCMs.  By default, the interval for sending CCMs is 1s. The interval for sending CCM packets cannot be modified when CCM delivery is enabled.   <b>Note</b>  When the device sends hardware CC packets in the Down direction or the Up direction of 802.1ag style, it can support the <b>3ms   10ms   100ms</b> parameters. When it sends software CC packets in the Up direction of the Y.1731 style, it does not support the <b>3ms   10ms   100ms</b> parameters.
5	<b>Raisecom(config-service)#service cc enable mep { mep-id-list   all }</b>	Enable MEPs to send CCMs.  By default, MEPs do not sending CCMs.
6	<b>Raisecom(config-service)#service remote-mep</b> <i>mep-id</i> [ <b>remote-mac</b> <i>mac-address</i> ] [ <b>interface-type</b> <i>interface-number</i> ]	Configure the static RMEP. This configuration is used with CCM detection.  You can specify the MAC address of the remote MEP by specifying the <b>remote-mac</b> <i>mac-address</i> parameter.
7	<b>Raisecom(config-service)#service remote-mep learning active</b>	(Optional) configure dynamic importing of learned remote MEPs.  After this function is configured, the service instance will converts the learned dynamic remote MEP into the static remote MEP after CCM packets are received.  By default, this function is disabled.

Step	Command	Description
8	<code>Raisecom(config-service)#service cvlan <i>vlan-id</i></code>	(Optional) configure the customer VLAN of CFM OAM packets. This configuration is required in the QinQ networking environment only.  By default, CFM OAM packets do not carry C-Tag. After the customer VLAN of the service instance is configured, CCMs, LBMs, LTMs, and DMMs sent by all MEPs in the service instance will carry double Tags, of which the C-Tag is the customer VLAN Tag configured by this command.
9	<code>Raisecom(config-service)#service priority <i>priority</i></code>	(Optional) configure the priority of CFM OAM packets.  After the priority is configured, CCMs, LBMs, LTMs, and DMMs sent by MEPs in a service instance will use the assigned priority.  By default, the priority is 7.
10	<code>Raisecom(config)#snmp -server trap cfm { all   macremerr   remerr   ccmerr   xcon   none } mep { all   <i>mep-list</i> }</code>	(Optional) configure the alarm level of CFM OAM.

### 9.3.6 Configuring fault acknowledgement

Configure CFM fault acknowledgement for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#service cis-id level <i>level</i></code>	Enter service instance configuration mode.
3	<code>Raisecom(config-service)#ping { <i>mac-address</i>   mep <i>mep-id</i> } [ count <i>count</i> ] [ size <i>packet-size</i> ] [ source <i>mep-id</i> ] [ intercal <i>interval</i> ] [ timeout <i>time</i> ] [ padding { prbs   pbrs-crc   null   null-crc } ] [ cos <i>cos-value</i> ] [ non-drop ]</code>	Perform Layer 2 Ping for acknowledging faults.  By default, 5 LBMs are sent. The TLV length of a packet is 64. The ISCOM2600G-HI series switch automatically looks for an available source MEP.  If Layer 2 Ping is performed with the



Step	Command	Description
	<code>Raisecom(config-service)#ping ethernet multicast [ size packet-size ] [ timeout time ] [ padding { prbs   pbrs-crc   null   null-crc } ] [ cos cos-value ] [ non-drop ]</code>	destination MEP ID specified, CFM cannot finish the Ping operation unless it finds the MAC address of the destination MEP based on the MEP ID.  The source MEP will save RMEP data in the source MEP database after it discovers the RMEP and keeps stable. According to the MEP ID, the source MEP can find the MAC address of the RMEP in the RMEP database.



## Note

- Before using this command, ensure that global CFM is enabled. Otherwise, the Ping operation will fail.
- If there is no MEP in a service instance, the Ping operation will fail due to failing to find the source MEP.
- The Ping operation will fail if the specified source MEP is invalid. For example, the specified source MEP does not exist or CFM is disabled on the interface where the specified source MEP is.
- If the Ping operation is performed on the specified destination MEP ID, it will fail when the MAC address of the destination MEP fails to be found according to the MEP ID.
- The Ping operation will fail if other users are using the specified source MEP to perform the Ping operation.

## 9.3.7 Configuring CFM fault location

Configure CFM fault location for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ether net cfm traceroute cache enable</code>	(Optional) enable the traceroute cache switch. When the traceroute cache switch is disabled, the result will be automatically erased by the <b>traceroute</b> command.  By default, the traceroute cache switch is disabled.
3	<code>Raisecom(config)#ether net cfm traceroute cache hold-time minute</code>	(Optional) configure the hold time of data in the traceroute cache. You can configure the hold time when the traceroute cache is enabled.  By default, the hold time is 100min.

Step	Command	Description
4	<b>Raisecom(config)#ether net cfm traceroute cache size size</b>	(Optional) configure the traceroute cache size. You can configure the traceroute cache size when the traceroute cache is enabled.  By default, the traceroute cache size is 100. The data are not saved when the traceroute cache is disabled.
5	<b>Raisecom(config)#servi ce cis-id level level</b>	Enter service instance configuration mode.
6	<b>Raisecom(config- service)#traceroute { mac-address [ ttl ttl ] [ source mep- id ] [ size packet- size ]   mep mep -id [ ttl ttl ] [ source mep-id ] [ interface- mode ] [ timeout second ] [ size packet-size ] }</b>	Perform Layer 2 Traceroute for locating faults.  By default, the TLV length of a packet is 64. The ISCOM2600G-HI series switch automatically looks for an available source MEP.



## Note

- Before executing this command, ensure that global CFM is enabled. Otherwise, the Traceroute operation fails.
- If there is no MEP in a service instance, the Traceroute operation will fail because of failing to find source MEP.
- The Traceroute operation will fail if the specified source MEP is invalid. For example, the specified source MEP does not exist or CFM is disabled on the interface where the specified source MEP is.
- If the Traceroute operation is performed on the specified destination MEP ID, it will fail when the MAC address of the destination MEP fails to be found according to the MEP ID.
- If CC is disabled, you can configure the static remote MEP and specify the MAC address to guarantee that the Layer 2 Traceroute operation will proceed normally.
- The Traceroute operation will fail if other users are using the specified source MEP to perform Traceroute operation.

## 9.3.8 Configuring alarm indication signal

- Configuring AIS on the server-layer device

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#serv ice cis-id level level</b>	Enter service instance configuration mode.
3	<b>Raisecom(config- service)#service ais enable</b>	Enable AIS delivery.  By default, this function is disabled.

Step	Command	Description
4	<b>Raisecom(config-service)#service ais period { 1   60 }</b>	Configure the AIS delivery period. By default, the period for sending AIS is 1s.
5	<b>Raisecom(config-service)#service ais level level</b>	Configure the level of the customer layer MD to which AIS is sent.

- Configuring AIS on the customer-layer device

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#service cis-id level level</b>	Enter service instance configuration mode.
3	<b>Raisecom(config-service)#service suppress-alarms enable mep { mep-id   all }</b>	Enable alarm suppression. By default, this function is enabled.

### 9.3.9 Configuring Ethernet locked signal

- Configuring Ethernet locked signal on the server-layer device

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#service cisid level level</b>	Enter service instance configuration mode.
3	<b>Raisecom(config-service)#service lck start mep { all   mep-list }</b>	Enable the function of sending LCK packets. By default, this function is disabled.
4	<b>Raisecom(config-service)#service lck period { 1   60 }</b>	Configure the period for sending LCK packets. By default, the period for sending LCK packets is 1s.
5	<b>Raisecom(config-service)#service lck level level</b>	Configure the level of LCK which is sent to the client-level MD.

- Configuring Ethernet locked signal on the client-layer device

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#service cis-id level level</b>	Enter service instance configuration mode.

Step	Command	Description
3	<code>Raisecom(config-service)#service suppress-alarms enable mep { mep-id   all }</code>	Enable alarm suppression. By default, this function is enabled.

## 9.3.10 Configuring Ethernet CSF

Configure the Ethernet Client Signal Fail (CSF) for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#service csi-id level ma-level</code>	Enter service instance configuration mode.
3	<code>Raisecom(config-service)#service csf enable mpid mep-id</code>	Enable the function of sending CSF packets. By default, this function is disabled.
4	<code>Raisecom(config-service)#service csf period { 1   60 }</code>	Configure the period for sending CSF packets. By default, the period for sending CSF packets is 1s.
5	<code>Raisecom(config-service)#service csf trap enable</code>	Enable the function of sending CSF Traps upstream. This function is applicable to PW OAM only. By default, this function is disabled.

## 9.3.11 Configuring performance monitoring

Configure the performance monitoring for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#service csi-id level ma-level</code>	Enter service instance configuration mode.
3	<code>Raisecom(config-service)#service pm enable mep { all   mep-id }</code>	Enable MEP performance monitoring.

## 9.3.12 Checking configurations

Use the following commands to check configuration results.

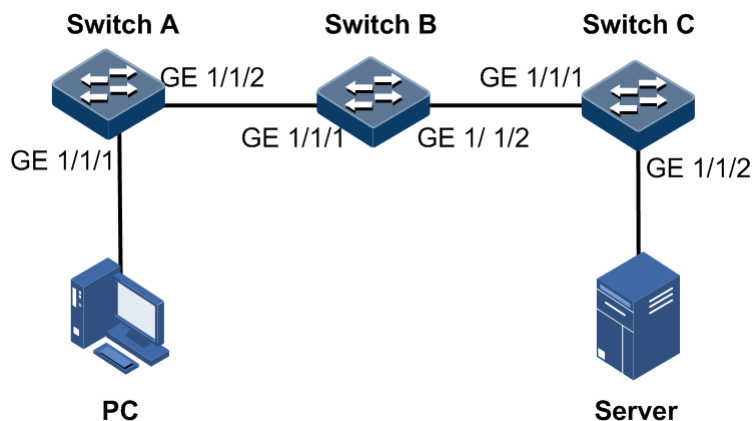
No.	Command	Description
1	<b>Raisecom#show ethernet cfm</b>	Show CFM global configurations.
2	<b>Raisecom#show ethernet cfm domain</b> <b>[ level level ]</b>	Show configurations of MD and service instance.
3	<b>Raisecom#show ethernet cfm errors</b> <b>[ level level ]</b>	Show information about the CCM errors in the database.
4	<b>Raisecom#show ethernet cfm lck</b> <b>[ level level ] [ source ]</b>	Show Ethernet locked signals.
5	<b>Raisecom#show ethernet cfm local-mp</b> <b>[ interface interface-type</b> <b>interface-number   level level ]</b>	Show configurations of the local MEP.
6	<b>Raisecom#show ethernet cfm remote-</b> <b>mep [ level level ] static</b>	Show configurations of the static RMEP.
7	<b>Raisecom#show ethernet cfm remote-</b> <b>mep [ level level [ service</b> <b>service-instance [ mpid mep-</b> <b>id ] ] ]</b>	Show information about RMEP discovery.
8	<b>Raisecom#show ethernet cfm</b> <b>suppress-alarms [ level level ]</b>	Show configurations of CFM alarm suppression.
9	<b>Raisecom#show ethernet cfm</b> <b>traceroute-cache</b>	Show information about route discovery of the Traceroute database.

### 9.3.13 Example for configuring CFM

#### Networking requirements

As shown in Figure 9-4, the PC communicates with the server through the network composed by Switch A, Switch B, and Switch C. You can deploy CFM features on Switch devices to realize carrier-grade service level, namely, to realize active fault detection, acknowledgement, and location. Switch A and Switch C are MEPs. Switch B is the MIP, detecting Ethernet fault from GE 1/1/1 on Switch A to GE 1/1/2 on Switch C. The MD level is 3.

Figure 9-4 CFM networking



## Configuration steps

Step 1 Add interfaces to the VLAN.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100 active
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#switchport access vlan 100
SwitchA(config-gigabitEthernet1/1/1)#exit
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/2)#exit
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#interface gigabitEthernet 1/1/1
SwitchB(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchB(config-gigabitEthernet1/1/1)#exit
SwitchB(config)#interface gigabitEthernet 1/1/2
SwitchB(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchB(config-gigabitEthernet1/1/2)#exit
```

Configure Switch C.

```
Raisecom#hostname SwitchC
SwitchC#config
SwitchC(config)#create vlan 100 active
SwitchC(config)#interface gigabitEthernet 1/1/2
```

```
SwitchC(config-gigaetherne1/1/2)#switch access vlan 100
SwitchC(config-gigaetherne1/1/2)#exit
SwitchC(config)#interface gigaetherne 1/1/1
SwitchC(config-gigaetherne1/1/1)#switchport mode trunk
SwitchC(config-gigaetherne1/1/1)#exit
```

Step 2 Configure CFM fault detection.

Configure Switch A.

```
SwitchA(config)#ethernet cfm domain level 3
SwitchA(config)#service ma1 level 3
SwitchA(config-service)#service vlan-list 100
SwitchA(config-service)#service mep up mpid 301 gigaetherne 1/1/1
SwitchA(config-service)#service remote-mep 302
SwitchA(config-service)#service cc enable mep all
SwitchA(config-service)#exit
SwitchA(config)#ethernet cfm enable
```

Configure Switch B.

```
SwitchB(config)#ethernet cfm domain level 3
SwitchB(config)#service ma1 level 3
SwitchB(config-service)#service vlan-list 100
SwitchB(config-service)#exit
SwitchB(config)#ethernet cfm enable
```

Configure Switch C.

```
SwitchC(config)#ethernet cfm domain level 3
SwitchC(config)#service ma1 level 3
SwitchC(config-service)#service vlan-list 100
SwitchC(config-service)#service mep up mpid 302 gigaetherne 1/1/2
SwitchC(config-service)#service remote mep 301
SwitchC(config-service)#service cc enable mep all
SwitchC(config-service)#exit
SwitchC(config)#ethernet cfm enable
```

Step 3 Execute CFM fault acknowledgement.

Take Switch A for example.

```
Switch(config)#service ma1 level 3
Switch(config-service)#ping mep 302 source 301
```

```
Sending 5 ethernet cfm loopback messages to 000e.5e03.688d, timeout is
2.5 seconds:
!!!!
Success rate is 100 percent (5/5).
Ping statistics from 000e.5e03.688d:
Received loopback replys:< 5/0/0 > (Total/Out of order/Error)
Ping successfully.
```

#### Step 4 Execute CFM fault location.

Take Switch A for example.

```
SwitchA(config)#service ma1 level 3
SwitchA(config-service)#traceroute mep 302 source 301
TTL: <64>
Tracing the route to 000E.5E00.0002 on level 3, service ma1.
Traceroute send via port1.
```

```
-----
-----
Hops  HostMac          Ingress/EgressPort  IsForwarded  RelayAction  NextHop
-----
1     000E.5E00.0003    2/1                 Yes          rlyFdb       000E.5E00.0003
2     000E.5E00.0003    1/2                 Yes          rlyFdb       000E.5E00.0001
3     000E.5E00.0001    1/-                 No           rlyHit       000E.5E00.0002
```

## Checking results

Use the **show ethernet cfm** command to show CFM configurations on the ISCOM2600G-HI series switch.

Take Switch A for example.

```
SwitchA#show ethernet cfm
Global CFM Admin Status: enable
Port CFM Enabled Portlist: P:1-28 PC:1-3
Archive hold time of error CCMS: 100(Min)
Remote mep aging time: 100(Min)
Device mode: Slave
```

## 9.4 SLA

### 9.4.1 Introduction

SLA is a telecommunication service evaluation standard negotiated by the ISP and users. It is an agreement reached by both sides in service quality, priority, and responsibility



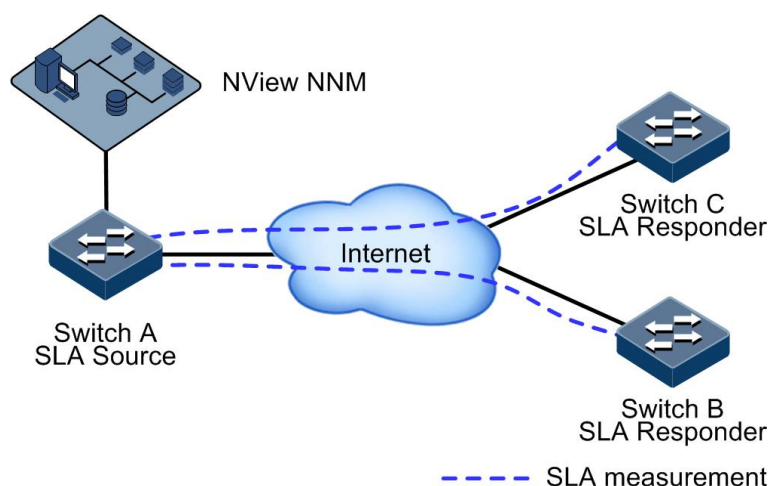
SLA is a technology for detecting network performance and gathering network statistics in real time, such as the responding time, network jitter, delay, and packet loss rate.

## SLA principle

SLA implements the end-to-end test, involving two ends:

- Source end: it sends the test packet, abstracts test data from the packet replied with by the destination end, and obtains test data through algorithms. It implements end-to-end performance test, including delay, jitter, and packet loss rate.
- Destination end: it replied the source end with the packet including test data.

Figure 9-5 SLA test networking



As shown in Figure 9-5, Switch A and Switch B are located in different spots but belong to the same user, and the user needs to test network performance between them. Configure SLA operation on Switch A with its destination address as Switch B, and then conduct scheduling to test network performance. In this way, the upper layer application (such as NVView NNM) can obtain the roundtrip packet loss rate, roundtrip delay, and jitter through SLA statistics, and then analyze network performance and provide the user with required data.

## Basic SLA concepts

- Operation

As a static concept, it is an SLA network performance testing task from end to end, including jitter test/packet loss rate (Y1731-jitter/Y1731-pkt-loss) on the Layer 2 network and delay/jitter test (ICMP-echo/ICMP-jitter) on the Layer 3 network.

- Schedule

As a dynamic concept, it is a schedule of an operation which contains multiple periodic tests. Only after the operation is scheduled can the network performance test be started.

- Test

As a dynamic concept, it is an execution of one operation. A schedule period may contain multiple test periods. Testing data output in test periods can be output as the network performance test result.

- Detection

As a dynamic concept, it is a procedure from sending a detection packet to receiving the packet. According to the definition of the operation, one operation test can contain multiple detections (one test contains only one detection for the Echo operation).

- SLA operation type
  - Loss Measurement (LM) operation: used to test packet loss rate
  - Delay Measurement (DM) operation: used to test delay and jitter
- Network performance test indexes
  - Delay: the period between receiving the packet by the receiver and sending the packet by the sender
  - Jitter: the interval for receiving two adjacent packets minus the interval for sending these two adjacent packets
  - Packet loss rate: the ratio of the number of lost packets to the number of total sent packets, usually tested within throughput range

## Supported SLA functions

Currently the ISCOM2600G-HI series switch supports the Layer 2 network delay and packet loss rate tests.

## 9.4.2 Preparing for configurations

### Scenario

The carrier and users sign SLA to guarantee that users can enjoy certain quality network service. To perform SLA protocol effectively, carrier needs to deploy SLA feature test performance on the device and the test result is evidence to ensure user's performance.

SLA chooses two testing nodes, configures SLA operation on one node, and schedules executing it to implement network performance test between the two nodes.

### Prerequisite

Deploy CFM between the tested devices.

## 9.4.3 Limits on SLA configuration

There are limits on SLA configuration.

For topology:

- For 1:1 topology, the ISCOM2600G-HI series switch supports Up on both ends, Down on both ends, or Up on one end and Down on the other end.
- For 1:n topology, SLA configuration depends on different service instances.

For statistic values:

- In bandwidth statistics, the ISCOM2600G-HI series switch gathers statistics about bandwidth based on Up MEP only.
- Services packets to be taken statistics about for packet loss rate must be known packets. The service packet VLAN and tested packet VLAN must be the same, and the service packet CoS must be the same with tested packet VLAN. For Up MEP, the statistics result

is for service packets of the UNI interface. For Down MEP, the statistics result is for service packets of the NNI interface.

- Packet loss ratio is for service packets, so SLA protocol packets should not be discarded. If SLA protocol packets are discarded, packet loss rate cannot be tested.

## 9.4.4 Default configurations of SLA

Default configurations of SLA are as below.

Function	Default value
SLA operation scheduling status	Disable
SLA Layer 2 operation CoS	0
Probe interval for SLA packet loss operations	1s
Life period for scheduling SLA operations	Forever
Test period for scheduling SLA operations	300s
SLA alarm status	<ul style="list-style-type: none"> <li>• Availability status change alarm: disable</li> <li>• Threshold alarm status: disable</li> </ul>

## 9.4.5 Creating SLA operation

Create an SLA operation for the ISCOM2600G-HI series switch as below.

All following steps are optional and in any sequence.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#sla oper-num y1731-pkt-loss slm remote-mac mac-address level level-id svlan vlan-id [ cos cos-value ] [ interval interval-num ] [ size size ]</b>	(Optional) configure SLA Y1731-pkt-loss operation according to the destination MAC address.
3	<b>Raisecom(config)#sla oper-num y1731-pkt-loss slm remote-mep mep-num level level-id svlan vlan-id [ cos cos-value ] [ interval interval-num ] [ size size ]</b>	(Optional) configure SLA Y1731-pkt-loss operation according to the destination MEP.
4	<b>Raisecom(config)#sla oper-num owner description string</b>	(Optional) configure the description of the SLA operation user.
5	<b>Raisecom(config)#sla private-tlv enable</b>	(Optional) enable the function of padding the SLA operation with the private TLV. By default, this function is disabled.



## Note

- After basic information about an operation is configured, the operation cannot be modified or reconfigured. To modify the operation, delete the operation and then reconfigure it.
- Up to 100 SLA operations can be concurrently scheduled. An operation being scheduled cannot be modified with basic information nor reconfigured before the scheduling is stopped. To reconfigure it, wait until the scheduling is stopped (the life time expires or the scheduling is interrupted).
- The private TLV is exclusively used by Raisecom devices. When you pad the SLA operation with the private TLV, you can configure the SLA operation as required and schedule it. When you do not pad the SLA operation with the private TLV, you cannot configure multiple DM or LM operations with the same VLAN, nor concurrently schedule the operation based on LB packets and these two operations.
- When you choose to pad the SLA operation with the private TLV, this may affect interoperability with devices of other vendors.

## 9.4.6 Configuring SLA scheduling

Configure SLA scheduling for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#sla schedule oper-num [ life { forever   life-time } ] [ period period ]</b>	Configure information about scheduling the SLA operation, and enable SLA operation scheduling.
3	<b>Raisecom(config)#sla schedule oper-num [ life { forever   life-time } ] [ period period ] begin</b>	(Optional) configure automatic loading of SLA operation scheduling; in other words, the ISCOM2600G-HI series switch automatically enables SLA operation scheduling upon startup.
4	<b>Raisecom(config)#exit Raisecom#write</b>	Configure and save auto-loading information.



## Note

Up to 64 SLA operations can be concurrently scheduled. An operation being scheduled cannot be modified with basic information nor reconfigured before the scheduling is stopped. To reconfigure it, wait until the scheduling is stopped (the life time expires or the scheduling is interrupted).

## 9.4.7 Configuring SLA threshold

Configure the SLA threshold for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	Raisecom(config)#sla oper-num { loss-rate-threshold   delay-threshold   jitter-threshold } { current   average } [ ds   sd   two-way ] threshold-value	(Optional) configure the packet loss rate threshold, delay threshold, or jitter threshold.
	Raisecom(config)#sla oper-num availability-threshold availability-threshod	(Optional) configure the availability threshold.
3	Raisecom(config)#sla oper-num loss-rate-threshold loss-threshod	(Optional) configure the packet loss rate threshold.



### Note

You can configure the delay threshold and jitter threshold only for the jitter operation. You can configure the packet loss rate threshold and availability threshold only for the packet loss rate operation.

## 9.4.8 Configuring maintenance window

Configure the maintenance window for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#sla maintenance{ start   stop }	Start/Stop the maintenance window of SLA operations.

## 9.4.9 Configuring availability test

Configure the availability test for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#sla oper-num availability-num-consecutive-meas-pdus number	Configure the number of test packets to be sent in the SLA availability test period.
3	Raisecom(config)#sla oper-num availability-flr-threshold threshold	Configure the packet loss rate threshold in the SLA availability test.
4	Raisecom(config)#sla oper-num availability-num-consecutive-intervals number	Configure the number of consecutive indicators in the SLA availability test.
5	Raisecom(config)#sla oper-num availability-num-consecutive-high-flr number	Configure the number of CHLI consecutive indicators in the SLA availability test.

Step	Command	Description
6	<code>Raisecom(config)#sla oper-num availability-threshold [ sd   ds ] threshold</code>	Configure the threshold in the SLA availability test.
7	<code>Raisecom(config)#sla oper-num { availability-trap   availabilitychange-trap } [ ds   sd ] enable</code>	Enable SLA availability threshold alarm or SLA availability threshold change alarm. By default, they are disabled.

## 9.4.10 Enabling alarms

Enable alarms for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#sla alarm availabilitychange enable</code>	(Optional) enable availability status change alarm.
3	<code>Raisecom(config)#sla oper-num loss-pkt-trap { current   average } enable</code> <code>Raisecom(config)#sla oper-num { delay-trap   jitter-trap } { current   average } [ ds   sd   two-way ] enable</code>	Enable threshold crossing alarm during operations.
4	<code>Raisecom(config)#sla alarm threshold enable</code>	(Optional) enable threshold alarm.

## 9.4.11 Checking configurations

Use the following commands to check configuration results.

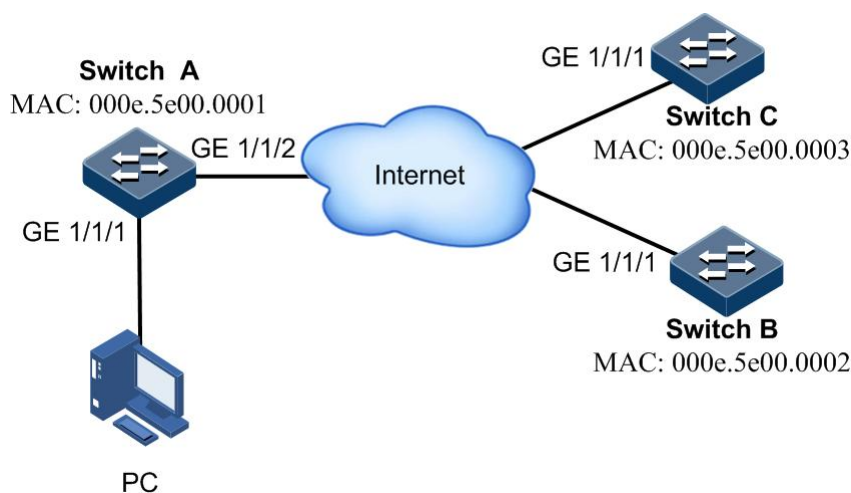
No.	Command	Description
1	<code>Raisecom#show sla { all   oper-num } configuration</code>	Show SLA configurations.
2	<code>Raisecom#show sla { all   oper-num } result</code>	Show information in the current SLA operation test period.
3	<code>Raisecom#show sla oper-num threshold</code>	Show the SLA operation threshold.
4	<code>Raisecom#show sla oper-num latest statistic</code>	Show statistics on the SLA operation in the last complete scheduling.
5	<code>Raisecom#show sla maintenance</code>	Show the maintenance window status of the device.

## 9.4.12 Example for configuring SLA

### Networking requirements

As shown in Figure 9-6, SLA is deployed on the Switch, and is periodically scheduled to test the network performance between Switch A and Switch C.

Figure 9-6 SLA test networking



### Configuration steps

Step 1 Configure CFM on the Switch.

For details, see section 9.3.13 Example for configuring CFM.

Step 2 Configure y1731-pkt-loss operation on Switch C, and enable operation scheduling.

```

Switch_C#config
Switch_C(config)#sla 2 y1731 pkt-loss remote-mac 000e.5e00.0001 level 3
svlan 3
Switch_C(config)#sla schedule 2 life 20 period 10
  
```

### Checking results

Use the **show sla configuration** command on Switch C to show SLA configurations.

```
Raisecom#show sla 2 configuration
```

```
-----
Operation <2>:
```

```

Type:          ETH-Y1731-PKT-LOSS
Frame Type:    SLM
Schedule Starttime: 0 days, 00:00:00
  
```

```
-----
Cos:          7
```

```

Service Vlan ID:          3
Customer Vlan ID:         0
MD Level:                 3
Remote DEST MAC:          000e.5e00.0001
Transmit Interval(msec):  1000
Frame Number:             5
Pdu Size(octets):         64
Avail Flr Threshold(0.001%): 50000
Avail Consec interval:    10
Avail consecutive high flr: 5
Schedule Life(sec):       20
Schedule Period(sec):     ----
Schedule Status:          Initial

```

## 9.5 BFD

### 9.5.1 Introduction

Bidirectional Forwarding Detection (BFD) is used to detect connectivity of data protocol between systems or in the same path. The can be a physical link, logical link, or channel. When finding a communication fault between systems, BFD notifies applications at the upper layer.

#### Detection mechanism

BFD establishes a session between two endpoints in the communication system, and periodically sends BFD control packets in the detection path. If one endpoint fails to receive BFD control packets within the required time, BFD considers that fault occurs in the path.

BFD control packets are encapsulated in the UDP packets and then are transmitted. At the initial stage of the session, both systems negotiate through parameters carried on the control packets (such as session identifiers of two endpoints, the minimum interval for receiving and sending packets, BFD session status of the local endpoint). When the negotiation is successful, both systems send BFD control packets according to negotiated time of receiving and sending packets.

#### Modes for establishing BFD sessions

There are two modes for establishing BFD sessions: statically establishing BFD sessions and dynamically establishing BFD sessions. BFD distinguishes these two session modes through identifiers of the local endpoint and remote endpoint in the control packet.

- Statically establishing BFD session: configure BFD session parameters manually, including identifiers of local and remote endpoints.
- Dynamically establishing BFD session: the system automatically assigns values within dynamic session identifier area to be those of the local BFD session, and the local and remote endpoints will negotiate. After receiving negotiated packets, the remote endpoint determines whether identifiers match the local BFD session. If yes, the remote endpoint automatically learns identifiers of the remote session.

The ISCOM2600G-HI series switch supports statically establishing BFD sessions.



## Application types of BFD

The ISCOM2600G-HI series switch supports the following BFD applications:

- BFD based on IP link: establish a BFD session on the IP link and use the BFD detection mechanism to detect faults rapidly. The ISCOM2600G-HI series switch supports single-hop IP detection or multi-hop IP detection on the IP link.
  - Single-hop IP detection: BFD rapidly detects communication faults between systems and supports IP connectivity detection between directly-connected devices.
  - Multi-hop IP detection: BFD rapidly detects communication faults between systems and supports IP connectivity detection between indirectly-connected devices.
- BFD based on LSP: establish a BFD session on the LSP link and use the BFD detection mechanism to detect faults of the LSP link rapidly. This BFD mode provides end-to-end protection.
- BFD based on PW: a mechanism for detecting faults of the L2VPN network. The L2VPN network rapidly detects faults of the Tunnel or PW, and guides the rapid switching of carried services, thus protecting services.
- BFD based on CR-LSP: use BFD to detect CR-LSP and thus rapidly detect LSP faults, thus triggering the switching of service traffic among different CR-LSPs in the same TE Tunnel.
- BFD based on ISIS
- BFD based on OSPF

## 9.5.2 Preparing for configurations

### Scenario

To reduce effect of faults on services and improve network availability, the ISCOM2600G-HI series switch needs to detect communication faults between itself and adjacent devices. Therefore, it can take actions immediately to ensure normal transmission of services.

### Prerequisite

N/A

## 9.5.3 Configuring BFD session binding




Configure BFD session binding for the ISCOM2600G-HI series switch as below.


Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#bfd session-id bind peer-ip ip-address [ source-ip ]</b>	Create a BFD session detection multi-hop IP path, and enter BFD session configuration mode.
	<b>Raisecom(config)#bfd session-id bind { peer-ip ip-address } interface interface-type interface-number</b>	Create a static BFD session, detect the single-hop IP path, and enter BFD session mode.

Step	Command	Description
3	<code>Raisecom(config)#bfd trap { enable   disable }</code>	(Optional) enable BFD Trap. By default, it is disabled.

## 9.5.4 Configuring BFD session parameters

Configure BFD session parameters for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#bfd session-id</code>	Enter BFD session mode.   <b>Note</b> You cannot use this command to enter BFD session mode until you create the BFD and bind it with the related path.
3	<code>Raisecom(config)#bfd { detect-multiplier multiplier   receive-interval interval   send-interval interval }*</code>	Configure the local detection multiplier, minimum sending interval, and minimum receiving interval for dynamic BFD sessions globally or on the interface.   <b>Note</b> Configure them globally for the multi-hop IP address. Configure them on the interface for single IP address or default IP address.
4	<code>Raisecom(config-bfd-session)#description description</code>	Configure the description of the BFD session.
5	<code>Raisecom(config-bfd-session)#local discriminator value</code>	Configure the local identifier of the BFD session. By default, the local identifier is displayed as 0, which indicates that no local identifier is configured.   <b>Note</b> The local identifier is automatically generated by the system if not configured.
6	<code>Raisecom(config-bfd-session)#min send- interval interval</code>	Configure the minimum sending interval for the BFD session. By default, it is 1000ms.
7	<code>Raisecom(config-bfd-session)#min receive-interval interval</code>	Configure the minimum receiving interval of the BFD session. By default, it is 1000ms.

Step	Command	Description
8	Raisecom(config-bfd-session)# <b>detect-multiplier</b> <i>multiplier</i>	Configure the local detection multiple of the BFD session. By default, it is 3.
9	Raisecom(config-bfd-session)# <b>remote discriminator</b> <i>value</i>	Configure the remote identifier of the BFD session. By default, the remote identifier is displayed as 0, which indicates that no remote identifier is configured.   <b>Note</b> The remote identifier is automatically generated by the system if not configured.
10	Raisecom(config-bfd-session)# <b>session enable</b>	Enable BFD session. By default, it is disabled.

## 9.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# <b>show bfd</b>	Show BFD global configurations.
2	Raisecom# <b>show bfd</b> [ <i>session-id</i> ] <b>config</b>	Show configurations of the specified BFD session.
3	Raisecom# <b>show bfd</b> [ <i>session-id</i> ] <b>state</b>	Show the status of the specified BFD session.
4	Raisecom# <b>show bfd</b> [ <i>session-id</i> ] <b>statistics</b>	Show statistics on the specified BFD session.
5	Raisecom# <b>show bfd</b> [ <i>session-id</i> ] <b>diagnostic-code</b>	Show the diagnostic code.

# 10 Security

---

This chapter describes basic principles and configuration procedures for security, and provides related configuration examples, including the following sections.

- ACL
- Port security MAC
- Dynamic ARP inspection
- RADIUS
- TACACS+
- Storm control
- 802.1x
- IP Source Guard
- PPPoE+
- Configuring CPU protection
- Configuring anti-ARP attack

## 10.1 ACL

### 10.1.1 Introduction

Access Control List (ACL) is a set of ordered rules, which can control the ISCOM2600G-HI series switch to receive or refuse some data packets.

You need to configure rules on the network to prevent illegal packets from affecting network performance and determine the packets allowed to pass. These rules are defined by ACL.

ACL is a series of rule composed of permit | deny sentences. The rules are described according to source address, destination address, and port ID of data packets. The ISCOM2600G-HI series switch judges receiving or rejecting packets according to the rules.

## 10.1.2 Preparing for configurations

### Scenario

ACL can help a network device recognize filter data packets. The device recognizes special objects and then permits/denies packets to pass according to the configured policy.

ACL is divided into the following types:

- Basic IPv4 ACL: define classification rules according to attributes carried in the header of IP packets, such as the source IP address and destination IP address.
- Extended IPv4 ACL: define classification rules according to attributes carried in the header of IP packets, such as the source IP address, destination IP address, bearing protocol type, and TCP or UDP port number (being 0 by default). This type can restrict Telnet/SSH login.
- MAC ACL: define classification rules according to attributes carried in the header of Layer 2 frames, such as the source MAC address, destination MAC address, and Layer 2 protocol type. When ACL denies packets with a destination MAC address, the device will not learn and show the source MAC address.
- User ACL: this type can perform the AND operation with the mask from a specified byte in the packet header or IP header, compares the character string extracted from the packet with the user-defined character string, and thus find matching packets. This type supports matching any field in the first 64 bytes of the Ethernet frame.
- IPv6 ACL: define classification rules according to attributes carried in the header of IP packets, such as the source IPv6 address, destination IPv6 address, IPv6 bearing protocol type, and TCP or UDP port number (being 0 by default). This type can restrict Telnet/SSH login.
- Advanced ACL: define classification rules according to attributes carried in the header of Layer 2 frames, such as the source MAC address and destination MAC address, and attributed carried in the header of IP packets, such as the source IP address and destination IP address.

There are 4 ACL modes according to different application environments:

- ACL based on device
- ACL based on interface
- ACL based on flow from the ingress interface to egress interface
- ACL based on VLAN

### Prerequisite

N/A

## 10.1.3 Configuring MAC ACL

Configure MAC ACL for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	Raisecom(config)# <b>access-list</b> <i>acl-number</i> [ <b>name</b> <i>acl-name</i> ]	Create an ACL, and enter ACL configuration mode. <ul style="list-style-type: none"> <li>• When the ACL number is 1000–1999, this configuration enters basic IP ACL configuration mode.</li> <li>• When the ACL number is 2000–2999, this configuration enters extended IP ACL configuration mode.</li> <li>• When the ACL number is 3000–3999, this configuration enters MAC ACL configuration mode.</li> <li>• When the ACL number is 5000–5999, this configuration enters User ACL configuration mode.</li> <li>• When the ACL number is 6000–6999, this configuration enters IPv6 ACL configuration mode.</li> <li>• When the ACL number is 7000–7999, this configuration enters advanced ACL configuration mode.</li> </ul>
3	Raisecom(config-acl-ip-std)# <b>rule</b> [ <i>rule-id</i> ] { <b>deny</b>   <b>permit</b> } { <i>source-ip-address</i> <i>source-ip-mask</i>   <b>any</b> }	(Optional) configure the matching rule for basic IP ACL.
4	Raisecom(config-acl-ip-ext)# <b>rule</b> [ <i>rule-id</i> ] { <b>deny</b>   <b>permit</b> } { <i>protocol-id</i>   <b>icmp</b>   <b>igmp</b>   <b>ip</b> } { <i>source-ip-address</i> <i>source-ip-mask</i>   <b>any</b> } { <i>destination-ip-address</i> <i>destination-ip-mask</i>   <b>any</b> } [ <b>dscp</b> <i>dscp-value</i> ] [ <b>ttl</b> <i>ttl-value</i> ] [ <b>fragment</b> ] [ <b>icmp-type</b> <i>icmp-type-value</i> ] [ <b>precedence</b> <i>precedence-value</i> ] [ <b>tos</b> <i>tos-value</i> ] [ <b>time-range</b> <i>time-range-name</i> ]	(Optional) configure the matching rule for extended IP ACL.

Step	Command	Description
	<pre> Raisecom(config-acl-ip-ext)# rule [ rule-id ] { deny   permit } { tcp   udp } { source-ip-address source-ip- mask   any } [ source-port ] [ range minimum source port maximum source port ] { destination-ip-address destination-ip-mask   any } [ destination-port ] [ ack ack- value ] [ dscp dscp-value ] [ fin fin-value ] [ fragment ] [ precedence precedence-value ] [ psh psh-value ] [ range minimum source port maximum source port ] [ rst rst-value ] [ syn syn-value ] [ tos tos-value ] [ urg urg-value ] [ ttl ttl-value ] [ time- range time-range-name ] </pre>	
5	<pre> Raisecom(config-acl-mac)#rule [ rule- id ] { deny   permit } { source-mac- address source-mac-mask   any } { destination-mac-address destination-mac-mask   any } [ ethertype { ethertype [ ethertype- mask ]   ip   arp } ] [ vlan vlanid ] [ cos cos-value ] [ cvlan cvlanid ] [ inner-cos inner-cos ] [ time-range time-range-name ] </pre>	(Optional) configure the matching rule for MAC ACL.
6	<pre> Raisecom(config-acl-udf)#rule [ rule- id ] { deny   permit } { ipv4   layer2   l2-head } [ rule-string rule-mask offset ] [ second rule- string rule-mask offset ] [ third rule-string rule-mask offset ] [ time-range time-range-name ] </pre>	(Optional) configure the matching rule for User ACL.

Step	Command	Description
7	<pre> Raisecom(config-acl-ipv6)#rule [ rule-id ] { deny   permit } { protocol-id   ipv6   icmpv6 } { source-ipv6-address/prefix   any } { destination- ipv6-address/prefix   any } [ dscp dscp-value ] [ fragment ] [flow-label flow label- value ] [ time-range time-range- name ] Raisecom(config-acl-ipv6)#rule [ rule-id ] { deny   permit } { tcp   udp } { source-ipv6-address/prefix source-ip-mask   any } { destination- ipv6-address/prefix   any } [ destination-port ] [ ack ack- value ] [ dscp dscp-value ] [ fin fin-value ] [ fragment ] [flow-label flow label-value ] [ psh psh-value ] [ rst rst-value ] [ syn syn-value ] [ urg urg-value ] [ time-range time- range-name ] </pre>	(Optional) configure the matching rule for MAP ACL.
8	<pre> Raisecom(config-acl-advanced)#rule [ rule-id ] { deny   permit } { source-mac-address source-mac-mask   any } { destination-mac-address destination-mac-mask   any } [ svlan svlanid ] [ cos cos-value ] [ cvlan cvlanid ] [ inner-cos inner-cos ] { source-ip-address source-ip-mask   any } { destination-ip-address destination-ip-mask   any } [ dscp dscp-value ] [ ttl ttl-value ] [ fragment ] [ precedence precedence- value ] [ tos tos-value ] [ time- range time-range-name ] Raisecom(config-acl-advanced)#exit </pre>	(Optional) configure the matching rule for advanced ACL.
9	<pre> Raisecom(config)#interface vlan vlan- id </pre>	Enter VLAN interface mode.
10	<pre> Raisecom(config-vlan1)#local-access access-list acl-number </pre>	(Optional) configure the SNMP ACL IP.

## 10.1.4 Configuring ACL period

Configure the ACL period for the ISCOM2600G-HI series switch as below.

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



Step	Command	Description
2	<code>Raisecom(config)#interface interface-type interface-number time-range time-range-name hour minute seconds to hour minute seconds { weekday-list   sun   mon   tue   wed   thu   fri   sat   off-day   working-day   daily } [ from hour minute seconds month-day-year ] [ to hour minute seconds month-day-year ] to hour minute seconds month-day-year</code>	Create a period for applying ACL rules.

## 10.1.5 Configuring filter

Configure the filter for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode. You can use this command on the VLAN interface.
3	<code>Raisecom(config- gigaethernet1/1/port)#filter { egress   ingress } access-list acl-number [ statistics ]</code>	Apply ACL on the interface.

## 10.1.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show access-list [ acl-number ]</code>	Show ACL configurations.
2	<code>Raisecom#show acl resource { egress   ingress }</code>	Show resources used by ACL.
3	<code>Raisecom#show filter interface</code>	Show filter configurations.
	<code>Raisecom#show filter interface interface-type interface-number [ ingress   egress ]</code>	
	<code>Raisecom#show filter interface interface-type interface-number [ ingress   egress ]</code>	
4	<code>Raisecom#show local-access access-list</code>	Show information about authentication by the SNMP server.

## 10.1.7 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
<code>Raisecom(config)#clear filter statistics interface { interface-type interface-number   vlan vlan-id } { egress   ingress } [ access-list acl-number ]</code>	Clear statistics on ACL filter configurations.

## 10.2 Port security MAC

### 10.2.1 Introduction

Port security MAC is used for the switching device on the edge of the network user side. It can ensure security of accessed data on an interface, and control the incoming packets according to the source MAC address.

You can enable port security MAC to limit and distinguish which users can access the network through secure interfaces. Only secure MAC addresses can access the network, unsecure MAC addresses will be dealt with as configured interface access violation mode.

### Secure MAC address classification

Secure MAC addresses supported by the device are divided into the following three categories:

- Static secure MAC address

The static secure MAC address is configured by user on secure interface manually; this MAC address will take effect when port security MAC is enabled. Static secure MAC address does not age and supports loading configuration.

- Dynamic secure MAC address

The dynamic secure MAC address is learnt by the device. You can configure the learnt MAC address to secure MAC address in the range of the maximum number of learnt MAC address. The dynamic secure MAC addresses are aged and does not support configuration load.

The dynamic secure MAC address can be converted to the sticky secure MAC address if necessary, so as not to be aged and supports auto-loading.

- Sticky secure MAC address

The sticky secure MAC address is generated from the manual configuration of user in secure interface or converted from dynamic secure MAC address. Different from static secure MAC address, the sticky secure MAC address needs to be used in conjunction with sticky learning:

- When sticky learning is enabled, the sticky secure MAC address will take effect and this address will not be aged.
- When sticky learning is disabled, the sticky secure MAC address will become invalid and be saved only in the system.



## Note

- When sticky learning is enabled, all dynamic secure MAC addresses learnt from an interface will be converted to sticky secure MAC addresses.
- When sticky learning is disabled, all sticky secure MAC addresses on an interface will be converted to dynamic secure MAC addresses.

## Processing mode for violating port security MAC

When the number of secure MAC addresses has already reached the maximum number, inputting of packets from a strange source MAC address will be regarded as a violation operation. For the illegal user access, there are different processing modes for configuring the switch according to secure MAC violation policy:

- Protect mode: for illegal access users, the secure interface will discard the user's packets directly.
- Restrict mode: for illegal access users, the secure interface will discard the user's packets, and the console will print Syslog information and send an alarm to the NMS.
- Shutdown mode: for illegal access users, the secure interface will discard the user's packets, and the console will print Syslog information, send an alarm to the NMS, and then shut down the secure interface.



## Caution

When the MAC address is flapping, in other words, secure interface A is accessed by a user corresponding to a secure MAC address that is already on secure interface B, secure interface A will process the access as violation.

## 10.2.2 Preparing for configurations

### Scenario

To ensure the security of data accessed by the interface of the switch, you can control the incoming packets according to source MAC address. With port security MAC, you can configure the feature of permitting specified users to access the interface, or permitting specified number of users to access from this interface only. However, when the number of users exceeds the limit, the accessed packets will be processed in accordance with port security MAC violation policies.

### Prerequisite

N/A

## 10.2.3 Default configurations of port security MAC

Default configurations of port security MAC are as below.

Function	Default value
Interface secure MAC	Disable
Aging time of dynamic secure MAC address	300s

Function	Default value
Aging type of dynamic secure MAC address	Absolute
Restoration time of port security MAC	Disable, namely, no restoration
Dynamic secure MAC sticky learning	Disable
Port secure MAC Trap	Disable
Port secure MAC violation processing mode	Protect
Maximum number of port security MAC	1

## 10.2.4 Configuring basic functions of port security MAC



### Caution

- We do not recommend enabling port security MAC on member interfaces of the LAG.
- We do not recommend using the MAC address management function to configure static MAC addresses when port security MAC is enabled.
- When the 802.1x interface adopts a MAC address-based authentication mode, port security MAC and 802.1x are mutually exclusive. We do not recommend co-configuring them concurrently.
- Port security MAC and interface-/interface VLAN-based MAC number limit are mutually exclusive, which cannot be configured concurrently.

Configure basic functions of port security MAC for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaetherne</b> <b>t1/1/port)#switchport</b> <b>port-security</b>	Enable port security MAC.
4	<b>Raisecom(config-</b> <b>gigaetherne</b> <b>t1/1/port)#switchport</b> <b>port-security maximum</b> <i>maximum</i>	(Optional) configure the maximum number of secure MAC addresses.
5	<b>Raisecom(config-</b> <b>gigaetherne</b> <b>t1/1/port)#switchport</b> <b>port-security violation { protect  </b> <b>restrict   shutdown }</b>	(Optional) configure secure MAC violation mode.
6	<b>Raisecom(config-</b> <b>gigaetherne</b> <b>t1/1/port)#no port-</b> <b>security shutdown</b> <b>Raisecom(config-</b> <b>gigaetherne</b> <b>t1/1/port)#exit</b>	(Optional) re-enable the interface which is shut down due to violating port security MAC.

Step	Command	Description
7	<b>Raisecom(config)#port-security recovery-time</b> <i>second</i>	(Optional) configure the restoration time of port security MAC.



### Note

When secure MAC violation policy is in Shutdown mode, you can use this command to re-enable this interface which is shut down due to violating port security MAC. When the interface is Up, the configured secure MAC violation mode will continue to be valid.

## 10.2.5 Configuring static secure MAC address

Configure the static secure MAC address for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/port)#switchport port-security</b>	Enable port security MAC.
4	<b>Raisecom(config-gigaethernet1/1/port)#switchport port-security mac-address</b> <i>mac-address vlan vlan-id</i>	Configure the static secure MAC address.

## 10.2.6 Configuring dynamic secure MAC address

Configure the dynamic secure MAC address for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#port-security aging-time</b> <i>period</i>	(Optional) configure the aging time of dynamic secure MAC address.
3	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config-gigaethernet1/1/port)#switchport port-security aging-type</b> { <b>absolute</b>   <b>inactivity</b> }	(Optional) configure the aging type of secure MAC addresses.

Step	Command	Description
5	Raisecom(config-gigaetherne1/1/port)# <b>switchport port-security</b>	(Optional) enable port dynamic security MAC learning.
6	Raisecom(config-gigaetherne1/1/port)# <b>switchport port-security trap enable</b>	(Optional) enable port security MAC Trap.
7	Raisecom(config-gigaetherne1/1/port)# <b>switchport port-security trap period</b> <i>value</i>	(Optional) configure the period for sending Traps for port security MAC.
8	Raisecom(config-gigaetherne1/1/port)# <b>switchport port-security trap period</b> <i>value</i>	(Optional) configure the period for sending Traps on the interface.



### Note

The **switchport port-security** command can enable port security MAC and dynamic secure MAC learning at the same time.

## 10.2.7 Configuring sticky secure MAC address



### Caution

We do not recommend configuring sticky secure MAC addresses when port sticky security MAC is disabled. Otherwise, port sticky security MAC may malfunction.

Configure the sticky secure MAC address for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaetherne1/1/port)# <b>switchport port-security</b>	Enable port security MAC.
4	Raisecom(config-gigaetherne1/1/port)# <b>switchport port-security mac-address sticky</b>	Enable sticky secure MAC learning.
5	Raisecom(config-gigaetherne1/1/port)# <b>switchport port-security mac-address sticky</b> <i>mac-address vlan vlan-id</i>	(Optional) manually configure sticky secure MAC addresses.



## Note

After sticky secure MAC address learning is enabled, the dynamic secure MAC address will be converted to the sticky secure MAC address; the manually configured sticky secure MAC address will take effect.

## 10.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show port-security [ interface-type interface-number ]</code>	Show configurations of port security MAC.
2	<code>Raisecom#show port-security mac-address [ interface-type interface-number ]</code>	Show configurations of secure MAC address and secure MAC address learning.

## 10.2.9 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
<code>Raisecom(config-gigaethernet1/1/port)#clear port-security { all   configured   dynamic   sticky }</code>	Clear a specified type of secure MAC addresses on a specified interface.

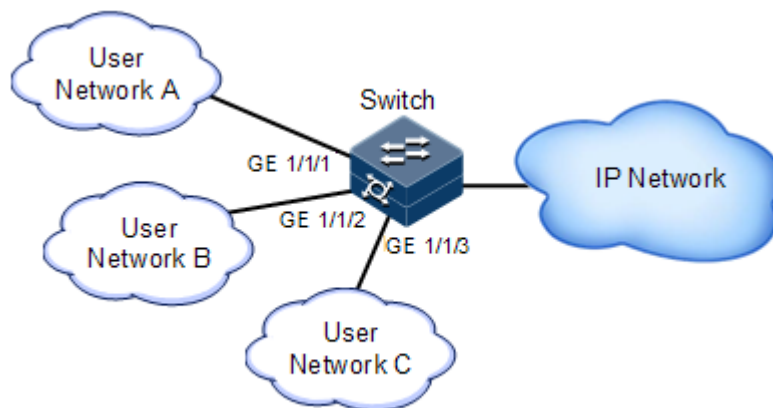
## 10.2.10 Example for configuring port security MAC

### Networking requirements

As shown in Figure 10-1, the Switch connects 3 user networks. To ensure security of data accessed from the interface, configure the Switch as below.

- GE 1/1/1 allows up to 3 users to access the network. One of specified user MAC addresses is 0000.0000.0001. The other two users are in dynamic learning mode. The NMS can receive Trap information once the user learns a MAC address. The violation mode is Protect mode and the aging time of the two learning user MAC addresses is 10min.
- GE 1/1/2 allows up to 2 users to access the network. MAC addresses of the 2 users are determined through learning; once they are learnt, they will not be aged. The violation mode is Restrict mode.
- GE 1/1/3 allows up to 1 user to access the network. The specified user MAC address is 0000.0000.0002. Whether MAC addresses are aged can be controlled. The violation mode is Shutdown mode.

Figure 10-1 Port security MAC networking



## Configuration steps

Step 1 Configure the secure MAC address on GE 1/1/1.

```
Raisecom#config
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#switchport port-security
Raisecom(config-gigabitEthernet1/1/1)#switchport port-security maximum 3
Raisecom(config-gigabitEthernet1/1/1)#switchport port-security mac-address
0000.0000.0001 vlan 1
Raisecom(config-gigabitEthernet1/1/1)#switchport port-security violation
protect
Raisecom(config-gigabitEthernet1/1/1)#switchport port-security trap enable
Raisecom(config-gigabitEthernet1/1/1)#exit
Raisecom(config)#port-security aging-time 10
```

Step 2 Configure the secure MAC address on GE 1/1/2.

```
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#switchport port-security
Raisecom(config-gigabitEthernet1/1/2)#switchport port-security maximum 2
Raisecom(config-gigabitEthernet1/1/2)#switchport port-security mac-address
sticky
Raisecom(config-gigabitEthernet1/1/2)#switchport port-security violation
restrict
Raisecom(config-gigabitEthernet1/1/2)#exit
```

Step 3 Configure the secure MAC address for GE 1/1/3.

```
Raisecom(config)#interface gigabitEthernet 1/1/3
Raisecom(config-gigabitEthernet1/1/3)#switchport port-security
Raisecom(config-gigabitEthernet1/1/3)#switchport port-security maximum 1
```



```
Raisecom(config-gigabitEthernet1/1/3)#switchport port-security mac-address
sticky 0000.0000.0002 vlan 1
Raisecom(config-gigabitEthernet1/1/3)#switchport port-security mac-address
sticky
Raisecom(config-gigabitEthernet1/1/3)#switchport port-security violation
shutdown
```

## Checking results

Use the **show port-security** command to show configurations of port security MAC.

```
Raisecom#show port-security
Port security aging time:10 (mins)
Port security recovery time:Disable (s)
port          status    Max-Num    Cur-Num    His-MaxNum    vio-Count
vio-action    Dynamic-Trap Aging-Type
-----
gigabitEthernet1/1/1    Enable    3          1          1             0
protect        Enable    Absolute
gigabitEthernet1/1/2    Enable    2          0          0             0
restrict       Disable   Absolute
gigabitEthernet1/1/3    Enable    1          1          1             0
shutdown       Disable   Absolute
gigabitEthernet1/1/4    Disable   1024       0          0             0
protect        Disable   Absolute
gigabitEthernet1/1/5    Disable   1024       0          0             0
...
```

Use the **show port-security mac-address** command to show configurations and learning of secure MAC addresses.

```
Raisecom#show port-security mac-address
VLAN  Security-MAC-Address  Flag          Port          Age(min)
-----
1      0000.0000.0001           Security-static  gigabitEthernet1/1/1  --
1      0000.0000.0002           sticky          gigabitEthernet1/1/3  --
```

## 10.3 Dynamic ARP inspection

### 10.3.1 Introduction

Dynamic ARP inspection is used for ARP protection of unsecure interface and prevents from responding ARP packets which do not meet the requirements, thus preventing ARP spoofing attack on the network.

There are 2 modes for dynamic ARP inspection:

- Static binding mode: configure the binding manually.
- Dynamic binding mode: in cooperation with the DHCP snooping to generate dynamic binding. When DHCP Snooping entry is changed, the dynamic ARP inspection will also update dynamic binding entry synchronously.

The ARP inspection table, which is used for preventing ARP attacks, consists of DHCP snooping entries and statically configured ARP inspection rules, including IP address, MAC address, and VLAN binding information. In addition, the ARP inspection table associates this information with specific interfaces. The dynamic ARP inspection binding table supports the combination of following entries:

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

Dynamic ARP inspection interfaces are divided into the following two types according to trust status:

- Trusted interface: the interface will stop ARP inspection, which conducts no ARP protection on the interface. All ARP packets are allowed to pass.
- Untrusted interface: the interface takes ARP protection. Only ARP packets that match the binding table rules are allowed to pass. Otherwise, they are discarded.

Figure 10-2 Principles of dynamic ARP inspection

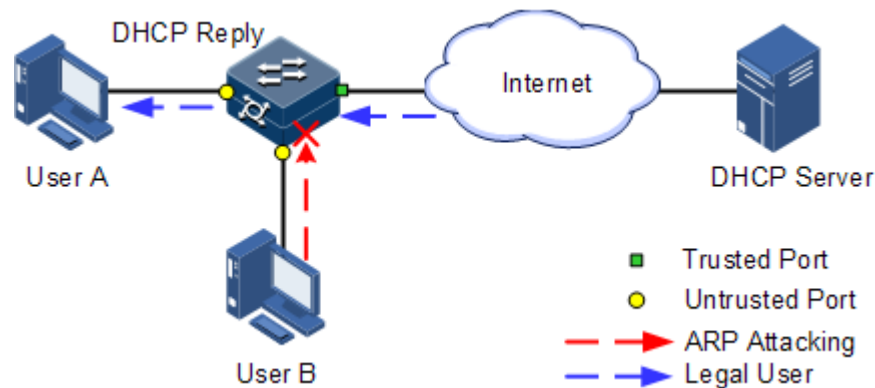


Figure 10-2 shows principles of dynamic ARP inspection. When the ISCOM2600G-HI series switch receives an ARP packet, it compares the source IP address, source MAC address, interface number, and VLAN information of the ARP packet with the DHCP Snooping entry information. If matched, it indicates that it is a legal user and the ARP packets are permitted to pass. Otherwise, it is an ARP attack and the ARP packet is discarded.

Dynamic ARP inspection also provides rate limiting on ARP packets to prevent unauthorized users from attacking the ISCOM2600G-HI series switch by sending a large number of ARP packets to the ISCOM2600G-HI series switch.

- When the number of ARP packets received by an interface per second exceeds the threshold, the system will determine that the interface encounters ARP attacks, and then discard all received ARP packets to avoid ARP attacks.

- The system provides auto-recovery and supports configuring the recovery time. The interfaces, where the number of received ARP packets is greater than the threshold, will recover to normal Rx/Tx status automatically after the recovery time expires.

Dynamic ARP inspection can also protect the specified VLAN. After the protection VLAN is configured, the ARP packets in specified VLAN on an untrusted interface will be protected. Only the ARP packets, which meet binding table rules, are permitted to pass. Other packets are discarded.

## 10.3.2 Preparing for configurations

### Scenario

Dynamic ARP inspection is used to prevent common ARP spoofing attacks on the network, which isolates ARP packets from unsafe sources. Whether to trust ARP packets depend on the trusting status of an interface while ARP packets meet requirements depends on the ARP binding table.

### Prerequisite

Enable DHCP Snooping if there is a DHCP user.

## 10.3.3 Default configurations of dynamic ARP inspection

Default configurations of dynamic ARP inspection are as below.

Function	Default value
Dynamic ARP inspection interface trust status	Untrusted
Dynamic ARP inspection static binding	Disable
Dynamic ARP inspection dynamic binding	Disable
Dynamic ARP inspection static binding table	N/A
Dynamic ARP inspection protection VLAN	All VLANs
Interface rate limiting on ARP packets	60 pps

## 10.3.4 Configuring trusted interfaces of dynamic ARP inspection

Configure trusted interfaces of dynamic ARP inspection for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.

Step	Command	Description
3	<b>Raisecom(config-gigaethernet1/1/port)#ip arp-inspection trust</b>	Configure the interface as a trusted interface. Use the <b>no ip arp-inspection trust</b> command to configure the interface to an untrusted interface; in other words, the interface does not trust the ARP packet.

### 10.3.5 Configuring static binding of dynamic ARP inspection

Configure static binding of dynamic ARP inspection for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip arp-inspection static-config</b>	Enable global static ARP binding.
3	<b>Raisecom(config)#ip arp-inspection binding</b> <i>ip-address mask [ mac-address ] [ vlan vlan-id ] interface-type interface-number</i>	Configure the static binding.

### 10.3.6 Configuring dynamic binding of dynamic ARP inspection



#### Caution

Before enabling dynamic binding of dynamic ARP inspection, you need to use the **ip dhcp snooping** command to enable DHCP Snooping.

Configure dynamic binding of dynamic ARP inspection for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip arp-inspection dhcp-snooping</b>	Enable global dynamic ARP binding.

### 10.3.7 Configuring protection VLAN of dynamic ARP inspection

Configure protection VLAN of dynamic ARP inspection for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<b>Raisecom(config)#ip arp-inspection binding dhcp-snooping { auto-update   static }</b>	Configure ARP entry conversion.
3	<b>Raisecom(config)#ip arp-inspection vlan <i>vlan-list</i></b>	Configure protection VLAN of dynamic ARP inspection.

### 10.3.8 Configuring rate limiting on ARP packets on interface

Configure rate limiting on ARP packets on the interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface <i>interface-type interface-number</i></b>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/port)#ip arp-rate-limit rate <i>rate-value</i></b>	Configure the rate limit of ARP packets on the interface.

### 10.3.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show ip arp-inspection</b>	Show configurations of dynamic ARP inspection.
2	<b>Raisecom#show ip arp-inspection binding [ <i>interface-type interface-number</i> ]</b>	Show information about the dynamic ARP inspection binding table.
3	<b>Raisecom#show ip arp-rate-limit</b>	Show configurations of rate limiting on ARP packets.

### 10.3.10 Example for configuring dynamic ARP inspection

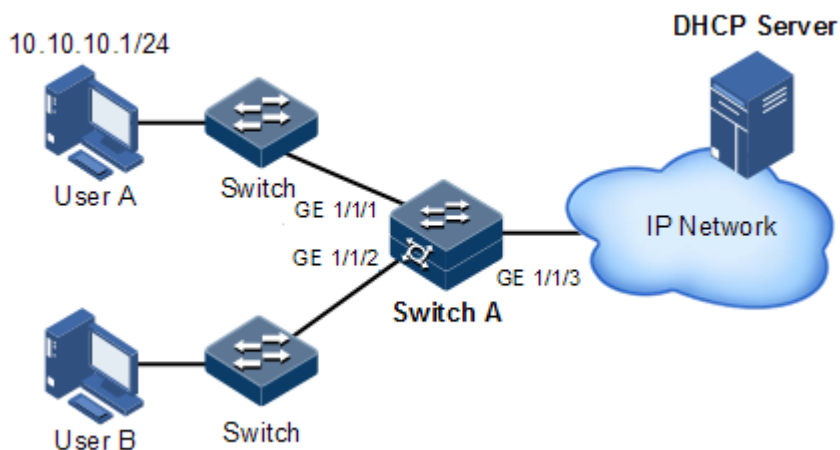
#### Networking requirements

To prevent ARP attacks, configure dynamic ARP inspection on Switch A, as shown in Figure 10-3.

- Uplink GE 1/1/3 allows all ARP packets to pass.
- Downlink GE 1/1/1 allows ARP packets with specified IP address 10.10.10.1 to pass.

- Other interfaces allow ARP packets complying with dynamic binding learnt by DHCP Snooping to pass.
- Configure rate limiting on ARP packets on downlink GE 1/1/2. The rate threshold is configured to 20 pps and recovery time for rate limiting is configured to 15s.

Figure 10-3 Configuring dynamic ARP inspection



## Configuration steps

Step 1 Configure GE 1/1/3 as the trusted interface.

```
Raisecom#config
Raisecom(config)#interface gigabitEthernet 1/1/3
Raisecom(config-gigabitEthernet1/1/3)#ip arp-inspection trust
Raisecom(config-gigabitEthernet1/1/3)#exit
```

Step 2 Configure static binding.

```
Raisecom(config)#ip arp-inspection static-config
Raisecom(config)#ip arp-inspection binding 10.10.10.1 gigabitEthernet 1/1/1
```

Step 3 Enable dynamic ARP inspection binding.

```
Raisecom(config)#ip dhcp snooping
Raisecom(config)#ip arp-inspection dhcp-snooping
```

Step 4 Configure rate limiting on ARP packets on the interface.

```
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#ip arp-rate-limit rate 20
Raisecom(config-gigabitEthernet1/1/2)#exit
```

## Checking results

Use the **show ip arp-inspection** command to show configurations of interface trust status and static/dynamic ARP binding.

```
Raisecom#show ip arp-inspection
Static Config ARP Inspection: Enable
Static Config ARP Inspection: Enable
DHCP Snooping ARP Inspection: Disable
ARP Inspection Protect Vlan : 1-4094
Bind Rule Num          : 1
Vlan Rule Num          : 0
Bind Acl Num           : 1
Vlan Acl Num           : 0
Remained Acl Num       : 511
```

Port	Trust
gigabitEthernet1/1/1	no
gigabitEthernet1/1/2	no
gigabitEthernet1/1/3	yes
gigabitEthernet1/1/4	no
gigabitEthernet1/1/5	no
gigabitEthernet1/1/6	no
gigabitEthernet1/1/7	no
.....	

Use the **show ip arp-inspection binding** command to show information about the dynamic ARP binding table.

```
Raisecom#show ip arp-inspection binding
Ip Address      Mac Address      VLAN      Port      Type
Inhw
-----
10.10.10.1      --              --        gigabitEthernet1/1/1      static
yes
Current Rules Num      : 1
History Max Rules Num : 1
```

Use the **show ip arp-rate-limit** command to show configurations of rate limiting on the interface and auto-recovery time for rate limiting.

```
Raisecom#show ip arp-rate-limit
Port                               Rate(Num/Sec)
-----
gigaethernet1/1/1                 --
gigaethernet1/1/2                 20
gigaethernet1/1/3                 --
gigaethernet1/1/4                 --
gigaethernet1/1/5                 --
gigaethernet1/1/6                 --
gigaethernet1/1/7                 --
gigaethernet1/1/8                 --
gigaethernet1/1/9                 --
```

## 10.4 RADIUS

### 10.4.1 Introduction

Remote Authentication Dial In User Service (RADIUS) is a standard communication protocol that provides centralized authentication of remote access users. RADIUS uses UDP as the transmission protocol (port 1812 and port 1813) which has a good instantaneity; at the same time, RADIUS features good reliability by supporting retransmission mechanism and standby server mechanism.

#### RADIUS authentication

RADIUS adopts client/server mode. The network access device is used as client of RADIUS server. The RADIUS server receives user connection requests, authenticates users, and replies them with configurations for providing services. In this way, RADIUS can control user to access devices and network, thus improving network security.

Communication between clients and RADIUS server is authenticated by the shared key, which will not be transmitted on the network. Besides, any user password to be transmitted between clients and RADIUS server must be encrypted to prevent it from being intercepted through sniffing through any insecure network.

#### RADIUS accounting

RADIUS accounting is used on users that have passed RADIUS authentication. When a user logs in, the device sends an Account-Start packet to the RADIUS accounting server. During user login, the device sends Account-Update packets to the RADIUS accounting server according to the accounting policy. When the user logs off, the device sends an Account-Stop packet, which contains user online time, to the RADIUS accounting server. The RADIUS accounting server can record the access time and operations of each user through these packets.



## 10.4.2 Preparing for configurations

### Scenario

You can deploy the RADIUS server on the network to conduct authentication and accounting to control users to access to the ISCOM2600G-HI series switch and network. The ISCOM2600G-HI series switch can be used as agent of the RADIUS server, which authorizes user to access according to feedback from RADIUS.

### Prerequisite

N/A

## 10.4.3 Default configurations of RADIUS

Default configurations of RADIUS are as below.

Function	Default value
RADIUS accounting	Disable
IP address of the RADIUS server	0.0.0.0
Timeout of the RADIUS server	3s
IP address of the RADIUS accounting server	0.0.0.0
Port ID of the RADIUS authentication server	1812
Port ID of the RADIUS accounting server	1813
Shared key for communicating with the RADIUS accounting server	N/A
Processing policy for accounting failure	Online
Period for sending Account-Update packets	0

## 10.4.4 Configuring RADIUS authentication

Configure RADIUS authentication for the ISCOM2600G-HI series switch as below.


Step	Command	Description
1	<code>Raisecom#radius [ backup ] { ipv4-address   ipv6-address } [ auth-port port-id ]</code>	Assign the IP address and port ID for RADIUS authentication server. Configure the <b>backup</b> parameter to assign the backup RADIUS authentication server.
2	<code>Raisecom#radius-key string</code>	Configure the shared key for RADIUS authentication.
3	<code>Raisecom#radius-encrypt-key word</code>	Configure the RADIUS authentication server to encrypt data in cyphertext mode.

Step	Command	Description
4	<b>Raisecom#radius backup key</b> <i>word</i>	Configure the shared key for the backup RADIUS authentication server.
5	<b>Raisecom#radius backup encrypt-key</b> <i>word</i>	Configure the backup RADIUS authentication server to encrypt data in cyphertext mode.
6	<b>Raisecom#user login { local-radius   radius-local</b> <b>[ server-no-response ]   radius-user }</b>	Configure users to perform login authentication through RADIUS.
7	<b>Raisecom#radius nas-ip-address</b> <i>ip-address</i>	Configure the NAS IP address of RADIUS authentication.
8	<b>Raisecom#radius response-timeout</b> <i>time</i>	Configure the timeout for response by the RADIUS authentication server.
9	<b>Raisecom#radius authorization no-privilege { default</b> <b> offline   priority }</b>	Configure the processing policy for RADIUS authorization failure.
10	<b>Raisecom#enable login { local-radius   radius-local</b> <b>[ server-no-response ]   radius-user }</b>	Configure the authentication mode for users to enter the privileged EXEC mode to RADIUS.

## 10.4.5 Configuring RADIUS accounting

Configure RADIUS accounting for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#aaa accounting login enable</b>	Enable RADIUS accounting.
2	<b>Raisecom#radius [ backup ] accounting-server</b> <i>ip-address</i> <i>[ account-port ]</i> <i>[ sourceip ip-address ]</i>	Assign IP address and UDP port ID for the RADIUS accounting server. Configure the <b>backup</b> parameter to assign the backup RADIUS accounting server.
3	<b>Raisecom#radius [ backup ] accounting-server key</b> <i>string</i> <b>Raisecom#radius [ backup ] accounting-server encrypt-key</b> <i>string</i>	Configure the shared plaintext or ciphertext key to communicate with the RADIUS accounting server. The shared key must be identical to the one configured on the RADIUS accounting server. Otherwise, accounting will fail.
4	<b>Raisecom#radius accounting nas-ip-address</b> <i>ip-address</i>	Configure the NAS IP address of the RADIUS accounting server.
5	<b>Raisecom#aaa accounting fail { offline   online }</b>	Configure the processing policy for accounting failure.

Step	Command	Description
6	<b>Raisecom#aaa accounting update <i>minute</i></b>	<p>Configure the period for sending Account-Update packets. If it is configured to 0, no Account-Update packet will be sent.</p> <div>  <b>Note</b> </div> <p>The RADIUS accounting server can record access time and operation for each user through Accounting-Start packets, Accounting-Update packets, and Accounting-End packets.</p>

## 10.4.6 Checking configurations

Use the following commands to check configuration results.

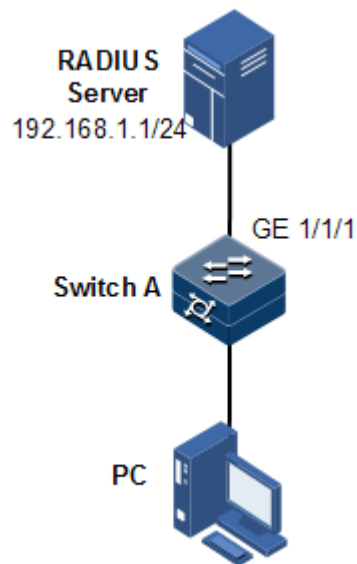
No.	Command	Description
1	<b>Raisecom#show radius-server</b>	Show configurations of the RADIUS server.
2	<b>Raisecom#show aaa</b>	Show configurations of RADIUS accounting.

## 10.4.7 Example for configuring RADIUS

### Networking requirements

As shown in Figure 10-4, to control a user from accessing the Switch, you need to configure RADIUS authentication and accounting on Switch A to authenticate login users on Switch A and record the operations. The period for sending Account-Update packets is 2 minutes. The user will be logged out if accounting fails.

Figure 10-4 RADIUS networking



## Configuration steps

Step 1 Configure authentication for login user through RADIUS.

```
Raisecom#radius 192.168.1.1
Raisecom#radius-key raisecom
Raisecom#user login radius-user
```

Step 2 Configure accounting for login user through RADIUS.

```
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 2
```

## Checking results

Use the **show radius-server** to show RADIUS configurations.

```
Raisecom#show radius-server
Radius timeout          :3s
Authentication server IP: 192.168.1.1 port:1812
Backup authentication server IP: port:1812
Authentication server key: I+NNa9u1uaix
Backup authentication server Key: --
Accounting server IP:    192.168.1.1 port:1813
```

```
Backup accounting server IP:    port:1813
Accounting server key:         orMCKszv2X38
Backup Accounting server Key:   --
```

```
Accounting fail policy:        offline
```

```
Accounting
NAS IP address:
```

Use the **show aaa** command to show RADIUS accounting.

```
Raisecom#show aaa
Accounting login:              enable
Update interval(minute):       2
Accounting fail policy:        offline
```

## 10.5 TACACS+

### 10.5.1 Introduction

Terminal Access Controller Access Control System (TACACS+) is a kind of network access authentication protocol similar to RADIUS. The differences between them are:

- TACACS+ uses TCP port 49, which has higher transmission reliability compared with UPD port used by RADIUS.
- TACACS+ encrypts the holistic of packets except the standard head of TACACS+, and there is a field to show whether the data packets are encrypted in the head of packet. Compared to RADIUS user password encryption, the TACACS+ is much safer.
- TACACS+ authentication function is separated from authorization and accounting functions; it is more flexible in deployment.

In a word, TACACS+ is safer and more reliable than RADIUS; however, as an open protocol, RADIUS is more widely used.

### 10.5.2 Preparing for configurations

#### Scenario

You can authenticate and account on users by deploying a TACACS+ server on the network to control users to access the ISCOM2600G-HI series switch and network. TACACS+ is safer and more reliable than RADIUS. The ISCOM2600G-HI series switch can be used as an agent of the TACACS+ server, and authorize users access according to feedback result from the TACACS+ server.

#### Prerequisite

N/A

## 10.5.3 Default configurations of TACACS+

Default configurations of TACACS+ are as below.

Function	Default value
TACACS+ function	Disable
Login mode	local-user
IP address of the TACACS+ authentication server	0.0.0.0, shown as "--"
IP address of the TACACS+ accounting server	0.0.0.0, shown as "--"
Shared key for communicating with the TACACS+ accounting server	N/A
Processing policy for accounting failure	Online
Period for sending Account-Update packet	0

## 10.5.4 Configuring TACACS+ authorization

Configure TACACS+ authorization for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#aaa command authorize</b> <b>{ enable   disable }</b>	Enable TACACS+ command authorization.

## 10.5.5 Configuring TACACS+ authentication

Configure TACACS+ authentication for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#tacacs-server</b> <b>[ backup ] ip-address</b> <b>[ auth-port port-id ]</b>	Assign the IP address and port number for the TACACS+ authentication server. Configure the <b>backup</b> parameter to assign the backup TACACS+ authentication server.
2	<b>Raisecom#tacacs-server</b> <b>quiet time</b>	Configure the time for the master TACACS+ authentication server to restore to the activation status.
3	<b>Raisecom#tacacs-server</b> <b>[ backup ] key string</b> <b>Raisecom#tacacs-server</b> <b>[ backup ] encrypt-key</b> <b>string</b>	Configure the shared plaintext or ciphertext key for TACACS+ authentication. Configure the <b>backup</b> parameter to assign the backup TACACS+ authentication server.
4	<b>Raisecom#user login</b> <b>{ local-tacacs   tacacs-</b> <b>local [ server-no-</b> <b>response ]   tacacs-user }</b>	Configure the login authentication mode to TACACS+.

Step	Command	Description
5	<b>Raisecom#enable login</b> <b>{ local-tacacs   tacacs-</b> <b>local [ server-no-</b> <b>response ]   tacacs-user }</b>	Configure the authentication mode for a user to enter privileged EXEC mode to TACACS+.
6	<b>Raisecom#radius response-</b> <b>timeout</b> <i>time</i>	Configure the timeout of response by the TACACS+ authentication server.

## 10.5.6 Configuring TACACS+ accounting

Configure TACACS+ accounting for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#aaa accounting</b> <b>login enable</b>	Enable TACACS+ accounting.
2	<b>Raisecom#tacacs-server</b> <b>[ backup ] { ipv4-address</b> <b>/ ipv6-address } [ acct-</b> <b>port port-id ]</b>	Assign the IP address and UDP port ID for the TACACS+ accounting server. Configure the <b>backup</b> parameter to assign the backup TACACS+ accounting server.
3	<b>Raisecom#tacacs-server key</b> <b>string</b> <b>Raisecom#tacacs [ backup ]</b> <b>accounting-server encrypt-</b> <b>key string</b>	Configure the shared plaintext or ciphertext key to communicate with the TACACS+ accounting server.
4	<b>Raisecom#aaa accounting</b> <b>fail { offline   online }</b>	Configure the processing policy for accounting failure.
5	<b>Raisecom#aaa accounting</b> <b>update period</b>	Configure the period for sending Account-Update packets. If it is configured to 0, no Account-Update packet will be sent.

## 10.5.7 Configuring TACACS+ authorization

Configure TACACS+ authorization for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#aaa command</b> <b>authorize{ enable   disable }</b>	Enable/Disable TACACS+ command authorization.

## 10.5.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show tacacs-server</b>	Show configurations of the TACACS+ authentication server.
2	<b>Raisecom#show aaa</b>	Show configurations of TACACS+ accounting.

## 10.5.9 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

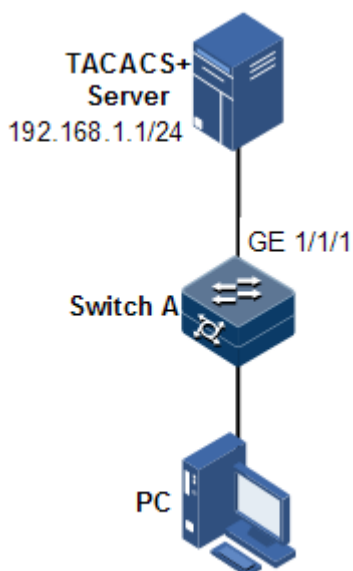
Command	Description
<b>Raisecom#clear tacacs statistics</b>	Clear TACACS+ statistics.

## 10.5.10 Example for configuring TACACS+

### Networking requirements

As shown in Figure 10-5, configure TACACS+ authentication on Switch A to authenticate login user and control users from accessing the ISCOM2600G-HI series switch.

Figure 10-5 TACACS+ networking



### Configuration steps

Configure user login authentication through TACACS+.

```
Raisecom#tacacs-server 192.168.1.1
Raisecom#tacacs-server key raisecom
```



```
Raisecom#user login tacacs-user
Raisecom#enable login local-tacacs
```

## Checking results

Use the **show tacacs-server** command to show TACACS+ configurations.

```
Raisecom#show tacacs-server
Server Address           : 192.168.1.1
Port: --
Backup Server Address    : --
Port: --
Server Shared Key        : oLMCKszV2X38
Backup Authentication server Shared Key: --
Accounting server Address : --
port: --
Backup Accounting server Address: --
Port: --
Accounting server Shared Key: --
Backup Accounting server Shared Key: --
Total Packet Sent        : 0
Total Packet Recv        : 0
Num of Error Packets     : 0
```

## 10.6 Storm control

### 10.6.1 Introduction

The Layer 2 network is a broadcast domain. When an interface receives excessive broadcast, unknown multicast, and unknown unicast packets, broadcast storm occurs. If you do not control broadcast packets, broadcast storm may occur and occupy much network bandwidth. Broadcast storm can degrade network performance and impact forwarding of unicast packets or even lead to communication halt.

Restricting broadcast flow generated from network on Layer 2 device can suppress broadcast storm and ensure common unicast forwarding normally.

### Occurrence of broadcast storm

The following flows may cause broadcast flow:

- Unknown unicast packets: unicast packets of which the destination MAC is not in the MAC address table, namely, the Destination Lookup Failure (DLF) packets. If these packets are excessive in a period, the system floods them and broadcast storm may occur.
- Unknown multicast packets: the ISCOM2600G-HI series switch neither supports multicast nor has a multicast MAC address table, so it processes received multicast packets as unknown multicast packets.

- Broadcast packets: packets of which the destination MAC is a broadcast address. If these packets are excessive in a period, broadcast storm may occur.

## Principles of storm control

Storm control allows an interface to filter broadcast packets received by the interface. After storm control is enabled, when the number of received broadcast packets reaches the pre-configured threshold, the interface will automatically discard the received packets. If storm control is disabled or if the number of received broadcast packets does not reach the pre-configured threshold, the broadcast packets are broadcasted to other interfaces of the switch properly.

## Types of storm control

Storm controls is performed in the following forms:

- Radio (bandwidth ratio): the allowed percentage of broadcast, unknown multicast, or unknown unicast traffic to total bandwidth
- Bits Per Second (BPS): the number of bits allowed to pass per second
- Packet Per Second (PPS): the number of packets allowed to pass per second

The ISCOM2600G-HI series switch supports BPS and PPS storm control.

## 10.6.2 Preparing for configurations

### Scenario

Configuring storm control on Layer 2 devices can prevent broadcast storm from occurring when broadcast packets increase sharply on the network. In this case, normal packets can be properly forwarded.

### Prerequisite

N/A

## 10.6.3 Default configurations of storm control

Default configurations of storm control are as below.

Function	Default value
Broadcast storm control	Enable
Storm control enhancement	Disable
Multicast and unknown unicast storm control	Disable
Bytes of frame gap and preamble	20 bytes
Storm control mode	pps
Number of allowed storm packets per second	1024 pps
DLF packet forwarding	Enable

Function	Default value
Action for storm control on the interface	Discarding packets
Restoration period of the interface	300s
Storm control Trap	Disable

## 10.6.4 Configuring storm control



### Caution

Storm control and VLAN-based rate limiting are exclusive. We do not recommend enabling them on the same interface concurrently.

Configure storm control for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#storm-control detection enable</b>	Enable storm control enhancement.
3	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i> <b>Raisecom(config)#vlan</b> <i>vlan-id</i> <b>Raisecom(config)#interface port-channel</b> <i>port-channel-number</i>	Enter physical layer interface configuration mode, VLAN configuration mode, or aggregation group configuration mode.
4	<b>Raisecom(config-gigaethernet1/1/port)#storm-control</b> <b>{ broadcast   unknown-multicast   dlf</b> <b>  all } { bps value [ burst value ]  </b> <b>pps value }</b> <b>Raisecom(config-vlan)#storm-control</b> <b>{ broadcast   unknown-multicast   dlf</b> <b>  all } { bps value [ burst value ]  </b> <b>pps value }</b> <b>Raisecom(config-portchannel)#storm-control</b> <b>{ broadcast   unknown-multicast   dlf   all } { bps value</b> <b>[ burst value ]   pps value }</b>	Enable storm control on the interface, VLAN, or the LAG, and configure the storm control threshold.
5	<b>Raisecom(config-gigaethernet1/1/port)#storm-control action { shutdown   drop }</b>	Configure the action for storm control on the interface.
6	<b>Raisecom(config-gigaethernet1/1/port)#storm-control interval second interval</b>	Configure the restoration period of the shutdown interface.
7	<b>Raisecom(config-gigaethernet1/1/port)#storm-control trap enable</b>	Enable storm control Trap.



## Caution

- Storm control supports only one rate limiting mode at a time. When you change the rate limiting mode of one type of packets, the ISCOM2600G-HI series switch will prompt you that the change of the rate limiting mode will cause the mode of other two types of packets to change to the same mode.
- To configure storm control in the VLAN, you must disable storm control on the interface, otherwise the configuration will not take effect.
- To configure storm control on the interface, you must disable storm control in the VLAN, otherwise the configuration will not take effect.
- If you configure storm control on the LAG, you cannot configure storm control on the interface. You must disable storm control in the VLAN, otherwise the configuration will not take effect.

## 10.6.5 Configuring DLF packet forwarding

Configure DLF packet forwarding for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#dlf-forwarding enable</b>	Enable DLF packet forwarding on an interface.

## 10.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show storm-control interface [ interface-type interface-number ]</b>	Show configurations of storm control.
2	<b>Raisecom#show dlf-forwarding</b>	Show DLF packet forwarding status.
3	<b>Raisecom#show storm-control status interface [ interface-type interface-number ]</b>	Show storm control status.
4	<b>Raisecom#show storm-control vlan [ vlan-list ]</b>	Show storm control status in the VLAN.

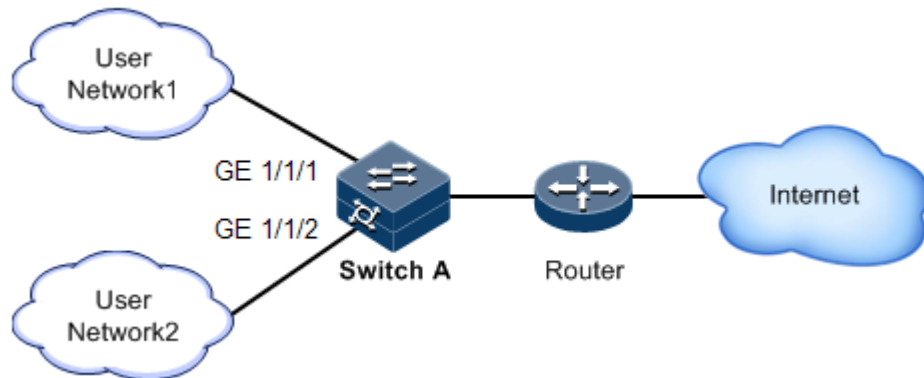
## 10.6.7 Example for configuring storm control

### Networking requirements

As shown in Figure 10-6, when GE 1/1/1 and GE 1/1/2 on the Switch receive excessive unknown unicast packets or broadcast packets, the Switch forwards these packets to all interfaces except the Rx interface, which may cause broadcast storm and lower forwarding performance of the Switch.

To restrict impacts on Switch A caused by broadcast storm, you need to configure storm control on Switch A to control broadcast packets from user networks 1 and 2, with the threshold of 640 pps.

Figure 10-6 Storm control networking



## Configuration steps

Enable storm control, and configure the threshold for storm control.

```

Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#storm-control broadcast bps 640
Raisecom(config-gigabitEthernet1/1/1)#exit
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#storm-control broadcast bps 640
  
```

## Checking results

Use the **show storm-control** command to show configurations of storm control.

```

Raisecom#show storm-control interface gigabitEthernet 1/1/1
Threshold: 0 kbps
Interface    Packet-Type    Pps(pps)      Bps(Kbps)     Cbs(kByte)
-----
GE1/1/1     Broadcast      --             640           4
            Multicast      --             0             0
            Dlf           --             0             0
  
```

## 10.7 802.1x

### 10.7.1 Introduction

802.1x, based on IEEE 802.1x, is a VLAN-based network access control technology. It is used to solve authentication and security problems for LAN users.

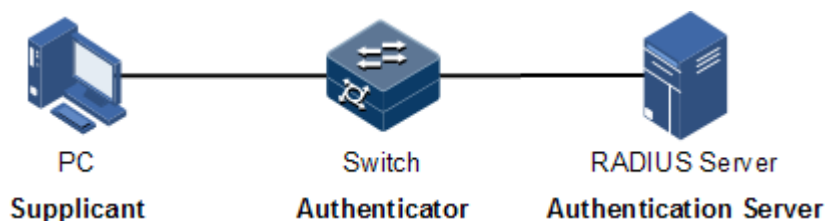
It is used to authenticate and control access devices at the physical layer of the network device. It defines a point-to-point connection mode between the device interface and user devices. User devices, connected to the interface, can access resources in the LAN if they are authenticated. Otherwise, they cannot access resources in the LAN through the switch.

### 802.1x structure

As shown in Figure 10-7, 802.1x authentication uses Client/Server mode, including the following 3 parts:

- **Supplicant:** a user-side device installed with the 802.1x client software (such as Windows XP 802.1x client), such as a PC
- **Authenticator:** an access control device supporting 802.1x authentication, such as a switch
- **Authentication Server:** a device used for authenticating, authorizing, and accounting users. Generally, the RADIUS server is taken as the 802.1x authentication server.

Figure 10-7 802.1x structure



### Interface access control modes

The authenticator uses the authentication server to authenticate clients that need to access the LAN and controls interface authorized/ unauthorized status through the authentication results. You can control the access status of an interface by configuring access control modes on the interface. 802.1x authentication supports the following 3 interface access control modes:

- **Protocol authorized mode (auto):** the protocol state machine determines the authorization and authentication results. Before clients are successfully authenticated, only EAPoL packets are allowed to be received and sent. Users are disallowed to access network resources and services provided by the switch. If clients are authorized, the interface is switched to the authorized state, allowing users to access network resources and services provided by the switch.
- **Force interface authorized mode (authorized-force):** the interface is in authorized state, allowing users to access network resources and services provided by the switch without being authorized and authenticated.
- **Force interface unauthorized mode (unauthorized-force):** the interface is in unauthorized mode. Users are disallowed to access network resources and services provided by the switch; in other words, users are disallowed to be authenticated.

## 802.1x authentication procedure

The 802.1x system supports finishing authentication procedure between the RADIUS server through EAP relay and EAP termination.

- EAP relay

The supplicant and the authentication server exchange information through the Extensible Authentication Protocol (EAP) packet while the supplicant and the authenticator exchange information through the EAP over LAN (EAPoL) packets. The EAP packet is encapsulated with authentication data. This authentication data will be encapsulated into the RADIUS protocol packet to be transmitted to the authentication server through a complex network. This procedure is call EAP relay.

Both the authenticator and the suppliant can initiate the 802.1x authentication procedure. This document takes the suppliant for example, as shown below:

- Step 1 The user enters the user name and password. The supplicant sends an EAPoL-Start packet to the authenticator to start the 802.1x authentication.
- Step 2 The authenticator sends an EAP-Request/Identity to the suppliant, asking the user name of the suppliant.
- Step 3 The suppliant replies an EAP-Response/Identity packet to the authenticator, which includes the user name.
- Step 4 The authenticator encapsulates the EAP-Response/Identity packet to the RADIUS protocol packet and sends the RADIUS protocol packet to the authentication server.
- Step 5 The authentication server compares the received user name with the one in the database, finds the password for the user, and encrypts the password with a randomly-generated encryption word. Meanwhile it sends the encryption word to the authenticator who then sends the encryption word to the suppliant.
- Step 6 The suppliant encrypts the password with the received encryption password, and sends the encrypted password to the authentication server.
- Step 7 The authentication server compares with received encrypted password with the one generated by itself. If identical, the authenticator modifies the interface state to authorized state, allowing users to access the network through the interface and sends an EAP-Success packet to the suppliant. Otherwise, the interface is in unauthorized state and sends an EAP-Failure packet to the suppliant.

- EAP termination

Terminate the EAP packet at the device and map it to the RADIUS packet. Use standard RADIUS protocol to finish the authorization, authentication, and accounting procedure. The device and RADIUS server adopt Password Authentication Protocol (PAP)/Challenge Handshake Authentication Protocol (CHAP) to perform authentication.

In the EAP termination mode, the random encryption character, used for encrypting the password, is generated by the device. And then the device sends the user name, random encryption character, and encrypted password to the RADIUS server for authentication.

## 802.1x timers

During 802.1x authentication, the following 5 timers are involved:

- Reauth-period: re-authorization timer. After the period is exceeded, the ISCOM2600G-HI series switch re-initiates authorization.
- Quiet-period: quiet timer. When user authorization fails, the ISCOM2600G-HI series switch needs to keep quiet for a period. After the period is exceeded, the ISCOM2600G-HI series switch re-initiates authorization. During the quiet time, the ISCOM2600G-HI series switch does not process authorization packets.
- Tx-period: transmission timeout timer. When the ISCOM2600G-HI series switch sends a Request/Identity packet to users, the ISCOM2600G-HI series switch will initiate the timer. If users do not send an authorization response packet during the tx-period, the ISCOM2600G-HI series switch will re-send an authorization request packet. The ISCOM2600G-HI series switch sends this packet three times in total.
- Supp-timeout: Supplicant authorization timeout timer. When the ISCOM2600G-HI series switch sends a Request/Challenge packet to users, the ISCOM2600G-HI series switch will initiate supp-timeout timer. If users do not send an authorization response packet during the supp-timeout, the ISCOM2600G-HI series switch will re-send the Request/Challenge packet. The ISCOM2600G-HI series switch sends this packet twice in total.
- Server-timeout: Authentication server timeout timer. The timer defines the total timeout period of sessions between authorizer and the RADIUS server. When the configured time is exceeded, the authenticator will end the session with the RADIUS server and start a new authorization process.

## 10.7.2 Preparing for configurations

### Scenario

To realize access authentication on LAN users and ensure access user security, you need to configure 802.1x authentication on the ISCOM2600G-HI series switch.

If users are authenticated, they are allowed to access network resources. Otherwise, they cannot access network resources. By performing authentication control on user access interface, you can manage the users.

### Prerequisite

If RADIUS authentication server is used, you need to perform following operations before configuring 802.1x authentication:

- Configure the IP address of the RADIUS server and the RADIUS shared key.
- The ISCOM2600G-HI series switch can ping through the RADIUS server successfully.

## 10.7.3 Default configurations of 802.1x

Default configurations of 802.1x are as below.

Function	Default value
Global 802.1x	Disable
Interface 802.1x	Disable
Global authentication mode	Chap
Interface access control mode	Auto



Function	Default value
Authentication method	Portbased
Re-authentication	Disable
802.1x re-authentication timer	3600s
802.1x quiet timer	60s
Transmission timeout timer	30s
Supplicant authorization timeout timer	30s

## 10.7.4 Configuring basic functions of 802.1x



### Caution

- 802.1x and STP are exclusive on the same interface. You cannot enable them concurrently.
- Only one user authentication request is processed on an interface at a time.

Configure basic functions of 802.1x for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#dot1x enable</b>	Enable global 802.1x.
3	<b>Raisecom(config)#dot1x authentication-method { chap   pap   eap }</b>	Configure global authentication mode.
4	<b>Raisecom(config)#dot1x auth-mode { radius   local   tacacs+ }</b>	Configure the mode of 802.1x authentication.
5	<b>Raisecom(config)#dot1x free-ip ip-address [ ip-mask   mask-length ]</b>	Configure the IP address segment available for 802.1x terminal users who fail to be authenticated or exit authentication.
6	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical layer interface configuration mode.
7	<b>Raisecom(config-gigaethernet1/1/port)#dot1x enable</b>	Enable interface 802.1x.
8	<b>Raisecom(config-gigaethernet1/1/port)#dot1x auth-control { auto   authorized-force   unauthorized-force }</b>	Configure access control mode on the interface.
9	<b>Raisecom(config-gigaethernet1/1/port)#dot1x auth-method { portbased   macbased }</b>	Configure access control mode of 802.1x authentication on the interface.

Step	Command	Description
10	<code>Raisecom(config-gigaethernet1/1/port)#dot1x keepalive { enable   disable }</code>	Enable or disable 802.1x handshake on the interface.
11	<code>Raisecom(config-gigaethernet1/1/port)#dot1x max-user user-number</code>	Configure the maximum number of users allowed to be authenticated by the 802.1x interface.



### Note

If 802.1x is disabled in global/interface configuration mode, the interface access control mode of 802.1x is configured to force interface authorized mode.

## 10.7.5 Configuring 802.1x re-authentication



### Caution

Re-authentication is initiated for authorized users. Before enabling re-authentication, you must ensure that global/interface 802.1x is enabled. Authorized interfaces are still in this mode during re-authentication. If re-authentication fails, the interfaces are in unauthorized state.

Configure 802.1x re-authentication for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/port)#dot1x reauthentication enable</code>	Enable 802.1x re-authentication.

## 10.7.6 Configuring 802.1x timers

Configure 802.1x timers for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/port)#dot1x timer reauth-period reauth-period</code>	Configure the time of the re-authentication timer.

Step	Command	Description
4	<code>Raisecom(config-gigaethernet1/1/port)#dot1x timer quiet-period second</code>	Configure the time of the quiet timer.
5	<code>Raisecom(config-gigaethernet1/1/port)#dot1x timer supp-timeout supp-timeout</code>	Configure the time of the supplicant authorization timeout timer.
6	<code>Raisecom(config-gigaethernet1/1/port)#dot1x timer server-timeout server-timeout</code>	Configure the time of the authentication server timeout timer.
7	<code>Raisecom(config-gigaethernet1/1/port)#dot1x timer keepalive-period second</code>	Configure the period for retransmitting KeepAlive packets by interface 802.1x.

## 10.7.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show dot1x interface-type interface-number</code>	Show 802.1x configurations on the interface.
2	<code>Raisecom#show dot1x interface-type interface-number statistics</code>	Show 802.1x statistics on the interface.
3	<code>Raisecom#show dot1x interface-type interface-number user</code>	Show user information of 802.1x authentication on the interface.
4	<code>Raisecom#show dot1x free-ip</code>	Configure the IP address segment available for 802.1x terminal users who fail to be authenticated or exit authentication.

## 10.7.8 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
<code>Raisecom(config)#clear dot1x interface-type interface-number statistics</code>	Clear interface 802.1x statistics.

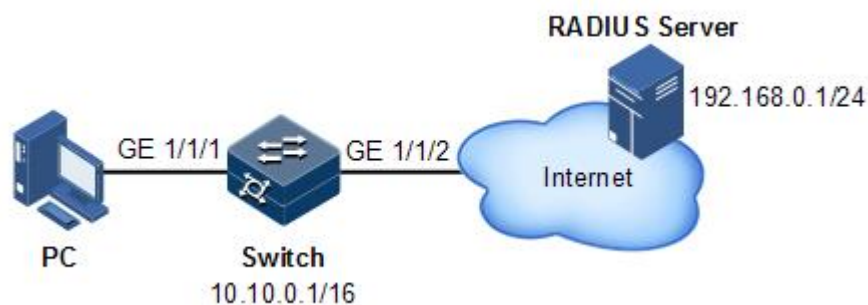
## 10.7.9 Example for configuring 802.1x

### Networking requirements

As shown in Figure 10-8, the network administrator configures 802.1x to control the PC to access the Internet.

- For the switch: the IP address is 10.10.0.1, the mask is 255.255.0.0, and default gateway is 10.10.0.2.
- The RADIUS server works to authenticate and authorize PCs. Its IP address is 192.168.0.1, and the password is raisecom.
- The interface control mode is auto.
- After the PC passes authentication, the Switch will start reauthentication every 600s.

Figure 10-8 Dot1x networking



### Configuration steps

Step 1 Configure the IP addresses of the Switch and RADIUS server.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 10.10.0.1 255.255.0.0
Raisecom(config-vlan1)#exit
Raisecom(config)#ip route 0.0.0.0 0.0.0.0 10.10.0.2
Raisecom(config)#exit
Raisecom#radius 192.168.0.1
Raisecom#radius-key raisecom
```

Step 2 Enable global 802.1x and interface 802.1x.

```
Raisecom#config
Raisecom(config)#dot1x enable
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#dot1x enable
```

- Step 3 (Optional) configure interface authorization mode to auto. By default, authentication is required and thus does not need to be configured.

```
Raisecom(config-gigabitEthernet1/1/1)#dot1x auth-control auto
```

- Step 4 Enable reauthentication, and configure the timer to 600s.

```
Raisecom(config-gigabitEthernet1/1/1)#dot1x reauthentication enable  
Raisecom(config-gigabitEthernet1/1/1)#dot1x timer reauth-period 600
```

## Checking results

Use the **show dot1x** command to show 802.1x configurations on the interface.

```
Raisecom#show dot1x gigabitEthernet 1/1/1  
802.1x Global Admin State: enable  
802.1x Authentication Method: chap  
802.1x Authentication Mode: radius  
Port gigabitEthernet1/1/1  
-----  
802.1X Port Admin State: enable  
PAE: Authenticator  
PortMethod: Portbased  
PortControl: Auto  
ReAuthentication: enable  
KeepAlive: enable  
QuietPeriod: 60(s)  
ServerTimeout: 100(s)  
SuppTimeout: 30(s)  
ReAuthPeriod: 600(s)  
TxPeriod: 30(s)  
KeepalivePeriod: 60(s)
```

## 10.8 IP Source Guard

### 10.8.1 Introduction

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:

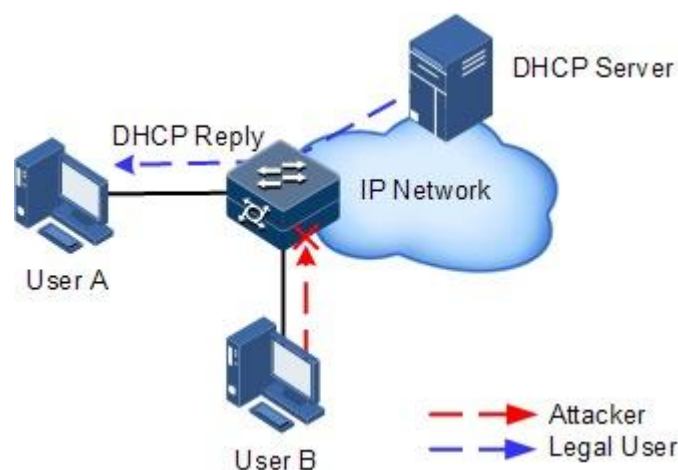
- Static binding: configure binding information manually and generate binding entry to complete the interface control, which fits for the case where the number of hosts is small or where you need to perform separate binding on a single host.
- Dynamic binding: obtain binding information automatically 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 within the ISCOM2600G-HI series switch. The IP source binding table is taken as the basis for each interface to test received data packets. Figure 10-9 shows principles of IP Source Guard.

- If the received IP packets meet the relationship of Port/IP/MAC/VLAN binding entries in IP source binding table, forward these packets.
- If the received IP packets are DHCP data packets, forward these packets.
- Otherwise, discard these packets.

Figure 10-9 Principles of IP Source Guard



Before forwarding IP packets, the ISCOM2600G-HI series switch compares the source IP address, source MAC address, interface ID, and VLAN ID of the IP packets with the binding table. If the information matches, it indicates that the user is legal and the packets are

permitted to forward normally. Otherwise, the user is an attacker and the IP packets are discarded.

## 10.8.2 Preparing for configurations

### Scenario

There are often some IP source spoofing attacks on the network. For example, the attacker forges legal users to send IP packets to the server, or the attacker forges the source IP address of another user to communicate. This prevents legal users from accessing network services normally.

With IP Source Guard binding, you can filter and control packets forwarded by the interface, prevent the illegal packets from passing through the interface, thus to restrict the illegal use of network resources and improve the interface security.

### Prerequisite

Enable DHCP Snooping if there are DHCP users.

## 10.8.3 Default configurations of IP Source Guard

Default configurations of IP Source Guard are as below.

Function	Default value
IP Source Guard static binding	Disable
IP Source Guard dynamic binding	Disable
Interface trust status	Untrusted

## 10.8.4 Configuring interface trust status of IP Source Guard

Configure the interface trust status of IP Source Guard for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)# interface interface-type interface-number</b>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config- gigaethernet1/1/p ort)#ip verify source trust</b>	(Optional) configure the interface to a trusted interface. Use the <b>no ip verify source trust</b> command to configure the interface as an untrusted interface. In this case, all packets, except DHCP packets and IP packets that meet binding relation, are not forwarded. When the interface is in trusted status, all packets are forwarded normally.

## 10.8.5 Configuring IP Source Guard binding

### Configuring IP Source Guard static binding

Configure IP Source Guard static binding for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip verify source</b>	Enable IP Source Guard static binding.
3	<b>Raisecom(config)#ip source binding</b> <i>ip-address</i> [ <i>ip-mask-address</i>   <i>mac-address</i>   <b>vlan</b> <i>vlan-id</i> } <i>interface-type interface-number</i>	Configure static binding.



#### Note

- The configured static binding does not take effect when global static binding is disabled. Only when global static binding is enabled can the static binding take effect.
- For an identical IP address, the manually configured static binding will cover the dynamic binding. However, it cannot cover the existing static binding. When the static binding is deleted, the system will recover the covered dynamic binding automatically.

### Configuring IP Source Guard dynamic binding

Configure IP Source Guard dynamic binding for the ISCOM2600G-HI series switch as below.

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.



#### Note

- The dynamic binding learnt through DHCP Snooping does not take effect when global dynamic binding is disabled. Only when global dynamic binding is enabled can the dynamic binding take effect.
- If an IP address exists in the static binding table, the dynamic binding does not take effect. In addition, it cannot cover the existing static binding.

### Configuring binding translation

Configure binding translation for the ISCOM2600G-HI series switch as below.



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)#ip source binding dhcp-snooping static</b>	Translate the dynamic binding to the static binding.
4	<b>Raisecom(config)#ip source binding auto-update</b>	(Optional) enable auto-translation. After it is enabled, dynamic binding entries learned through DHCP Snooping are directly translated into static binding entries.

## 10.8.6 Configuring priority and rate limit of IP source guard

Configure the priority and rate limit of IP source guard for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#ip verify source [ ip-address ip-mask ] set-cos cos-value [ rate-limit rate-value ]</b>	Configure the priority and rate limit of IP source guard.

## 10.8.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show ip verify source</b>	Show global binding status and interface trusted status.
2	<b>Raisecom#show ip source binding [ interface-type interface-number ]</b>	Show configurations of IP Source Guard binding, interface trusted status, and binding table.
3	<b>Raisecom#show ip verify source set-cos</b>	Show priority configurations.

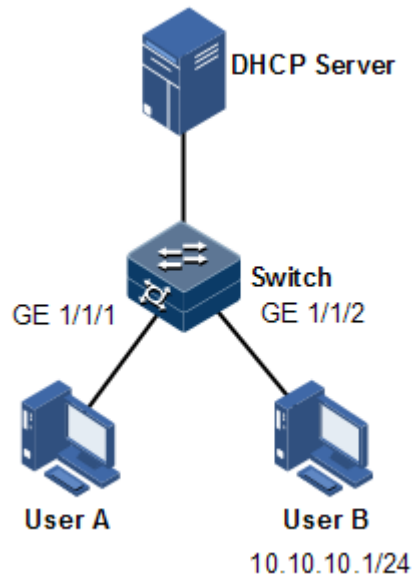
## 10.8.8 Example for configuring IP Source Guard

### Networking requirements

As shown in Figure 10-10, to prevent IP address embezzlement, you need to configure IP Source Guard on the Switch.

- The Switch permits all IP packets on GE 1/1/1 to pass.
- GE 1/1/2 permits those IP packets to pass, of which the IP address is 10.10.10.1, the subnet mask is 255.255.255.0, and the status meets the dynamic binding learnt by DHCP Snooping.
- Other interfaces only permit the packets meeting DHCP Snooping learnt dynamic binding to pass.

Figure 10-10 Configuring IP Source Guard



## Configuration steps

Step 1 Configure GE 1/1/1 to the trusted interface.

```
Raisecom#config
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#ip verify source trust
Raisecom(config-gigabitEthernet1/1/1)#exit
```

Step 2 Configure static binding.

```
Raisecom(config)#ip verify source
Raisecom(config)#ip source binding 10.10.10.1 gigabitEthernet 1/1/2
```

Step 3 Enable global dynamic IP Source Guard binding.

```
Raisecom(config)#ip verify source dhcp-snooping
```

## Checking results

Use the **show ip source binding** command to show configurations of the static binding table.

```
Raisecom#show ip source binding
History Max Entry Num: 1
Current Entry Num: 1
Ip Address          Mac Address      VLAN   Port
Type               Inhw
-----
10.10.10.1         --              --     gigaethernet1/1/2
static             yes
```

Use the **show ip verify source** command to show interface trusting status and configurations of IP Source Guard static/dynamic binding.

```
Raisecom#show ip verify source
Static Bind: Enable
Dhcp-Snooping Bind: Enable
Port               Trust
-----
gigaethernet1/1/1  yes
gigaethernet1/1/2  no
gigaethernet1/1/3  no
gigaethernet1/1/4  no
gigaethernet1/1/5  no
gigaethernet1/1/6  no
gigaethernet1/1/7  no
.....
```

## 10.9 PPPoE+

### 10.9.1 Introduction

PPPoE Intermediate Agent (PPPoE+) is used to process authentication packets. PPPoE+ adds more information about access devices into the authentication packet to bind account and access device so that the account is not shared and stolen, and the carrier's and users' interests are protected. This provides the server with enough information to identify users, avoiding account sharing and theft and ensuring the network security.

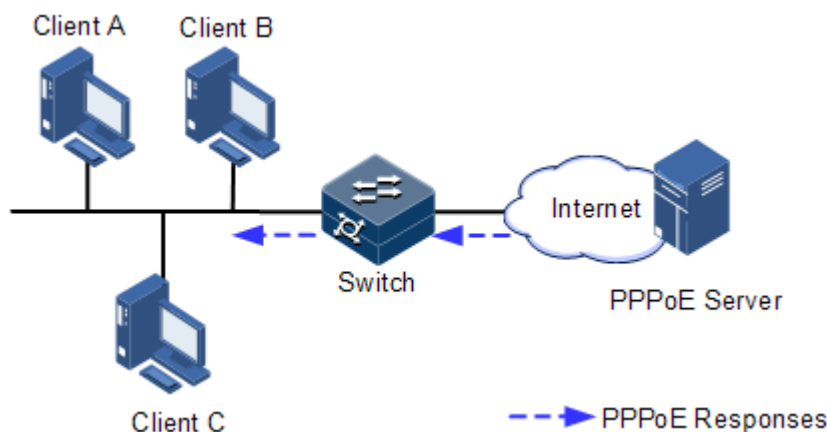
In PPPoE dial-up mode, you can access the network through various interfaces on the device as long as authentication by the authentication server is successful.

However, the server cannot accurately differentiate users just by the authentication information, which contains the user name and password. With PPPoE+, besides the user name and the password, other information, such as the interface ID, is included in the authentication packet for authentication. If the interface ID identified by the authentication

server cannot match with the configured one, authentication will fail. This helps prevent illegal users from stealing accounts of other legal users for accessing the network.

The PPPoE protocol adopts Client/Server mode, as shown in Figure 10-11. The Switch acts as a relay agent. Users access the network through PPPoE authentication. If the PPPoE server needs to locate users, more information should be contained in the authentication packet.

Figure 10-11 Accessing the network through PPPoE authentication



To access the network through PPPoE authentication, you need to pass through the following 2 stages: discovery stage (authentication stage) and session stage. PPPoE+ is used to process packets at the discovery stage. The following steps show the whole discovery stage.

- Step 1 To access the network through PPPoE authentication, the client sends a broadcast packet PPPoE Active Discovery Initiation (PADI). This packet is used to query the authentication server.
- Step 2 After receiving the PADI packet, the authentication server replies a unicast packet PPPoE Active Discovery Offer (PADO).
- Step 3 If multiple authentication servers reply PADO packets, the client selects one from them and then sends a unicast PPPoE Active Discovery Request (PADR) to the authentication server.
- Step 4 After receiving the PADR packet, if the authentication server believes that the user is legal, it sends a unicast packet PPPoE Active Discovery Session-confirmation (PADS) to the client.

PPPoE is used to add user identification information in to PADI and PADR. Therefore, the server can identify whether the user identification information is identical to the user account for assigning resources.

## 10.9.2 Preparing for configurations

### Scenario

To prevent illegal client access during PPPoE authentication, you need to configure PPPoE+ to add additional user identification information in PPPoE packets for network security.

Because the added user identification information is related to the specified switch and interface, the authentication server can bind the user with the switch and interface to effectively prevent account sharing and theft. In addition, this helps users enhance network security.

## Prerequisite

N/A

### 10.9.3 Default configurations of PPPoE+

Default configurations of I PPPoE+ are as below.

Function	Default value
Global PPPoE	Disable
Interface PPPoE	Disable
Padding mode of Circuit ID	Switch
Circuit ID information	Interface ID/VLAN ID/attached string
Attached string of Circuit ID	hostname
Padded MAC address of Remote ID	MAC address of the switch
Padding mode of Remote ID	Binary
Interface trusted status	Untrusted
Tag overriding	Disable



#### Note

By default, PPPoE packets are forwarded without being attached with any information.

### 10.9.4 Configuring basic functions of PPPoE+



#### Caution

PPPoE+ is used to process PADI and PADR packets. It is designed for the PPPoE client. Generally, PPPoE+ is only enabled on interfaces that are connected to the PPPoE client. Trusted interfaces are interfaces through which the switch is connected to the PPPoE server. PPPoE+ and trusted interface are exclusive; in other words, an interface enabled with PPPoE+ cannot be configured as a trusted interface.

#### Enabling PPPoE+

After global PPPoE+ and interface PPPoE+ is enabled, PPPoE authentication packets sent to the interface will be attached with user information and then are forwarded to the trusted interface.

Enable PPPoE+ for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<code>Raisecom(config)#pppoeagent enable</code>	Enable global PPPoE+.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
4	<code>Raisecom(config- gigaethernet1/1/1)#pppoeagent enable</code>	Enable interface PPPoE+.

## Configuring PPPoE trusted interface

The PPPoE trusted interface can be used to prevent PPPoE server from being cheated and avoid security problems because PPPoE packets are forwarded to other non-service interfaces. Generally, the interface connected to the PPPoE server is configured to the trusted interface. PPPoE packets from the PPPoE client to the PPPoE server are forwarded by the trusted interface only. In addition, only PPPoE received from the trusted interface can be forwarded to the PPPoE client.

Configure the PPPoE trusted interface for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#pppoeagent trust</code>	Configure the PPPoE trusted interface.



### Note

Because PPPoE+ is designed for the PPPoE client instead of the PPPoE server, downlink interfaces of the device cannot receive the PADO and PADS packets. It means that interfaces, where PPPoE+ is enabled, should not receive PADO and PADS packet. If there interfaces receive these packets, it indicates that there are error packets and the packets should be discarded. However, these interfaces can forward PADO and PADS packets of trusted packet. In addition, PADI and PADR packets are forwarded to the trusted interface only.

## 10.9.5 Configuring PPPoE+ packet information

PPPoE is used to process a specified Tag in PPPoE packets. This Tag contains Circuit ID and Remote ID.

- Circuit ID: is padded with the VLAN ID, interface number, and host name of request packets at the RX client.
- Remote ID: is padded with the MAC address of the client or the switch.

## Configuring Circuit ID

The Circuit ID has 2 padding modes: Switch mode and ONU mode. By default, Switch mode is adopted. In ONU mode, the Circuit ID has a fixed format. The following commands are used to configure the padding contents of the Circuit ID in Switch mode.

In switch mode, the Circuit ID supports 2 padding modes:

- Default mode: when customized Circuit ID is not configured, the padding content is the VLAN ID, interface number, or the attached string. If the attached string is not defined, it is configured to hostname by default.
- Customized mode: when customized Circuit ID is configured, the padding content is the Circuit ID string.

Configure Circuit ID for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#pppoeagent circuit-id { attach-string   format   hex } string</b>	Configure the attached string of Circuit ID.
3	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config- gigaethernet1/1/1)#pppoeagent circuit-id string</b>	(Optional) configure the Circuit ID to the customized string.

In default mode, the Circuit ID contains an attached string. By default, the attached string is configured to the hostname of the switch. You can configure it to a customized string.

Configure the attached string of the Circuit ID for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config )#pppoeagent circuit-id attach-string string</b>	(Optional) configure the attached string of the Circuit ID. If the Circuit ID is in default mode, attached string configured by this command will be added to the Circuit ID.

## Configuring Remote ID

The Remote ID is padded with a MAC address of the switch or a client. In addition, you can specify the form (binary/ASCII) of the MAC address.

Configure the Remote ID for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/1)#pppoeagent</b> <b>remote-id { client-mac   switch-</b> <b>mac }</b>	(Optional) configure PPPoE+ Remote ID to be padded with the MAC address.
4	<b>Raisecom(config-</b> <b>gigaethernet1/1/1)#pppoeagent</b> <b>remote-id format { ascii   binary }</b>	(Optional) configure the padding modes of the PPPoE+ Remote ID.

## Configuring Tag overriding

Tags of some fields may be forged by the client because of some reasons. The client overrides the original Tags. After Tag overriding is enabled, if PPPoE packets contain Tags, these Tags are overridden. If not, add Tags to these PPPoE packets.

Configure Tag overriding for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/1)#pppoeagent</b> <b>vendor-specific-tag overwrite enable</b>	Enable Tag overriding.

## 10.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show pppoeagent</b>	Show PPPoE+ configurations.
2	<b>Raisecom#show pppoeagent statistic</b>	Show PPPoE+ statistics.

## 10.9.7 Maintenance

Maintain the ISCOM2600G-HI series switch as below.



Command	Description
<code>Raisecom(config)#clear pppoeagent statistic interface-type interface-number</code>	Clear PPPoE+ statistics. The device supports clearing PPPoE+ statistics on the specified interface.

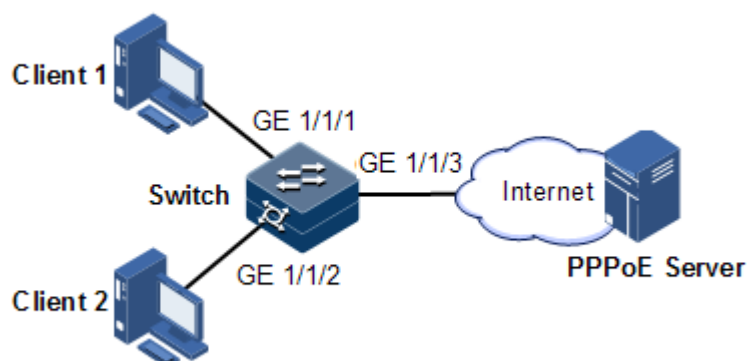
## 10.9.8 Example for configuring PPPoE+

### Networking requirements

As shown in Figure 10-12, to prevent illegal clients from accessing and managing legal users, you can configure PPPoE+ on the Switch.

- GE 1/1/1 and GE 1/1/2 are connected to Client 1 and Client 2 respectively. GE 1/1/3 is connected to the PPPoE server.
- Enable global PPPoE+, and PPPoE on GE 1/1/1 and GE 1/1/2. Configure GE 1/1/3 as the trusted interface.
- Configure the attached string of Circuit ID to raisecom, padding information about Circuit ID on GE 1/1/1 to user01, padding information about Circuit ID on GE 1/1/2 to the MAC address of Client 2, in ASCII format.
- Enable Tag overwriting on GE 1/1/1 and GE 1/1/2.

Figure 10-12 PPPoE+ networking



### Configuration steps

Step 1 Configure GE 1/1/3 as the trusted interface.

```

Raisecom#config
Raisecom(config)#interface gigabitEthernet 1/1/3
Raisecom(config-gigabitEthernet1/1/3)#pppoenagent trust
Raisecom(config-gigabitEthernet1/1/3)#exit
  
```

Step 2 Configure packet information about GE 1/1/1 and GE 1/1/2.

```
Raisecom(config)#pppoeagent circuit-id attach-string raisecom
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#pppoeagent circuit-id user01
Raisecom(config-gigabitEthernet1/1/1)#exit
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#pppoeagent remote-id client-mac
Raisecom(config-gigabitEthernet1/1/2)#pppoeagent remote-id format ascii
Raisecom(config-gigabitEthernet1/1/2)#exit
```

Step 3 Enable Tag overwriting on GE 1/1/1 and GE 1/1/2.

```
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#pppoeagent vendor-specific-tag
overwrite enable
Raisecom(config-gigabitEthernet1/1/1)#exit
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#pppoeagent vendor-specific-tag
overwrite enable
Raisecom(config-gigabitEthernet1/1/2)#exit
```

Step 4 Enable global PPPoE+, and PPPoE on GE 1/1/1 and GE 1/1/2.

```
Raisecom(config)#pppoeagent enable
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#pppoeagent enable
Raisecom(config-gigabitEthernet1/1/1)#exit
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#pppoeagent enable
```

## Checking results

Use the **show pppoeagent** command to show PPPoE+ configurations.

```
Raisecom#show pppoeagent
Global PPPoE+ status: enable
Attach-string: %default%
Circuit ID padding mode: switch

Port      :gigabitEthernet1/1/1
State     :enable
Overwrite  :enable
Format-rules :binary
Remote-ID  :client-mac
Circuit-ID  :(21ra

Port      :gigabitEthernet1/1/2
State     :disable
```

```

overwrite :disable
Format-rules :binary
Remote-ID :switch-mac
Circuit-ID :%default%

Port :gigaethernet1/1/3
State :disable
overwrite :disable
Format-rules :binary

```

## 10.10 Configuring CPU protection

### 10.10.1 Preparing for configurations

#### Scenario

When the ISCOM2600G-HI series switch receives massive attacking packets in a short period, the CPU will run with full load and the CPU utilization rate will reach 100%. This will cause device malfunction. CPU CAR helps efficiently limit the speed of packets which enters the CPU.

#### Prerequisite

N/A

### 10.10.2 Configuring global CPU CAR

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#cpu-protect car</b> <b>{ arp   dhcp   global   icmp   igmp</b> <b>  bpdu } { kbps cir cir cbs cbs  </b> <b>pps pps value }</b>	Configure the protocol type, CIR, and CBS of global CPU packet protection.
3	<b>Raisecom(config)#cpu-protect car</b> <b>period time</b>	Configure the restoration time. Use the <b>no</b> form of this command to delete the configuration.
4	<b>Raisecom(config)#cpu-protect car</b> <b>trap { enable   disable }</b>	Enable or disable global CPU packet protection Trap.

### 10.10.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show cpu-protect car statistics</b> [ <i>interface-type interface-number</i> ] [ <b>dynamic</b> ]	Show CPU CAR statistics.

## 10.10.4 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
<b>Raisecom(config)#clear cpu-protect car { arp   bpdu   dhcp   global   icmp   igmp   llbp   mld   stp } statistics</b>	Clear global CPU CAR statistics.

## 10.11 Configuring anti-ARP attack

### 10.11.1 Preparing for configurations

#### Scenario

ARP is simple and easy to use, but vulnerable to attacks due to no security mechanism.

Attackers can forge ARP packets from users or gateways. When they send excessive IP packets, whose IP addresses cannot be resolved, to the ISCOM2600G-HI series switch, they will cause the following harms:

- The ISCOM2600G-HI series switch sends excessive ARP request packets to the destination network segment, so this network segment is overburdened.
- The ISCOM2600G-HI series switch repeatedly resolve destination IP addresses, so the CPU is overburdened.

To prevent these harms due to attacks on IP packets, the ISCOM2600G-HI series switch supports anti-ARP attack.

#### Prerequisite

N/A

### 10.11.2 Configuring ARP

Configure ARP for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface vlan</b> <i>vlan-id</i>	Enter VLAN interface configuration mode.

Step	Command	Description
3	<b>Raisecom(config-vlan1)#arp learning strict enable</b>	Enable the device to learn ARP entries requested by itself.
4	<b>Raisecom(config-vlan1)#arp check-destination-ip enable</b>	Enable the check of ARP destination IP address.
5	<b>Raisecom(config-vlan1)#arp filter { gratuitous   mac-illegal   tha-filled-request }</b>	Configure ARP filtering.
6	<b>Raisecom(config-vlan1)#arp anti-attack entry-check { fixed-all   fixed-mac   send-ack }</b>	Configure the fixing of ARP entries.
7	<b>Raisecom(config-vlan1)#ip arp-rate-limit rate <i>rate value</i></b>	Configure rate limiting of ARP.

### 10.11.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show arp</b>	Show ARP information.
2	<b>Raisecom#show ip arp filter</b>	Show information about ARP filtering.

# 11 Reliability

---

This chapter describes basic principles and configuration procedures for reliability, and provides related configuration examples, including the following sections:

- Link aggregation
- Interface backup
- Link-state tracking
- UDLD
- mLACP

## 11.1 Link aggregation

### 11.1.1 Introduction

Link aggregation refers to aggregating multiple physical Ethernet interfaces to a Link Aggregation Group (LAG) and taking multiple physical links in the same LAG as one logical link. Link aggregation helps share traffic among members in the LAG. Besides effectively improving reliability on links between two devices, link aggregation helps gain higher bandwidth without upgrading hardware.

Generally, the link aggregation consists of manual link aggregation, static Link Aggregation Control Protocol (LACP) link aggregation, and dynamic LACP link aggregation.

- Manual link aggregation

Manual link aggregation refers to aggregating multiple physical interfaces to one logical interface so that they can balance load.

- Static LACP link aggregation

Link Aggregation Control Protocol (LACP) is a protocol based on IEEE802.3ad. LACP communicates with the peer through the Link Aggregation Control Protocol Data Unit (LACPDU). In addition, you should manually configure the LAG. After LACP is enabled on an interface, the interface sends a LACPDU to inform the peer of its system LACP protocol priority, system MAC address, interface LACP priority, interface number, and operation Key.

After receiving the LACPDU, the peer compares its information with the one received from other interfaces to select an interface able to be in Selected status, on which both sides can

agree. The operation key is a configuration combination automatically generated based on configurations of the interface, such as the speed, duplex mode, and Up/Down status. In a LAG, interfaces in the Selected status share the identical operation key.

- Dynamic LACP link aggregation

In dynamic LACP link aggregation, the system automatically creates and deletes the LAG and member interfaces through LACP. Interfaces cannot be automatically aggregated into a group unless their basic configurations, speeds, duplex modes, connected devices, and the peer interfaces are identical.

In manual aggregation mode, all member interfaces are in forwarding status, sharing loads. In static/dynamic LACP mode, there are backup links.

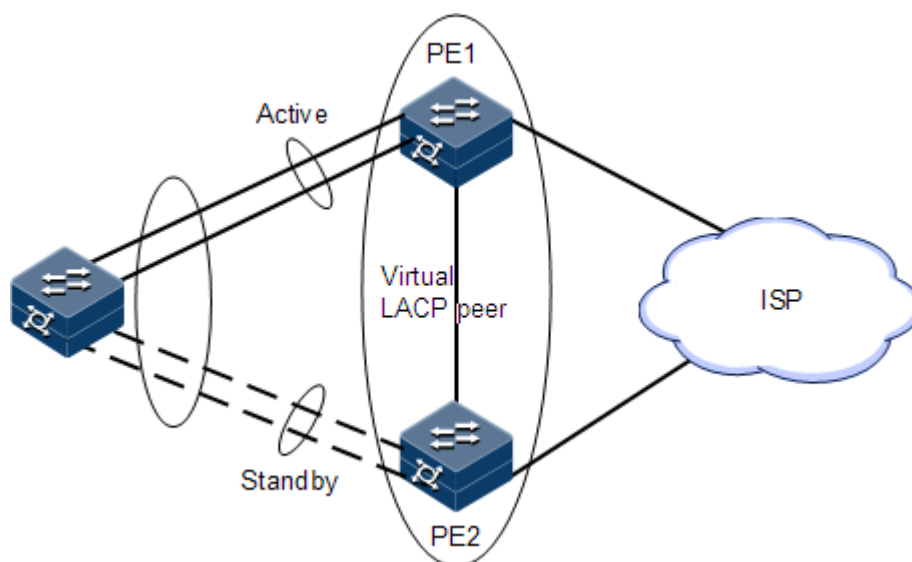
Link aggregation is the most widely used and simplest Ethernet reliability technology.

- mLACP

On the carrier-grade Ethernet, various redundancy mechanisms provide nodes and networks with reliable links. Choosing redundancy mechanisms depends on factors, such as the transmission technology, topology, multi-homing of a single node to the entire network, device capability, AS boundary, carrier's service model, and carrier's choice. High reliability of the carrier-grade Ethernet is accessible from concurrently applying the redundancy mechanism inside the device and that between racks.

When technologies keep growing, the Dual Home Device (DHD) emerges, which features two uplink access points as a redundancy mechanism. Sometimes, the DHD does not want or is incapable of running any loop detection protocols. To provide more choices, Raisecom realizes Multi-Chassis Link Aggregation Control Protocol (mLACP) to select paths for the DHD.

Figure 11-1 Dual-homed application based on LACP



As shown in Figure 11-1, the DHD exchanges LACP packets with PE 1 and PE 2, and two PEs exchange configuration information through InterChassis Communication Protocol (ICCP), synchronizing the status of each other (each PE receives and saves information about the other). The two PEs form a virtual LACP peer and appear as a single device to the DHD.

Links that connect the DHD are configured to the same Link Aggregation Group (LAG). Interface selection and link aggregation are implemented through LACP. In this case, the two PEs in the same LAG appear to be in one Inter-Chassis Group (ICG).

The whole system, according to the configured priority, selects a PE from the ICG to be the active one by using LACP. The active PE will communicate with DHD. In one ICG, only one PE can be active and the other standby.

When the number of Up links between the active PE and the DHD is smaller than the configured number of LAG links, or all uplink interfaces on the PE becomes Down, the system will perform fault switching, making the other PoA active and the local PE standby. When faults at the local PoA are cleared, the system will perform fault recovery, re-electing the local PoA as the active one.

## 11.1.2 Preparing for configurations

### Scenario

To provide higher bandwidth and reliability for a link between two devices, configure link aggregation.

### Prerequisite

- Configure physical parameters of interfaces and make them Up.
- In the same LAG, member interfaces that share loads must be identically configured. Otherwise, data cannot be forwarded properly. These configurations include QoS, QinQ, VLAN, interface properties, and MAC address learning.
  - QoS: traffic policing, traffic shaping, congestion avoidance, rate limit, SP queue, WRR queue scheduling, interface priority and interface trust mode
  - QinQ: QinQ enabling/disabling status on the interface, added outer VLAN tag, policies for adding outer VLAN Tags for different inner VLAN IDs
  - VLAN: the allowed VLAN, default VLAN and the link type (Trunk or Access) on the interface, subnet VLAN configurations, protocol VLAN configurations, and whether VLAN packets carry Tag
  - Port properties: whether the interface is added to the isolation group, interface rate, duplex mode, and link Up/Down status
  - MAC address learning: whether MAC address learning is enabled and whether the interface is configured with MAC address limit.

## 11.1.3 Configuring manual link aggregation

Configure manual link aggregation for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface port-channel <i>channel-number</i></b>	Enter LAG configuration mode.
3	<b>Raisecom(config-port-channel1)#mode manual</b>	Configure manual link aggregation mode.



Step	Command	Description
4	<code>Raisecom(config-port-channel)#{ <b>max-active</b>   <b>min-active</b> } <b>links</b> <i>value threshold</i></code>	(Optional) configure the maximum or minimum number of active links in LACP LAG.  By default, the maximum number is 8 while the minimum is 1.
5	<code>Raisecom(config-port-channel)#<b>load-sharing mode</b> { <b>dst-ip</b>   <b>dst-mac</b>   <b>src-dst-ip</b>   <b>src-dst-mac</b>   <b>src-ip</b>   <b>src-mac</b> }</code>	(Optional) configure a load balancing mode for link aggregation.  By default, the load balancing algorithm is configured to sxdm. In this mode, select a forwarding interface based on the OR result of the source and destination MAC addresses.

### 11.1.4 Configuring static LACP link aggregation

Configure static LACP link aggregation for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#<b>config</b></code>	Enter global configuration mode.
2	<code>Raisecom(config)#<b>lACP system-priority</b> <i>system-priority</i></code>	(Optional) configure the system LACP priority. The device with higher priority is the active end. LACP chooses active and backup interfaces according to configurations of the active end. The smaller the number is, the higher the priority is. The device with the smaller MAC address will be chosen as the active end if system LACP priorities of the two devices are identical.  By default, the system LACP priority is 32768.
3	<code>Raisecom(config)#<b>lACP timeout</b> { <b>fast</b>   <b>slow</b> }</code>	(Optional) configure LACP timeout mode.  By default, it is slow.
4	<code>Raisecom(config)#<b>interface port-channel</b> <i>channel-number</i></code>	Enter LAG configuration mode.
5	<code>Raisecom(config-port-channel)#<b>mode</b> <b>lACP</b></code>	Configure the working mode of the LAG to static LACP LAG.
6	<code>Raisecom(config-port-channel)#{ <b>max-active</b>   <b>min-active</b> } <b>links</b> <i>value threshold</i></code>	(Optional) configure maximum or minimum number of active links in LACP LAG.  By default, the maximum number is 8 while the minimum number is 1.
7	<code>Raisecom(config-port-channel)#<b>lACP priority preempt</b> <b>enable</b></code>	Enable priority preempt on the LAG.

Step	Command	Description
8	<code>Raisecom(config-port-channel)#lcp wait-timer time</code>	Configure the wait time on the interface.
9	<code>Raisecom(config-port-channel)#exit</code>	Return to global configuration mode.
10	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter Layer 2 physical interface configuration mode.
11	<code>Raisecom(config-gigaethernet1/1/port)#port-channel channel-number</code>	Add the Layer 2 interface to the LAG.
12	<code>Raisecom(config-gigaethernet1/1/port)#lcp mode { active   passive }</code>	(Optional) configure the LACP mode for member interfaces. The LACP connection will fail to be established when both ends of it are in passive mode. By default, it is in active mode.
13	<code>Raisecom(config-gigaethernet1/1/port)#lcp port-priority port-priority</code>	(Optional) configure the interface LACP priority. The priority affects election for the default interface for LACP. The smaller the value is, the higher the priority is. By default, it is 32768.



## Note

- In a static LACP LAG, a member interface can be an active/standby one. Both the active interface and standby interface can receive and send LACPDU. However, the standby interface cannot forward user packets.
- The system chooses default interface in the order of neighbor discovery, interface maximum speed, interface highest LACP priority, and interface minimum ID. The interface is in active status by default, the interface with identical speed, identical peer and identical device operation key is also in active status; other interfaces are in standby status.

## 11.1.5 Configuring manual master/slave link aggregation


Configure manual master/slave link aggregation for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface port-channel channel-number</code>	Enter LAG configuration mode.
3	<code>Raisecom(config-port-channel)#mode manual backup</code>	Configure the working mode of the LAG to manual backup LAG.

Step	Command	Description
4	<code>Raisecom(config-port-channel)#master-port interface-type interface-number</code>	Configure the active interface of the LAG.
5	<code>Raisecom(config-port-channel)#restore-mode { non-revertive   revertive [ restore-delay second ] }</code>	Configure the restoration mode and wait-to-restore time of the LAG. By default, the restoration mode is non-revertive.
6	<code>Raisecom(config-port-channel)#exit</code>	Return to global configuration mode.
7	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
8	<code>Raisecom(config-gigaethernet1/1/port)#port-channel channel-number</code>	Add member interfaces to the LAG.
9	<code>Raisecom(config-gigaethernet1/1/port)#exit</code>	Return to global configuration mode.

## 11.1.6 Checking configurations

Use the following commands to check configuration results.

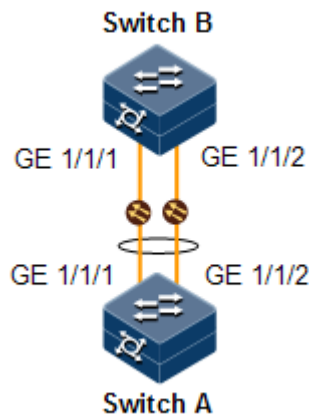
No.	Command	Description
1	<code>Raisecom#show lacp internal</code>	Show local system LACP interface status, flag, interface priority, administration key, operation key, and interface status machine status.
2	<code>Raisecom#show lacp neighbor</code>	Show information about LACP neighbors, including tag, interface priority, device ID, Age, operation key value, interface ID, and interface status machine status.
3	<code>Raisecom#show lacp statistics</code>	Show statistics about interface LACP, including the total number of received/sent LACP packets, the number of received/sent Marker packets, the number of received/sent Marker Response packets, and the number of errored Marker Response packets,
4	<code>Raisecom#show lacp sys-id</code>	Show global LACP status of the local system, device ID, including system LACP priority and system MAC address.
5	<code>Raisecom#show port-channel</code>	Show link aggregation status of the current system, load balancing mode of link aggregation, all LAG member interfaces, and active member interfaces.  <div style="display: flex; align-items: center;">  <div> <p><b>Note</b></p> <p>The active member interface refers to the one whose interface status is Up.</p> </div> </div>

## 11.1.7 Example for configuring static LACP link aggregation

### Networking requirements

As shown in Figure 11-2, to improve link reliability between Switch A and Switch B, you can configure static LACP link aggregation. That is to add GE 1/1/1 and GE 1/1/2 to one LAG; GE 1/1/1 is used as the active interface while GE 1/1/2 as the standby interface.

Figure 11-2 Static LACP mode Link aggregation networking



### Configuration steps

Step 1 Create static LACP link aggregation on Switch A. Configure Switch A as the active end.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#lACP system-priority 1000
SwitchA(config)#interface port-channel 1
SwitchA(config-port-channel1)#mode lacp
SwitchA(config-port-channel1)#max-active links 1
SwitchA(config-port-channel1)#exit
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#port-channel 1
SwitchA(config-gigabitEthernet1/1/1)#lACP port-priority 1000
SwitchA(config-gigabitEthernet1/1/1)#exit
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#port-channel 1
SwitchA(config-gigabitEthernet1/1/2)#exit
```

Step 2 Create static LACP link aggregation on Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#interface gigabitEthernet 1/1/1
```

```
SwitchB(config-gigaetherne1/1/1)#port-channel 1
SwitchB(config)#interface port-channel 1
SwitchB(config-port-channel1)#mode lacp
SwitchB(config-port-channel1)#max-active links 1
SwitchB(config-gigaetherne1/1/1)#exit
SwitchB(config)#interface gigaetherne1 1/1/2
SwitchB(config-gigaetherne1/1/2)#port-channel 1
SwitchB(config-gigaetherne1/1/2)#exit
```

## Checking results

Use the **show port-channel** command to show global configurations of the static LACP link aggregation on Switch A.

```
SwitchA#show port-channel
Group 1 information:
Mode       : Lacp           Load-sharing mode : src-dst-mac
MinLinks:   1               Max-links           : 1
UpLinks : 2                 Priority-Preemptive: Disable
Member Port : gigaetherne1/1/1 gigaetherne1/1/2
Efficient Port: gigaetherne1/1/1
```

Use the **show lacp internal** command to show configurations of local LACP interface status, flag, interface priority, administration key, operation key, and interface state machine on Switch A.

```
SwitchA#show lacp internal
Flags:
S - Device is requesting Slow LACPDUS F - Device is requesting Fast
LACPDUS
A - Device in Active mode P - Device in Passive mode MP - MLACP Peer
Port
Interface          State      Flag   Port-Priority  Admin-key Oper-
key   Port-State
-----
gigaetherne1/1/1   Active    SA     1000           1         1
0x3D
gigaetherne1/1/2   Standby   SA     32768          1         1
0x5
```

Use the **show lacp neighbor** command to show configurations of LACP interface status, flag, interface priority, administration key, operation key, and interface state machine of the peer system on Switch A.

```
Raisecom#show lacp neighbor
Flags:
```

S - Device is requesting Slow LACPDUS F - Device is requesting Fast LACPDUS  
A - Device in Active mode P - Device in Passive mode MP - MLACP Peer Port

Interface	Flag	Port-Priority	Age	Device-ID	Oper-key
Partner-Port	Port-State				
-----					
gigaethernet1/1/1	SA	32768	23s	000E.5EAB.CDEF	1
0x3D					17
gigaethernet1/1/2	SA	32768	14s	000E.5EAB.CDEF	1
0xD					18

## 11.2 Interface backup

### 11.2.1 Introduction

In dual uplink networking, Spanning Tree Protocol (STP) is used to block the redundancy link and implements backup. Though STP can meet users' backup requirements, it fails to meet switching requirements. Though Rapid Spanning Tree Protocol (RSTP) is used, the convergence is second level only. This is not a satisfying performance parameter for high-end Ethernet switch which is applied to the core of the carrier-grade network.

Interface backup, targeted for dual uplink networking, implements redundancy backup and quick switching through working and protection lines. It ensures performance and simplifies configurations.

Interface backup is another STP solution. When STP is disabled, you can realize basic link redundancy by manually configuring interfaces. If the switch is enabled with STP, you should disable interface backup because STP has provided similar functions.

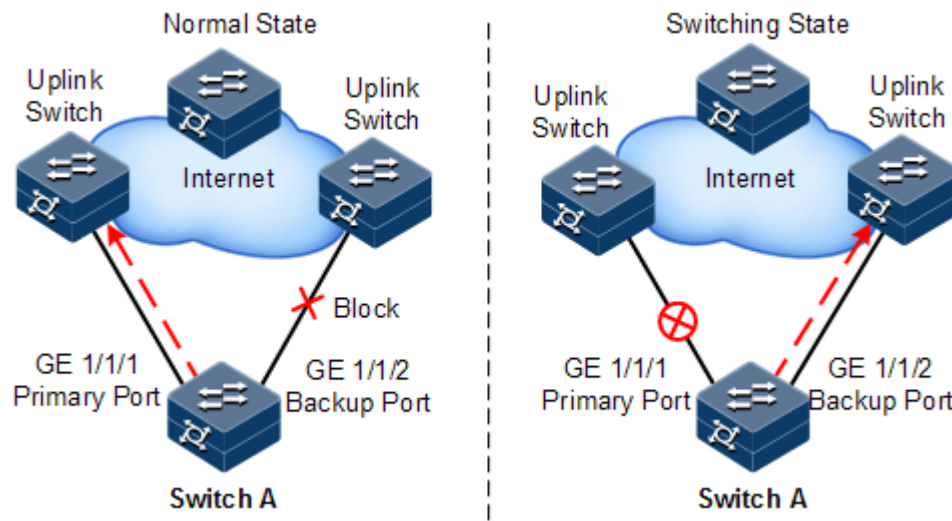
When the primary link fails, traffic is switched to the backup link. In this way, not only 50ms fast switching is ensured, but also configurations are simplified.

### Principles of interface backup

Interface backup is implemented by configuring the interface backup group. Each interface backup group contains a primary interface and a backup interface. The link, where the primary interface is, is called a primary link while the link, where the backup interface is, is called the backup interface. Member interfaces in the interface backup group supports physical interfaces and LAGs. However, they do not support Layer 3 interfaces.

In the interface backup group, when an interface is in Forward status, the other interface is in Block status. At any time, only one interface is in Forward status. When the Forward interface fails, the Block interface is switched to the Forward status.

Figure 11-3 Principles of interface backup



As shown in Figure 11-3, GE 1/1/1 and GE 1/1/2 on Switch A are connected to their uplink devices respectively. The interface forwarding states are shown as below:

- Under normal conditions, GE 1/1/1 is the primary interface while GE 1/1/2 is the backup interface. GE 1/1/1 and the uplink device forward packet while GE 1/1/2 and the uplink device do not forward packets.
- When the link between GE 1/1/1 and its uplink device fails, the backup GE 1/1/2 and its uplink device forward packets.
- When GE 1/1/1 restores normally and keeps Up for a period (restore-delay), GE 1/1/1 restores to forward packets and GE 1/1/2 restores standby status.

When a switching between the primary interface and the backup interface occurs, the switch sends a Trap to the NView NNM system.

## Application of interface backup in different VLANs

By applying interface backup to different VLANs, you can enable two interfaces to share service load in different VLANs, as shown in Figure 11-4.

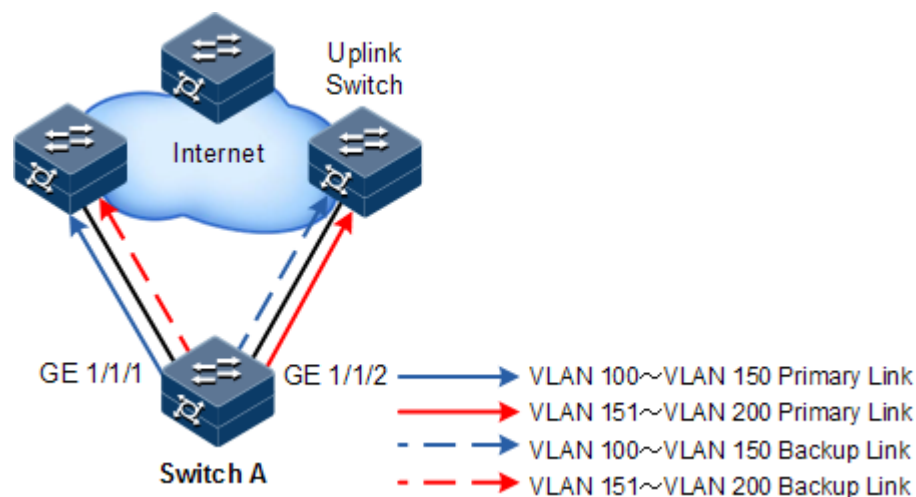


Figure 11-4 Networking with interface backup in different VLANs

In different VLANs, the forwarding status is shown as below:

- Under normal conditions, configure Switch A in VLANs 100–150.
- In VLANs 100–150, GE 1/1/1 is the primary interface and GE 1/1/2 is the backup interface.
- In VLANs 151–200, GE 1/1/2 is the primary interface and GE 1/1/1 is the backup interface.
- GE 1/1/1 forwards traffic of VLANs 100–150, and GE 1/1/2 forwards traffic of VLANs 151–200.
- When GE 1/1/1 fails, GE 1/1/2 forwards traffic of VLANs 100–200.
- When GE 1/1/1 restores normally and keeps Forward for a period (restore-delay), GE 1/1/1 forwards traffic of VLANs 100–150, and GE 1/1/2 forwards VLANs 151–200.

Interface backup is used to balance service load in different VLANs without depending on configurations of uplink switches, thus facilitating users' operation.

## 11.2.2 Preparing for configurations

### Scenario

By configuring interface backup in a dual uplink network, you can realize redundancy backup and fast switching of the primary/backup link, and load balancing between different interfaces.

Compared with STP, interface backup not only ensures millisecond-level switching, also simplifies configurations.

### Prerequisite

N/A

## 11.2.3 Default configurations of interface backup

Default configurations of interface backup are as below.

Function	Default value
Interface backup group	N/A
Restore-delay	15s
Restoration mode	Revertive mode

## 11.2.4 Configuring basic functions of interface backup

Configure basic functions of interface backup for the ISCOM2600G-HI series switch as below.



### Caution

Interface backup may interfere with STP, loop detection, Ethernet ring, and G.8032. We do not recommend configuring them concurrently on the same interface.



Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type primary-</i> <i>interface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)# port</b> <b>backup interface-type backup-</b> <b>interface-number vlanlist vlan-</b> <b>list</b> <b>Raisecom(config-port-</b> <b>channel1)#port backup interface-</b> <b>type backup-interface-number</b> <b>[ vlanlist vlan-list ]</b>	Configure the interface backup group.  In the VLAN list, configure the interface <i>backup-interface-number</i> to the backup interface and configure the interface <i>primary-interface-number</i> to the primary interface.  If no VLAN list is specified, the VLAN ranges from 1 to 4094.
4	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#port</b> <b>backup fault-detect lldp</b>	(Optional) configure LLDP fault detection.
5	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#port</b> <b>backup restore-mode { non-</b> <b>revertive   revertive [ restore-</b> <b>delay second ] }</b>	(Optional) configure restoration mode.



### Note

- In an interface backup group, an interface is either a primary interface or a backup interface.
- In a VLAN, an interface or a LAG cannot be a member of two interface backup groups simultaneously.

## 11.2.5 (Optional) configuring FS on interfaces



### Caution

- After FS is successfully configured, the primary/backup link will be switched; in other words, the current link is switched to the backup link (without considering Up/Down status of the primary/backup interface).
- In the FS command, the backup interface number is optional. If different VLANs of the primary interface are configured with multiple interface backup groups, you should enter the backup interface ID.

Configure FS on interfaces for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<b>Raisecom(config)#interface</b> <i>interface-type primary-</i> <i>interface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
3	<b>Raisecom(config-</b> <b>gigaethernet1/1/port)#port</b> <b>backup</b> [ <i>interface-type</i> <i>backup-interface-number</i> ] <b>force-switch</b>	Configure FS on the interface. Use the <b>no port backup</b> [ <i>interface-type</i> <i>backup-interface-number</i> ] <b>force-switch</b> command to cancel FS. Then, the principles of selecting the current link according to link status are as below: <ul style="list-style-type: none"><li>• If the Up/Down status of the two interfaces is the same, the primary interface is of high priority.</li><li>• If the Up/Down status of the two interfaces is different, the Up interface is of high priority.</li></ul>
	<b>Raisecom(config-port-</b> <b>channel1)#port backup</b> [ <i>interface-type backup-</i> <i>interface-number</i> ] <b>force-</b> <b>switch</b>	

## 11.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show</b> <b>switchport backup</b>	Show status information about interface backup.
2	<b>Raisecom#show port</b> <b>backup group</b>	Show configurations of interface backup.

## 11.2.7 Example for configuring interface backup

### Networking requirements

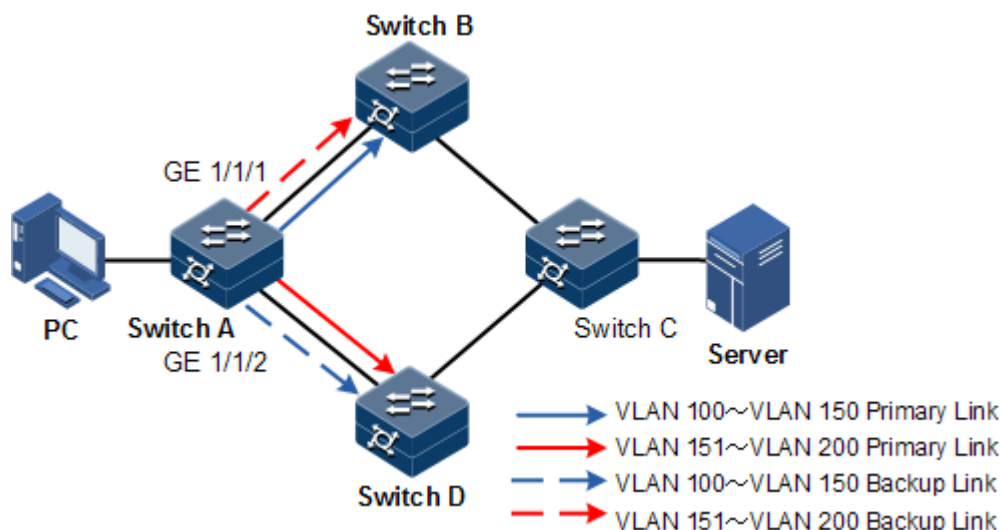
As shown in Figure 11-5, the PC accesses the server through the Switch. To implement a reliable remote access from the PC to the server, configure an interface backup group on Switch A and specify the VLAN list so that the two interfaces concurrently forward services in different VLANs and balance load. Configure Switch A as below:

- Add GE 1/1/1 to VLANs 100–150 as the primary interface and GE 1/1/2 as the backup interface.
- Add GE 1/1/2 to VLANs 151–200 as the primary interface and GE 1/1/1 as the backup interface.

When GE 1/1/1 or its link fails, the system switches traffic to the backup interface GE 1/1/2 to resume the link.

Switch A is required to support interface backup while other switches are not.

Figure 11-5 Interface backup networking



## Configuration steps

Step 1 Create VLANs 100–400, and add GE 1/1/1 and GE 1/1/2 to these VLANs.

```
Raisecom#config
Raisecom(config)#create vlan 100-200 active
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#switchport mode trunk
Raisecom(config-gigabitEthernet1/1/1)#switchport trunk allowed vlan 100-200
confirm
Raisecom(config-gigabitEthernet1/1/1)#exit
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#switchport mode trunk
Raisecom(config-gigabitEthernet1/1/2)#switchport trunk allowed vlan 100-200
confirm
Raisecom(config-gigabitEthernet1/1/2)#exit
```

Step 2 Configure GE 1/1/1 as the primary interface of VLANs 100–150 and GE 1/1/2 as the backup interface.

```
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#port backup gigabitEthernet 1/1/2
vlanlist 100-150
Raisecom(config-gigabitEthernet1/1/1)#exit
```

Step 3 Configure GE 1/1/2 as the primary interface of VLANs 151–200 and GE 1/1/1 as the backup interface.

```
Raisecom(config)#interface gigabitEthernet 1/1/2
```

```
Raisecom(config-gigaetherne1/1/2)#port backup gigaetherne1 1/1/1
vlanlist 151-200
```

## Checking results

Use the **show port backup group** command to show status of interface backup under normal or faulty conditions.

When both GE 1/1/1 and GE 1/1/2 are Forward, GE 1/1/1 forwards traffic of VLANs 100–150, and GE 1/1/2 forwards traffic of VLANs 151–200.

```
Raisecom#show port backup group
```

Active Port(State)	Backup Port(State)	ForceSwitch	vlanlist
GE1/1/1(Forward)	GE1/1/2(Block)	NO	100-150
GE1/1/2(Forward)	GE1/1/1(Block)	NO	151-200

Manually disconnect the link between Switch A and Switch B to emulate a fault. Then, GE 1/1/1 becomes Down, and GE 1/1/2 forwards traffic of VLANs 100–200.

```
Raisecom#show port backup group
```

Active Port(State)	Backup Port(State)	ForceSwitch	vlanlist
GE1/1/1(Down)	GE1/1/2(Forward)	NO	100-150
GE1/1/2(Forward)	GE1/1/1(Down)	NO	151-200

When GE 1/1/1 resumes and keeps Forward for 15s (restore-delay), it forwards traffic of VLANs 100–150 while GE 1/1/2 forwards traffic of VLANs 151–200.

```
Raisecom#show port backup group
```

Active Port(State)	Backup Port(State)	ForceSwitch	vlanlist
GE1/1/1(Forward)	GE1/1/2(Block)	NO	100-150
GE1/1/2(Forward)	GE1/1/1(Block)	NO	151-200

## 11.3 Link-state tracking

### 11.3.1 Introduction

Link-state tracking is used to provide interface linkage scheme for specific application and it can extend range of link backup. By monitoring uplinks and synchronizing downlinks, add uplink and downlink interfaces to a link-state group. Therefore, the fault of the upstream device can be informed to the downstream device to trigger switching. Link-state tracking can be used to prevent traffic loss due to failure in sensing the uplink fault by the downstream device.

When all uplink interfaces fail, down link interfaces are configured to Down status. When at least one uplink interface recovers, the downlink interface recovers to Up status. Therefore, the fault of the upstream device can be informed to the downlink device immediately. Uplink interfaces are not influenced when the downlink interface fail.

### 11.3.2 Preparing for configurations

#### Scenario

When uplink fails, traffic cannot be switched to the standby link if the downlink device fails to be notified in time. Then traffic will be disrupted.

Link-state tracking can be used to add downlink interfaces and uplink interfaces of the middle device to a link-state group and monitor uplink interfaces. When all uplink interfaces fails, the fault of the upstream device can be informed to the downstream device to trigger switching from the active link to the standby link and to reduce traffic loss.

#### Prerequisite

N/A

### 11.3.3 Default configurations of link-state tracking

Default configurations of link-state tracking are as below.

Function	Default value
Link-state group	N/A
Action for processing faults on the interface	N/A
Link-state group Trap	Disable

### 11.3.4 Configuring link-state tracking



#### Note

Link-state tracking supports being configured on the physical interface and LAG interface.

Configure link-state tracking for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#link-state-tracking group group-number</b>	Create the link-state group and enable link-state tracking.
3	<b>Raisecom(config)#link-state-tracking group group-number action { block-vlan vlan-id interface-type interface-number   delete-vlan vlan-id   flush-erps rind-id   suspend-vlan vlan-id }</b>	Configure the mode for processing fault on the link-state interface.
4	<b>Raisecom(config)#link-state-tracking group group-number trap { enable   disable }</b>	Configure Trap sending on link-state tracking.
5	<b>Raisecom(config)#interface interface-type interface-number</b>	Enter physical layer interface configuration mode.
6	<b>Raisecom(config-gigaethernet1/1/port)#link-state-tracking group group-number { downstream   upstream } ma-name ma-name cfm mepid level level</b>	Configure the link-state group of the interface and interface type. One interface can belong to only one link-state group and be configured as an either uplink or downlink interface. The interface can be bound with CC.



## 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 will link-state tracking occur.
- In global configuration mode, when you use the **no link-state-tracking group group-number** command to disable link-state tracking, the link-state group without interfaces will be deleted.
- In physical layer interface configuration mode, use the **no link-state-tracking group group-number** command to delete an interface. During the execution of this command, if the link-state group contains no other interfaces and is disabled, it will also be deleted.

## 11.3.5 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	<b>Raisecom#show link-state-tracking group group-number</b>	Show configurations and status of the link-state group.

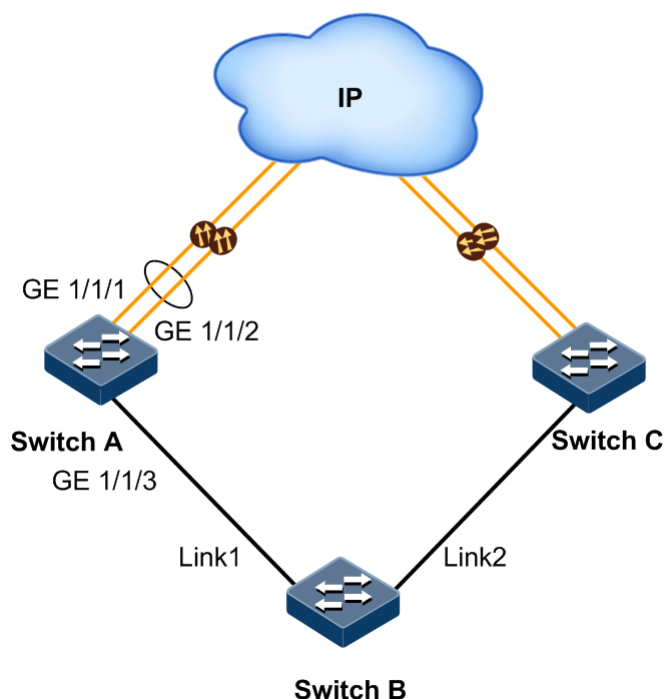
## 11.3.6 Example for configuring link-state tracking

### Networking requirements

As shown in Figure 11-6, to improve network reliability, Link 1 and Link 2 of Switch B are connected to Switch A and Switch C respectively. Link 1 is the active link and Link 2 is the standby link. Link 2 will not be used to forward data until Link 1 is faulty.

Switch A and Switch C are connected to the uplink network in link aggregation mode. When all uplink interfaces on Switch A and Switch C fails, Switch B needs to sense the fault in time and switches traffic to the standby link. Therefore, you should deploy link-state tracking on Switch A and Switch C.

Figure 11-6 Link-state tracking networking



### Configuration steps

Step 1 Configure link-state tracking on Switch A.

Create a LAG. Add uplink interfaces GE 1/1/1 and GE 1/1/2 to the LAG.

```
Raisecom#config
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#port-channel 1
Raisecom(config-gigabitEthernet1/1/1)#exit
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#port-channel 1
Raisecom(config-gigabitEthernet1/1/2)#exit
```

Create link-state group 1. Add LAG interfaces to the link-state group.

```
Raisecom(config)#link-state-tracking group 1
Raisecom(config)#interface port-channel 1
Raisecom(config-port-channel1)#link-state-tracking group 1 upstream
Raisecom(config-port-channel1)#exit
```

Add downlink interface GE 1/1/3 to the link-state group.

```
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#link-state-tracking group 1 downstream
```

Step 2 Configure link-state tracking on Switch C.

Configurations are identical to the ones on Switch A.

## Checking results

Take Switch A for example.

Use the **show link-state-tracking group** command to show configurations of the link-state group.

```
SwitchA#show link-state-tracking group 1
Link-state-tracking Group: 1
Trap State: disable
UpStream Type: port
UpStream PortList: portchannel 1
Action Mode: Shutdown-port
Action PortList: gigaethernet 1/1/3
Link-state-tracking State: normal
Fault-type: none
```

Use the **show link-state-tracking group** command to show configurations of the link-state group after all uplinks of Switch A fails. In this case, you can learn that link-state tracking is performed.

```
SwitchA#show link-state-tracking group 1
Link-state-tracking Group: 1
Trap State: enable
UpStream Type: port
UpStream PortList: portchannel 1
Action Mode: Shutdown-port
Action PortList: gigaethernet 1/1/3
Link-state-tracking State: failover
Fault-type: port-shutdown
```



## 11.4 UDLD

### 11.4.1 Introduction

UniDirectional Link Detection (UDLD) is used to monitor configurations of the physical connection by the fiber or Ethernet cable. When a unidirectional link (transmitting data in only one direction) is present, UDLD can detect it, shut down the corresponding interface, and send a Trap. The unidirectional link may cause various problems, such as the spanning tree problems which may cause a loop.

### 11.4.2 Preparing for configurations

#### Scenario

When a unidirectional link (transmitting data in only one direction) is present, UDLD can detect the fault, shut down the corresponding interface, and send a Trap.

#### Prerequisite

Devices at both ends of the link should support UDLD.

### 11.4.3 Default configurations of UDLD

Default configurations of UDLD are as below.

Function	Default value
UDLD	Disable

### 11.4.4 Configuring UDLD

Configure UDLD for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b> <b>Raisecom(config)#interface</b> <i>interface-type primary-interface-number</i>	Enter global configuration mode or interface configuration mode.
2	<b>Raisecom(config)#uldp enable</b> <b>Raisecom(config-gigaethernet1/1/port) #uldp enable</b>	Enable global UDLD or interface UDLD.
3	<b>Raisecom(config)#uldp recovery-time time</b>	(Optional) configure the recovery time for the unidirectional link.

### 11.4.5 Checking configurations

Use the following commands to check configuration results.

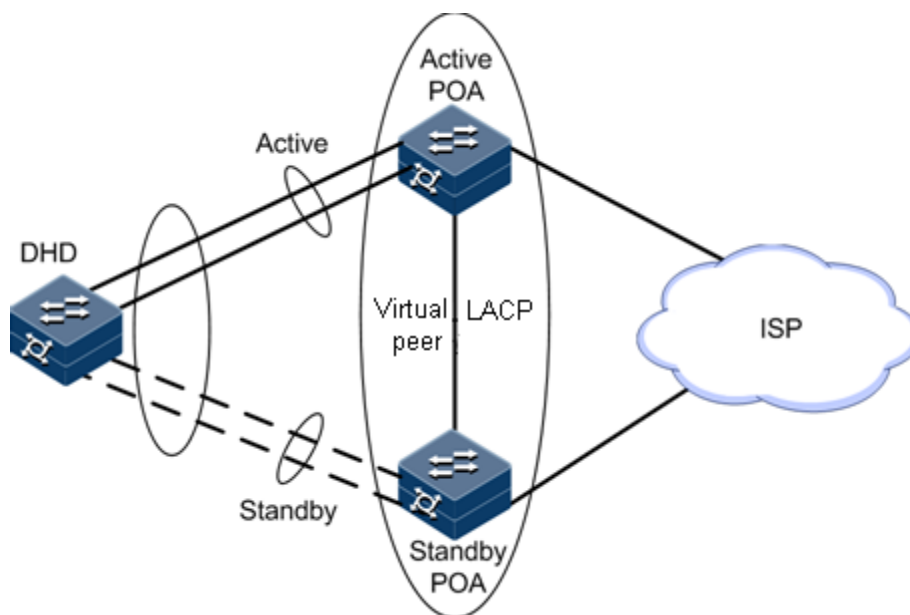
No.	Command	Description
1	<code>Raisecom#show u1dp</code>	Show UDLD configurations.

## 11.5 mLACP

### 11.5.1 Introduction

A loop may occur when a device has two uplink Points of Access (PoAs), which means that the device is a Dual Home Device (DHD). Sometimes, the DHD is incapable of running any loop detection protocols. In this case, you can use the Multi-Chassis Link Aggregation Control Protocol (mLACP), which offers you another choice, to select paths for the DHD.

Figure 11-7 Dual-homed application based on LACP



As shown in Figure 11-1, two PoAs exchange configuration information through InterChassis Communication Protocol (ICCP), synchronizing the status of each other (each PoA receives and saves information about the other PoA). The two PoAs form a virtual LACP peer and appear as a single device to the DHD.

Links that connect the DHD are configured to the same Link Aggregation Group (LAG). Interface selection and link aggregation are implemented through LACP. In this case, the two PoAs in the same LAG appear to be in one Inter-Chassis Group (ICG).

The whole system, according to the configured priority, will select a PoA from the ICG to be the active one by using LACP. The active PoA will communicate with DHD. In one ICG, only one PoA can be active and the other standby.

When the number of Up links between the active PoA and the DHD is smaller than the configured number of LAG links, the system will perform fault switching, making the other

PoA active and the local PoA standby. When faults at the local PoA are cleared, the system will perform fault recovery, reselecting the local PoA as the active one.

## 11.5.2 Preparing for configurations

### Scenario



Create an ICCP channel on the PoA. Make the two independent PoAs form a virtual redundant ICG which can implement mLACP.

### Prerequisite

The special VLAN for the ICCP channel has been established. The special Layer 3 interface IP address for the special VLAN of the 2 PoAs is configured differently and in the same network segment. The LAG in each device has been established. The interfaces which are to be added to the LAG have been switched to Layer 2 interfaces and are added to the LAG without any configurations. Interfaces on the DHD which are to be added to the LAG should be the ones connecting all links to the 2 PoAs. However, interfaces on the 2 PoAs which are to be added to the LAG contain the local interfaces which connect the DHD only.



## 11.5.3 Configuring ICCP channel

Configure the ICCP channel for the ISCOM2600G-HI series switch as below.

Step	Configuration	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#iccp local-ip ip-address</b>	Configure the IP address of the local interface in the ICCP channel.   <b>Caution</b> The configured IP address must be the IP address of the local Layer 3 interface. When modifying the IP address of the local Layer 3 interface, you have to reconfigure the IP address of the local ICCP.
3	<b>Raisecom(config)#iccp-channel channel-id</b>	Create a communication channel and enter ICCP configuration mode.
4	<b>Raisecom(config-iccp)#member-ip ip-address</b>	Configure the IP address of the peer ICCP.   <b>Caution</b> The configured IP address must be the IP address of the peer Layer 3 interface. When modifying the IP address of the peer Layer 3 interface, you have to reconfigure the IP address of the ICCP peer.
5	<b>Raisecom(config-iccp)#iccp enable</b>	Enable ICCP. By default, it is disabled.

## 11.5.4 Configuring mLACP link aggregation

Configure mLACP link aggregation for the ISCOM2600G-HI series switch as below.

Step	Configuration	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#mlacp-group</b> <i>icg-id</i>	Create an ICG and enter ICG configuration mode.
3	<b>Raisecom(config-ic-group)#iccp-channel</b> <i>channel-id</i>	Bind the ICG with an ICCP channel.
4	<b>Raisecom(config-ic-group)#mlacp { master   slave }</b>	Configure the mLACP role for the local device in the ICG.
5	<b>Raisecom(config-ic-group)#port-channel</b> <i>group-id</i>	Bind the ICG with a LAG.   <b>Caution</b> The LAG ID to be bound must be the already established LAG ID. Otherwise, it will be unavailable for use. For how to create a LAG, see descriptions about the <b>port-channel</b> command.
6	<b>Raisecom(config-ic-group)#restore-mode { non-revertive   revertive [ restore-delay second ] }</b>	Configure the LAG fault restore mode and restore-delay time on the ICG.
7	<b>Raisecom(config-ic-group)#mlacp system-priority</b> <i>system-priority</i>	Configure the system priority of the local device in the ICG. By default, the mLACP system priority of the device is 32768.   <b>Caution</b> The priority of the device in the ICG should be higher than that of the DHD. The smaller the value is, the higher the priority will be.

## 11.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show iccp channel</b> [ <i>channel-id</i> ] <b>statistics</b>	Check statistics on packets received by or sent from the ICCP channel.
2	<b>Raisecom#show iccp channel</b> [ <i>channel-id</i> ]	Check the configurations and running status of the ICCP channel.

No.	Command	Description
3	<b>Raisecom#show mlacp-group</b> [ <i>group-id</i> ]	Check the mLACP configurations and running status.

## 11.5.6 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
<b>Raisecom(config)#clear iccp channel</b> [ <i>channel-id</i> ] <b>statistics</b>	Clear statistics on packets received by or sent from the ICCP channel.
<b>Raisecom(config)#clear mlacp mlacp-group</b> [ <i>group-id</i> ] <b>statistics</b>	Clear statistics on packets received by or sent from the ICG.

## 11.5.7 Example for configuring mLACP

### Networking requirements

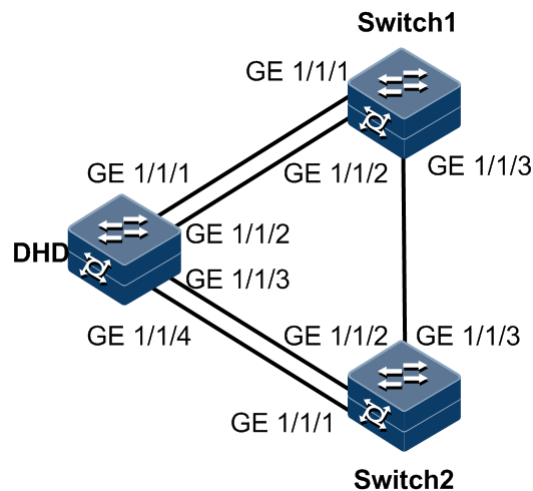
Prepare two mLACP devices: Switch1 and Switch2. The two devices exchange configuration information through ICCP. Switch1 and switch2 appear as a virtual LACP peer to the DHD.

The DHD exchanges LACPDU with the virtual LACP peer to aggregate links. At the same time, the link between the DHD and one switch is active and that between the DHD with the other switch is standby.

As shown in Figure 5-2, GE 1/1/1, GE 1/1/2, GE 1/1/3, and GE 1/1/4 on the DHD are in the same LAG. GE 1/1/1 and GE 1/1/2 on Switch 1 and Switch 2 are in the same LAG. Configure the maximum active links and minimum active links to 2 respectively. Configure the priority of Switch 1 or Switch 2 higher than that of the DHD. For example, if you configure the system priority of Switch1 higher than that of the DHD, Switch1 will be the active link and Switch 2 will be the standby link when priority pre-emption is enabled.

When the number of active links between the DHD and Switch 1 is smaller than 2, link switching will occur. Traffic will be switched to the link between the DHD and Switch 2. When the number of active links between the DHD and Switch 1 is 2, the link will recover. Traffic will be switched back to the link between the DHD and Switch 1.

Figure 11-8 mLACP networking



## Configuration steps

- Step 1 Configure a LAG. Add GE 1/1/1, GE 1/1/2, GE 1/1/3, and GE 1/1/4 on the DHD to the LAG and enable priority pre-emption of the LAG.

```

DHD#config
DHD(config)#interface port-channel 1
DHD(config-port-channel1)#mode lacp
DHD(config-port-channel1)#max-active links 2
DHD(config-port-channel1)#min-active links 2
DHD(config-port-channel1)#lacp priority preempt enable
DHD(config-port-channel1)#interface gigabitEthernet 1/1/1
DHD(config-gigabitEthernet1/1/1)#port-channel 1
DHD(config-gigabitEthernet1/1/1)#interface gigabitEthernet 1/1/2
DHD(config-gigabitEthernet1/1/2)#port-channel 1
DHD(config-gigabitEthernet1/1/2)#interface gigabitEthernet 1/1/4
DHD(config-gigabitEthernet1/1/4)#port-channel 1
DHD(config-gigabitEthernet1/1/4)#interface gigabitEthernet 1/1/3
DHD(config-gigabitEthernet1/1/3)#port-channel 1
  
```

Configure a LAG for Switch1. Add GE 1/1/1 and GE 1/1/2 on Switch 1 to the LAG and enable priority pre-emption of the LAG.

```

Switch1#config
Switch1(config)#interface port-channel 1
Switch1(config-port-channel1)#mode lacp
Switch1(config-port-channel1)#max-active links 2
Switch1(config-port-channel1)#min-active links 2
Switch1(config-port-channel1)#lacp priority preempt enable
Switch1(config-port-channel1)#interface gigabitEthernet 1/1/1
Switch1(config-gigabitEthernet1/1/1)#port-channel 1
Switch1(config-gigabitEthernet1/1/1)#interface gigabitEthernet 1/1/2
Switch1(config-gigabitEthernet1/1/2)#port-channel 1
  
```

Configure a LAG for Switch 2. Add GE 1/1/1 and GE 1/1/2 on Switch 2 to the LAG and enable priority pre-emption of the LAG.

```
Switch2#config
Switch2(config)#interface port-channel 1
Switch2(config-port-channel1)#mode lacp
Switch2(config-port-channel1)#max-active links 2
Switch2(config-port-channel1)#min-active links 2
Switch2(config-port-channel1)#lacp priority preempt enable
Switch2(config-port-channel1)#interface gigabitEthernet 1/1/1
Switch2(config-gigabitEthernet1/1/1)#port-channel 1
Switch2(config-gigabitEthernet1/1/1)#interface gigabitEthernet 1/1/2
Switch2(config-gigabitEthernet1/1/2)#port-channel 1
```

Step 2 Configure an ICCP channel and bind it with the ICG. Apply the ICCP channel to the LAG.

Configure Switch 1 as below:

```
Switch1#config
Switch1(config)#create vlan 6 active
Switch1(config)#interface gigabitEthernet 1/1/3
Switch1(config-gigabitEthernet1/1/3)#switchport access vlan 6
Switch1(config-gigabitEthernet1/1/3)#interface vlan 6
Switch1(config-vlan6)#ip address 10.110.3.1 255.255.255.0
Switch1(config-vlan6)#exit
Switch1(config)#iccp local-ip 10.110.3.1
Switch1(config)#iccp channel 1
Switch1(config-iccp)#member-ip 10.110.3.2
Switch1(config-iccp)#iccp enable
Switch1(config-iccp)#exit
Switch1(config)#mlacp-group 1
Switch1(config-ic-group)#iccp-channel 1
Switch1(config-ic-group)#mlacp master
Switch1(config-ic-group)#mlacp system-priority 20000
Switch1(config-ic-group)#port-channel 1
Switch1(config-ic-group)#restore-mode revertive restore-delay 20
Switch1(config-ic-group)#exit
```

Configure Switch 2 as below:

```
Switch2#config
Switch2(config)#create vlan 6 active
Switch2(config)#interface gigabitEthernet 1/1/3
Switch2(config-gigabitEthernet1/1/3)#switchport access vlan 6
Switch2(config-gigabitEthernet1/1/3)#interface vlan 6
Switch2(config-vlan6)#ip address 10.110.3.2 255.255.255.0
Switch2(config-vlan6)#exit
Switch2(config)#iccp local-ip 10.110.3.2
Switch2(config)#iccp channel 1
```

```
Switch2(config-iccp)#member-ip 10.110.3.1
Switch2(config-iccp)#iccp enable
Switch2(config-iccp)#exit
Switch2(config)#mlacp-group 1
Switch2(config-ic-group)#iccp-channel 1
Switch2(config-ic-group)#port-channel 1
Switch2(config-ic-group)#mlacp slave
Switch2(config-ic-group)#restore-mode revertive restore-delay 20
Switch2(config-ic-group)#exit
```

## Checking results

Use the following command to show LACP configurations of the DHD.

```
DHD#show port-channel 1
Group 1 information:
Mode       : Lacp                      Load-sharing mode : src-dst-mac
MinLinks:   2                      Max-links         : 2
UpLinks    : 4                      Priority-Preemptive: Enable
Member Port : gigabitEthernet1/1/1 gigabitEthernet1/1/2 gigabitEthernet1/1/4
gigabitEthernet1/1/3
Efficient Port: gigabitEthernet1/1/1 gigabitEthernet1/1/2
```

Use the following command to show mLACP configurations of Switch 1.

```
Switch1#show mlacp-group 1
mlacp group      : 1

System information:
MAC address running      : 000E.5E11.2233
System priority running  : 20000

Configuration information:
Local information      Peer information
system mac:           000E.5E55.0001           000E.5E11.2233
System priority:      20000                     32768
Port-channel:         1                        N/A
Type:                 master                    slave
Iccp-channel:         1                        N/A
Iccp-State:           connect                   N/A
Track PwId:           0                        N/A
Pw Ip:                0.0.0.0                  N/A
Pw state:             N/A                      N/A
State:                Active                   Standby
Restore Type:         revertive                  N/A
Restore Time(s):      20                       N/A
```

Use the following command to show mLACP configurations of Switch 2.



```
Switch2#show mllacp-group 1
mlacp group      : 1
```

```
System information:
MAC address running      : 000E.5E11.2233
System priority running  : 20000
```

```
Configuration information:
```

	Local information	Peer information
system mac:	000E.5E11.2233	000E.5E55.0001
System priority:	32768	20000
Port-channel:	1	N/A
Type:	slave	master
Iccp-channel:	1	N/A
Iccp-State:	connect	N/A
Track PwId:	0	N/A
Pw Ip:	0.0.0.0	N/A
Pw state:	N/A	N/A
State:	Standby	Active
Restore Type:	revertive	N/A
Restore Time(s):	20	N/A

# 12 System management

---

This chapter describes basic principles and configuration procedures for system management and maintenance, and provides related configuration examples, including the following sections:

- SNMP
- RMON
- LLDP
- Optical module DDM
- System log
- Alarm management
- Hardware environment monitoring
- CPU monitoring
- Cable diagnosis
- Memory monitoring
- Ping
- Traceroute
- Performance statistics

## 12.1 SNMP

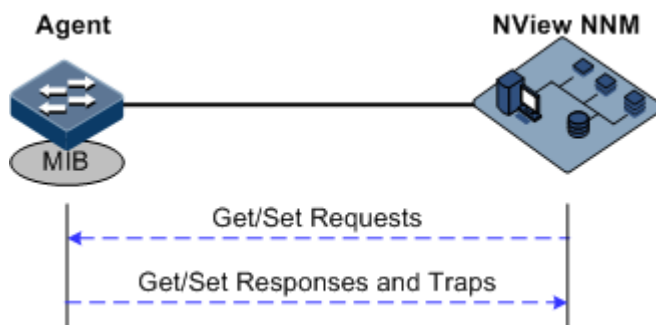
### 12.1.1 Introduction

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 that 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.

## Principles

A SNMP system consists of two parts: Agent and the NView NNM system. The Agent and the NView NNM system communicate through SNMP packets sent through UDP. Figure 12-1 shows the SNMP principle.

Figure 12-1 Principles of SNMP



The Raisecom NView NNM system can provide friendly Human Machine Interface (HMI) to facilitate network management. The following functions can be implemented through it:

- Send request packets to the managed device.
- Receive reply packets and Trap packets from the managed device, and show result.

The Agent is a program installed on the managed device, implementing the following functions:

- Receive/Reply request packets from the NView NNM system
- To read/write packets and generate replay packets according to the packets type, then return the result to the NView NNM system
- Define trigger condition according to protocol modules, enter/exit system or restart the ISCOM2600G-HI series switch when conditions are satisfied; replying module sends Trap packets to the NView NNM system through agent to report current status of the ISCOM2600G-HI series switch.



### Note

An Agent can be configured with several versions, and different versions communicate with different NMSs. But SNMP version of the NMS must be consistent with that of the connected agent so that they can intercommunicate properly.

## Version of protocol

Till now, SNMP has three versions: v1, v2c, and v3, described as below.

- SNMPv1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a secret. The network management system can visit the agent only by specifying its community name correctly. If the community name carried in a SNMP packet is not accepted by the ISCOM2600G-HI series switch, the packet will be discarded.
- Compatible with SNMPv1, SNMPv2c also uses community name authentication mechanism. SNMPv2c supports more operation types, data types, and errored codes, and thus better identifying errors.

- SNMPv3 uses User-based Security Model (USM) authentication mechanism. You can configure whether USM authentication is enabled and whether encryption is enabled to provide higher security. USM authentication mechanism allows authenticated senders and prevents unauthenticated senders. Encryption is used to encrypt packets transmitted between the network management system and agents, thus preventing interception.

The ISCOM2600G-HI series switch supports v1, v2c, and v3 of SNMP.

## MIB

Management Information Base (MIB) is the collection of all objects managed by the NMS. It defines attributes for the managed objects:

- Name
- Access right
- 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 ISCOM2600G-HI series switch.

MIB stores information in a tree structure, and 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 protocol packets can access network devices by checking the nodes in MIB tree directory.

The ISCOM2600G-HI series switch supports standard MIB and Raisecom-customized MIB.

### 12.1.2 Preparing for configurations

#### Scenario

To log in to the ISCOM2600G-HI series switch through NMS, configure SNMP basic functions for the ISCOM2600G-HI series switch in advance.

#### Prerequisite

Configure the routing protocol and ensure that the route between the ISCOM2600G-HI series switch and NMS is reachable.

### 12.1.3 Default configurations of SNMP

Default configurations of SNMP are as below.

Function	Default value												
SNMP view	system and internet views (default)												
SNMP community	public and private communities (default) <table><tr><td>Index</td><td>CommunityName</td><td>ViewName</td><td>Permission</td></tr><tr><td>1</td><td>public</td><td>internet</td><td>ro</td></tr><tr><td>2</td><td>private</td><td>internet</td><td>rw</td></tr></table>	Index	CommunityName	ViewName	Permission	1	public	internet	ro	2	private	internet	rw
Index	CommunityName	ViewName	Permission										
1	public	internet	ro										
2	private	internet	rw										
SNMP access group	initialnone and initial access groups (default)												

Function	Default value			
SNMP user	none, md5nopriv, shapriv, md5priv, and shanopriv users (default)			
Mapping relationship between SNMP user and access group	Index	GroupName	UserName	SecModel
	-----			
	0	initialnone	none	usm
	1	initial	md5priv	usm
	2	initial	shapriv	usm
	3	initial	md5nopriv	usm
	4	initial	shanopriv	usm
Logo and the contact method of the administrator	support@Raisecom.com			
Device physical location	world china raisecom			
Trap	Enable			
SNMP target host address	N/A			
SNMP engine ID	800022B603000E5E000016			

## 12.1.4 Configuring basic functions of SNMPv1/SNMPv2c

To protect itself and prevent its MIB from unauthorized access, the SNMP Agent proposes the concept of community. Management stations in the same community must use the community name in all Agent operations, or their requests will not be accepted.

The community name is used by different SNMP strings to identify different 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 access permission can configure the ISCOM2600G-HI series switch in addition to querying the device information.

SNMPv1/SNMPv2c uses the community name authentication scheme, and the SNMP packets of which the names are inconsistent to the community name will be discarded.

Configure basic functions of SNMPv1/SNMPv2c for the ISCOM2600G-HI series switch as below.

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> ] { <b>excluded</b>   <b>included</b> }	(Optional) create SNMP view and configure MIB variable range.  The default view is internet view. The MIB variable range contains all MIB variables below "1.3.6" node of MIB tree.

Step	Command	Description
3	<code>Raisecom(config)#snmp-server community com-name [ view view-name ] { ro   rw }</code>	Create community name and configure the corresponding view and authority. Use default view internet if <b>view view-name</b> option is empty.

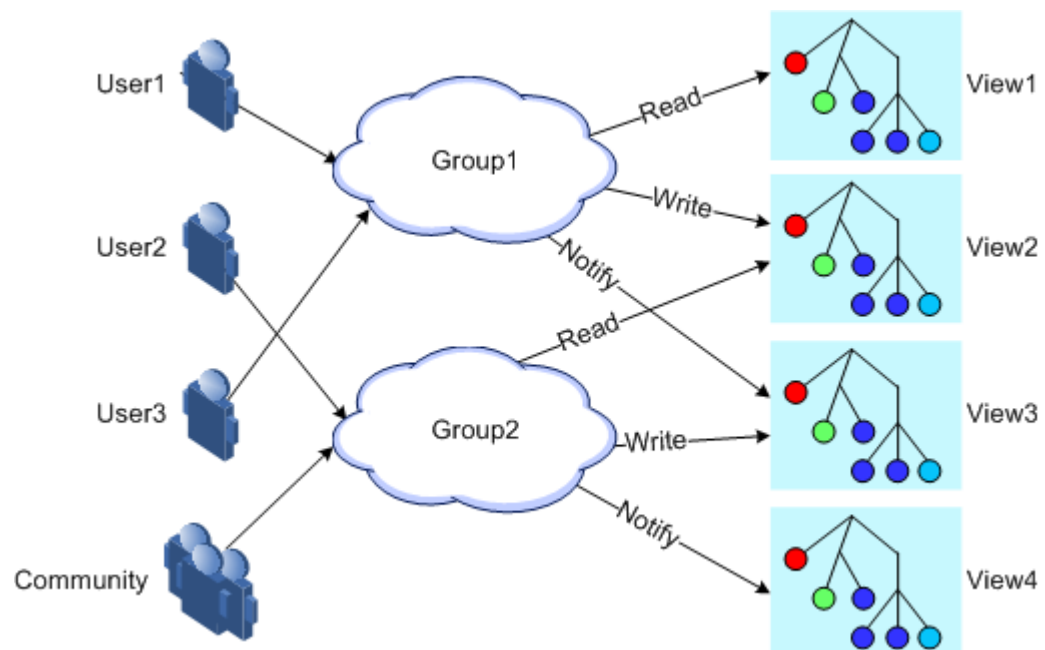
## 12.1.5 Configuring basic functions of SNMPv3

SNMPv3 uses USM over user authentication mechanism. USM comes up with the concept of access group: one or more users correspond to one access group, each access group configures the related read, write and announce view; users in access group have access permission in this view. The user access group to send Get and Set request must have permission corresponding to the request, otherwise the request will not be accepted.

As shown in Figure 12-2, the network management station uses the normal access from SNMPv3 to switch and the configuration is as below.

- Configure users.
- Check the access group to which the user belongs.
- Configure view permission for access groups.
- Create views.

Figure 12-2 SNMPv3 authentication mechanism



Configure basic functions of SNMPv3 for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<code>Raisecom(config)#snmp-server view view-name oid-tree [ mask ] { excluded   included }</code>	(Optional) create SNMP view and configure MIB variable range.
3	<code>Raisecom(config)#snmp-server user user-name [ remote engine-id ] authentication { md5   sha } authpassword [privkey privkeypassword ]</code>	Create users and configure authentication modes.
4	<code>Raisecom(config)#snmp-server user user-name [ remote engine-id ] authkey { md5   sha } keyword [privkey privkeypassword ]</code>	(Optional) modify the authentication key and the encryption key.
5	<code>Raisecom(config)#snmp-server access group-name [ read view-name ] [ write view-name ] [ notify view-name ] [ context context-name { exact   prefix } ] usm { authnopriv   authpriv   noauthnopriv }</code>	Create and configure the SNMPv3 access group.
6	<code>Raisecom(config)#snmp-server group group-name user user-name usm</code>	Configure the mapping between users and the access group.

## 12.1.6 Configuring IP address authentication by SNMP server

Configure IP address authentication by SNMP server for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#snmp- server server-auth { enable   disable }</code>	Enable or disable IP address authentication by the SNMP server.
3	<code>Raisecom(config)#snmp- server server-auth ip- address</code>	Configure the IP address of the SNMP server for authentication.


## 12.1.7 Configuring other information about SNMP

Other information about SNMP includes:

- Logo and contact method of the administrator, which is used to identify and contact the administrator
- Physical location of the device: describes where the device is located

SNMPv1, SNMPv2c, and SNMPv3 support configuring this information.

Configure other information about SNMP for the ISCOM2600G-HI series switch as below.

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 the logo and contact method of the administrator.   <b>Note</b> For example, configure the E-mail to the logo and contact method of the administrator.
3	<b>Raisecom(config)#snmp-server location</b> <i>location</i>	(Optional) specify the physical location of the device.

## 12.1.8 Configuring Trap



### Note

Trap configurations on SNMPv1, SNMPv2c, and SNMPv3 are identical except for Trap target host configurations. Configure Trap as required.

Trap is unrequested information sent by the ISCOM2600G-HI series switch to the NMS automatically, which is used to report some critical events.

Before configuring Trap, you need to perform the following configurations:

- Configure basic functions of SNMP. SNMPv1 and v2c need to configure the community name; SNMPv3 needs to configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the ISCOM2600G-HI series switch and NMS is reachable.

Configure Trap of SNMP for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#snmp-server host</b> <i>ip-address version 3 { authnopriv   authpriv   noauthnopriv } user-name [ udpport udpport ]</i>	(Optional) configure the SNMPv3 Trap target host.
3	<b>Raisecom(config)#snmp-server host</b> <i>ip-address version { 1   2c } community-name [ udpport udpport ]</i>	(Optional) configure the SNMPv1/SNMPv2c Trap target host.
4	<b>Raisecom(config)#snmp-server enable traps</b>	Enable Trap.
5	<b>Raisecom(config)#snmp-server trap-source</b> <i>interface-type interface-number</i>	Specify the source interface for the switch to send Traps.



## 12.1.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show snmp access</b>	Show SNMP access group configurations.
2	<b>Raisecom#show snmp community</b>	Show SNMP community configurations.
3	<b>Raisecom#show snmp config</b>	Show SNMP basic configurations, including the local SNMP engine ID, logo and contact method of the administrator, physical location of the device, and Trap status.
4	<b>Raisecom#show snmp group</b>	Show the mapping between SNMP users and the access group.
5	<b>Raisecom#show snmp host</b>	Show Trap target host information.
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.
9	<b>Raisecom#show snmp server-auth</b>	Show SNMP server authentication configurations.

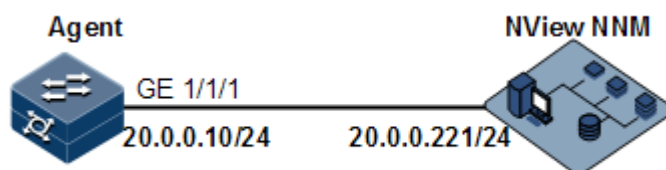
## 12.1.10 Example for configuring SNMPv1/SNMPv2c and Trap

### Networking requirements

As shown in Figure 12-3, the route between the NView NNM system and the ISCOM2600G-HI series switch is available. The NView NNM system can check the MIB under view corresponding to the remote Switch by SNMPv1/SNMPv2c, and the ISCOM2600G-HI series switch can send Trap automatically to the NView NNM system in emergency.

By default, there is VLAN 1 on the ISCOM2600G-HI series switch and all physical interfaces belong to VLAN 1.

Figure 12-3 SNMPv1/SNMPv2c networking



## Configuration steps

Step 1 Configure the IP address of the ISCOM2600G-HI series switch.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 20.0.0.10 255.255.255.0
Raisecom(config-vlan1)#exit
```

Step 2 Configure SNMPv1/SNMPv2c views.

```
Raisecom(config)#snmp-server view mib2 1.3.6.1.2.1 included
```

Step 3 Configure SNMPv1/SNMPv2c community.

```
Raisecom(config)#snmp-server community raisecom view mib2 ro
```

Step 4 Configure Trap sending.

```
Raisecom(config)#snmp-server enable traps
Raisecom(config)#snmp-server host 20.0.0.221 version 2c raisecom
```

## Checking results

Use the **show ip interface brief** command to show configurations of the IP address.

```
Raisecom#show ip interface brief
```

VRF	IF	Address	NetMask
Category			
-----			
Default-IP-Routing-Table	fastethernet1/0/1	192.168.0.1	
255.255.255.0	primary		
Default-IP-Routing-Table	vlan1	20.0.0.10	
255.255.255.0	primary		

Use the **show snmp view** command to show view configurations.

```
Raisecom#show snmp view
Index: 0
```

```
View Name: mib2
OID Tree: 1.3.6.1.2.1
Mask:    --
Type:    include
...
```

Use the **show snmp community** command to show community configurations.

```
Raisecom#show snmp community
```

Index	Community Name	View Name	Permission
1	private	internet	rw
2	public	internet	ro
3	raisecom	mib2	ro

Use the **show snmp host** command to show configurations of the target host.

```
Raisecom#show snmp host
Index:      0
IP family:  IPv4
IP address:  20.0.0.221
Port:       162
User Name:   raisecom
SNMP Version: v2c
Security Level: noauthnopriv
TagList:     bridge config interface rmon snmp ospf
```

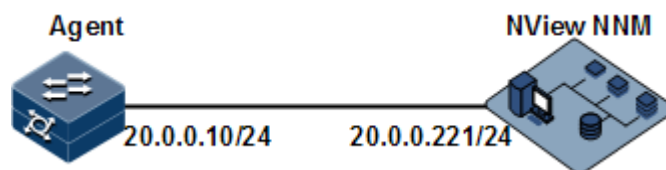
## 12.1.11 Example for configuring SNMPv3 and Trap

### Networking requirements

As shown in Figure 12-4, the route between the NView NNM system and ISCOM2600G-HI series switch is available, the NView NNM system monitors the Agent through SNMPv3, and the ISCOM2600G-HI series switch can send Trap automatically to the NView NNM system when the Agent is in emergency.

By default, there is VLAN 1 on the ISCOM2600G-HI series switch and all physical interfaces belong to VLAN 1.

Figure 12-4 SNMPv3 and Trap networking



## Configuration steps

Step 1 Configure the IP address of the ISCOM2600G-HI series switch.

```
Raisecom#config  
Raisecom(config)#interface vlan 1  
Raisecom(config-vlan1)#ip address 20.0.0.10 255.255.255.0  
Raisecom(config-vlan1)#exit
```

Step 2 Configure SNMPv3 access.

Create access view mib2, including all MIB variables under 1.3.6.1.x.1.

```
Raisecom(config)#snmp-server view mib2 1.3.6.1.2.1 1.1.1.1.0.1 included
```

Create user guestuser1, and use md5 authentication algorithm. The password is raisecom.

```
Raisecom(config)#snmp-server user guestuser1 authentication md5 raisecom
```

Create a guest group access group. The security mode is usm, security level is authentication without encryption, and readable view name is mib2.

```
Raisecom(config)#snmp-server access guestgroup read mib2 usm authnopriv
```

Configure the guestuser1 user to be mapped to the access group guestgroup.

```
Raisecom(config)#snmp-server group guestgroup user guestuser1 usm
```

Step 3 Configure Trap sending.

```
Raisecom(config)#snmp-server enable traps  
Raisecom(config)#snmp-server host 20.0.0.221 version 3 authnopriv  
guestuser1
```

## Checking results

Use the **show snmp access** command to show configurations of the SNMP access group.

```
Raisecom#show snmp access
...
Index:          1
Group:          guestgroup
Security Model:  usm
Security Level:  authnopriv
Context Prefix:  --
Context Match:  exact
Read View:      mib2
Write View:     --
Notify View:    internet
...
```

Use the **show snmp group** command to show mapping between users and access groups.

```
Raisecom#show snmp group
Index  GroupName      UserName      SecModel
-----
0      initialnone    none         usm
1      initial       md5priv      usm
2      initial       shapriv      usm
3      initial       md5nopriv    usm
4      initial       shanopriv    usm
5      guestgroup     guestuser1    usm
```

Use the **show snmp host** command to show configurations of the Trap target host.

```
Raisecom#show snmp host
Index:          0
IP family:      IPv4
IP address:     20.0.0.221
Port:          162
User Name:      guestuser1
SNMP Version:   v3
Security Level:  authnopriv
TagList:        bridge config interface rmon snmp ospf
```

## 12.2 RMON

### 12.2.1 Introduction

Remote Network Monitoring (RMON) is a standard stipulated by Internet Engineering Task Force (IETF) for network data monitoring through different network Agents and NMS.

RMON is achieved based on SNMP architecture, including the NView NNM system and the Agent running on network devices. On the foundation of SNMP, increase the subnet flow,

statistics, and analysis used to achieve the monitoring to one segment and the whole network, while SNMP only can monitor the partial information about a single device and it is difficult for it to monitor one segment.

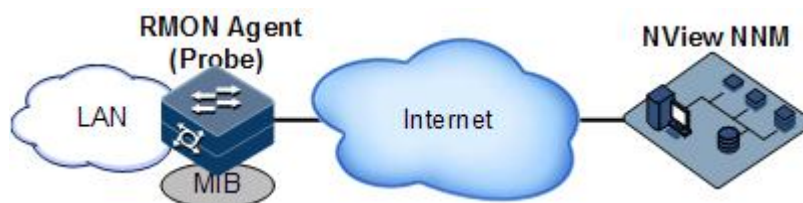
The RMON Agent is commonly referred to as the probe program. The RMON Probe can take the communication subnet statistics and performance analysis. Whenever it finds network failure, RMON Probe can report the NView NNM system, and describes the capture information under unusual circumstances so that the NView NNM system does not need to poll the device constantly. Compared with SNMP, RMON can monitor remote devices more actively and more effectively, network administrators can track the network, segment or device malfunction more quickly. This method reduces the data flows between the NView NNM system and Agent, makes it possible to manage large networks simply and powerfully, and makes up the limitations of SNMP in growing distributed Internet.

RMON Probe collects data in the following modes:

- Distributed RMON. Network management center obtains network management information and controls network resources directly from RMON Probe through dedicated RMON Probe collection data.
- Embedded RMON. Embed RMON Agent directly to network devices (such as switches) to make them with RMON Probe function. Network management center will collect network management information through the basic operation of SNMP and the exchange data information about RMON Agent.

The Raisecom ISCOM2600G-HI series switch is embedded with RMON. As shown in Figure 12-5, the ISCOM2600G-HI series switch implements RMON Agent function. Through this function, the management station can obtain the overall flow, error statistics and performance statistics about this segment connected to the managed network device interface so as to achieve the monitoring to one segment.

Figure 12-5 RMON networking



RMON MIB can be divided into nine groups according to function. Currently, there are four function groups achieved: statistics group, history group, alarm group, and event group.

- Statistic group: collect statistics on each interface, including receiving packets accounts and size distribution statistics.
- History group: similar with statistic group, it only collects statistics in an assigned detection period.
- Alarm group: monitor an assigned MIB object and configure upper threshold and lower threshold in assigned interval, trigger an event if the monitor object receives threshold value.
- Event group: cooperating with alarm group. When an alarm triggers an event, it records the event, such as sending Trap, and writes the event into log.

## 12.2.2 Preparing for configurations

### Scenario

RMON helps monitor and account network traffics.

Compared with SNMP, RMON is a more high-efficient monitoring method. After you specifying the alarm threshold, the ISCOM2600G-HI series switch actively sends alarms when the threshold is exceeded without obtaining variable information. This helps reduce traffic of Central Office (CO) and managed devices and facilitates network management.

### Prerequisite

The route between the ISCOM2600G-HI series switch and the NView NNM system is reachable.

## 12.2.3 Default configurations of RMON

Default configurations of RMON are as below.

Function	Default value
Statistics group	Enabled on all interfaces
History group	Disable
Alarm group	N/A
Event group	N/A

## 12.2.4 Configuring RMON statistics

RMON statistics is used to gather statistics on an interface, including the number of received packets, undersized/oversized packets, collision, CRC and errors, discarded packets, fragments, unicast packets, broadcast packets, multicast packets, and received packet size.

Configure RMON statistics for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#rmon statistics</b> <i>interface-type interface-list</i> [ <b>owner owner-name</b> ]	Enable RMON statistics on an interface and configure related parameters.



### Note

When using the **no rmon statistics interface-type interface-list** command to disable RMON statistics on an interface, you cannot continue to obtain the interface statistics, but the interface can still count data.

## 12.2.5 Configuring RMON historical statistics

Configure RMON historical statistics for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#rmon history interface-type interface-list [ shortinterval short-period ] [ longinterval long-period ] [ buckets buckets-number ] [ owner owner-name ]</b>	Enable RMON historical statistics on an interface and configure related parameters.



### Note

When you use the **no rmon history interface-type interface-list** command to disable RMON historical statistics on an interface, the interface will not count data and clear all historical data collected previously.

## 12.2.6 Configuring RMON alarm group

Configure one RMON alarm group instance (alarm-id) to monitor one MIB variable (mibvar). When the value of monitoring data exceeds the defined threshold, an alarm event will generate. Record the log to send Trap to network management station according to the definition of alarm event.

The monitored MIB variable must be real, and the data value type is correct.

- If the configured variable does not exist or value type variable is incorrect, return error.
- In the successfully configured alarm, if the variable cannot be collected later, close the alarm; reconfigure the alarm if you want to monitor the variable again.

By default, the triggered event number is 0; in other words, no event will be triggered. If the number is not zero, and there is no corresponding configuration in event group, when the control variable is abnormal, it cannot trigger the event successfully until the event is established.

An alarm will be triggered as long as matching the condition when the upper or lower limit for one of the events is configured in the event table. If there is no configuration for the upper and lower limits related alarm event (rising-event-id, falling-event-id) in the event table, no alarm will not be generated even alarm conditions are met.

Configure the RMON alarm group for the ISCOM2600G-HI series switch as below.

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



Step	Command	Description
2	<code>Raisecom(config)#rmon alarm alarm-id mibvar [ interval period ] { absolute   delta } rising-threshold rising-value [ rising-event-id ] falling-threshold falling-value [ falling-event-id ] [ owner owner-name ]</code>	Add alarm instances to the RMON alarm group and configure related parameters.

## 12.2.7 Configuring RMON event group

Configure the RMON event group for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#rmon event event-id [ log ] [ trap ] [ description string ] [ owner owner-name ]</code>	Add events to the RMON event group and configure processing modes of events.

## 12.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show rmon</code>	Show RMON configurations.
2	<code>Raisecom#show rmon alarms</code>	Show information about the RMON alarm group.
3	<code>Raisecom#show rmon events</code>	Show information about the RMON event group.
4	<code>Raisecom#show rmon statistics [ interface-type interface-list]</code>	Show information about the RMON statistics group.
5	<code>Raisecom#show rmon latest statistics [ long   short ] portlist interface-type interface-number</code>	Show RMON statistics in the last 5s or 5min.
6	<code>Raisecom#show rmon history interface-type interface-list</code>	Show information about the RMON history group.

## 12.2.9 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
<code>Raisecom(config)#clear rmon</code>	Clear all RMON configurations.

## 12.2.10 Example for configuring RMON alarm group

### Networking requirements

As shown in Figure 12-6, the ISCOM2600G-HI series switch is the Agent, connected to terminal through the Console interface, connected to remote NView NNM system through Internet. Enable RMON statistics and gather performance statistic on GE 1/1/3. When packets received on GE 1/1/1 exceeds the threshold in a period, logs are recorded and Trap is sent.

Figure 12-6 RMON networking



### Configuration steps

- Step 1 Create an event with index ID 1, used to record and send logs with description string High-ifOutErrors. The owner of logs is system.

```

Raisecom#config
Raisecom(config)#rmon statistics gigaehternet 1/1/1
Raisecom(config)#rmon event 1 log description High-ifOutErrors owner
system
  
```

- Step 2 Create an alarm item with index ID 10, used to monitor MIB variables 1.3.6.1.2.1.2.2.1.20.1 every 20s. If the variable increases by more than 15, the Trap alarm will be triggered. The owner of alarm message is also system.

```

Raisecom(config)#rmon alarm 10 1.3.6.1.2.1.2.2.1.20.1 interval 20 delta
rising-threshold 15 1 falling-threshold 0 owner system
  
```

## Checking results

Use the **show rmon alarms** command to check whether there is information about event group events on the ISCOM2600G-HI series switch.

```
Raisecom#show rmon alarms
Alarm group information:
Alarm 10 is active, owned by system
Monitors 1.3.6.1.2.1.2.2.1.20.1 every 20 seconds
Taking delta samples, last value was 0
Rising threshold is 15, assigned to event 1
Falling threshold is 0, assigned to event 0
On startup enable rising and falling alarm
```

Use the **show rmon events** command to check whether there is information about alarm group on the ISCOM2600G-HI series switch.

```
Raisecom#show rmon events
Event group information:
Event 1 is active, owned by system
Event description: high.
Event generated at 0:0:0
Register log information when event is fired.
```

When an alarm event is triggered, you can also check related information in the alarm management part of the NView NNM system.

## 12.3 LLDP

### 12.3.1 Introduction

With the enlargement of network scale and increase of network devices, the network topology becomes more and more complex and network management becomes more 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 the Layer 3 network and cannot ensure the interfaces to be connected 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.

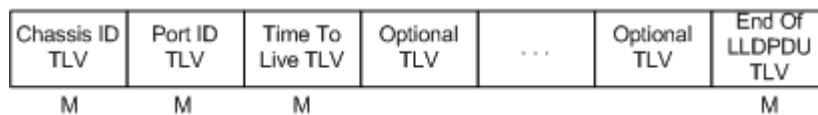
## LLDP packet

The LLDP packet is used to encapsulate LLDPDU Ethernet packet in data unit and transmitted by multicast.

LLDPDU is the data unit of LLDP. The device encapsulates local information in TLV before forming LLDPDU, then several TLV fit together in one LLDPDU and encapsulated in Ethernet data for transmission.

As shown in Figure 12-7, LLDPDU is made by several TLV, including 4 mandatory TLV and several optional TLV.

Figure 12-7 Structure of a LLDPDU



M - mandatory TLV required for all LLDPDUs

As shown in Figure 12-8, each TLV denotes a piece of information at local. For example, the device ID and interface ID correspond with the Chassis ID TLV and Port ID TLV respectively, which are fixed TLVs.

Figure 12-8 Structure of a TLV packet

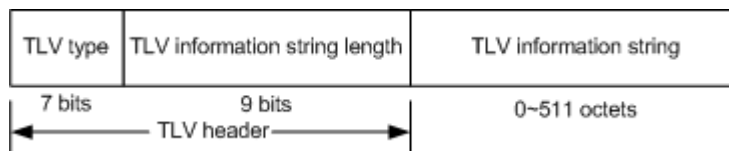


Table 12-1 lists TLV types. At present only types 0~8 are used.

Table 12-1 TLV types

TLV type	Description	Optional/Required
0	End Of LLDPDU	Required
1	Chassis ID	Required
2	Interface number	Required
3	Time To Live	Required
4	Interface description	Optional
5	System name	Optional
6	System description	Optional
7	System capabilities	Optional
8	Management address	Optional

Organization-defined TLVs are optional TLVs and are advertised in the LLDPDU as required. Table 12-2 and Table 12-3 list common organization-defined TLVs.

Table 12-2 IEEE 802.1 organization-defined TLVs

Type	Description
Port VLAN ID TLV	VLAN ID on the interface
Port And Protocol VLAN ID TLV	Protocol VLAN ID on the interface
VLAN Name TLV	VLAN name on the interface
Protocol Identity TLV	Type of the protocol supported by the interface

Table 12-3 IEEE 802.3 organization-defined TLVs

Type	Description
MAC/PHY Configuration//Status TLV	Rate and duplex mode of the interface, whether auto-negotiation is supported or enabled
Power Via MDI TLV	Power supply capability on the interface
Link Aggregation TLV	Link aggregation capability on the interface and current link aggregation status
Maximum Frame Size TLV	Size of the maximum frame able to be transmitted by the interface

## Principles

LLDP is a kind of point-to-point one-way issuance protocol, which notifies local device link status to peer end by sending LLDPDU (or sending LLDPDU when link status changes) periodically from the local end to the peer end.

The procedure of packet exchange:

- When the local device transmits packet, it gets system information required by TLV from NView NNM (Network Node Management) and gets configurations from LLDP MIB to generate TLV and form LLDPDU to transmit to 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.

When the device status is changed, the ISCOM2600G-HI series switch sends a LLDP packet to the peer. To avoid sending LLDP packet continuously because of device status changes frequently, you can configure a delay timer for sending the LLDP packet.

The aging time of Time To Live (TTL) in local device information about the neighbour node can be adjusted by modifying the parameter values of aging coefficient, sends LLDP packets to neighbour node, after receiving LLDP packets, neighbour node will adjust the aging time of its neighbour nodes (sending side) information. Aging time formula,  $TTL = \text{Min} \{65535, (\text{interval} \times \text{hold-multiplier})\}$ :

- Interval indicates the time period to send LLDP packets from neighbor node.

- Hold-multiplier refers to the aging coefficient of device information in neighbor node.

## 12.3.2 Preparing for configurations

### Scenario

When you obtain connection information between devices through NView NNM system for topology discovery, the ISCOM2600G-HI series switch needs to enable LLDP, notify their information to the neighbours mutually, and store neighbour information to facilitate the NView NNM system queries.

### Prerequisite

N/A

## 12.3.3 Default configurations of LLDP

Default configurations of LLDP are as below.

Function	Default value
Global LLDP	Disable
LLDP interface status	Enable
Delay timer	2s
Period timer	30s
Aging coefficient	4
Restart timer	2s
Alarm function	Enable
Alarm notification timer	5s
Destination MAC address of LLDP packets	0180.c200.000e

## 12.3.4 Enabling global LLDP



### Caution

After global LLDP is disabled, you cannot re-enable it immediately. Global LLDP cannot be enabled unless the restart timer times out.

When you obtain connection information between devices through the NView NNM system for topology discovery, the ISCOM2600G-HI series switch needs to enable LLDP, sends their information to the neighbours mutually, and stores neighbour information to facilitate query by the NView NNM system.

Enable global LLDP for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#lldp enable</b>	Enable global LLDP.

### 12.3.5 Enabling interface LLDP

Enable interface LLDP for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface</b> <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/1)#lldp enable</b>	Enable LLDP on an interface.

### 12.3.6 Configuring basic functions of LLDP



#### Caution

When configuring the delay timer and period timer, the value of the delay timer should be smaller than or equal to a quarter of the period timer value.

Configure basic functions of LLDP for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#lldp message-transmission interval</b> <i>period</i>	(Optional) configure the period timer of the LLDP packet.
3	<b>Raisecom(config)#lldp message-transmission delay</b> <i>period</i>	(Optional) configure the delay timer of the LLDP packet.
4	<b>Raisecom(config)#lldp message-transmission hold-multiplier</b> <i>hold-multiplier</i>	(Optional) configure the aging coefficient of the LLDP packet.
5	<b>Raisecom(config)#lldp restart-delay</b> <i>period</i>	(Optional) restart the timer. When configuring the delay timer and period timer, the value of the delay timer should be smaller than or equal to a quarter of the period timer value.

## 12.3.7 Configuring LLDP alarm

When the network changes, you need to enable LLDP alarm notification function to send topology update alarm to the NView NNM system immediately.

Configure the LLDP alarm for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#lldp trap-interval <i>period</i></b>	(Optional) configure the period of the timer for sending LLDP alarm Traps.

## 12.3.8 Configuring TLV

Configure TLV for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#interface <i>interface-type interface-number</i></b>	Enter physical layer interface configuration mode.
3	<b>Raisecom(config-gigaethernet1/1/1)#lldp tlv-select basic-tlv {all   port-description   system-capability   system-name   system-description }</b>	Configure the basic TLV allowed to issue.
4	<b>Raisecom(config-gigaethernet1/1/1)#lldp tlv-select med-tlv {all   capability   inventory   network-policy   location-id }</b>	Configure the MED TLV allowed to issue.
5	<b>Raisecom(config-gigaethernet1/1/1)#lldp tlv-select dot1-tlv {all   port-vlan-id   vlan-name }</b>	Enable 802.1 TLV type allowed to issue.
6	<b>Raisecom(config-gigaethernet1/1/1)#lldp tlv-select dot3-tlv { all   link-aggregation   mac-physic   max-frame-size   power }</b>	Enable 802.3 TLV type allowed to be issued.

## 12.3.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show lldp local config</b>	Show LLDP local configurations.
2	<b>Raisecom#show lldp local system-data [ <i>interface-type interface-number</i> ]</b>	Show information about the LLDP local system.



No.	Command	Description
3	Raisecom# <b>show lldp remote</b> [ <i>interface-type interface-number</i> ] [ <b>detail</b> ]	Show information about the LLDP neighbor.
4	Raisecom# <b>show lldp statistic</b> [ <i>interface-type interface-number</i> ]	Show statistics about LLDP packets.
5	Raisecom# <b>show lldp tlv-select</b> [ <i>interface-type interface-number</i> ]	Show information about the optional TLV sent by the interface.

## 12.3.10 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

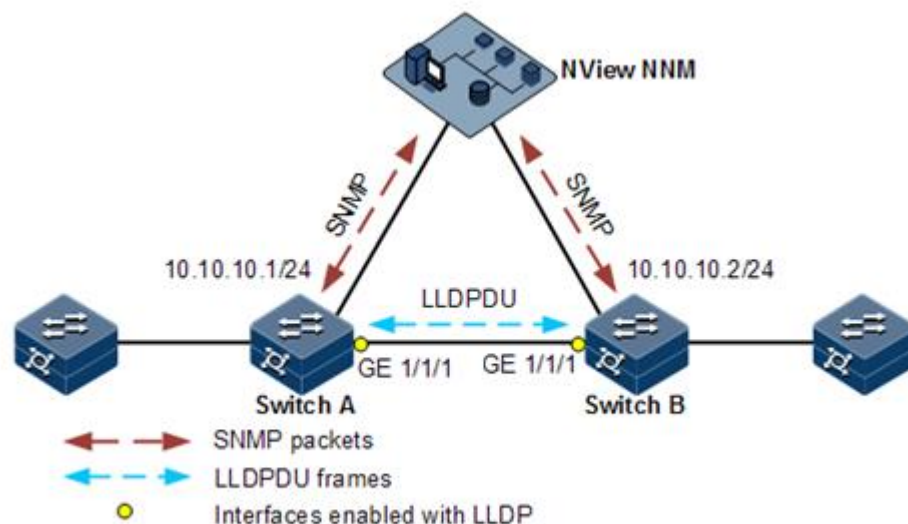
Command	Description
Raisecom(config)# <b>clear lldp statistic</b> <i>interface-type interface-number</i>	Clear LLDP statistics.
Raisecom(config)# <b>clear lldp remote-table</b> [ <i>interface-type interface-number</i> ]	Clear LLDP neighbor information.
Raisecom(config)# <b>clear lldp global statistic</b>	Clear global LLDP statistics.

## 12.3.11 Example for configuring LLDP

### Networking requirements

As shown in Figure 12-9, the Switch is connected to the NView NNM system; enable LLDP between Switch A and Switch B, query Layer 2 link change through the NView NNM system. The neighbor aging, new neighbor and neighbor information changes will be reported as LLDP alarms to the NView NNM system.

Figure 12-9 LLDP networking



## Configuration steps

Step 1 Enable global LLDP and LLDP alarm.

Configure Switch A.

```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#lldp enable
```

Configure Switch B.

```
Raisecom#name SwitchB
SwitchB#config
SwitchB(config)#lldp enable
```

Step 2 Configure the management IP address.

Configure Switch A.

```
SwitchA(config)#create vlan 1024 active
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#switchport access vlan 1024
SwitchA(config-gigabitEthernet1/1/1)#exit
SwitchA(config)#interface vlan 1024
SwitchA(config-vlan1)#ip address 10.10.10.1 255.255.255.0
SwitchA(config-vlan1)#exit
```

Configure Switch B.

```
SwitchB(config)#create vlan 1024 active
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport access vlan 1024
SwitchB(config)#interface vlan 1024
SwitchB(config-vlan1)#ip address 10.10.10.2 255.255.255.0
SwitchB(config-vlan1)#exit
```

Step 3 Configure LLDP attributes.

Configure Switch A.

```
SwitchA(config)#lldp message-transmission interval 60
SwitchA(config)#lldp message-transmission delay 9
SwitchA(config)#lldp trap-interval 10
```

Configure Switch B.

```
SwitchB(config)#lldp message-transmission interval 60
SwitchB(config)#lldp message-transmission delay 9
SwitchB(config)#lldp trap-interval 10
```

## Checking results

Use the **show lldp local config** command to show local configurations.

```
SwitchA#show lldp local config
System configuration:
```

```
-----
LLDP enable status:          enable (default is disabled)
LldpMsgTxInterval:          60    (default is 30s)
LldpMsgTxHoldMultiplier:    4     (default is 4)
LldpReinitDelay:            2     (default is 2s)
LldpTxDelay:                 9     (default is 2s)
LldpNotificationInterval:    10    (default is 5s)
LldpNotificationEnable:      enable (default is enabled)
-----
```

Port	Status	Packet destination-mac
GE1/1/1	enable	0180.C200.010e
GE1/1/2	enable	0180.C200.010e
GE1/1/3	enable	0180.C200.010e
GE1/1/4	enable	0180.C200.010e
GE1/1/5	enable	0180.C200.010e
GE1/1/6	enable	0180.C200.010e

```
.....
SwitchB#show lldp local config
System configuration:
-----
LLDP enable status:          enable (default is disabled)
LldpMsgTxInterval:          60      (default is 30s)
LldpMsgTxHoldMultiplier:    4       (default is 4)
LldpReinitDelay:            2       (default is 2s)
LldpTxDelay:                9       (default is 2s)
LldpNotificationInterval:    10     (default is 5s)
LldpNotificationEnable:      enable (default is enabled)
-----
```

Port	Status	Packet destination-mac
GE1/1/1	enable	0180.C200.000E
GE1/1/2	enable	0180.C200.000E
GE1/1/3	enable	0180.C200.000E
GE1/1/4	enable	0180.C200.000E
GE1/1/5	enable	0180.C200.000E
GE1/1/6	enable	0180.C200.000E

```
.....
```

Use the **show lldp remote** command to show neighbor information.

```
SwitchA#show lldp remote
Port  ChassisId          PortId          SysName  MgtAddress  ExpiredTime
-----
gigaethernet1/1/1  000E.5E02.B010  gigaethernet1/1/1  SwitchB
10.10.10.2        106
.....
SwitchB#show lldp remote
Port  ChassisId          PortId          SysName  MgtAddress  ExpiredTime
-----
gigaethernet1/1/1  000E.5E12.F120  gigaethernet1/1/1  SwitchA
10.10.10.1        106
.....
```

## 12.4 Optical module DDM

### 12.4.1 Introduction

Optical module Digital Diagnostics Monitoring (DDM) on the ISCOM2600G-HI series switch supports Small Form-factor Pluggable (SFP) and 10GE SFP+ diagnosis.

The fault diagnostics function of SFP provides the system a performance monitor method. The network administrator analysis the monitor data provided by SFP to predict the age of transceiver, isolate system fault and authenticate modules compatibility during installation.

The performance parameters of optical module which are monitored by optical module DDM are as below:

- Modular temperature
- Inner power voltage
- Tx offset current
- Tx optical power
- Rx optical power

When the performance parameters reach alarm threshold or status information changes, the corresponding Trap alarm will be generated.

## 12.4.2 Preparing for configurations

### Scenario

Fault diagnostics of optical modules provide a method for detecting SFP performance parameters. You can predict the service life of optical module, isolate system fault and check its compatibility during installation through analyzing monitoring data.

### Prerequisite

The optical module used on the ISCOM2600G-HI series switch should be a Raisecom-certified one. If you use an optical module of other vendors, problems of unstable services, failure in supporting DDM, or incorrect DDM information will happen.

## 12.4.3 Default configurations of optical module DDM

Default configurations of optical module DDM are as below.

Function	Default value
Global optical module DDM	Disable
Interface optical module DDM	Disable
Global optical DDM Trap	Disable
Interface optical DDM Trap	Disable

## 12.4.4 Enabling optical module DDM

Enable optical module DDM for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#transceiver ddm enable</b>	Enable optical module DDM globally.
3	<b>Raisecom(config)#transceiver ddm poll-interval interval</b>	Configure the polling interval for optical module DDM.

Step	Command	Description
3	<b>Raisecom(config)#interface</b> <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config-gigaethernet1/1/port)#transceiver ddm enable</b>	Enable interface optical module DDM. Only when global optical DDM is enabled, the optical module, where interface optical module DDM is enabled, can the ISCOM2600G-HI series switch perform DDM.

## 12.4.5 Enabling optical module DDM Trap

Enable optical module DDM Trap for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#snmp-server trap transceiver enable</b>	Enable optical module DDM Trap globally.
3	<b>Raisecom(config)#interface</b> <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
4	<b>Raisecom(config-gigaethernet1/1/port)#transceiver trap enable</b>	Enable interface optical module DDM Trap. Only when global optical DDM Trap is enabled, the optical module, where interface optical module DDM Trap is enabled, can the ISCOM2600G-HI series switch send Traps.

## 12.4.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show transceiver</b>	Show global optical module DDM and interface optical module DDM configurations.
2	<b>Raisecom#show transceiver ddm</b> <i>interface-type</i> <i>interface-list</i> [ <b>detail</b> ]	Show optical module DDM performance parameters.
3	<b>Raisecom#show transceiver</b> <i>interface-type</i> <i>interface-list</i> <b>history</b> [ <b>15m</b>   <b>24h</b> ]	Show historical information about optical module DDM.
4	<b>Raisecom#show transceiver information</b> <i>interface-type</i> <i>interface-list</i>	Show basic information about the optical module.

No.	Command	Description
5	<b>Raisecom#show transceiver threshold-violations</b> <i>interface-type interface-list</i>	Show the information when the optical module parameters exceed the thresholds.
6	<b>Raisecom(config)#show transceiver ddm brief</b>	Show brief information about optical module DDM.

## 12.5 System log

### 12.5.1 Introduction

The system log refers that the ISCOM2600G-HI series switch records the system information and debugging information in a log and sends the log to the specified destination. When the ISCOM2600G-HI series switch fails to work, you can check and locate the fault easily.

The system information and some scheduling output will be sent to the system log to deal with. 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.
- File: send the log message to the Flash of the device.
- Buffer: send the log message to the buffer.
- SNMP server: convert logs to Trap and then outputs Trap to the SNMP server.

According to the severity level, the log is identified by 8 severity levels, as listed in Table 12-4.

Table 12-4 Log levels

Severity	Level	Description
Emergency	0	The system cannot be used.
Alert	1	Need to deal immediately.
Critical	2	Serious status
Error	3	Errored status
Warning	4	Warning status
Notice	5	Normal but important status
Informational	6	Informational event
Debug	7	Debugging information



## Note

The severity of output information can be manually configured. When you send information according to the configured severity, you can just send the information whose severity is less than or equal to that of the configured information. For example, when the information is configured with the level 3 (or the severity is errors), the information whose level ranges from 0 to 3, in other words, the severity ranges from emergencies to errors, can be sent.

## 12.5.2 Preparing for configurations

### Scenario

The ISCOM2600G-HI series switch generates the login successes or failures, key information, debugging information, and error information to system log, outputs them as log files, and sends them to the logging host, Console interface, or control console to facilitate checking and locating faults.

### Prerequisite

N/A

## 12.5.3 Default configurations of system log

Default configurations of system log are as below.

Function	Default value
System log	Enable
Output log information to Console	Enable, the default level is information (6).
Output log information to host	N/A, the default level is information (6).
Output log information to file	Enable, the default level is debugging (7).
Output log information to monitor	Disable, the default level is information (6).
Output log information to buffer	Disable, the default level is information (6).
Log Debug level	Low
Output log information to history list	Disable
Log history list size	1
Transfer log to Trap	Disable. The default level is warning (4).
Log buffer size	4 Kbytes
Transmitting rate of system log	No limit
Timestamp of system log information	<ul style="list-style-type: none"><li>• Debug: no timestamp to debug level (7) Syslog information.</li><li>• Log: The timestamp to 0–6 levels Syslog information is absolute time.</li></ul>



## 12.5.4 Configuring basic information of system log

Configure basic information of system log for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#logging on</b>	(Optional) enable system log.
3	<b>Raisecom(config)#logging time-stamp</b> { <b>debug</b>   <b>log</b> } { <b>datetime</b>   <b>none</b>   <b>uptime</b> }	(Optional) configure timestamp for system log. The optional parameter <b>debug</b> is used to assign debug level (7) system log timestamp; by default, this system log does not have timestamp The optional parameter <b>log</b> is used to assign debug level 0–6 system log timestamp; by default, this system log adopts date-time as timestamp.
4	<b>Raisecom(config)#logging rate-limit</b> <i>log-num</i>	(Optional) configure transmitting rate of system log.
5	<b>Raisecom(config)#logging sequence-number</b>	(Optional) configure sequence of system log. The sequence number only applies to the console, monitor, log file, and log buffer, but not log host and history list.
6	<b>Raisecom(config)#logging discriminator</b> <i>discriminator-number</i> { <b>facility</b>   <b>mnemonics</b>   <b>msg-body</b> } { { <b>drops</b>   <b>includes</b> } <i>key</i>   <b>none</b> }	(Optional) create and configure system log filter. The filter can filter output log from the console, monitor, log file and log buffer.
7	<b>Raisecom(config)#logging buginf</b> [ <b>high</b>   <b>normal</b>   <b>low</b>   <b>none</b> ]	(Optional) configure sending Debug-level logs.

## 12.5.5 Configuring system log output

Configure system log output for the ISCOM2600G-HI series switch as below.

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

Step	Command	Description
2	<b>Raisecom(config)#logging console</b> [ <i>log-level</i>   <b>alerts</b>   <b>critical</b>   <b>debugging</b>   <b>emergencies</b>   <b>errors</b>   <b>informational</b>   <b>notifications</b>   <b>warnings</b>   <b>distriminator</b> <i>distriminator-number</i> ]	(Optional) output system logs to the console.
3	<b>Raisecom(config)#logging host ip-address</b> [ <i>log-level</i>   <b>alerts</b>   <b>critical</b>   <b>debugging</b>   <b>emergencies</b>   <b>errors</b>   <b>informational</b>   <b>notifications</b>   <b>warnings</b>   <b>distriminator</b> <i>distriminator-number</i> ]  <b>Raisecom(config)#logging</b> [ <i>host ip-address</i> ] <b>facility</b> { <b>alert</b>   <b>audit</b>   <b>auth</b>   <b>clock</b>   <b>cron</b>   <b>daemon</b>   <b>ftp</b>   <b>kern</b>   <b>local0</b>   <b>local1</b>   <b>local2</b>   <b>local3</b>   <b>local4</b>   <b>local5</b>   <b>local6</b>   <b>local7</b>   <b>lpr</b>   <b>mail</b>   <b>news</b>   <b>ntp</b>   <b>sercurity</b>   <b>syslog</b>   <b>user</b>   <b>uucp</b> }	(Optional) output system logs to the log host. Up to 10 log hosts are supported.  Configure the facility field of the log to be sent to the log host.  Configuration may fail if you do not create the log host.  This configuration is available for all log hosts configured on the ISCOM2600G-HI series switch.
4	<b>Raisecom(config)#logging monitor</b> [ <i>log-level</i>   <b>alerts</b>   <b>critical</b>   <b>debugging</b>   <b>emergencies</b>   <b>errors</b>   <b>informational</b>   <b>notifications</b>   <b>warnings</b>   <b>distriminator</b> <i>distriminator-number</i> ]	(Optional) output system logs to the monitor.
5	<b>Raisecom(config)#logging file</b> [ <b>discriminator</b> <i>discriminateor-number</i> ]	(Optional) output system logs to the Flash of the ISCOM2600G-HI series switch.  Only warning-level logs are available.
6	<b>Raisecom(config)#logging buffered</b> [ <i>log-level</i>   <b>alerts</b>   <b>critical</b>   <b>debugging</b>   <b>emergencies</b>   <b>errors</b>   <b>informational</b>   <b>notifications</b>   <b>warnings</b>   <b>distriminator</b> <i>distriminator-number</i> ]  <b>Raisecom(config)#logging buffered size</b> <i>size</i>	(Optional) output system logs to the buffer.  (Optional) configure the system log buffer size.
7	<b>Raisecom(config)#logging history</b>	(Optional) output system logs to the log history list.  The level of the output logs is the one of the translated Trap.

Step	Command	Description
	<b>Raisecom(config)#logging history size size</b>	(Optional) configure the log history list size.
	<b>Raisecom(config)#logging trap [ log-level   alerts   critical   debugging   emergencies   errors   informational   notifications   warnings   discriminator discriminator-number ]</b>	(Optional) enable translating specified logs in the history list to Traps.  Configurations may fail if the system logs are not output to the log history list.

## 12.5.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show logging</b>	Show configurations of system log.
2	<b>Raisecom#show logging buffer</b>	Show information about the system log buffer.
3	<b>Raisecom#show logging discriminator</b>	Show filter information.
4	<b>Raisecom#show logging file</b>	Show contents of system log. The device supports this configuration at millisecond level.
5	<b>Raisecom#show logging history</b>	Show information about the system log history list.

## 12.5.7 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

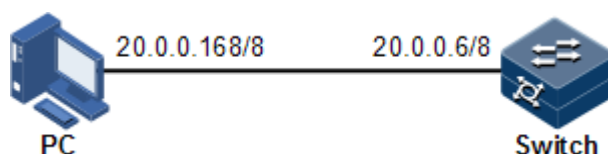
Command	Description
<b>Raisecom(config)#clear logging buffer</b>	Clear log information in the buffer.
<b>Raisecom(config)#clear logging statistics</b>	Clear log statistics.

## 12.5.8 Example for configuring outputting system logs to log host

### Networking requirements

As shown in Figure 12-10, configure system log, and output device log information to log host for user to check.

Figure 12-10 Networking of outputting system log to log host



## Configuration steps

Step 1 Configure the IP address of the ISCOM2600G-HI series switch.

```

Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 20.0.0.6 255.0.0.0
Raisecom(config-vlan1)#exit
  
```

Step 2 Configure the system log to be output to the log host.

```

Raisecom(config)#logging on
Raisecom(config)#logging time-stamp log datetime
Raisecom(config)#logging rate-limit 2
Raisecom(config)#logging host 20.0.0.168 warnings
  
```

## Checking results

Use the **show logging** command to show configurations of system log.

```

Raisecom#show logging
Syslog logging:          enable
Dropped Log messages:    0
Dropped debug messages:  0
Rate-limited:            2 messages per second
Sequence number display: disable
Debug level time stamp:  none
Log level time stamp:    datetime
Log buffer size:         4kB
Debug level:             low
Syslog history logging:  disable
Syslog history table size:1
Dest      Status  Level          LoggedMsgs  DroppedMsgs  Discriminator
-----
---
buffer    enable   informational(6) 10          0            0
console   enable   informational(6) 10          0            0
trap      disable  warnings(4)      0           0            0
file      enable   debugging(7)     17          0            0
Log host information:
  
```

```

Max number of log server:    10
Current log server number:   1
Target Address      Level      Facility      Sent      Drop
Discriminator
-----
20.0.0.168          warnings(4)  local7       0         0         0

```

## 12.6 Alarm management

### 12.6.1 Introduction

Alarm means when a fault is generated on the ISCOM2600G-HI series switch or some working condition changes, the system will generate alarm according to different faults.

Alarm information is used to report some urgent and important events and notify them to the network administrator promptly, which provides strong support for monitoring device operation and diagnosing faults.

Alarm information is stored in the alarm buffer. Meanwhile, the alarm is generated to log information. If a Network Management System (NMS), the alarm will be sent to network management system through SNMP. The information sent to the NMS is called Trap information.

### Alarm classification

Alarms can be divided into three types according to properties:

- Fault alarm: refer to alarms for some hardware fault or some abnormal important functions, such as port Down alarm;
- Recovery alarm: refer to alarms that are generated when device failure or abnormal function returns to normal, such as port Up alarm;
- Event alarm: refer to prompted alarms or alarms that are generated because of failure in relating the fault to the recovery, such as alarms generated by failing to Ping.

Alarms can be divided into five types according to functions:

- Communication alarm: refer to alarms related to the processing of information transmission, including alarms that are generated by communication fault between Network Elements (NE), NEs and NMS, or NMS and NMS.
- Service quality alarm: refer to alarms caused by service quality degradation, including congestion, performance decline, high resource utilization rate, and the bandwidth reducing.
- Processing errored alarm: refer to alarms caused by software or processing errors, including software errors, memory overflow, version mismatching, and the abnormal program aborts.
- Environmental alarm: refer to alarms caused by equipment location-related problems, including the environment temperature, humidity, ventilation and other abnormal working conditions.

- Device alarm: refer to alarms caused by failure of physical resources, including power, fan, processor, clock, Rx/Tx interfaces, and other hardware.

## Alarm output

There are three alarm output modes:

- Alarm buffer: alarm is recorded in tabular form, including the current alarm table and history alarm table.
  - Current alarm table, recording alarm which is not cleared, acknowledged or restored.
  - History alarm table, consisting of acknowledged and restored alarm, recording the cleared, auto-restored or manually acknowledged alarm.
- Log: alarm is generated to system log when recorded in the alarm buffer, and stored in the alarm log buffer.
- Trap information: alarm sent to NMS when the NMS is configured.

Alarm will be broadcasted according to various terminals configured by the ISCOM2600G-HI series switch, including CLI terminal and NMS.

Log output of alarm starts with the symbol "#", and the output format is as below:

```
#Index TimeStamp HostName ModuleName/Severity/name:Arise From Description.
```

Table 12-5 describes alarm fields.

Table 12-5 Alarm fields

Field	Description
TimeStamp	Time when an alarm is generated
ModuleName	Name for a module where alarms are generated
Severity	Alarm level
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 12-6.

Table 12-6 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)

Level	Description	Syslog
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 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)

## Related concepts

Related concepts about alarm management are displayed as below:

- Alarm suppression

The ISCOM2600G-HI series switch only records root-cause alarms but incidental alarms when enabling alarm suppression. For example, the generation of alarm A will inevitably produce alarm B which is in the inhibition list of alarm A, then alarm B is inhibited and does not appear in alarm buffer and record the log information when enabling alarm suppression. By enabling alarm suppression, the ISCOM2600G-HI series switch can effectively reduce the number of alarms.

Alarm A and alarm B will be recorded on the ISCOM2600G-HI series switch and reported to the NMS when alarm suppression is disabled.

- Alarm auto-report

Auto-report refers that an alarm will be reported to NMS automatically with its generation and you do not need to initiate inquiries or synchronization.

You can configure auto-report to some alarm, some alarm source, or the specified alarm from specified alarm source.



### Note

The alarm source refers to an entity that generates related alarms, such as ports, devices, and cards.

- Alarm monitoring

Alarm monitoring is used to process alarms generated by modules:

- When the alarm monitoring is enabled, the alarm module will receive alarms generated by modules, and process them according to the configurations of the alarm module, such as recording alarm in alarm buffer, or recording system logs.
- When the alarm monitoring is disabled, the alarm module will discard alarms generated by modules without follow-up treatment. In addition, alarms will not be recorded on the ISCOM2600G-HI series switch.

You can perform the alarm monitoring on some alarm, alarm source or specified alarm on from specified alarm source.

- Alarm reverse mode

Alarm reverse refers to the device will report the information opposite to actual status when recording alarm, or report the alarm when there is no alarm. Alarms are not reported if there are alarms.

Currently, the device is only in support of reverse mode configuration of the interface. There are three reverse modes to be configure; the specific definitions are as below:

- Non-reverse mode

The device alarm is reported normally.

- Manual reverse mode

Configure the alarm reverse mode of an interface as manual reverse mode. In this mode, no matter what the current alarm status is, the reported alarm status of the interface will be changed opposite to the actual alarm status immediately; in other words, alarms are not reported when there are alarms, and alarms are reported when there are no alarms actually. The interface will maintain the opposite alarm status regardless of the alarm status changes before the alarm reverse status being restored to non-reverse mode.

- Auto-reverse mode

Configure the alarm reverse mode as auto-reverse mode. If no reversible alarm is on the interface, this configuration will be prompted as failure. If reversible alarms are on the interface, this configuration will succeed and enter reverse mode; in other words, the reported alarm status of the interface will be changed opposite to the actual alarm status immediately. After the alarm is finished, the enabling state of interface alarm reverse will end automatically and changes to non-reverse alarm mode so that the alarm status can be reported normally in the next alarm.

- Alarm delay

Alarm delay refers that the ISCOM2600G-HI series switch will record alarms and report them to NMS after a delay but not immediately when alarms generate. Delay for recording and reporting alarms are identical.

By default, the device alarm is reported once generating (0s), which is instant reporting; clear alarm once it ends (0s), which is instant clearing.

- Alarm storage mode

Alarm storage mode refers to how to record new generated alarms when the alarm buffer is full. There are two ways:

- stop: stop mode, when the alarm buffer is full, new generated alarms will be discarded without recording.
- loop: wrapping mode, when the alarm buffer is full, the new generated alarms will replace old alarm and take rolling records.



Use configured storage mode to deal with new generated alarm when the alarm in device alarm table is full.

- Clearing alarms

Clear the current alarm, which means deleting current alarms from the current alarm table. The cleared alarms will be saved to the history alarm table.

- Viewing alarms

The administrator can check alarms and monitor alarm directly on the ISCOM2600G-HI series switch. If the ISCOM2600G-HI series switch is configured with NView NNM system, the administrator can monitor alarms on the NView NNM system.

## 12.6.2 Preparing for configurations

### Scenario

When the device fails, alarm management module will collect fault information and output alarm occurrence time, alarm name and description information in log format to help users locate problem quickly.

If the device is configured with the NMS, alarm can be reported directly to the NMS, providing possible alarm causes and treatment recommendations to help users deal with fault.

If the device is configured with hardware monitoring, it will record the hardware monitoring alarm table, generated Syslog, and sent Trap when the operation environment of the device becomes abnormal, and notify the user of taking actions accordingly and prevent faults.

Alarm management facilitates alarm suppression, alarm auto-reporting, alarm monitoring, alarm reverse, alarm delay, alarm memory mode, alarm clear and alarm view directly on the device.

### Prerequisite

Hardware environment monitoring alarm output:

- In Syslog output mode: alarms will be generated into system logs. To send alarm to the system log host, configure the IP address of the system log host for the device.
- In Trap output mode: configure the IP address of the NMS for the device.

## 12.6.3 Configuring basic functions of alarm management

Configure basic information of alarm management for the ISCOM2600G-HI series switch as below.

All following steps are optional and no sequence between them.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#alarm inhibit enable</b>	Enable alarm suppression. By default, it is enabled.
3	<b>Raisecom(config)#alarm auto-report all enable</b>	Enable alarm auto-reporting.

Step	Command	Description
	<b>Raisecom(config)#alarm auto-report</b> <i>alarm-restype alarm-restype-value</i> <b>enable</b>	Enable alarm auto-reporting of a specified alarm source.
	<b>Raisecom(config)#alarm auto-report</b> <b>type</b> <i>alarm-type</i> <b>enable</b>	Enable alarm auto-reporting of a specified alarm type.
	<b>Raisecom(config)#alarm auto-report</b> <b>type</b> <i>alarm-type</i> <i>alarm-restype</i> <i>alarm-restype-value</i> <b>enable</b>	Enable alarm auto-reporting of a specified alarm source and type.
4	<b>Raisecom(config)#alarm monitor all</b> <b>enable</b>	Enable alarm monitoring.
	<b>Raisecom(config)#alarm monitor</b> <i>alarm-restype alarm-restype-value</i> <b>enable</b>	Enable alarm monitoring of a specified alarm source.
	<b>Raisecom(config)#alarm monitor type</b> <i>alarm-type</i> <b>enable</b>	Enable alarm monitoring of a specified alarm type.
	<b>Raisecom(config)#alarm monitor type</b> <i>alarm-type alarm-restype alarm-restype-value</i> <b>enable</b>	Enable alarm monitoring of a specified alarm source and type.
5	<b>Raisecom(config)#alarm inverse</b> <i>interface-type interface-number</i> { <b>none</b>   <b>auto</b>   <b>manual</b> }	Configure alarm reverse modes.  By default, it is none; in other words, alarm reverse is disabled.
6	<b>Raisecom(config)#alarm { active  </b> <b>cleared } delay</b> <i>second</i>	Configure alarm delay.  By default, it is 0s.
7	<b>Raisecom(config)#alarm active</b> <b>storage-mode</b> { <b>loop</b>   <b>stop</b> }	Configure alarm storage modes.  By default, it is stop.
8	<b>Raisecom(config)#alarm clear all</b>	(Optional) clear all current alarms.
	<b>Raisecom(config)#alarm clear index</b> <i>index</i>	(Optional) clear current alarms of the specified alarm index.
	<b>Raisecom(config)#alarm clear</b> <i>alarm-restype alarm-restype-value</i>	(Optional) clear current alarms of the specified alarm source.
	<b>Raisecom(config)#alarm clear type</b> <i>alarm-type</i>	(Optional) clear current alarms of the specified alarm type.
	<b>Raisecom(config)#alarm clear type</b> <i>alarm-type alarm-restype alarm-restype-value</i>	(Optional) clear current alarms of the specified alarm source and type.

Step	Command	Description
9	<code>Raisecom(config)#alarm syslog enable</code>	(Optional) enable alarms to be output to system logs. By default, it is disabled.
10	<code>Raisecom(config)#exit</code> <code>Raisecom#show alarm active</code> <code>[ module_name   severity severity ]</code>	(Optional) show information about current alarms.
	<code>Raisecom#show alarm cleared</code> <code>[ module_name   severity severity ]</code>	(Optional) show information about historical alarms.



### Note

You can enable/disable alarm monitoring, alarm auto-reporting, and alarm clearing on modules that support alarm management.

## 12.6.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show alarm management</code> <code>[ alarm_type ]</code>	Show parameters of current alarms, including status of alarm suppression, alarm reverse mode, alarm delay, and alarm storage mode, maximum alarm buffer size, and alarm log size.
2	<code>Raisecom#show alarm log</code>	Show alarm statistics in the system log.
3	<code>Raisecom#show alarm management statistics</code>	Show statistics about alarm management module.
4	<code>Raisecom#show alarm active</code>	Show information about current alarms.

## 12.7 Hardware environment monitoring



### Note

The ISCOM2624G-4GE-HI and ISCOM2608G-2GE-HI adopt fanless design, so they do not support abnormal temperature alarm. For details, see their descriptions.

### 12.7.1 Introduction

Hardware environment monitoring mainly refers to monitor the running environment of the ISCOM2600G-HI series switch. The monitoring alarm events include:

- Power supply state alarm

- Temperature beyond threshold alarm
- Flash monitoring alarm

There are several ways to notify users when an alarm is generated. The alarm event output methods are as below:

- Save to the device hardware environment monitoring alarm buffer.
- Output Syslog system log.
- Send Trap to the NMS.

You can take appropriate measures to prevent failure when alarm events happen.

## Alarm events

- Power supply monitoring alarms
- Power supply state change alarms

Power supply state change refers that unplugged power supply is plugged into the device and vice versa. The ISCOM2600G-HI series switch supports dual power supplies. Therefore, power supply state change alarms are divided into the single power supply state change alarm and device dying gasp alarm.

- Dual power supply state change alarm: notify uses that power supply 1/power supply 2 changes. The ISCOM2600G-HI series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.
- Device dying gasp alarm: dual power modules are unplugged, in other words, two power modules are out of position. The ISCOM2600G-HI series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.
- Temperature beyond threshold alarm

The device supports temperature beyond threshold alarm event, when the current temperature is lower than low temperature threshold, the low temperature alarm event will generate. The ISCOM2600G-HI series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.

When the device current temperature is higher than high temperature threshold, the high temperature alarm event will generate. The ISCOM2600G-HI series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.

## Alarm output modes

Hardware environment monitoring alarm output modes are as below.

- Hardware environment monitoring alarm buffer output, which is recorded to the hardware environment monitoring alarm table
  - The hardware environment monitoring current alarm table, recording current alarm which has not been cleared and restored.
  - The hardware environment monitoring history alarm table, recording current, restored, and manually cleared alarms.

Hardware environmental monitoring alarm can be recorded in the current hardware environment monitoring alarm table and hardware environment monitoring history alarm table automatically without configuring manually.

- Trap output

Alarms are output to the NMS in Trap mode.

Trap output has global switch and all monitored alarm events still have their own Trap alarm output switches. When enabling the global switch and monitored alarm events switches simultaneously, the alarm will generate Trap output.

Table 12-7 describes Trap information.

Table 12-7 Trap information

Field	Description
Alarm status	<ul style="list-style-type: none"> <li>• asserted (current alarm)</li> <li>• cleared (alarm recovery)</li> <li>• clearall (clear all alarm)</li> </ul>
Alarm source	<ul style="list-style-type: none"> <li>• device (global alarm)</li> <li>• Interface number (interface status alarm)</li> </ul>
Timestamp	Alarm time, in the form of absolute time
Alarm event type	<ul style="list-style-type: none"> <li>• dev-power-down (power-down alarm)</li> <li>• power-abnormal (power-abnormal alarm, one of two powers is power down.)</li> <li>• high-temperature (high-temperature alarm)</li> <li>• low-temperature (low-temperature alarm)</li> <li>• all-alarm (clear all alarms)</li> </ul>

- Syslog output

Record alarms to Syslog.

Syslog output has global switch and all monitored alarm events still have their own Syslog alarm output switches. When the global switch and monitored alarm events switches are concurrently enabled, the alarm will generate Syslog output.

Table 12-8 describes Syslog information.

Table 12-8 Syslog information

Field	Description
Facility	The module name generating alarm, the hardware environment monitoring module is fixed as alarm.
Severity	Level, the same as defined in system logs. For details, see Table 12-4.
Mnemonics	Alarm event type. For details, see Table 12-7.
Msg-body	Main body, describing alarm event contents.

## 12.7.2 Preparing for configurations

### Scenario

Hardware environment monitoring provides environment monitoring for the devices, through which you can monitor the fault. When device operation environment is abnormal, this function will record hardware environment monitoring alarm list, generate system log, or send Trap and other alarms to notify taking corresponding measures and preventing fault.

### Prerequisite

Hardware environment monitoring alarm output:

- In Syslog output mode: alarms will be generated into system logs. To send alarm to the system log host, configure system log host IP address for the device.
- In Trap output mode: configure the management IP address of the device.

## 12.7.3 Default configurations of hardware environment monitoring

Default configurations of hardware environment monitoring are as below.

Function	Default value
Global hardware environment monitoring alarm Syslog output	Disable
Global hardware environment monitoring alarm Trap output	Disable
Power down event alarm	• Enable Trap output. • Enable Syslog system log output.
Temperature alarm output	
High temperature alarm threshold	102 ℃
Low temperature alarm threshold	-40 ℃

## 12.7.4 Enabling global hardware environment monitoring

Enable global hardware environment monitoring for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#logging alarm</b>	(Optional) enable global hardware environment monitoring alarm Syslog output.
3	<b>Raisecom(config)#snmp-server alarm-trap enable</b>	(Optional) enable global hardware environment monitoring alarm Trap.



## Note

- When enabling global hardware environment monitoring alarm Syslog output, alarm event can generate Syslog only when Syslog output under alarm event is also enabled.
- When enabling global hardware environment monitoring alarm sending Trap, alarm event can send Trap only when Trap output under alarm event is also enabled.

## 12.7.5 Configuring temperature monitoring alarm

Configure temperature monitoring alarm for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)# alarm temperature { notifies   syslog }</b>	Enable abnormal temperature alarm.
3	<b>Raisecom(config)# alarm temperature { high <i>high-value</i>   low <i>low-value</i>   notifies   syslog }</b>	Enable temperature monitoring alarm output and configure temperature monitoring alarm output modes. <ul style="list-style-type: none"> <li>• The high temperature threshold (high-value) must be greater than the low temperature threshold (low-value).</li> <li>• The low temperature threshold (low-value) must be smaller than the high temperature threshold (high-value).</li> </ul>


## 12.7.6 Configuring power supply alarm

Configure voltage monitoring alarm for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)# alarm power-supply { notifies   syslog }</b>	Enable power supply alarm and configure alarm output mode.

## 12.7.7 Clearing all hardware environment monitoring alarms manually

Clear all hardware environment monitoring alarms manually for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#conf ig</b>	Enter global configuration mode.
2	<b>Raisecom(conf ig)#clear alarm</b>	<p>Clear alarms manually.</p> <p> <b>Note</b></p> <p>Use this command to clear all alarms in current alarm list and generate an all-alarm alarm in history alarm list.</p> <p>If enabling global sending Trap, the all-alarm alarm will be output in Trap mode; if enabling global Syslog, the all-alarm alarm will be output in Syslog mode.</p>

## 12.7.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show alarm</b>	Show global hardware environment monitoring alarm configurations.
2	<b>Raisecom#show alarm current</b>	Show current alarms of hardware environment monitoring.
3	<b>Raisecom#show alarm history</b>	Show history alarms of hardware environment monitoring.
4	<b>Raisecom#show environment</b> [ <b>temperature</b>   <b>power</b> ]	Show information about the current environment, such as power supply, temperature, and alarms.

## 12.8 CPU monitoring

### 12.8.1 Introduction

The ISCOM2600G-HI series switch supports CPU monitoring. It can monitor state, CPU utilization rate, and application of stacking of each task in real time in the system. It helps locate faults.

CPU monitoring can provide the following functions:

- Viewing CPU utilization rate

It can be used to view unitization of CPU in each period (5s, 1minute, 10minutes, 2hours). Total unitization of CPU in each period can be shown dynamically or statically.



It can be used to view the operational status of all tasks and the detailed running status information about assigned tasks.

It can be used to view history utilization of CPU in each period.

It can be used to view information about dead tasks.

- Threshold alarm of CPU unitization

If CPU utilization of the system is more than configured upper threshold or less than preconfigured lower threshold in specified sampling period, Trap will be sent, and Trap will provide serial number of 5 tasks whose unitization rate of CPU is the highest in the latest period (5s, 1minute, 10minutes) and their CPU utilization rate.

## 12.8.2 Preparing for configurations

### Scenario

CPU monitoring can provide realtime monitoring to the task status, CPU utilization rate and stack usage in the system, provide CPU utilization rate threshold alarm, detect and eliminate hidden dangers, or help administrator for fault location.

### Prerequisite

When the CPU monitoring alarm needs to be output in Trap mode, configure Trap output target host address, which is IP address of NView NNM system.

## 12.8.3 Default configurations of CPU monitoring

Default configurations of CPU monitoring are as below.

Function	Default value
CPU utilization rate alarm Trap output	Enable
Upper threshold of CPU utilization alarm	99%
Lower threshold of CPU utilization alarm	79%
Sampling period of CPU utilization	60s

## 12.8.4 Showing CPU monitoring information

Show CPU monitoring information for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<code>Raisecom#show cpu-utilization [ dynamic   history { 10min   1min   2hour   5sec } ]</code>	Show CPU utilization.
2	<code>Raisecom#show process [ sorted { normal-priority   process-name } ]</code>	Show states of all tasks.
3	<code>Raisecom#show process cpu [ sorted [ 10min   1min   5sec   invoked ] ]</code>	Show CPU utilization of all tasks.

Step	Command	Description
4	Raisecom# <b>show process dead</b>	Show information about dead tasks.
5	Raisecom# <b>show process pid range</b>	Show information about the specified task.

## 12.8.5 Configuring CPU monitoring alarm

Configure CPU monitoring alarm for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>config</b>	Enter global configuration mode.
2	Raisecom(config)# <b>cpu threshold recovering recovering-threshold-value rising rising-threshold-value</b>	(Optional) configure the recovering threshold and rising threshold for CPU alarms.
3	Raisecom(config)# <b>cpu interval interval-value</b>	(Optional) configure the interval for sampling CPU alarms.

## 12.8.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# <b>show cpu-utilization</b>	Show CPU utilization and related configurations.

## 12.9 Cable diagnosis

### 12.9.1 Introduction

The ISCOM2600G-HI series switch supports cable diagnosis, which helps you detect lines.

Cable diagnosis contains the following results:

- Time for last cable diagnosis
- Detection result of the Tx cable
- Errored location of the Tx cable
- Detection result of the Rx cable
- Errored location of the Rx cable

## 12.9.2 Preparing for configurations

### Scenario

After cable diagnosis is enabled, you can learn the running status of cables, locate and clear faults, if any, in time.

### Prerequisite

N/A

## 12.9.3 Configuring cable diagnosis

Configure cable diagnosis for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom(config)#test cable-diagnostics noshutdown enable</b>	Enable the function of not restarting the interface upon cable diagnosis.
2	<b>Raisecom#test cable-diagnostics interface-type interface-number</b>	Enable cable diagnosis. The device supports this configuration on multiple interfaces.



### Note

When you enable the function of not restarting the interface upon cable diagnosis, the interface that is in Up status will be restarted once and then obtain cable diagnosis data. Then, when cable diagnosis is ongoing, the interface that is in Up status will not be restarted but directly read cable diagnosis data saved in the buffer, and the interface that is in Down status will obtain the length to the faulty point during cable diagnosis. The newly inserted interface will automatically execute cable diagnosis and save results in the buffer.

## 12.9.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show cable-diagnostics [ interface-type interface-number ]</b>	Show results of cable diagnosis.

## 12.10 Memory monitoring

### 12.10.1 Preparing for configurations

#### Scenario

Memory monitoring enables you to learn the memory utilization in real time, and provides memory utilization threshold alarms, thus facilitating you to locate and clear potential risks and help network administrator to locate faults.

#### Prerequisite

To output memory utilization threshold alarms as Trap, configure the IP address of the target host, namely, the IP address of the NMS server.

### 12.10.2 Configuring memory monitoring

Configure memory monitoring for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#memory threshold recovering recovering-threshold-value rising rising-threshold-value</b>	Configure the rising threshold and recovering threshold for memory utilization alarms.
3	<b>Raisecom(config)#memory interval observation- interval-value</b>	Configure the interval for sampling memory alarms.

### 12.10.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show memory [ module { value   bufferpool   diff }]</b>	Show information about the system memory, including the alarm enabling status, rising threshold, recovering threshold, sampling interval, total memory, used memory, idle memory, memory utilization, and memory used by each module, and memory change.

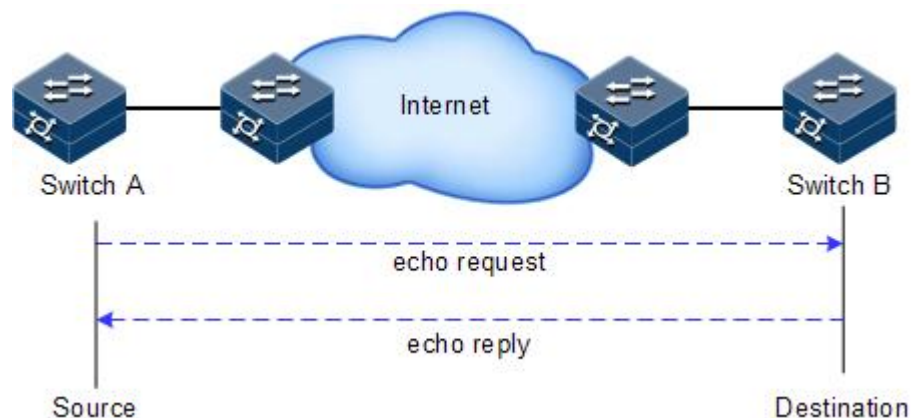
## 12.11 Ping

### 12.11.1 Introduction

Packet Internet Groper (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 12-11 shows principles of Ping.

Figure 12-11 Principles of Ping



### 12.11.2 Configuring Ping

Configure Ping for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>ping</b> <i>ip-address</i> [ <b>count</b> <i>count</i> ] [ <b>size</b> <i>size</i> ] [ <b>waittime</b> <i>period</i> ] [ <b>source</b> <i>ip-address</i> ]	(Optional) test the connectivity of the IPv4 network by the <b>ping</b> command.
2	Raisecom# <b>ping ipv6</b> <i>ipv6-address</i> [ <b>count</b> <i>count</i> ] [ <b>size</b> <i>size</i> ] [ <b>waittime</b> <i>period</i> ]	(Optional) test the connectivity of the IPv6 network by the <b>ping</b> command.



#### Note

The ISCOM2600G-HI series switch cannot perform other operations in the process of Ping. It can perform other operations only when Ping is finished or break off Ping by pressing **Ctrl+C**.

## 12.12 Traceroute

### 12.12.1 Introduction

Similar with 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

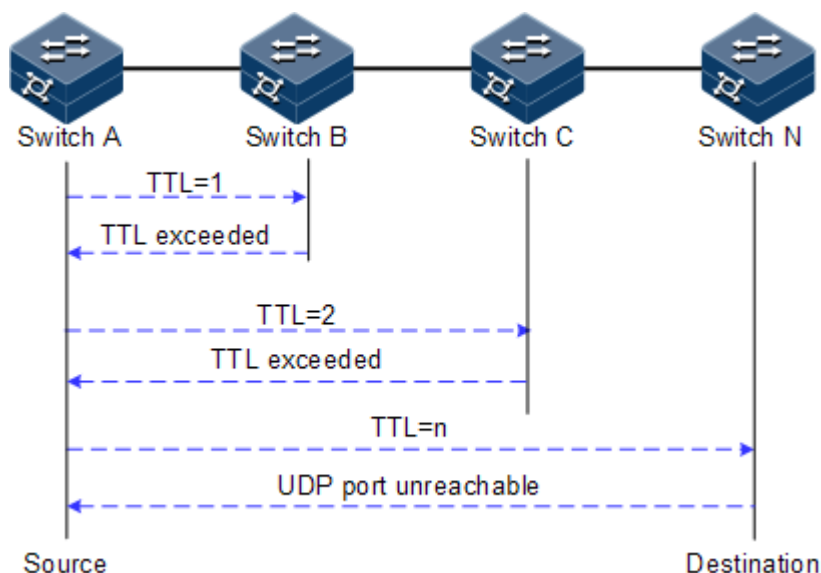
Traceroute works as below:

- Step 1 Send a piece of TTL1 sniffer packet (where the UDP port ID of the packet is unavailable to any application programs in destination side).
- Step 2 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.
- Step 3 The sending host adds 1 to TTL and resends this packet.
- Step 4 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 previous steps continue until the packet reaches the destination host, which will not return ICMP timeout packets. Because the port ID of 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 12-12 shows principles of traceroute.

Figure 12-12 Principles of Traceroute



### 12.12.2 Configuring Traceroute

Before using Traceroute, you should configure the IP address and default gateway of the ISCOM2600G-HI series switch.

Configure Traceroute for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	Raisecom# <b>traceroute</b> [ <i>vrf name</i> ] [ <i>ip-address</i> [ <b>firstttl</b> <i>first-ttl</i> ] ] [ <b>maxttl</b> <i>max-ttl</i> ] [ <b>port</b> <i>port-number</i> ] [ <b>waittime</b> <i>period</i> ] [ <b>count</b> <i>times</i> ] [ <b>size</b> <i>size</i> ]	(Optional) test the connectivity of the IPv4 network and view nodes passed by the packet by the <b>traceroute</b> command.
2	Raisecom# <b>traceroute ipv6</b> <i>ipv6-address</i> [ <b>firstttl</b> <i>first-ttl</i> ] [ <b>maxttl</b> <i>max-ttl</i> ] [ <b>port</b> <i>port-id</i> ] [ <b>waittime</b> <i>second</i> ] [ <b>count</b> <i>times</i> ] [ <b>size</b> <i>size</i> ]	(Optional) test the connectivity of the IPv6 network and view nodes passed by the packet by the <b>traceroute</b> command.

## 12.13 Performance statistics

### 12.13.1 Introduction

Performance statistics is used to gather statistics about service packets on the interface of a monitoring device and enable you to learn network performance. It can be based on interface or service flow in a short or long period. The short period is 15 minutes while the long period is 24 hours. Data in a statistical period is written as data block to the Flash for your review.

### 12.13.2 Preparing for configurations

#### Scenario

To learn performance of the ISCOM2600G-HI series switch, you can use performance statistics to gather current or historical statistics about packets based on interface or service flow.

#### Prerequisite

N/A

### 12.13.3 Default configurations of performance statistics

Default configurations of performance statistics are as below.

Function	Default value
Performance statistics	Enable
Number of data blocks saved in period statistics mode	16

### 12.13.4 Configuring performance statistics

Configure performance statistics for the ISCOM2600G-HI series switch as below.

Step	Command	Description
1	<b>Raisecom#config</b>	Enter global configuration mode.
2	<b>Raisecom(config)#performance statistics interval buckets</b> <i>buckets-number</i>	Configure the number of data blocks saved in the Flash for performance statistics in different statistics period mode.

### 12.13.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<b>Raisecom#show performance statistics interface</b> <i>interface-type interface-number { current   history }</i> <b>Raisecom#show performance statistics interval buckets</b>	Show performance statistics.

### 12.13.6 Maintenance

Maintain the ISCOM2600G-HI series switch as below.

Command	Description
<b>Raisecom(config)#clear performance statistics history</b>	Clear performance statistics.



# 13 Appendix

This chapter lists terms, acronyms, and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

## 13.1 Terms

### A

Access Control List (ACL)	A series of ordered rules composed of permit   deny sentences. These rules are based on the source MAC address, destination MAC address, source IP address, destination IP address, and interface ID. The device determines to receive or refuse the packets based on these rules.
Automatic Laser Shutdown (ALS)	The technology that is used for automatically shutting down the laser to avoid the maintenance and operation risks when the fiber is pulled out or the output power is too great.
Auto-negotiation	The interface automatically chooses the rate and duplex mode according to the result of negotiation. The auto-negotiation process is: the interface adapts its rate and duplex mode to the highest performance according to the peer interface; in other words, both ends of the link adopt the highest rate and duplex mode they both support after auto-negotiation.
Automatic Protection Switching (APS)	APS is used to monitor transport lines in real time and automatically analyze alarms to discover faults. When a critical fault occurs, through APS, services on the working line can be automatically switched to the protection line, thus the communication is recovered in a short period.

### B

Bracket	Small parts at both sides of the chassis, used to install the chassis into the cabinet
---------	--

## C

Challenge Handshake Authentication Protocol (CHAP)	CHAP is a widely supported authentication method in which a representation of the user's password, rather than the password itself, is sent during the authentication process. With CHAP, the remote access server sends a challenge to the remote access client. The remote access client uses a hash algorithm (also known as a hash function) to compute a Message Digest-5 (MD5) hash result based on the challenge and a hash result computed from the user's password. The remote access client sends the MD5 hash result to the remote access server. The remote access server, which also has access to the hash result of the user's password, performs the same calculation using the hash algorithm and compares the result to the one sent by the client. If the results match, the credentials of the remote access client are considered authentic. A hash algorithm provides one-way encryption, which means that calculating the hash result for a data block is easy, but determining the original data block from the hash result is mathematically infeasible.
--	---

## D

Dynamic ARP Inspection (DAI)	A security feature that can be used to verify the ARP data packets in the network. With DAI, the administrator can intercept, record, and discard ARP packets with invalid MAC address/IP address to prevent common ARP attacks.
Dynamic Host Configuration Protocol (DHCP)	A technology used for assigning IP address dynamically. It can automatically assign IP addresses for all clients in the network to reduce workload of the administrator. In addition, it can implement centralized management of IP addresses.

## E

Ethernet in the First Mile (EFM)	Complying with IEEE 802.3ah protocol, EFM is a link-level Ethernet OAM technology. It provides the link connectivity detection, link fault monitoring, and remote fault notification for a link between two directly-connected devices. EFM is mainly used for the Ethernet link on edges of the network accessed by users.
Ethernet Ring Protection Switching (ERPS)	It is an APS protocol based on ITU-T G.8032 standard, which is a link-layer protocol specially used for the Ethernet ring. In normal conditions, it can avoid broadcast storm caused by the data loop on the Ethernet ring. When the link or device on the Ethernet ring fails, services can be quickly switched to the backup line to enable services to be recovered in time.

## F

Full duplex	In a communication link, both parties can receive and send data concurrently.
-------------	---

## G

**GFP encapsulation** Generic Framing Procedure (GFP) is a generic mapping technology. It can group variable-length or fixed-length data for unified adaption, making data services transmitted through multiple high-speed physical transmission channels.

**Ground cable** The cable to connect the device to ground, usually a yellow/green coaxial cable. Connecting the ground cable properly is an important guarantee to lightning protection, anti-electric shock, and anti-interference.

## H

**Half duplex** In a communication link, both parties can receive or send data at a time.

## I

**Institute of Electrical and Electronics Engineers (IEEE)** A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.

**Internet Assigned Numbers Authority (IANA)** The organization operated under the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the NIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP suite, including autonomous system numbers.

**Internet Engineering Task Force (IETF)** A worldwide organization of individuals interested in networking and the Internet. Managed by the Internet Engineering Steering Group (IESG), the IETF is charged with studying technical problems facing the Internet and proposing solutions to the Internet Architecture Board (IAB). The work of the IETF is carried out by various working groups that concentrate on specific topics, such as routing and security. The IETF is the publisher of the specifications that led to the TCP/IP protocol standard.

## L

**Label** Symbols for cable, chassis, and warnings

**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. The LACPDU is used to exchange information with the peer device.

**Link-state tracking** Link-state tracking provides an interface linkage scheme, extending the range of link backup. Through monitoring upstream links and synchronizing downstream links, faults of the upstream device can be transferred quickly to the downstream device, and primary/backup switching is triggered. In this way, it avoids traffic loss because the downstream device does not sense faults of the upstream link.

## M

**Multi-Mode Fiber (MMF)** In this fiber, multi-mode optical signals are transmitted.

## N

**Network Time Protocol (NTP)** A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed time server and clients. NTP is used to perform clock synchronization on all devices that have clocks in the network. Therefore, the devices can provide different applications based on a unified time. In addition, NTP can ensure a very high accuracy with an error of 10ms or so.

## O

**Open Shortest Path First (OSPF)** An internal gateway dynamic routing protocol, which is used to determine the route in an Autonomous System (AS)

**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.

## P

**Password Authentication Protocol (PAP)** PAP is an authentication protocol that uses a password in Point-to-Point Protocol (PPP). It is a twice handshake protocol and transmits unencrypted user names and passwords over the network. Therefore, it is considered insecure.

**Point-to-point Protocol over Ethernet (PPPoE)** PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames. With PPPoE, the remote access device can control and account each access user.

**Private VLAN (PVLAN)** PVLAN adopts Layer 2 isolation technology. Only the upper VLAN is visible globally. The lower VLANs are isolated from each other. If you partition each interface of the switch or IP DSLAM device into a lower VLAN, all interfaces are isolated from each other.

## 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 network security mechanism, used to solve problems of network delay and congestion. When the network is overloaded or congested, QoS can ensure that packets of important services are not delayed or discarded and the network runs high efficiently. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio.

## R

**Rapid Spanning Tree Protocol (RSTP)** Evolution of the Spanning Tree Protocol (STP), which provides improvements in the speed of convergence for bridged networks

**Remote Authentication Dial In User Service (RADIUS)** RADIUS refers to a protocol used to authenticate and account users in the network. RADIUS works in client/server mode. The RADIUS server is responsible for receiving users' connection requests, authenticating users, and replying configurations required by all clients to provide services for users.

## S

**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.

**Single-Mode Fiber (SMF)** In this fiber, single-mode optical signals are transmitted.

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 backup link.
------------------------------	--

## V

Virtual Local Area Network (VLAN)	VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segments logically rather than physically, thus implementing multiple virtual work groups which are based on Layer 2 isolation and do not affect each other.
-----------------------------------	--

VLAN mapping	VLAN mapping is mainly used to replace the private VLAN Tag of the Ethernet service packet with the ISP's VLAN Tag, making the packet transmitted according to ISP's VLAN forwarding rules. When the packet is sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Thus, the packet is sent to the destination correctly.
--------------	---

## 13.2 Acronyms and abbreviations

### A

AAA	Authentication, Authorization and Accounting
ABR	Area Border Router
AC	Alternating Current
ACL	Access Control List
ANSI	American National Standards Institute
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
AS	Autonomous System
ASCII	American Standard Code for Information Interchange
ASE	Autonomous System External
ATM	Asynchronous Transfer Mode
AWG	American Wire Gauge

### B

BC	Boundary Clock
BDR	Backup Designated Router

BITS	Building Integrated Timing Supply System
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BTS	Base Transceiver Station
<b>C</b>	
CAR	Committed Access Rate
CAS	Channel Associated Signaling
CBS	Committed Burst Size
CE	Customer Edge
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CST	Common Spanning Tree
<b>D</b>	
DAI	Dynamic ARP Inspection
DBA	Dynamic Bandwidth Allocation
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Service
DNS	Domain Name System
DRR	Deficit Round Robin
DS	Differentiated Services
DSL	Digital Subscriber Line
<b>E</b>	

EAP	Extensible Authentication Protocol
EAPoL	EAP over LAN
EFM	Ethernet in the First Mile
EMC	Electro Magnetic Compatibility
EMI	Electro Magnetic Interference
EMS	Electro Magnetic Susceptibility
ERPS	Ethernet Ring Protection Switching
ESD	Electro Static Discharge
EVC	Ethernet Virtual Connection
<b>F</b>	
FCS	Frame Check Sequence
FE	Fast Ethernet
FIFO	First Input First Output
FTP	File Transfer Protocol
<b>G</b>	
GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GMRP	GARP Multicast Registration Protocol
GPS	Global Positioning System
GVRP	Generic VLAN Registration Protocol
<b>H</b>	
HDLC	High-level Data Link Control
HTTP	Hyper Text Transfer Protocol
<b>I</b>	
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IE	Internet Explorer
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronics Engineers



IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System Routing Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector

## **L**

LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LAN	Local Area Network
LCAS	Link Capacity Adjustment Scheme
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit

## **M**

MAC	Medium Access Control
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface cross-over
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Between Failure
MTU	Maximum Transmission Unit
MVR	Multicast VLAN Registration

## **N**

NMS	Network Management System
NNM	Network Node Management
NTP	Network Time Protocol
NView NNM	NView Network Node Management

**O**

OAM	Operation, Administration and Management
OC	Ordinary Clock
ODF	Optical Distribution Frame
OID	Object Identifiers
Option 82	DHCP Relay Agent Information Option
OSPF	Open Shortest Path First

**P**

P2MP	Point to Multipoint
P2P	Point-to-Point
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADS	PPPoE Active Discovery Session-confirmation
PAP	Password Authentication Protocol
PDU	Protocol Data Unit
PE	Provider Edge
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
Ping	Packet Internet Grope
PPP	Point to Point Protocol
PPPoE	PPP over Ethernet
PTP	Precision Time Protocol

**Q**

QoS	Quality of Service
-----	--------------------

**R**

RADIUS	Remote Authentication Dial In User Service
RCMP	Raisecom Cluster Management Protocol
RED	Random Early Detection
RH	Relative Humidity
RIP	Routing Information Protocol

RMON	Remote Network Monitoring
RNDP	Raisecom Neighbor Discover Protocol
ROS	Raisecom Operating System
RPL	Ring Protection Link
RRPS	Raisecom Ring Protection Switching
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource Reservation Protocol
RTDP	Raisecom Topology Discover Protocol

## S

SCADA	Supervisory Control And Data Acquisition
SF	Signal Fail
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SPF	Shortest Path First
SSHv2	Secure Shell v2
STP	Spanning Tree Protocol

## T

TACACS+	Terminal Access Controller Access Control System
TC	Transparent Clock
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service
TPID	Tag Protocol Identifier
TTL	Time To Live

## U

UDP	User Datagram Protocol
UNI	User Network Interface
USM	User-Based Security Model
<b>V</b>	
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
<b>W</b>	
WAN	Wide Area Network
WRR	Weight Round Robin

